МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
федеральное государственное автономное образовательное учреждение высшего образования «Балтийский федеральный университет имени Иммануила Канта»

Институт физико-математических наук и информационных технологий

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

«Иностранный язык (английский)»

Шифр: 10.05.01
Специальность: «Компьютерная безопасность»
Специализация: «Математические методы защиты информации»
Квалификация (степень) выпускника: специалист по защите информации

Калининград
2022

Лист согласования

Составитель: Игнатович Юлия Олеговна, старший преподаватель Ресурсного центра иностранных языков.

Рабочая программа утверждена на заседании учебно-методического совета института физико-математических наук и информационных технологий

Протокол № 01/22 от «01» февраля 2022 г.

Председатель учебно-методического
совета института физико-
математических наук и информационных
технологий

Первый заместитель директора Шпилевой А. А
ИФМНиИТ, к. ф.-м. н., доцент

Ведущий менеджер Е.П.Ставицкая

Содержание

1.Наименование дисциплины: «Иностранный язык».

Цель дисциплины «Иностранный язык» (английский) является владение иностранным языком как средством, обеспечивающим потребности социально-культурной деятельности, что предполагает, прежде всего, умение самостоятельно, «через всю жизнь», работать над изучением языка, поддерживать и пополнять свои знания и умения, развивать свою коммуникативную и информационную культуру.

В результате освоения ООП обучающийся должен овладеть следующими результатами обучения по дисциплине.

2. Перечень планируемых результатов обучения по дисциплине, соотнесенных с планируемыми результатами освоения образовательной программы.

Код компетенции	Результаты освоения образовательной программы (ИДК)	Результаты обучения по дисциплине
УК-4. Способен применять современные коммуникативные технологии, в том числе на иностранном(ых) языке(ах), для академического и профессионального взаимодействия	УК.4.1. Демонстрирует умение вести обмен профессиональной информацией в устной и письменной формах в том числе и на иностранном языке. УК.4.2. Использует современные информационно-коммуникативные технологии для академического взаимодействия и с соблюдением этики делового общения; Использует современные информационно-коммуникативные технологии для взаимодействия в профессиональной сфере. УК.4.3. Способен осуществлять деловую коммуникацию в устной и письменной формах на государственном языке РФ.	**Знать:** - иностранный язык, на уровень, предусмотренный рамками высшего образования; -знать способы поиска новой и нужной языковой информации. **Уметь:** -пользоваться наиболее употребительными и относительно простыми языковыми средствами во всех видах речевой деятельности: устной речи, аудировании, чтении и письме; -планировать работу; -ставить перед собой цели и задачи предстоящей деятельности; -уметь целесообразно распределять нагрузку. **Владеть:** компьютерной грамотностью (навыки работы в компьютерных программах “Word”, “Power Point”, навыки работы с принтером, сканером, навыки работы с электронной почтой и в сети Интернет, в том числе дистанционными платформами обучения, навыки общения онлайн).
УК-5. Способен анализировать и учитывать разнообразие культур в процессе межкультурного	УК.5.1. Выявление общего и особенного в историческом развитии России. УК.5.2. Анализирует современное состояние общества на основе знания	**Знать:** - особенности социальной организации общества, специфику менталитета и мировоззрения культур России, Запада и Востока; - особенности представлений

взаимодействия	истории. УК.5.3. Способен использовать основы философских знаний для формирования мировоззренческой позиции.	культур друг о друге с учетом наличия общего ценностного контекста, этностерео и гетеростереотипов, формируемых информационной средой; - основы теории коммуникации, проблемы культурной идентичности и межкультурных контактов. **Уметь:** - достигать эффективности коммуникации; - преодолевать культурный барьер, воспринимая межкультурные различия избегать предубеждений и настраиваться на совместные действия с представителями других культур; - сохраняя национальную идентичность, избегать этноцентризма; - соблюдать нормы этикета, моральные и культурные нормы. **Владеть:** - способностью преодолевать стереотипы; - творческим отношением к процессу коммуникации; - способностью использовать набор коммуникативных средств и делать их правильный выбор в зависимости от ситуации общения (тон, стиль, стратегии, речевые жанры, тематика и т. д.).

3. Место дисциплины в структуре образовательной программы.

Дисциплина «Иностранный язык» представляет собой дисциплину базовой части блока дисциплин подготовки студентов.

4. Виды учебной работы по дисциплине.

Виды учебной работы по дисциплине зафиксированы учебным планом основной профессиональной образовательной программы по указанному направлению и профилю, выражаются в академических часах. Часы контактной работы и самостоятельной работы студента и часы, отводимые на процедуры контроля, могут различаться в учебных планах ОПОП по формам обучения. Объем контактной работы включает часы контактной аудиторной работы (практические занятия), контактной внеаудиторной работы (контроль самостоятельной работы), часы контактной работы в период аттестации. Контактная работа, в том числе может проводиться посредством электронной информационно-образовательной среды университета с использованием ресурсов сети Интернет и дистанционных технологий.

5. Содержание дисциплины, структурированное по темам (разделам).

Исходя из рамок, установленных учебным планом по трудоемкости и видам учебной работы по дисциплине, преподаватель самостоятельно выбирает тематику занятий по формам и количеству часов проведения контактной работы: лекции и иные учебные занятия, предусматривающие преимущественную передачу учебной информации преподавателем и (или) занятия семинарского типа (семинары, практические занятия, практикумы, лабораторные работы, коллоквиумы и иные аналогичные занятия), и (или) групповые консультации, и (или) индивидуальную работу обучающихся с преподавателем, в том числе индивидуальные консультации (по курсовым работам/проектам – при наличии курсовой работы/проекта по данной дисциплине в учебном плане). Рекомендуемая тематика занятий максимально полно реализуется в контактной работе со студентами очной формы обучения. В случае реализации образовательной программы в заочной / очно-заочной форме трудоемкость дисциплины сохраняется, однако объем учебного материала в значительной части осваивается студентами в форме самостоятельной работы. При этом требования к ожидаемым образовательным результатам студентов по данной дисциплине не зависят от формы реализации образовательной программы.

№	Наименование раздела	Содержание раздела
1.	***Модуль 1: IDENTITY***	*Грамматический материал* “to be”, to have в Present Simple, повелительное наклонение; личные местоимения; указательные местоимения; множественное число существительных. Present Simple, Present Continuous, Past Simple, Past Continuous. Виды вопросительных предложений. *1.1 Устные разговорные темы* Personality types. About Myself. Men and women. Family and friends. Talking about yourself. Interview advice. *1.2 Аудирование* Personality types. Child of our time. *1.3 Письмо* Email of Introduction *1.4 Чтение* Carl Jung, who do you think you are? *1.5 DVD* BBC film Second life *1.6 Лексико-грамматический тест* *Lookback* *1.7 Самостоятельная работа студентов* Изучение грамматического материла. Грамматика (My grammar lab) : модуль1,2 5,6. Презентации студентов по темам, связанным со специальностью.
2.	***Модуль 2: TALES***	*Грамматический материал* Present Perfect, Past Simple, Past Perfect *2.1 Устные разговорные темы* Your life experience, Important news/ event, Tell a true story or lie *2.2 Аудирование* Radio program about important roles in films, News report, People talking anecdotes.

		2.3 Письмо News report. *2.4 Чтение* Hollywood versus history, The world's best-known conspiracy theories. *2.5 DVD* Hustle *2.6 Лексико-грамматический тест на закрепление материала* Lookback *2.7 Самостоятельная работа студентов* Внеаудиторное чтение - 5 тыс. знаков (по специальности). Изучение грамматического материла. Грамматика (My grammar lab): модуль 7. Презентация: «Моя жизнь в кино». Презентации по темам, связанным со специальностью.
3.	***Модуль 3: CONTACT***	*Грамматический материал* The future (plans): the present continuous, going to, will, might The future (predictions): will, might, may, could, going to, likely *3.1 Устные разговорные темы* Talk about how things will change in the future, Talk about communication preferences. *3.2 Аудирование* Listen to predictions about future communications, listen to telephone conversations involving misunderstanding. *3.3 Письмо* Writing a memo. *3.4 Чтение* Life on planet teen *3.5 DVD* The Virtual Revolution *3.6 Лексико-грамматический тест на закрепление материала* Lookback *3.7 Самостоятельная работа студентов* Внеаудиторное чтение - 5 тыс. знаков (по специальности). Изучение грамматического материла. Грамматика (My grammar lab): модуль 8. Презентация «Виртуальная революция». Презентации по темам, связанным со специальностью.
4.	***Модуль 4: PROJECT***	Проектная групповая деятельность студентов по представленным ниже темам: Living in a digital age? What is a computer? Types. What is inside a PC system? ***Зачет.*** Структура зачета: 1. Монологическое высказывание по одной из предложенных тем: Personality types. My personality; My Family and friends; Men and women; Conspiracy theories; Teenage communication. 2. Лексико-грамматический тест (ЛМС).

5.	***Модуль 5: JOBS***	*Грамматический материал* Modal verbs, used to *5.1 Устные разговорные темы* The qualities needed for different jobs, Homeworking, talking about past habits, creating business plan, Describing a day in your life *5.2 Аудирование* Dream Jobs gone wrong, Jobs *5.3 Письмо* Covering letter Write about daily routines *5.4 Чтение* Have you got what it takes? Childhood dreams. Homeworking. *5.5 DVD* Gavin and Stacey *5.6 Лексико-грамматический тест на закрепление материала* Lookback *5.7 Самостоятельная работа студентов* Внеаудиторное чтение - 5 тыс. знаков (по специальности). Изучение грамматического материла. Грамматика (My grammar lab): модуль 9. Составление резюме и сопроводительного письма. Презентации по темам, связанным со специальностью.
6.	***Модуль 6: SOLUTIONS***	*Грамматический материал* Comparatives/ Superlatives *6.1 Устные разговорные темы* Different forms of transport and their uses, Describing a new machine. *6.2 Аудирование* Conversation about technical problems, People answering difficult questions *6.3 Письмо* An advantage/ disadvantage essay Advertisment Write about daily routines *6.4 Чтение* 20th Century, The advantages and disadvantages of modern technology *6.5 DVD* Top Gear *6.6 Лексико-грамматический тест на закрепление материала* Lookback *6.7 Самостоятельная работа студентов* Внеаудиторное чтение - 5 тыс. знаков (по специальности). Изучение грамматического материла. Грамматика (My grammar lab): модуль 4. Презентации по темам, связанным со специальностью.
7.	***Модуль 7: EMOTION***	*Грамматический материал* Zero and first conditionals, Second Conditional -Ing/ Ed adjectives *7.1 Устные разговорные темы* Talk about your emotions, discuss what you would do in different situations, Talk about memorable moments

		7.2 Аудирование Radio show about therapies, Conversation where people hear news *7.3 Письмо* A letter of advice A website entry *7.4 Чтение* The six basic emotions, The people watchers *7.5 DVD* My worst week. *7.6 Лексико-грамматический тест на закрепление материала* Lookback. *7.7 Самостоятельная работа студентов* Внеаудиторное чтение - 5 тыс. знаков (по специальности). Изучение грамматического материла. Грамматика (My grammar lab) : модуль 4,10. Презентации по темам, связанным со специальностью.
8.	***Модуль 8: PROJECT***	Проектная групповая деятельность студентов по представленным ниже темам: The eyes of your computer? How screen displays work? Printer ***Зачет.*** Структура зачета: 1. Монологическое высказывание по одной из предложенных тем: Jobs. My dream Job Working from home Machines. Transport Six basic emotions How to cope with stress 2. Лексико-грамматический тест (БРС).
9.	***Модуль 9: SUCCESS***	*Грамматический материал* Present Perfect/ Present Perfect Continuous Modal Verbs *9.1 Устные разговорные темы* Talk about success, talk about your abilities, describe an achievement *9.2 Аудирование* Radio program about success *9.3 Письмо* Summary An internet post *9.4 Чтение* What is the secret of success? The human camera *9.5 DVD* Water ski challenge *9.6 Лексико-грамматический тест на закрепление материала* Lookback *9.7 Самостоятельная работа студентов* Внеаудиторное чтение - 5 тыс. знаков (по специальности). Изучение грамматического материла. Грамматика (My grammar lab) : модуль 10. Презентации по темам, связанным со специальностью.
10.	***Модуль 10:***	Аудиторная работа – 12 часов, самостоятельная работа – 12

	COMMUNITIES	часов. *10.1 Грамматический материал* Articles and Quantifiers Relative clauses *10.2 Устные разговорные темы* Describe your neighbourhood, compare real-world and online activities, Discuss social situations *10.3 Аудирование* Listen to descriptions of online communities, listen to people describing guest /host experience *10.4 Письмо* Website review An advertisement *10.5 Чтение* How well do you know your neighbours? How to be the world's best guest *10.6 DVD* Tribe *10.7 Лексико-грамматический тест на закрепление материала* Lookback *10.8 Самостоятельная работа студентов* Внеаудиторное чтение - 5 тыс. знаков (по специальности). Изучение грамматического материла. Грамматика (My grammar lab): модуль 1,2. Презентация «Успешный человек». Презентации по темам, связанным со специальностью.
11.	***Модуль 11: HISTORY***	*Грамматический материал* Third Conditional Passive voice *11.1 Устные разговорные темы* Talk about important events in history, talk about your own history, Describe a role model *11.2 Аудирование* Listen to descriptions of past decades, listen to people doing a quiz in history *11.3 Письмо* Short essay A wiki entry *11.4 Чтение* Leaps Time travel *11.5 DVD* Michelangelo *11.6 Лексико-грамматический тест на закрепление материала* Lookback *11.7 Самостоятельная работа студентов* Внеаудиторное чтение - 5 тыс. знаков (по специальности). Изучение грамматического материла. Грамматика (My grammar lab): модуль 10,16. Презентация «Величайший шаг человечества». Презентации по темам, связанным со специальностью.
12.	***Модуль 12:***	***Проектная групповая работа*** студентов по предложенным

	PROJECT	темам: Computers for the disabled Magnetic storage Optical discs and drivers Flash memory Spreadsheets and databases ЗАЧЕТ : лексико-грамматический тест (БРС)
13.	***Модуль 13: WORLD***	*Грамматический материал* Reported speech *13.1 Устные разговорные темы* Eco-living, ask for/give travel advice, Talk about special place *13.2 Аудирование* Discription of the world's best cities People giving advice/warning *13.3 Письмо* A restaurant review An email campaigning for action *13.4 Чтение* Ethical man World food Ten things not to do in an airport *13.5 DVD* The great melt *13.6 Лексико-грамматический тест на закрепление материала* Lookback *13.7 Самостоятельная работа студентов* Внеаудиторное чтение - 5 тыс. знаков (по специальности). Изучение грамматического материла. Грамматика (My grammar lab): модуль 13. Презентация «Защита окружающей среды». Презентации по темам, связанным со специальностью.
14.	***Модуль 14: PROJECT***	***Проектная групповая работа*** студентов по предложенным темам: The Web. Cybersecurity. Internet Security. Graphics and design.
15.	***Модуль 15: ПОДГОТОВКА К ЭЗАМЕНУ***	*Самостоятельная работа студентов+ грамматика* Внеаудиторное чтение - 5 тыс. знаков (по специальности). Изучение грамматического материла. Грамматика (My grammar lab): модуль 3,11,14,15,17,18,19,20 ***Экзамен.*** Структура экзамена: 1. Лексико-грамматический тест (проводиться до экзамена) 2. Перевод текста и краткое его изложение (проводиться до экзамена) Беседа по теме (в день экзамена).

6. Рекомендуемая тематика учебных занятий в форме контактной работы

Рекомендуемая тематика *практических* занятий:

Тема 1: Computers today.

Вопросы для обсуждения: Living in a digital age; Computers essentials; Inside the system; Buying a. computer.

Тема 2: Input and output devices.

Вопросы для обсуждения: Capture your favourite image; Display screens and ergonomics; Choosing a printer; Devices for disabled.

Тема 3: Storage devices.

Вопросы для обсуждения: Magnetic storage; Optical storage; Flash storage;

Тема 4: Basic software.

Вопросы для обсуждения: The operating system; Word processing; Spreadsheets and databases.

Тема 5: Faces of the Internet.

Вопросы для обсуждения: The Internet and the email; Chat and conferencing; Internet security.

Тема 6: Creative software.

Вопросы для обсуждения: Graphics and design; Desktop publishing; Multimedia; Web design.

Тема 7: Programming. Jobs in ICT.

Вопросы для обсуждения: Programm design and computer languages; Jobs in ICT.

Тема 8: Computers tomorrow.

Вопросы для обсуждения: Communication systems; Networks; Video games; New technologies.

Требования к самостоятельной работе студентов:

- подготовка к практическим занятиям;
- выполнение домашних и индивидуальных заданий по отдельным разделам дисциплины;
- написание различных видов речевых произведений;
- внеаудиторное чтение литературы по специальности и периодики;
- восприятие радио- и телепередач, художественных фильмов, театральных постановок, лекций, аудиозаписей на иностранном языке;
- подготовка к контрольным работам;
- подготовка к промежуточной аттестации по дисциплине (зачету и экзамену).

Учебно-методическое обеспечение для самостоятельной работы обучающихся составляют:

1) Учебники, учебно-методические пособия, словари и справочные пособия;
2) Обучающая платформа ЛМС;
3) Ресурсы информационно-телекоммуникационной сети «Интернет»;
4) Фонды оценочных средств.

Руководствуясь положениями статьи 47 и статьи 48 Федерального закона от 29 декабря 2012 г. N 273-ФЗ «Об образовании в Российской Федерации» научно-педагогические работники и иные лица, привлекаемые университетом к реализации данной образовательной программы, пользуются предоставленными академическими правами и свободами в части свободы преподавания, свободы от вмешательства в профессиональную деятельность; свободы выбора и использования педагогически обоснованных форм, средств, методов обучения и воспитания; права на творческую инициативу, разработку и применение авторских программ и методов обучения и воспитания в пределах реализуемой образовательной программы и отдельной дисциплины.

Исходя из рамок, установленных учебным планом по трудоемкости и видам учебной работы по дисциплине, преподаватель самостоятельно выбирает тематику занятий по формам и количеству часов проведения контактной работы: лекции и иные

учебные занятия, предусматривающие преимущественную передачу учебной информации преподавателем и (или) занятия семинарского типа (семинары, практические занятия, практикумы, лабораторные работы, коллоквиумы и иные аналогичные занятия), и (или) групповые консультации, и (или) индивидуальную работу обучающихся с преподавателем, в том числе индивидуальные консультации (по курсовым работам/проектам – при наличии курсовой работы/проекта по данной дисциплине в учебном плане).

Рекомендуемая тематика занятий максимально полно реализуется в контактной работе со студентами очной формы обучения. В случае реализации образовательной программы в заочной / очно-заочной форме трудоемкость дисциплины сохраняется, однако объем учебного материала в значительной части осваивается студентами в форме самостоятельной работы. При этом требования к ожидаемым образовательным результатам студентов по данной дисциплине не зависят от формы реализации образовательной программы.

7. Методические рекомендации по видам занятий

Практические занятия.

На практических занятиях в зависимости от темы занятия выполняется поиск информации по решению проблем, практические упражнения, контрольные работы, выработка индивидуальных или групповых решений, итоговое обсуждение с обменом знаниями, участие в круглых столах, разбор конкретных ситуаций, командная работа, представление портфолио и т.п.

Самостоятельная работа.

Самостоятельная работа осуществляется в виде изучения литературы, эмпирических данных по публикациям и конкретных ситуаций из практики, подготовке индивидуальных работ, работа с различным материалом на платформе LMS, самостоятельное изучение отдельных тем дисциплины; поиск и обзор литературы и электронных источников; чтение и изучение учебника и учебных пособий.

8. Фонд оценочных средств

8.1. Перечень компетенций с указанием этапов их формирования в процессе освоения образовательной программы в рамках учебной дисциплины

Основными этапами формирования указанных компетенций при изучении обучающимися дисциплины являются последовательное изучение содержательно связанных между собой тем учебных занятий. Изучение каждой темы предполагает овладение обучающимися необходимыми компетенциями. Результат аттестации обучающихся на различных этапах формирования компетенций показывает уровень освоения компетенций.

Контролируемые разделы (темы) дисциплины	Контролируемой компетенции	Оценочные средства по этапам формирования компетенций	
		рубежный контроль	промежуточный

			контроль
		текущий контроль	
1. Identity	УК-4, УК-5	Лексико-грамматический тест на закрепление материала	-
		Устный опрос	
2. Tales	УК-4, УК-5	Лексико-грамматический тест на закрепление материала	-
		Устный опрос	
3. Contact	УК-4, УК-5	Лексико-грамматический тест на закрепление материала	–
		Устный опрос	
4. Living in a digital age? What is a computer? Types What is inside a PC system?	УК-4	Лексико-грамматический тест на закрепление материала	-
		Презентация	
	УК-4, УК-5		Зачет
5. Jobs	УК-4, УК-5	Лексико-грамматический тест на закрепление материала	-
		Устный опрос	
6. Solutions	УК-4, УК-5	Лексико-грамматический тест на закрепление материала	-
		Устный опрос	
7. Emotions	УК-4, УК-5	Лексико-грамматический тест на закрепление материала	-
		Устный опрос	
8. The eyes of your computer? How screen displays work? Printer	УК-4	Лексико-грамматический тест на закрепление материала	-
		Презентация	
	УК-4, УК-5		Зачет
9. Success	УК-4, УК-5	Лексико-грамматический тест на закрепление материала	-
		Устный опрос	
10. Communities	УК-4, УК-5	Лексико-грамматический тест на закрепление материала	-
		Устный опрос	

11. Histoty	УК-4, УК-5	Лексико-грамматический тест на закрепление материала	-
		Устный опрос	
12. Computers for the disabled Magnetic storage Optical discs and drivers Flash memory Spreadsheets and databases	УК-4	Лексико-грамматический тест на закрепление материала	
		Презентация	
	УК-4, УК-5		Зачет
13. World	УК-4, УК-5	Лексико-грамматический тест на закрепление материала	
		Устный опрос	
14. The Web. Cybers. Internet Security. Graphics and design	УК-4, УК-5	Лексико-грамматический тест на закрепление материала	
		Презентация	
15. Подготовка к экзамену	УК-4, УК-5	Лексико-грамматический тест на закрепление материала	
		Устный опрос	
	УК-4, УК-5		Экзамен

8.2. Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений и навыков и (или) опыта деятельности процессе текущего контроля

Тест: Listening.

1 *Track 11* Listen and tick ✓ the correct answer: a), b) or c).

1 Jo thinks she could be _____ Native American.

5%	15%	50%
a) ___	b) ___	c) ✓

2 The woman felt the bed moving so she got up and _____.

got under the table	went outside	got dressed
a) ___	b) ___	c) ___

3 The girl's going to save _____ to go to the Moon.

$1m	for a long time	for 25 years
a) ___	b) ___	c) ___

4 Jack _____ Nick's idea for a new business.

likes	agrees with	doesn't agree with
a) ___	b) ___	c) ___

5 The shop doesn't have a _____.

price list	computer	dishwasher
a) ___	b) ___	c) ___

6 The woman says she couldn't live without a _____.

fridge	cooker	tin opener
a) ___	b) ___	c) ___

10

Pronunciation

2 *Track 12* Listen and cross out the word with a different vowel sound in bold.

1 f**a**mily ~~dr**a**ma~~ m**a**rried **a**mbitious
2 **i**nquiry r**i**sk sc**i**ence f**i**ction
3 r**o**mantic forg**o**t c**o**medy j**o**b
4 gen**e**tic rem**e**mber **e**ngineering p**e**riod
5 h**ea**r **ea**rn l**ea**der fr**ee**ze
6 f**u**n disc**u**ssion f**u**rious w**o**nderful

5

Vocabulary and Grammar

3 Match the compound nouns.

1 great-	*d*	a) power
2 romantic	___	b) taker
3 washing	___	c) family
4 risk	___	d) ~~grandparents~~
5 psychological	___	e) networks
6 solar	___	f) comedy
7 genetic	___	g) drama
8 extended	___	h) fiction
9 period	___	i) machine
10 computer	___	k) thriller
11 science	___	l) engineering

5

4 Underline the correct preposition.

1 I'm meeting them *at / in* lunchtime.
2 He complimented her *on / of* her new hairstyle.
3 I dialled the wrong number *for / by* mistake.
4 We can't possibly predict what changes will take place *in / on* ten years' time.
5 You haven't said a word for an hour. What's *at / on* your mind?
6 He couldn't stop for a chat because he was *from / in* a hurry.
7 I warned him *about / from* the traffic jams.
8 She had to apologise *on / for* forgetting the time of the meeting.
9 He couldn't finish the exam because he ran *up / out* of time.
10 I think the situation will get slightly worse *of / in* the short term.

11 She forgot to switch *up / off* the lights when she left the house.

5

5 Complete the sentences. Use the correct form of the word in capitals.

1 He's been *unemployed* for six months. He can't find a job. EMPLOY
2 They're trying to find a _____ solution to the conflict. PEACE
3 I can't use my mobile. The battery needs _____. CHARGE
4 They had to close the business because it had become _____. PROFIT
5 There are fewer _____ people sleeping on the streets now there are more shelters for them. HOME
6 Commuting to work in big cities is more _____ than it used to be. EXHAUST

5

6 Correct <u>two</u> mistakes in each sentence.

1 My students don't hear me and that's why they do mistakes.
My students don't ***listen to*** *me and that's why they* ***make*** *mistakes.*
2 My ancestors are coming for lunch today. My uncle says very funny stories.
_____.
3 He got fired from his boss so he's looking for a new work.
_____.
4 I said him I'd be late because I forgot my purse at home.
_____.
5 You didn't remember me about Alan's birthday and now I'm in boiling water!
_____.
6 She made medical research after university, but she didn't win much money.
_____.

5

7 Write questions for the answers in *italics*.

1 He was *talking on his mobile* when I saw him.
What *was he doing when you saw him*?
2 I used to play *tennis and hockey* before I broke my leg.
Which _____?
3 They were looking for *you* just now.
Who _____?
4 *The Arsenal football team* is likely to win the championship.
Which _____?
5 He realised *later* that he'd given her the wrong address.
When _____?
6 *Maria* sent me a beautiful card for my birthday.
Who _____?

5

8 Complete the second sentence so that it means the same as the first. Use the word in brackets.

1 You can't smoke in the office. (must)
You *mustn't smoke in the office*.
2 His flat's not as messy as it used to be. (less)
His flat _____.
3 The plane will probably be late. (likely)
The plane _____.
4 This one's a bit more expensive. (slightly)
This one _____.

5 I told him not to forget to buy the bread. (remind)
I _____.
6 We used to have a family lunch every Sunday. (would)
We _____.

5

9 Choose the correct answers to complete the sentences: a), b), c) or d).

1 You __*b*__ eat so much junk food.
a) might b) shouldn't c) must d) have to
2 We _____ to stay with friends when we get to Sydney.
a) will b) would c) likely d) 're going
3 I've never been to China, but I _____ to Japan last year.
a) went b) 've been c) used to go d) gone
4 He _____ her name now.
a) isn't remembering b) don't remember
c) doesn't remember d) remember
5 When she got to the airport, she realised she _____ her passport at home.
a) left b) forgot c) 'd forgotten d) 'd left
6 We met them _____ we were living in Tanzania.
a) during b) until c) while d) as soon as
7 My ancestors _____ from Ireland.
a) came b) comes c) lived d) are coming
8 Have you seen his latest play _____?
a) just b) yet c) ever d) last night
9 When we were children, we _____ in the garden all day.
a) 'd played b) 'd play c) were playing
d) 've played
10 You _____ to go now. You can go later.
a) don't have b) must c) mustn't d) ought
11 The house was _____ more beautiful than he remembered.
a) very b) little bit c) far d) not as

5

10 Complete the article with one suitable word in each gap.

New words from old

The English [1] *language* is constantly growing in response to changes in the world around us, and new [2]_____ are added every day. The word 'framily' for example, first came into use in 2006 and is made [3]_____ two words: 'family' and 'friends'. It refers to close friends who [4]_____ become like a family, providing company and support to each other.

The concept has probably developed as a result [5]_____changes in our society, where people don't live as near to [6]_____families as they [7]_____to. The word 'framily' has been used in the USA [8]_____quite a while, especially by younger people living [9]_____cities, as reflected in popular TV shows like *Friends*. If you like being with both 'framily' and family, you might want [10]_____try 'togethering', which means to go on holiday with both your extended [11]_____and friends!

5

Reading

11 Match gaps 1–6 in the text with sentences a)–f) opposite.

Living Tomorrow

If you want to find out what houses might look like in the future, you should visit the *Living Tomorrow* exhibition. It's a permanent exhibition near Brussels in Belgium, where you can see for yourself how tomorrow's technologies will integrate into our daily lives.

[1] *c*. Everything works via remote control, from warming up food, to authorising access to the supermarket delivery man. The living room has touch screens which control the light, music and windows. You might want to read, relax or just chat to friends there. [2]_____.You'll find out why when you go upstairs.

The kitchen can be whatever you want it to be. Appliances like the oven, fridge and dishwasher slide in or out of view as needed. They even change colour automatically when you adjust the lighting. [3]_____. The only thing that doesn't move here is the flat screen on the wall. Among other things, you can use this screen to do your shopping easily and safely online.

Upstairs is the 'home theatre', with specialised acoustics and large screens. The latest 3D technology makes watching TV a whole new experience! [4]_____.

The bathroom, which has water-free toilets and voice-controlled taps, is also equipped with an 'intelligent mirror'. This acts as both a mirror and an electrically controlled screen. [5]_____. The mirror will even check your blood pressure and temperature, and remind you to take your medicine if necessary!

Finally, there's the 'home office'. [6]_____. This means that the office will become much more central to our lives. In fact, in 'the house of the future', it will hardly be necessary to leave home at all!

a) You can watch the news on it, check the weather forecast or listen to music while you clean your teeth.
b) Next to this, in the 'sleeping space', you can try out a bed that adapts to your size and shape.
c) ~~The 'House of the Future' consists of a living room, bathroom, kitchen, home theatre, sleeping space and office.~~
d) Thanks to tomorrow's interactive multimedia technology, more and more people will be working from home.
e) The oven and microwave are designed to recognise different kinds of food and decide automatically how to cook them.
f) However, you won't see a TV there.

	10

12 Read the text in Exercise 11 again and choose the correct answer: a), b) or c).

1 The *Living Tomorrow* exhibition *a*.
a) shows what daily life will be like in the future
b) is only going to be on for a short time
c) shows you what houses will be like in the future

2 In the 'House of the Future', you _____.
a) won't have to switch the lights on
b) can watch TV in the living room
c) will have to open the door when your shopping is delivered

3 In the kitchen, _____.
a) the fridge and dishwasher are white
b) you can move the domestic appliances around
c) the oven decides what food you'll eat

4 There's a 'home theatre' upstairs _____.
a) where you can watch 3D TV

b) which has an ‘intelligent mirror’
c) where you can sleep

5 In the bathroom, _____.
a) the taps turn on automatically
b) music starts playing when you clean your teeth
c) you can check what the weather is like outside

6 In the future, _____.
a) people won’t be able to go outside very much
b) the ‘home office’ will be more essential than it is now
c) people won’t need to work

5

Текст: GREEC SCHOOL OF MATHEMATICS (classical period)

Historians traditionally place the beginning of Greek mathematics proper to the age of Thales of Miletus (ca. 624–548 BC). Little is known about the life and work of Thales, so little indeed that his date of birth and death are estimated from the eclipse of 585 BC, which probably occurred while he was in his prime. Despite this, it is generally agreed that Thales is the first of the seven wise men of Greece. The two earliest mathematical theorems, Thales' theorem and Intercept theorem are attributed to Thales. The former, which states that an angle inscribed in a semicircle is a right angle, may have been learned by Thales while in Babylon but tradition attributes to Thales a demonstration of the theorem. It is for this reason that Thales is often hailed as the father of the deductive organization of mathematics and as the first true mathematician. Thales is also thought to be the earliest known man in history to whom specific mathematical discoveries have been attributed. Although it is not known whether or not Thales was the one who introduced into mathematics the logical structure that is so ubiquitous today, it is known that within two hundred years of Thales the Greeks had introduced logical structure and the idea of proof into mathematics.

Another important figure in the development of Greek mathematics is Pythagoras of Samos (ca. 580–500 BC). Like Thales, Pythagoras also traveled to Egypt and Babylon, then under the rule of Nebuchadnezzar, but settled in Croton, Magna Graecia. Pythagoras established an order called the Pythagoreans, which held knowledge and property in common and hence all of the discoveries by individual Pythagoreans were attributed to the order. And since in antiquity it was customary to give all credit to the master, Pythagoras himself was given credit for the discoveries made by his order. Aristotle for one refused to attribute anything specifically to Pythagoras as an individual and only discussed the work of the Pythagoreans as a group. One of the most important characteristics of the Pythagorean order was that it maintained that the pursuit of philosophical and mathematical studies was a moral basis for the conduct of life. Indeed, the words philosophy (love of wisdom) and mathematics (that which is learned) are said[by whom?] to have been coined by Pythagoras. From this love of knowledge came many achievements. It has been customarily said[by whom?] that the Pythagoreans discovered most of the material in the first two books of Euclid's Elements.

Distinguishing the work of Thales and Pythagoras from that of later and earlier mathematicians is difficult since none of their original works survive, except for possibly the surviving "Thales-fragments", which are of disputed reliability. However many historians, such as Hans-Joachim Waschkies and Carl Boyer, have argued that much of the mathematical knowledge ascribed to Thales was developed later, particularly the aspects that rely on the concept of angles, while the use of general statements may have appeared earlier, such as those found on Greek legal texts inscribed on slabs. The reason it is not clear exactly what either Thales or Pythagoras actually did is that almost no contemporary documentation has survived. The only evidence comes from traditions recorded in works such as Proclus’ commentary on

Euclid written centuries later. Some of these later works, such as Aristotle's commentary on the Pythagoreans, are themselves only known from a few surviving fragments.

8.3. Перечень вопросов и заданий для промежуточной аттестации по дисциплине

1.Типы личности. О Себе

2. Моя семья и мои друзья

3. Самые известные мировые теории заговора

4.Проблемы общения поколений

5. Работа мечты. Моя будущая профессия

6.Работа на дому

7.Современные технологии

8.Транспорт. Путешествие

9.Базовые эмоции. Стресс

10. Успех. Люди, которые изменили мир

11. Мой образ жизни. Мое место в гиперпространстве

12.Величайщие события в истории

13. Экология. Этическая личность

14. Разница между мужчинами и женщинами

15.Моя специальность

8.4. Планируемые уровни сформированности компетенций обучающихся и критерии оценивания

Уровни	Содержательное описание уровня	Основные признаки выделения уровня (этапы формирования компетенции, критерии оценки сформированности)	Пятибалльная шкала (академическая) оценка	Двухбалльная шакала, зачет	ЛМС, % освоения (рейтинговая оценка)
Повышенный	Творческая деятельность	*Включает нижестоящий уровень.* Умение самостоятельно принимать решение, решать проблему/задачу теоретического и прикладного характера на основе изученных методов, приемов, технологий	отлично	зачтено	86-100

Базовый	Применение знаний и умений в более широких контекстах учебной и профессиональной деятельности, нежели по образцу с большей степени самостоятельности и инициативы	*Включает нижестоящий уровень.* Способность собирать, систематизировать, анализировать и грамотно использовать информацию из самостоятельно найденных теоретических источников и иллюстрировать ими теоретические положения или обосновывать практику применения	хорошо		71-85
Удовлетворительный (достаточный)	Репродуктивная деятельность	Изложение в пределах задач курса теоретически и практически контролируемого материала	удовлетворительно		55-70
Недостаточный	Отсутствие признаков удовлетворительного уровня		неудовлетворительно	не зачтено	Менее 55

9. Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины.

Основная литература:

1. Кузьменкова, Ю. Б. Английский язык [Электронный ресурс]: учеб. для бакалавров/ Ю. Б. Кузьменкова; Высш. школа экономики, Нац. исслед. ун-т. - Москва: Юрайт, 2013. - 1 on-line, 441 с.. - (Учебники НИУ ВШЭ). - Б.ц. Имеются экземпляры в отделах /There are copies in departments: ЭБС Кантиана(1)

Дополнительная литература:

1.Вводно-фонетический курс английского языка: учеб.-практ. пособие для студентов 1-2 курсов / под ред. Т. П. Желонкиной; Балт. федер. ун-т им. И. Канта. - Калининград: Изд-во БФУ им. И. Канта, 2011. - 132 с. - Имеются экземпляры в отделах: всего 1: ЭБС Кантиана(1)

2. Качалова, К. Н. Практическая грамматика английского языка с упражнениями и ключами: учебник/ К. Н. Качалова, Е. Е. Израилевич. - Москва: ЮНВЕСТ, 1996. - 717 с. -

ISBN 5-88682-003-5: 28000=;22000= р.Имеются экземпляры в отделах /There are copies in departments: всего /all 59: НА(2), УБ(57)

10. Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины (модуля).

Образовательная платформа BRITISH COUNCIL https://learnenglish.britishcouncil.org;
ENGVID Free video English lessons Бесплатные видео уроки https://www.engvid.com**;**
Электронно-библиотечная система (ЭБС) Кантитана (https://elib.kantiana.ru/) -BBC podcasts https://www.youtube.com;
Cambridge dictionary https://dictionary.cambridge.org/ru.

11. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине.

Программное обеспечение обучения включает в себя:
система электронного образовательного контента БФУ им. И. Канта – www.lms-3.kantiana.ru, обеспечивающую разработку и комплексное использование электронных образовательных ресурсов;
серверное программное обеспечение, необходимое для функционирования сервера и связи с системой электронного обучения через Интернет;
корпоративная платформа Microsoft Teams;
установленное на рабочих местах студентов ПО: Microsoft Windows 7, Microsoft Office Standart 2010, антивирусное программное обеспечение Kaspersky Endpoint Security.
специализированное ПО (при наличии):

12. Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине.

Для проведения занятий лекционного типа, практических и семинарских занятий используются специальные помещения (учебные аудитории), оборудованные техническими средствами обучения – мультимедийной проекционной техникой. Для проведения занятий лекционного типа используются наборы демонстрационного оборудования.

Для проведения лабораторных работ, (практических занятий – при необходимости) используются специальные помещения (учебные аудитории), оснащенные специализированным лабораторным оборудованием: персональными компьютерами с возможностью выхода в интернет и с установленным программным обеспечением, заявленным в п.11.

Для проведения групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации используются специальные помещения (учебные аудитории), оборудованные специализированной мебелью (для обучающихся), меловой / маркерной доской.

Для организации самостоятельной работы обучающимся предоставляются помещения, оснащенные компьютерной техникой с возможностью подключения к сети «Интернет» и обеспечением доступа в электронную информационно-образовательную среду университета.

Для обучения инвалидов и лиц с ограниченными возможностями здоровья университетом могут быть представлены специализированные средства обучения, в том числе технические средства коллективного и индивидуального пользования.

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
федеральное государственное автономное образовательное учреждение высшего образования «Балтийский федеральный университет имени Иммануила Канта»
Институт физико-математических наук и информационных технологий

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

«Иностранный язык (немецкий)»

Шифр: 10.05.01
Специальность: «Компьютерная безопасность»
Специализация: «Математические методы защиты информации»
Квалификация (степень) выпускника: специалист по защите информации

Калининград
2022

Лист согласования

Составитель: старший преподаватель Ресурсного центра (кафедры) иностранных языков, Попова М.Г.

Рабочая программа утверждена на заседании учебно-методического совета института физико-математических наук и информационных технологий

Протокол № 01/22 от «01» февраля 2022 г.

Председатель учебно-методического
совета института физико-
математических наук и информационных
технологий
Первый заместитель директора Шпилевой А. А
ИФМНиИТ, к. ф.-м. н., доцент

Ведущий менеджер Е.П.Ставицкая

Содержание

1.Наименование дисциплины: «Иностранный язык (немецкий)».

Целью дисциплины является использование немецкого языка как средства общения для решения задач межличностного и профессионального взаимодействия с представителями других культур.

2. Перечень планируемых результатов обучения по дисциплине, соотнесенных с планируемыми результатами освоения образовательной программы

Код компетенции	Результаты освоения образовательной программы (ИДК)	Результаты обучения по дисциплине
УК-4. Способен применять современные коммуникативные технологии, в том числе на иностранном(ых) языке(ах), для академического и профессионального взаимодействия	УК.4.1. Демонстрирует умение вести обмен профессиональной информацией в устной и письменной формах в том числе и на иностранном языке. УК.4.2. Использует современные информационно-коммуникативные технологии для академического взаимодействия и с соблюдением этики делового общения; Использует современные информационно-коммуникативные технологии для взаимодействия в профессиональной сфере. УК.4.3. Способен осуществлять деловую коммуникацию в устной и письменной формах на государственном языке РФ.	**Знать:** - иностранный язык на уровне предусмотренном рамками высшего образования, -знать способы поиска новой и нужной языковой информации, **Уметь:** -пользоваться наиболее употребительными и относительно простыми языковыми средствами во всех видах речевой деятельности: устной речи, аудировании, чтении и письме, -планировать работу, -ставить перед собой цели и задачи предстоящей деятельности, -уметь целесообразно распределять нагрузку. **Владеть:** компьютерной грамотностью (навыки работы в компьютерных программах “Word”, “Power Point”, навыки работы с принтером, сканером, навыки работы с электронной почтой и в сети Интернет).
УК-5. Способен анализировать и учитывать разнообразие культур в процессе межкультурного взаимодействия	УК.5.1. Выявление общего и особенного в историческом развитии России. УК.5.2. Анализирует современное состояние общества на основе знания истории. УК.5.3. Способен использовать основы философских знаний для формирования	**Знать:** - особенности социальной организации общества, специфику менталитета и мировоззрения культур России, Запада и Востока; - особенности представлений культур друг о друге с учетом наличия общего ценностного контекста, этностерео и гетеростереотипов, формируемых информационной средой;

	мировоззренческой позиции.	- основы теории коммуникации, проблемы культурной идентичности и межкультурных контактов. **Уметь:** - достигать эффективности коммуникации; - преодолевать культурный барьер, воспринимая межкультурные различия избегать предубеждений и настраиваться на совместные действия с представителями других культур; - сохраняя национальную идентичность, избегать этноцентризма; - соблюдать нормы этикета, моральные и культурные нормы. **Владеть:** - способностью преодолевать стереотипы; - творческим отношением к процессу коммуникации; - способностью использовать набор коммуникативных средств и делать их правильный выбор в зависимости от ситуации общения (тон, стиль, стратегии, речевые жанры, тематика и т. д.).

3. Место дисциплины в структуре образовательной программы

Дисциплина «Иностранный язык» относится к обязательной части Блока 1 Дисциплины (модули).

4. Виды учебной работы по дисциплине.

Виды учебной работы по дисциплине зафиксированы учебным планом основной профессиональной образовательной программы по указанному направлению и профилю, выражаются в академических часах. Часы контактной работы и самостоятельной работы студента и часы, отводимые на процедуры контроля, могут различаться в учебных планах ОПОП по формам обучения. Объем контактной работы включает часы контактной аудиторной работы (лекции/практические занятия/ лабораторные работы), контактной внеаудиторной работы (контроль самостоятельной работы), часы контактной работы в период аттестации. Контактная работа, в том числе может проводиться посредством электронной информационно-образовательной среды университета с использованием ресурсов сети Интернет и дистанционных технологий

5. Содержание дисциплины, структурированное по темам (разделам)

Исходя из рамок, установленных учебным планом по трудоемкости и видам учебной работы по дисциплине, преподаватель самостоятельно выбирает тематику

занятий по формам и количеству часов проведения контактной работы: лекции и иные учебные занятия, предусматривающие преимущественную передачу учебной информации преподавателем и (или) занятия семинарского типа (семинары, практические занятия, практикумы, лабораторные работы, коллоквиумы и иные аналогичные занятия), и (или) групповые консультации, и (или) индивидуальную работу обучающихся с преподавателем, в том числе индивидуальные консультации (по курсовым работам/проектам – при наличии курсовой работы/проекта по данной дисциплине в учебном плане). Рекомендуемая тематика занятий максимально полно реализуется в контактной работе со студентами очной формы обучения. В случае реализации образовательной программы в заочной / очно-заочной форме трудоемкость дисциплины сохраняется, однако объем учебного материала в значительной части осваивается студентами в форме самостоятельной работы. При этом требования к ожидаемым образовательным результатам студентов по данной дисциплине не зависят от формы реализации образовательной программы.

Название темы	**Содержание темы**
Wohnräume. Wohnträume	беседа о видах жилых помещений; сообщение о своем любимом месте в доме/квартире; описание интерьера; порядок слов в простом и вопросительном предложениях; спряжение сильных и слабых глаголов; особенности употребление предлогов in, an, auf, neben, zwischen, vor, hinter, über, unter
Ausbildung und Praktikum	информирование о видах образовательных учреждении; беседа о возможностях прохождения практики в ходе обучения; сообщение о дуальной системе образования в Германии; описание учебы в университете; модальные глаголы wollen, mögen, müssen; предлоги для указания времени seit, vor, für
Tagesordnung und Freizeitgestaltung	беседа о плюсах и минусах распорядка дня; сообщение о своем обычном дне; сообщение о любимом виде досуга; беседа об увлечениях; описание возможностей для проведения свободного времени в родном городе; предлоги указания времени um, an, in; глаголы с отделяемыми приставками; модальные глаголы sollen, dürfen
Essgewohnheiten. Gesundes Leben	беседа о здоровом образе жизни; сообщение о собственных привычках в еде; рекомендации для здорового питания; конструкция du solltest/ Sie sollten для выражения совета, рекомендации; союзы denn/ weil
Konsum und Geldverhalten	беседа об отношении к деньгам; сообщение о собственных расходах; информирование о потреблении в современном обществе и роли рекламы; вопросительные слова Wofür/ Für wen?; косвенный вопрос; придаточные предложения с союзом dass
Urlaubsland Deutschland	беседа о приоритетных направлениях для отдыха; информирование о возможностях для отдых в Германии; сообщение о своих планах на каникулы; предлоги mit, nach,

	aus, zu, von, bei, seit, außer, entgegen, gegnüber; Perfekt
Umweltprobleme: Wie kann jeder zum Umweltschutz beitragen?	информирование о проблемах окружающей среды; беседа о мерах по защите окружающей среды; сообщение о возможностях личного вклада в защиту окружающей среды; придаточное предложение условия
Filmkunst: Warum sehen Jugendliche Daily-Soaps?	беседа о видах кино; информирование о значимых кинофестивалях;сообщение о собственных предпочтениях; рассуждение об интернете как универсальном сми; предлоги um, gegen, durch, ohne, für; Präteritum
Junge Leute von heute	информирование об отношении молодежи к традиционным ценностям; сообщение о собственных жизненных ориентирах; описание роли семьи; конструкции ich bin der Meinung; meiner Ansicht nach; ich stimme (nicht) zu; инфинитивные обороты um … zu/statt…zu/ ohne … zu; придаточное предложение цели
Fachstudium	информирование о возможностях профессионального обучения в университете; сообщение о направлении обучения в институте; описание учебного дня; определительные придаточные предложения
Deutsch im Beruf	информирование о возможностях обучения за границей; беседа об образе специалиста, его профессиональных задачах; описание собственных представлений о будущей профессиональной деятельности; причастия в качестве определений
Die Welt der Technik	беседа о роли научно-технического прогресса в современном обществе; информирование об этапах развития науки и техники; сообщение о современных технологиях в промышленности; описание возможностей применения информационных технологий в разных сферах жизни; страдательный залог
Ostpreußen: wichtige Abschnitte der Geschichte	беседа об истории региона; информирование об основных этапах в истории Восточной Пруссии; сообщение об интересных исторических местах родного города; придаточные предложения времени с союзами als/wenn/nachdem
Albertina: erste Universität in Ostpreußen	информирование о становлении Альбертины – первого университета в Восточной Пруссии; сообщение об образовательных учреждения Кенигсберга; описание деятельности одного из представителей точных наук Альбертины; придаточные предложения времени с союзами während/bevor/bis
Zur Entwicklung der Zahlen	информирование о концептуальных представлениях о появлении чисел; сообщение о видах чисел и основных вычислительных операциях; глаголы, требующие предложного дополнения

Digitale Massenmedien	информирование о видах сми; сообщение о цифровых носителях информации; описание возможностей применения цифровых технологий в сми; прилагательные и наречия с предложными дополнениями
Weiterbildung	информирование о возможностях пост-дипломного образования в России и заграницей; сообщение о роли постоянного самообразования и повышения квалификации; сослагательное наклонение для описания потенциальной возможности

6. Рекомендуемая тематика учебных занятий в форме контактной работы

Рекомендуемая тематика *практических* занятий:

1. Wohnräume. Wohnträume
2. Ausbildung und Praktikum
3. Tagesordnung und Freizeitgestaltung
4. Essgewohnheiten. Gesundes Leben
5. Konsum und Geldverhalten
6. Urlaubsland Deutschland
7. Umweltprobleme: Wie kann jeder zum Umweltschutz beitragen?
8. Filmkunst: Warum sehen Jugendliche Daily-Soaps?
9. Junge Leute von heute
10. Fachstudium
11. Deutsch im Beruf
12. Die Welt der Technik
13. Ostpreußen: wichtige Abschnitte der Geschichte
14. Albertina: erste Universität in Ostpreußen
15. Zur Entwicklung der Zahlen
16. Digitale Massenmedien
17. Weiterbildung

Требования к самостоятельной работе студентов

Работа с пройденным тематическим материалом, предусматривающая проработку учебной литературы, лексического и грамматического материала, по указанным в пункте 6 темам с использованием:
1) учебников, учебно-методических пособий, словарей и справочных пособий;
2) ресурсов информационно-телекоммуникационной сети «Интернет»;

3) фонда оценочных средств.

Руководствуясь положениями статьи 47 и статьи 48 Федерального закона от 29 декабря 2012 г. N 273-ФЗ «Об образовании в Российской Федерации» научно-педагогические работники и иные лица, привлекаемые университетом к реализации данной образовательной программы, пользуются предоставленными академическими правами и свободами в части свободы преподавания, свободы от вмешательства в профессиональную деятельность; свободы выбора и использования педагогически обоснованных форм, средств, методов обучения и воспитания; права на творческую инициативу, разработку и применение авторских программ и методов обучения и воспитания в пределах реализуемой образовательной программы и отдельной дисциплины.

Исходя из рамок, установленных учебным планом по трудоемкости и видам учебной работы по дисциплине, преподаватель самостоятельно выбирает тематику занятий по формам и количеству часов проведения контактной работы: лекции и иные учебные занятия, предусматривающие преимущественную передачу учебной информации преподавателем и (или) занятия семинарского типа (семинары, практические занятия, практикумы, лабораторные работы, коллоквиумы и иные аналогичные занятия), и (или) групповые консультации, и (или) индивидуальную работу обучающихся с преподавателем, в том числе индивидуальные консультации (по курсовым работам/проектам – при наличии курсовой работы/проекта по данной дисциплине в учебном плане).

Рекомендуемая тематика занятий максимально полно реализуется в контактной работе со студентами очной формы обучения. В случае реализации образовательной программы в заочной / очно-заочной форме трудоемкость дисциплины сохраняется, однако объем учебного материала в значительной части осваивается студентами в форме самостоятельной работы. При этом требования к ожидаемым образовательным результатам студентов по данной дисциплине не зависят от формы реализации образовательной программы.

Тема	**Задание**
Da wohne ich	письменная работа: описать интерьер собственной комнаты
Ein ganz normaler Studientag	устное сообщение-описание типичного учебного дня
Hier kann man sich richtig entspannen	письменная работа: описать на основе личных впечатлений лучшее место для отдыха
Was heißt gesund leben?	письменная работа: представить рекомендации в пользу здорового образа жизни
Geld regiert die Welt?	письменная работа: рассуждение о роли денег в современном обществе
Jeder ist für die Umwelt verantwortlich	письменная работа: рассуждение о необходимости экологического воспитания
Berlin, Venedig, Cannes – europäische	устное сообщение-презентация одного из

Filmfestivals	европейский кинофестивалей
Pragmatische Generation von heute	подготовка к дискуссии: составление тезисов, отражающих мировоззрение современного поколения
Eine Führung durch das Institut	устное сообщение-презентация: экскурсия по институту в День открытых дверей
Mein Traumberuf	письменная работа: описание плюсов и минусов будущей профессии
Vom Stein bis zum Laser	письменная работа: резюме содержания текстового материала по теме "Die Welt der Technik"
Architektonische Denkmäler meiner Heimatstadt	устное сообщение-презентация об интересных местах родного города
Prominente an der Albertina	устное сообщение-презентация о выдающихся деятелях Альбертины
Zahlenzoo	письменная работа: резюме статьи "Zahlen lernen"
Tradition vs Innovation	самостоятельное поисковое чтение и собеседование по теме "Digitale Massenmedien"
Man lernt im Leben nie aus	письменная работа: рассуждение в отношении поговорки "Век живи – век учись"

7. Методические рекомендации по видам занятий

Лекционные занятия.

В ходе лекционных занятий обучающимся рекомендуется выполнять следующие действия. Вести конспектирование учебного материала. Обращать внимание на категории, формулировки, раскрывающие содержание тех или иных явлений и процессов, научные выводы и практические рекомендации по их применению. Задавать преподавателю уточняющие вопросы с целью уяснения теоретических положений, разрешения спорных ситуаций.

Желательно оставить в рабочих конспектах поля, на которых во внеаудиторное время можно сделать пометки из рекомендованной литературы, дополняющие материал прослушанной лекции, а также подчеркивающие особую важность тех или иных теоретических положений.

Практические и семинарские занятия.

На практических и семинарских занятиях в зависимости от темы занятия выполняется поиск информации по решению проблем, практические упражнения, контрольные работы, выработка индивидуальных или групповых решений, итоговое

обсуждение с обменом знаниями, участие в круглых столах, разбор конкретных ситуаций, командная работа, представление портфолио и т.п.

Самостоятельная работа.

Самостоятельная работа осуществляется в виде изучения литературы, эмпирических данных по публикациям и конкретных ситуаций из практики, подготовке индивидуальных работ, работа с лекционным материалом, самостоятельное изучение отдельных тем дисциплины; поиск и обзор литературы и электронных источников; чтение и изучение учебника и учебных пособий.

8. Фонд оценочных средств

8.1. Перечень компетенций с указанием этапов их формирования в процессе освоения образовательной программы в рамках учебной дисциплины

Основными этапами формирования указанных компетенций при изучении обучающимися дисциплины являются последовательное изучение содержательно связанных между собой тем учебных занятий. Изучение каждой темы предполагает овладение обучающимися необходимыми компетенциями. Результат аттестации обучающихся на различных этапах формирования компетенций показывает уровень освоения компетенций.

Уровень A1-A2 (темы 1-8: бакалавр должен уметь бегло и фонетически корректно читать; переводить и пересказывать учебные, адаптированные, а также аутентичные тексты; вести беседы на пройденные общие и личностно-ориентированные темы)

Уровень B1-B2 (темы 9-15: должен уметь перевести специальные тексты; отвечать на вопросы по прочитанным текстам; уметь пересказывать тексты общего и специального характера; владеть навыками перевода и реферирования специального текста;
навыками письменной речи; уметь вести беседу на темы по специальности; участвовать в учебных конференциях по специальности и уметь обсуждать специальные темы с коллегами, студентами - носителями языка).

Контролируемые модули, разделы (темы) дисциплины	Индекс контролируемой компетенции (или ее части)	Оценочные средства по этапам формирования компетенций
		Текущий контроль
Wohnräume. Wohnträume.	УК-4, УК-5	Устный опрос Лексико-грамматический тест на закрепление материала
Ausbildung und Praktikum	УК-4, УК-5	Устный опрос Лексико-грамматический тест на закрепление материала
Tagesordnung und Freizeitgestaltung	УК-4, УК-5	Устный опрос Лексико-грамматический тест на закрепление материала
Essgewohnheiten.	УК-4, УК-5	Устный опрос

Gesundes Leben		Лексико-грамматический тест на закрепление материала
Konsum und Geldverhalten	УК-4, УК-5	Устный опрос Лексико-грамматический тест на закрепление материала
Urlaubsland Deutschland	УК-4, УК-5	Устный опрос Лексико-грамматический тест на закрепление материала
Umweltprobleme: Wie kann jeder zum Umweltschutz beitragen?	УК-4, УК-5	Устный опрос Лексико-грамматический тест на закрепление материала
Filmkunst: Warum sehen Jugendliche gerne Daily-Soaps?	УК-4, УК-5	Устный опрос Лексико-грамматический тест на закрепление материала
Junge Leute von heute	УК-4, УК-5	Устный опрос Лексико-грамматический тест на закрепление материала
Fachstudium	УК-4, УК-5	Устный опрос Лексико-грамматический тест на закрепление материала
Deutsch im Beruf	УК-4, УК-5	Устный опрос Лексико-грамматический тест на закрепление материала
Die Welt der Technik	УК-4, УК-5	Устный опрос Лексико-грамматический тест на закрепление материала
Ostpreußen: wichtige Abschnitte der Geschichte	УК-4, УК-5	Устный опрос Лексико-грамматический тест на закрепление материала
Albertina: erste Universität in Ostpreußen	УК-4, УК-5	Устный опрос Лексико-грамматический тест на закрепление материала
Zur Entwicklung der Zahlen	УК-4, УК-5	Устный опрос Лексико-грамматический тест на закрепление материала
Digitale Massenmedien	УК-4, УК-5	Устный опрос Лексико-грамматический тест на закрепление материала
Weiterbildung	УК-4, УК-5	Устный опрос Лексико-грамматический тест на закрепление материала

8.2. Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений и навыков и (или) опыта деятельности процессе текущего контроля

Примеры контрольных заданий: тесты, лексико-грамматические задания, аудирование, перевод, письмо:

1 семестр

LESEVERSTEHEN

Welches Wort passt nicht?

1. Das Haus liegt …. zentral / günstig / lang / ruhig
2. Das Haus kann man … besichtigen / einziehen / mieten / kaufen
3. In unserem Haus gibt es … einen Spielplatz / eine Wohnküche / ein Bad / einen langen Gang
4. Nicht weit von unserem Haus gibt es … eine Fußgängerzone / einen Spielplatz / einen Keller / einen Parkplatz
5. Ein neues Haus kann man … planen / bauen / mieten / wohnen

Silbenrätsel. Wie heißen die Wörter? Raten Sie.

stuhl /dach /erd /ge /haus /hof /mei /mie /mie /nung/ schoss /ster /te /ter /ver /warm /woh /fahr

1. Die Person, die ein Haus oder eine Wohnung vermietet. ….
2. Wenn man nicht Treppe steigen will, nimmt man den …
3. Diese Person kümmert sich um Reparaturen im Haus. …
4. Der Platz hinter den Miethäusern in einer Stadt. Hier spielen oft die Kinder. …
5. Die oberste Wohnung in einem Haus. …
6. Die Höhe der monatlichen Miete inklusive der Heizkosten. …
7. Das untere Stockwerk im Haus. …

Lesen und übersetzen Sie den Text.

Ich wohne in einem neuen Hochhaus nicht weit vom Stadtzentrum. Alles ist nicht weit – Schule, Geschäfte, Kinos und sogar ein nettes Café. Unser Wohnhaus ist achtstöckig. Im Erdgeschoß ist eine Apotheke. Unser Haus ist modern und gut gepflegt. Die Treppenhäuser sind immer sauber. An der Wand hängen die Briefkästen. Im Hof gibt es einen Parkplatz und Grünflächen. Außerdem haben wir dort sehr nette Nachbarn.

Meine Wohnung liegt im sechsten Stock, darum nehme ich immer den Fahrstuhl. Er ist ständig in Betrieb. Ich habe eine gute Dreizimmerwohnung. Sie ist sechzig Quadratmeter groß und hat allen Komfort: es gibt Fernheizung, Warmwasser, Telefon und Internet.

Die Wohnung hat ein Wohnzimmer, ein Schlafzimmer, ein Kinderzimmer. Es gibt natürlich eine Küche, einen Flur, ein Bad und eine Toilette. Ich finde meine Wohnung prima. Sie gefällt auch meinen Freunden und Verwandten.

In zwei Wochen will ich mein Schlafzimmer neu tapezieren. Das Zimmer ist nicht sonnig, darum braucht es helle Tapeten. Mein Mann und unsere Tochter helfen mir beim Tapezieren. Wir brauchen auch etwas Neues für unser Schlafzimmer. Am Wochenende gehen wir in ein Möbelgeschäft. Wir wollen eine neue Stehlampe und einen originellen Spiegeltisch für mich kaufen.

Was ist richtig, was ist falsch?

1. Olga wohnt in einem Privathaus.
2. Ihr Haus ist zweistöckig.
3. Dieses Haus ist modern und gut gepflegt
4. Leider liegt das Haus weit vom Zentrum.
5. Olga wohnt im ersten Stock.
6. Sie nimmt keinen Fahrstuhl.
7. Der Fahrstuhl ist ständig in Betrieb.
8. Im Hof gibt es leider keinen Parkplatz.
9. Olgas Nachbarn sind nette Leute.
10. Ihre Zweizimmerwohnung ist mit allem Komfort.
11. Die Freunde und Verwandten finden Olgas Wohnung gut.
12. Helle Tapeten machen das Schlafzimmer gemütlicher.
13. Für ihr Schlafzimmer braucht Olga nicht nur helle Tapeten, sondern auch ein Bett.
14. Die Möbel bestellen sie im Internet-Geschäft.

Ergänzen Sie die Lücken.

1. Olga…….in einem neuen Hochhaus.
2. Ihr Wohnhaus ……nicht weit vom Stadtzentrum.
3. Im Erdgeschoß …… es eine Apotheke.
4. Olga…….immer den Fahrstuhl.
5. Der Fahrstuhl …….ständig in Betrieb.
6. Die Treppenhäuser ……. sauber und gepflegt.
7. Im Hof …… es einen Parkplatz.
8. Außerdem ….. Olga sehr nette Nachbarn.
9. Die Wohnung liegt … …. Stock.
10. Sie hat eine …. mit allem Komfort.
11. Im …. empfängt Olga ihre Gäste.

12. Ihr… braucht helle Tapeten.
13. … …. ist das Zimmer ihrer Tochter.
14. … … geht die ganze Familie in das Möbelgeschäft.
15. Olga braucht … … und … … für ihr Schlafzimmer.

Stellen Sie Fragen.

1. ……...? Ja, Olga wohnt in einem Hochhaus.
2. ……? Nein, ihr Haus liegt nicht weit vom Stadtzentrum.
3. ……? Im Hof gibt es einen Parkplatz und Grünflächen.
4. ……? Sie wohnt im sechsten Stock.
5. ……? Nein, sie nimmt immer den Fahrstuhl.
6. ……? Ja, dieses Haus ist modern und gut gepflegt.
7. ……? Die Wohnung ist 60 Quadratmeter groß.
8. ……? Denn das Schlafzimmer ist zu dunkel.
9. ……? Sie will das in zwei Wochen machen.
10. ……? Nein, Olga macht das zusammen mit ihrem Mann und ihrer Tochter.
11. ……? Ja, sie braucht auch eine Stehlampe und einen Spiegeltisch.

SCHREIBEN

Sehen Sie die Bilder an. Beschreiben Sie die Gebäude. Antworten Sie dabei auf folgende Fragen:

1. Was für ein Gebäude ist das? (ein Landhaus, ein Hochhaus, ein Universitätsgebäude, ein Museum usw.)
2. Wie hoch ist dieses Gebäude?
3. Was ist im Erdgeschoß /im ersten/zweiten Stock?
4. Gib es hier einen Hof? Was gibt es in diesem Hof?
5. Wie finden Sie dieses Haus?
6. Wer kann in diesem Haus wohnen? Begründen Sie Ihre Meinung?

SPRECHEN

Situation 1: Was ist Ihr Lieblingsort zu Hause? Warum mögen Sie den?

Situation 2: Was meinen Sie, ist das Praktikum wichtig für den Einstieg in den Beruf?

Situation 3: Könnten Sie bitte erzählen, wie Sie gewöhnlich Ihre Freizeit verbringen?

Situation 4: Was halten Sie vom gesunden Leben? Ist das nur mit Sport verbunden?

2 семестр

LESEVERSTEHEN

I. Lesen und übersetzen Sie den folgenden Text.

Der neue Trend: Jugendliche wohnen länger bei den Eltern

Immer mehr junge Leute bleiben im Elternhaus, obwohl sie schon lange arbeiten und Geld verdienen. Warum denn wohnen die Twens von heute bei ihren Eltern? Sind sie zu anspruchsvoll? Haben sie Angst vor der Unabhängigkeit oder kein Geld für eine eigene Wohnung?

Früher war in Deutschland solch eine Wohnform bei jungen Erwachsenen beliebt wie die Wohngemeinschaft (kurz WG). In diesem Alter wollte man schon weg von zu Hause, mit den anderen Leuten zusammenleben. Große Wohnungen waren zu teuer, aber zu viert oder zu fünft konnte man die Miete gut bezahlen. Außerdem konnte man anders als die Eltern wohnen.

Heute ist die WG für die meisten keine Alternative mehr, weil WG für viele nur Chaos und Streit um die Hausarbeiten bedeutet. Und eine eigene Wohnung mieten, alleine wohnen? Viele zögern, obwohl sie gerne unabhängig sein wollen.

Vor allem sind in den Großstädten Wohnungen sehr teuer – besonders für Lehrlinge und Studenten. Deshalb bleiben die meisten jungen Leute zu Hause, bis sie ihre Lehre oder ihr Studium beendet haben. Und auch danach führt der Weg nicht automatisch in die eigene Wohnung, weil viele nach Abschluss der Ausbildung keine Arbeit finden können. Auch ein Universitätsabschluss und gute Noten sind heute keine Garantie mehr für eine sichere berufliche Zukunft.

Häufig ziehen einige junge Erwachsene aus, kommen aber bald zu ihren Eltern zurück, weil sie arbeitslos werden, weil sie ihre Wohnung nicht mehr bezahlen können oder weil sie Probleme mit dem Alleinsein haben.

Natürlich gibt es auch junge Leute, die gar nicht ausziehen wollen. Sie bleiben im Elternhaus, obwohl sie genug Geld für ihre eigene Wohnung haben. Für sie ist das kostenlose oder günstige Wohnen bei den Eltern attraktiv, weil sie so nicht auf das eigene Auto und teure Urlaube verzichten müssen. Sie genießen den „Rund-um-die-Uhr-Service“ und müssen keine Hausarbeiten machen. Außerdem ist da immer jemand, der zuhört und hilft, wenn man Probleme hat. Warum also ausziehen? – zu Hause ist doch alles so einfach.

II. Bestimmen Sie, welche Aussage richtig, welche – falsch ist.

1. Fast alle jungen Leute möchten heutzutage wie möglich schneller aus dem Elternhaus ausziehen.
2. Früher war die Wohngemeinschaft eine beliebte Wohnform für die Jugendlichen.
3. Wohngemeinschaften sind wie früher sehr populär.
4. Die meisten haben Angst, eigene Wohnung zu mieten und alleine zu wohnen.
5. In den Großstädten ist die Wohnungsmiete für Studenten sehr günstig.
6. Viele können nach dem Abschluss einer Beruf- oder Hochschule keine Arbeit finden, darum bleiben sie bei den Eltern.
7. Der Universitätsabschluß ist eine Garantie für sichere berufliche Zukunft.
8. Viele Jugendliche kommen bald zu ihren Eltern zurück, weil sie viele Probleme mit dem Alleinsein haben.
9. Es gibt auch junge Leute, die gar nicht ausziehen wollen.
10. Warum also ausziehen? - zu Hause ist immer jemand, der zuhört und hilft, wenn man Probleme hat.

III. Переведите и придумайте несколько примеров со следующими выражениями.

aus dem Elternhaus/ aus der Wohnung ausziehen
Wann ziehen in deinem Land junge Leute aus dem Elternhaus aus?
unabhängig sein (von D)
Bist du von deinen Eltern unabhängig?
etwas bezahlen
Die Eltern bezahlen mein Studium.
Arbeit finden
Nach dem Universitätsabschluß will ich eine gut bezahlte Arbeit finden.
verzichten (auf A)
Worauf kannst du nicht verzichten?
Ich kann nicht auf Fleisch verzichten.

zuhören
Sie kann immer gut zuhören.
Probleme lösen
Ich muß meine Probleme selbst lösen.

IV. Ergänzen Sie folgende Sätze. Beachten Sie die Wortfolge im Nebensatz mit den Konjunktionen weil und obwohl.

1. Die jungen Leute von heute bleiben im Elternhaus, weil …
   a) Sie haben Angst vor der Unabhängigkeit.
   b) Sie haben kein Geld für eigene Wohnung.
   c) Sie können zu Hause den „Rund-um-die-Uhr-Service“ genießen.
   d) Zu Hause ist alles viel einfacher und bequemer.
2. Die WG ist heute nicht so beliebt wie früher, weil …
   a) Junge Leute oft um Hausarbeiten und Hausordnung streiten.
   b) Man muss die Gewohnheiten anderer Leute berücksichtigen.
   c) Das Leben in der WG ist nicht immer ruhig.
3. Sie leben bei den Eltern, obwohl …
   a) Sie verdienen Geld schon lange selbst.
   b) Sie haben eine gut bezahlte Arbeit.
   c) Sie können eine Mietwohnung selbst bezahlen.
   d) Sie können nicht anders als ihre Eltern leben.

V. Finden Sie die passende Antwort im Text.

1. Warum war früher die Wohngemeinschaft eine beliebte Wohnform für die Jugendlichen?
2. Warum ist die WG heute für die meisten keine Alternative mehr?
3. Warum ist es nicht leicht, eine Wohnung in einer Großstadt zu mieten?
4. Warum können viele nach dem Abschluss der Ausbildung keine eigene Wohnung haben?
5. Warum kommen bald einige junge Erwachsene zu ihren Eltern zurück?
6. Warum gibt es auch solche jungen Leute, die gar nicht ausziehen wollen?

SREIBEN

I. Wie steht es mit diesem Problem in Ihrem Heimatland? Wann ziehen junge Erwachsene aus? Wie wohnen sie dann? Warum? Schreiben Sie darüber.

Wörter und Redewendungen
mit …..Jahren ausziehen
mit dem Partner/der Partnerin leben
in einer anderen Stadt arbeiten/studieren
zum Militär gehen
Streit mit den Eltern haben
bei Verwandten wohnen
unabhängig sein
mit Freunden zusammenwohnen
gerne allein leben
seine Ruhe haben
genug Geld haben
bis zur Heirat/zum Examen bei den Eltern wohnen
Kinder haben

II. Überlegen Sie sich die Deutung von dem Begriff "Bumerang-Kinder". Äußern Sie Ihre Überlegungen schriftlich. Folgende Erläuterung kann helfen

Bumerang (der); -s; Plural –s oder –e
(engl., aus austral. Wumera);

Wurfholz, das in einem Kreis zum Werfer zurückfliegt.
Heute in vielen Formen als Spiel- und Sportgerät zu finden.

SPRECHEN

Situation 1: Was meinen Sie, ist Fernsehen heute bei Jugendlichen so beliebt wie vor zehn Jahren?

Situation 2: Könnten Sie bitte sagen, was Sie machen, wenn Ihr Taschengeld nicht reicht?

Situation 3: Was ist Ihrer Meinung nach in unserer Stadt in erster Linie zu besichtigen?

Situation 4: Könnten Sie damit zustimmen, dass heutige Jugend sehr pragmatisch ist?

Situation 5: Was kann jeder von uns täglich für den Umweltschutz tun? Könnten Sie bitte ein paar Tipps geben?

3 семестр

LESEVERSTEHEN

I. Ergänzen Sie die Lücken

IT-Branche # kommunikativ # herstellen/ betreuen # überprüfen # Schlüsselkompetenzen # Kontakt zu Kunden # Programmiersprachen # entwickelt/ pflegt # Softwaresysteme

(1)Ein Softwareentwickler … und … datenbankorientierte Informationssysteme. (2)Softwareentwickler arbeiten meist in der …, vor allem in Unternehmen, die Softwaresysteme … und (3)… . Auch Ingenieurbüros kommen als Arbeitgeber in Betracht.

(4) Im ersten Arbeitsschritt analysieren Softwareentwickler … , um dann einzelne Komponenten so zu programmieren und zu verbessern, dass sie den Vorstellungen der Anwender entsprechen. Neben der (6) Arbeit am Computer haben Softwareentwickler deshalb oft … , denn sie sind auch dafür zuständig, Benutzer zu beraten. Dies kann entweder im Unternehmen selbst oder zuhause beim Kunden erfolgen. Auch die Teamarbeit ist bei dem Job des Softwareentwicklers gefragt.

(9) Softwareentwickler sollten … sein, um die Aufgaben nach Absprache mit Kollegen effizient und kundenorientiert durchführen zu können. Im Gegensatz zu einem Programmierer ist der Softwareentwickler in mehrere Arbeitsprozesse involviert. Denn als Softwareentwickler ist es wichtig, anstehende (12) Arbeitsschritte zu planen und diese dann auch auf Wirtschaftlichkeit und Effizienz zu … . Kenntnisse in Datenbanktechnologien, Programmierung und Webtechnologien sind zudem unerlässlich. In Stellenanzeigen werden vom Bewerber meist analytisches Denkvermögen und das Interesse für technische (15)und kaufmännische Prozesse erwartet. Die Beherrschung von … , Softwareentwicklungsmethoden und (16) der Umgang mit modernen Betriebssystemen sind … im Job des Softwareentwicklers.

II. Was passt? Ordnen Sie zu.

a) Das Menü kann man leicht bedienen. Es ist …	online
b) Die Webseite gibt auf Eingaben Rückmeldungen. Sie ist …	langsam
c) Die Datenübertragung war korrekt. Sie war …	kaputt
d) Die Hardware funktioniert nicht mehr. Sie ist …	schnell
e) Das Programm passt nicht zu dem Betriebssystem. Beide sind …	fehlerfrei bedienerfreundlich
f) Die DSL-Verbindung ist ziemlich gut. Sie ist …	interaktiv
g) Die Software reagiert schlecht. Sie ist zu …	inkompatibel
h) Wenn man im Internet ist, ist man …	

SCHREIBEN

Aufgabe 1

Schreiben Sie folgende Sätze im Passiv um.

Mikroelektroniker erforschen und entwickeln neu Technologien.

Zuerst entwerfen die Ingenieure die neuen Produkte am Computer.

Dabei überlegen sie sich, wie sie das neue Produkt gestalten müssen*.

Nach der Herstellung des Produktes überwachen die Ingenieure die Produktion.

Sie müssen auch die Kosten für die Herstellung kontrollieren*.

Sie müssen das fertige Produkt regelmäßig testen*.

Danach nehmen die Ingenieure die Maschine oder die Anlage in Betrieb.

Wenn es technische Probleme gibt, muss man den Fehler suchen und beheben.

Aufgabe 2

Akademie für ONLINE MARKETING bietet allen Interessenten Seminare zu verschiedenen Themen in der Telekommunikationsbranche. Lesen Sie zuerst allgemeine Information über eines der Seminare, dann die Meinungen von 3 Seminarteilnehmern. Fassen Sie dann kurz zusammen, was die Teilnehmer von diesem Seminar halten.

Die Welt der modernen Telekommunikation wird von Tag zu Tag komplexer und undurchsichtiger. Die Schnelllebigkeit der technischen Entwicklung und die Informationsüberflutung insgesamt machen es zunehmend schwerer, den Überblick zu behalten. In unserem Seminar möchten wir Sie durch den Dschungel an Produkten und Dienstleistungen der modernen Telekommunikation führen. Der Schwerpunkt unseres Seminars liegt in der Vermittlung von Zusammenhängen und Anwendungsszenarien, nicht der Technik.

Mir hat das Seminar sehr gut gefallen und ich konnte als Quereinsteiger in die Branche davon profitieren. Der Aufbau war so gestaltete, dass die Teilnehmer wirklich „bei Null“ abgeholt wurden und man somit Eine gute Basis erhält, um die Entwicklung innerhalb der Telekommunikationsbranche zu verstehen. / *Christopher Kahl, teliko GmbH*

Das Seminar bildet die facettenreiche Welt der Telekommunikationsbranche sehr gut ab. Durch einen kurzen Blick in die Vergangenheit und die Entwicklung bis heute werden die Zusammenhänge deutlich. Die Inhalte sind didaktisch strukturiert, so dass man jederzeit gut folgen kann.

Die abwechslungsreiche Art der Präsentation, die kleine Teilnehmerzahl und die angenehme Atmosphäre runden die zweitägige Veranstaltung ab. / *Ingo Apelt, Project Manager, Gasunie Deutschland GmbH & Co. KG*

Das Seminar hat uns persönlich von allen bisher besuchten Seminaren am besten gefallen. Gründe dafür sind, die sehr gute Organisation und Moderation des Trainers.

Diese zwei Tage waren eine echte Bereicherung und ich würde dieses Seminar definitiv jedem empfehlen der neu in der Telekommunikationsbranche ist oder der eine Auffrischung für das tägliche Geschäft in Sachen Telefon und Internet benötigt. Die Art der Präsentation war sehr bildlich und übersichtlich strukturiert. / *Sabrina Zierenberg, Teamleiter „Verkaufsservice“ & Steffen Schröter, Teamleiter „interner Service“ Stadtwerke Finsterwalde GmbH*

Aufgabe 3

Wie würden Sie als IT-Mitarbeiter/in reagieren? Schreiben Sie.

Situation 1.

Ein Benutzer bekommt zu viele SPAM-Mails. Das stört ihn sehr. Er fragt Sie, was er tun soll. Wahrscheinlich könnte er selbst etwas unternehmen, z.B. den SPAM-Filter an seinem PC neu einstellen…

Situation 2.

Ein Benutzer informiert Sie, dass er keine Internetverbindung herstellen kann. Es könnte sein, dass der Server überlastet sei, deshalb sollte man etwas warten und später noch einmal versuchen…

SPRECHEN

Situation 1: Könnten Sie bitte Ihren ganz normalen Studientag beschreiben?

Situation 2: Was denken Sie, was ermöglicht das Erlernen von Fremdsprachen?

Situation 3: Was soll Ihrer Meinung nach die Wendung "Kehrseite des technischen Fortschritts" bedeuten?

4 семестр

LESEVERSTEHEN 1

I. Lesen Sie den folgenden Text, machen Sie dann die Aufgaben II - V

Architektonische Denkmäler in Kaliningrad

Kaliningrad ist reich an alten Denkmälern aus verschiedenen Epochen. Eines der größten architektonischen Denkmäler ist der Dom, der sich auf der Pregelinsel erhebt. Die erste auf dem Dom bezogene Urkunde stammt aus dem Jahre 1333. Seit 1523 begann im Dom der evangelische Gottesdienst. Im Turm des Domes befand sich die weltberühmte Wallenrodtsche Bibliothek. Sie enthielt etwa 10 Tausend Bände, darunter viele Handschriften. Während des Zweiten Weltkrieges wurde der Dom im Laufe zweier englischen Luftangriffe im August 1944 stark zerstört. Nur das Grabmal des weltbekannten Philosophen Immanuel Kant war gut erhalten geblieben. Seit den achtziger Jahren steht der Dom mit dem Grabmal von I. Kant unter Denkmalschutz.

Nicht weit vom Dom kann man das Gebäude der ehemaligen Königsberger Börse sehen. Sie wurde 1875 nach dem Entwurf des Architekten H. Müller auf 2 Tausend Pfählen errichtet. Zahlreiche Plastiken schmückten dieses Gebäude. Leider sind von diesen Plastiken nur zwei sitzende Löwen erhalten geblieben.

Unter den architektonischen Denkmälern der Stadt Kaliningrad sind die Stadttore zu nennen, die in der mittelalterlichen Zeit nicht nur als Einfahrten nach Königsberg, sondern auch als Festungsanlagen dienten. Im 19. Jahrhundert wurden sie modernisiert. Gegenwärtig sind sechs Stadttore erhalten geblieben – das Roßgarter Tor, das Königstor, das Sackheimer Tor, das Friedländer Tor, das Brandenburger Tor, das Friedrichsburgtor.

II. Sind folgende Aussagen falsch oder richtig?

1. Kaliningrad ist reich an alten Denkmälern aus verschiedenen Epochen.
2. Das Gebäude des Domes befindet sich nicht weit vom Dramentheater.
3. Der evangelische Gottesdienst begann im Dom seit 1333.
4. Die Wallenrodtsche Bibliothek hatte etwa 5 000 Bände.
5. Während des Krieges wurde der Dom stark zerstört.
6. Heute steht der Dom unter Denkmalschutz.
7. Die Stadttore dienten nur als Einfahrten nach Königsberg.
8. Nur sechs Stadttore sind heute erhalten geblieben.
9. Die Königsberger Börse wurde 1885 errichtet.
10. Das Gebäude der Börse wurde auf 1200 Pfählen errichtet.

11. Die Börse schmückten zahlreiche Plastiken. Leider sind sie nicht erhalten geblieben.

IV. Ergänzen Sie die Sätze.

1. Kaliningrad ist …. an alten Denkmälern.
2. Der Dom … … auf der Pregelinsel
3. Seit 1523 … im Dom der evangelische Gottesdienst
4. Im Turm des Domes … … die berühmte Wallenrodtsche Bibliothek
5. Sie … etwa 10 000 Bände.
6. Während des Zweiten Weltkrieges … der Dom stark …
7. Seit den 80-ger Jahren … das Gebäude des Domes unter Denkmalschutz
8. Die ersten Stadttore … nicht nur als Einfahrten, sondern auch als Festungsanlagen.
9. Nicht weit vom Dom … man das Gebäude der alten Börse …
10. Sie … nach dem Entwurf des Architekten Müller …
11. Das Gebäude …….. zahlreiche Plastiken.
12. Von diesen Plastiken … nur zwei sitzende Löwen …

V. Beantworten Sie folgende Fragen zum Text.

1. Welche alten architektonischen Denkmäler sind in Kaliningrad erhalten geblieben?
2. Wo befindet sich der Dom?
3. Wann entstand der Königsberger Dom?
4. Was für eine Bibliothek befand sich im Turm des Domes? Was können Sie über diese Bibliothek erzählen?
5. Was kann man heute im Dom besichtigen?
6. Wozu dienten die ersten Stadttore um Königsberg herum?
7. Wann wurden sie modernisiert?
8. Welche der Stadttore sind heutzutage erhalten geblieben
9. Welches Stadttor ist zum Stadtjubiläum restauriert worden?
10. Wessen Skulpturen schmücken dieses Tor?
11. Wo befindet sich das Gebäude der alten Börse?
12. Wann und von wem wurde die alte Börse errichtet?
13. Was ist ein besonderes Merkmal dieses Gebäudes?
14. Was ist heute in diesem Gebäude?

LESEVERSTEHEN 2

Lesen Sie den folgenden Text und machen Sie die Aufgaben I-IV zum Text.

Von der Steinzeit bis zur Entwicklung einer primitiven Arithmetik

Unsere ersten Vorstellungen von Zahl und Form reichen bis in ferne Zeiten, bis in die ältere Steinzeit (Paläolithikum) zurück. Während der hundert oder mehr Jahrtausende dieser Periode lebten die Menschen in Höhlen und unter Bedingungen, die sich nur wenig von denen der Tiere unterschieden. Ihre Anstrengungen galten hauptsächlich dem elementaren Bedürfnis, sich Nahrung zu verschaffen, wo immer dies möglich war. Sie verfertigten Waffen zum Jagen und Fischen, entwickelten die Sprache, um sich untereinander verständigen zu können, und in den späteren Epochen der älteren Steinzeit bereicherten sie ihr Leben durch schöpferische Kunstformen, Figuren und Malereien. Die Höhlenmalereien in Frankreich und Spanien (schätzungsweise vor etwa 15 000 Jahren entstanden) hatten vermutlich eine gewisse rituelle Bedeutung; auf jeden Fall verraten sie einen bemerkenswerten Formensinn.

Das Verständnis für Zahlen und räumliche Beziehungen machte so lange geringe Fortschritte, bis der Übergang vom bloßen Sammeln der Nahrung zu ihrer tatsächlichen Produktion, vom Jagen und Fischen zum Ackerbau, vollzogen wurde. Mit diesem grundlegenden Wandel, einer Umwälzung, in der sich die passive Einstellung des Menschen zur Natur in eine aktive verwandelte, treten wir in die jüngere Steinzeit (Neolithikum) ein.

Dieses große Ereignis in der Geschichte der Menschheit fand wahrscheinlich vor ungefähr 10 000 Jahren statt, als die Eisdecke, die vordem Europa und Asien bedeckte, geschmolzen war und Wäldern und Wüsten gemacht hatte. Die nomadenhaften Wanderungen zur Nahrungssuche hörten allmählich auf. In großem Umfange traten primitive Bauern an die Stelle der Fischer und Jäger. Diese Bauern, die so lange an einer Stelle blieben, wie dort der Boden noch fruchtbar war, begannen mit der Errichtung dauerhafter Wohnstätten; es entstanden Dörfer als Schutz gegen die Witterung und gegen räuberische Feinde. Viele derartige Siedlungen aus der jüngeren Steinzeit sind ausgegraben worden. Die Überreste zeigen, wie sich nach und nach einfache Formen des Handwerks, wie Töpferei, Zimmerhandwerk und Weberei entwickelten. Es gab Kornspeicher, so daß die Bewohner in der Lage waren, sich gegen den Winter und gegen schlechte Zeiten durch Vorräte zu sichern. Man buk Brot, braute Bier, und in den späteren Abschnitten der Jugendzeit wurden Kupfer und Bronze geschmolzen und verarbeitet. Erfindungen wurden gemacht, vor allem die Topfscheibe und das Wagenrad; Boote und Schuppen wurden verbessert. Alle diese bedeutsamen Neuerungen entstanden nur innerhalb bestimmter Bezirke und verbreiteten sich nicht immer in andere Gegenden. Die amerikanischen Indianer beispielsweise wussten bis zum Eindringen der Weißen nicht viel von der Verwendung des Wagenrades. Dessen ungeachtet wurde das Tempo der Vervollkommnung der Technik im Vergleich zur Altsteinzeit außerordentlich beschleunigt.

Zwischen den Dörfern entstand ein umfangreicher Handel, der sich so ausbreitete, dass Verbindungen über Hunderte von Meilen hinweg nachweisbar sind. Die Entdeckung der Technik

des Erschmelzens zuerst von Kupfer, dann von Bronze und der Herstellung von Werkzeugen und Waffen daraus trug viel zur Verstärkung dieser Handelstätigkeit bei. Dies wiederum trieb die weitere Ausbildung der Sprachen voran. Die Worte dieser Sprache drückten sehr konkrete Dinge und sehr wenige Abstraktionen aus, aber sie ließen doch schon einigen Raum für einfache Zahlenausdrücke und einige Beziehungen zwischen Formen. Viele australische, amerikanische und afrikanische Stämme befanden sich zu dieser Zeit ihrer ersten Berührung mit den Weißen in diesem Stadium; einige Stämme leben noch heute noch unter diesen Bedingungen, so dass es möglich ist, ihre Ausdrucksarten und – formen zu studieren.

I. Ergänzen Sie das passende Wort.

Ausbildung der Sprachen, Formensinn, Höhlenmalerei, Fortschritt, Töpferei, Zimmerhandwerk, Weberei, Sammeln, Zahlen, Beziehungen zwischen Formen, Ackerbau, Vorstellungen, Zahlen, räumliche Beziehungen, Nahrung, Schutz, Fischer, Jäger.

1) Der Mensch bekam die ersten ….über die Form und über die Zahl noch in der Steinzeit.
2) Das Leben des Höhlenmenschen wurde durch ….wesentlich bereichert.
3) … und … waren Hauptbedürfnisse der Höhlenmenschen.
4) Neben der rituellen Bedeutung verraten schöpferische Kunstformen, Figuren und Malereien auch einen …. .
5) Im Neolithikum begann der Übergang vom … zum … .
6) Das Verständnis für … und … … ermöglichte die aktive Einstellung des Menschen zur Natur.
7) An die Stelle der … und … traten primitive Bauern.
8) …, … und …. sind einfache Formen des Handwerks.
9) Die Verstärkung der Handelstätigkeit ermöglichte die … … .
10) Die ersten Worte drückten einfache … und einige …. … … .

II. Was ist richtig, was ist falsch?

1) Nach den architektonischen Funden kann man die Vorstellung von den Formen des Handwerks in der Jungendzeit bekommen.
2) Man konnte Kupfer und Bronze bereits in der älteren Steinzeit schmelzen.
3) Die wichtigen Erfindungen der Jugendzeit waren der Wagenrad und die Topfscheibe.
4) Die in Kornspeichern gelagerten Vorräte ließen die Bewohner gegen dem Hunger widerstehen.
5) Die Erfindungen, die in einer Gegend gemacht wurden, verbreiteten sich sofort in die anderen Gegenden.

6) Wenn wir das Tempo der technischen Entwicklung damals in verschiedenen Orten der Erde vergleichen, finden wir keinen großen Unterschied zwischen verschiedenen Gegenden.
7) Die Handelstätigkeit wurde durch die Entdeckung der Technik des Erschmelzens von Kupfer und Bronze verstärkt.
8) Die Verstärkung der Handelstätigkeit trug zur weiteren Ausbildung der Sprachen bei.
9) In der damaligen Sprache wurden ausführlich sowohl konkrete Dinge als auch Abstrakta dargestellt.

III. Ergänzen Sie die Lücken.

1) …, …, … sind die einfachen Formen des Handwerks.
2) Es gab auch … zur Lagerung von den Vorräten.
3) Die Bewohner waren in der …, sich gegen den Hunger zu sichern.
4) Mann konnte … backen und … brauen.
5) Damals … Kupfer und Bronze …. .
6) Bereits in der Jugendzeit … der Wagenrad und die Topfscheibe … .
7) Das Tempo der technischen Entwicklung … …. .
8) Man begann die Werkzeuge und Waffen …. .
9) In der Sprache der Jugendzeit … konkrete Dinge …. .
10) …. und einige …. wurden auch in der Sprache der Jugendzeit dargestellt.

IV. Beantworten Sie folgende Fragen zum Text.

1) Wann bekam der Mensch die ersten Vorstellungen von Zahl und Form?
2) Wie waren die Lebensbedingungen der Menschen in der älteren Steinzeit?
3) Was waren die Hauptbedürfnisse des Höhlenmenschen?
4) Was konnte der Mensch der älteren Zeit machen?
5) Was förderte das Verständnis für Zahlen und räumliche Beziehungen?
6) Womit begann der Eintritt der Menschheit in die jüngere Steinzeit?
7) Was wurde von den Bauern, die an Stelle der Fischer und Jäger traten, in erster Linie errichtet?
8) Welche Formen des Handwerks wurden damals entwickelt?
9) Was konnten die Bewohner in der jüngeren Steinzeit machen?
10) Welche Erfindungen wurden damals gemacht?
11) Wie war das Tempo der technischen Entwicklung im Vergleich zur Altsteinzeit?
12) Wozu trugen die gemachten Entdeckungen bei?
13) Was wurde neben der Handelstätigkeit entwickelt?
14) Was wurde in der Sprache der jüngeren Steinzeit ausgedrückt?

SCHREIBEN

Aufgabe 1

Äußern Sie sich schriftlich zum Thema "Meine Heimatstadt früher und heute". Berücksichtigen Sie dabei folgende Aspekte:

- was Sie über die Geschichte Ihrer Heimatstadt wissen;
- ob es in unserer Stadt nur alte architektonische Denkmäler gibt;
- welche Denkmäler Sie am besten finden;
- was für ein Denkmal unsere Stadt unbedingt haben sollte;

Aufgabe 2.

Äußern Sie sich schriftlich zum Thema "Wer hat bessere Chancen auf dem Arbeitsmarkt?". Berücksichtigen Sie dabei folgende Aspekte:

- wie groß heutzutage die Konkurrenz auf dem Arbeitsmarkt ist;
- welche Fachleute besonders nachgefragt werden;
- ob das erfolgreiche Abitur und gute Noten Erfolg im Beruf garantieren;
- was Sie von Ihrem zukünftigen Beruf erwarten?

TEXTWIEDERGABE

Lesen Sie den Text und geben Sie den Inhalt wieder.

Computer-Pionier Konrad Zuse: Seiner Zeit voraus

Konrad Zuse leistete in den Jahren 1935 bis 1945 Pionierarbeit bei der Entwicklung von Computern.

Die statischen Berechnungen per Hand langweilten Konrad Zuse. Konnte man diese mühsame Prozedur nicht automatisieren? Eine gute Idee. So machte sich der junge Bauingenieur im Berlin der 1930er-Jahre daran, eine Maschine zu bauen, die diese Routinearbeiten erledigen konnte, die noch mechanisch arbeitende Z 1, Vorläuferin des Computers. Eine raumgreifende Maschine mit Drähten und zahllosen Relais, ein Monstrum mit minimaler Leistung im Vergleich zu heutigen Laptops oder Smartphones. Jedoch nicht zur damaligen Zeit.

Zehn Jahre lang, von 1935 bis 1945, gehörte Zuse mit seinen Maschinen weltweit zu den Vordenkern - wie Alan Turing in Großbritannien oder John Atanasoff und Howard Aiken in den USA. Was Konrad Zuse (1910 - 1995) wie und unter welchen Bedingungen entwickelte, das ist Gegenstand einer Ausstellung, die der Informatikprofessor Raúl Rojas eigens zum Heidelberg Laureaten Forum konzipiert hat.

"Es gibt nicht den einen Erfinder des Computers. Es gibt nur viele Erfinder des Computers."

Eines gleich vorneweg: Auf die gerne geführte Diskussion, wer denn nun den allerersten, wirklich allerersten Computer erfunden hat, lässt sich Rojas gar nicht ein. "Es gibt nicht den einen Erfinder, es gibt nur viele Erfinder des Computers", sagt der gebürtige Mexikaner, der an der Freien Universität Berlin lehrt und dessen Fachgebiet künstliche Intelligenz ist. Neben dem Projekt des selbstfahrenden Autos gehört zu Rojas' Arbeit auch die Betreuung des Studententeams, das fußballspielende Roboter entwickelt. Die "FUmanoids" errangen mehrmals den ersten Platz beim Robo-Cup. Rojas wurde vergangenes Jahr vom Deutschen Hochschulverband zum Hochschullehrer des Jahres gewählt.

Für die Geschichte der Informatik interessiert sich der Wissenschaftler schon lange. "Ich habe mich aus historischem Interesse schon früh mit Zuse auseinandergesetzt, weil es immer wieder hieß, er sei der Vater des Computers. Aber ich habe damals nichts dazu gefunden", erläutert Rojas. Also hat er sich auf die Suche gemacht.

Interessant ist aus Sicht des Professors, dass weltweit zur gleichen Zeit, also in den späten 1930er- und frühen 1940er-Jahren, verschiedene Wissenschaftler unabhängig voneinander an ähnlichen Systemen gearbeitet haben. Innerhalb nur weniger Jahre entstanden der Atanasoff-Berry-Computer, Mark I von IBM und Harvard, Colossus in Großbritannien oder die Maschine ENIAC für die US-Armee - und alles während des Zweiten Weltkriegs.

Von Johanna Pfund

SPRECHEN

Situation 1: Könnten Sie bitte sagen, ob Sie sich für die Geschichte interessieren?

Situation 2: Was meinen Sie, gibt es in unserer Heimatstadt interessante Orte, die mit der Geschichte der Region verbunden sind?

Situation 3: Könnten Sie bitte über Ihr Institut erzählen?

Situation 4: Was meinen Sie, was sind die Voraussetzungen für erfolgreiche berufliche Tätigkeit?

Situation 5: Könnten Sie der Aussage zustimmen, dass digitale Massenmedien alle andere in der Zukunft verdrängen?

8.4. Планируемые уровни сформированности компетенций обучающихся и критерии оценивания

Уровни	Содержательное описание уровня	Основные признаки выделения уровня (этапы формирования компетенции, критерии оценки сформированности)	Пятибалльная шкала (академическая) оценка	Двухбалльная шакала, зачет	БРС, % освоения (рейтинговая оценка)

Повышенный	Творческая деятельность	*Включает нижестоящий уровень.* Умение самостоятельно принимать решение, решать проблему/задачу теоретического и прикладного характера на основе изученных методов, приемов, технологий	отлично	зачтено	86-100
Базовый	Применение знаний и умений в более широких контекстах учебной и профессиональной деятельности, нежели по образцу с большей степени самостоятельности и инициативы	*Включает нижестоящий уровень.* Способность собирать, систематизировать, анализировать и грамотно использовать информацию из самостоятельно найденных теоретических источников и иллюстрировать ими теоретические положения или обосновывать практику применения	хорошо		71-85
Удовлетворительный (достаточный)	Репродуктивная деятельность	Изложение в пределах задач курса теоретически и практически контролируемого материала	удовлетворительно		55-70
Недостаточный	Отсутствие признаков удовлетворительного уровня		неудовлетворительно	не зачтено	Менее 55

9. Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины.

Основная литература

1. Акиншина, И. Б. Немецкий язык : учебник / И.Б. Акиншина, Л.Н. Мирошниченко. — Москва : ИНФРА-М, 2020. — 247 с. — (Высшее образование: Бакалавриат). — DOI 10.12737/textbook_5d2437f6d0c8f9.98818547. - ISBN 978-5-16-013841-1. - Текст : электронный. - URL: https://znanium.com/catalog/product/1073457 (дата обращения: 29.03.2022). – Режим доступа: по подписке.

Дополнительная литература

1. Брандес, М. П. Стилистика текста. Немецкий язык. Теоретический курс: учебник / М. П. Брандес. - 5-е изд., испр. и перераб.. - Москва: Кн. дом "Университет", 2014. - 427 с. - Вар. загл.: Немецкий язык. Теоретический курс. - Библиогр.: с. 411-422. - ISBN 978-5-

98227-949-1: 430.10, 430.10, р. Имеются экземпляры в отделах: УБ(10)
2. Глотова, Ж. В. Немецкий язык как второй иностранный: учебно-практ. пособие/ Ж. В. Глотова ; Рос. гос. ун-т им. И. Канта. - Калининград: Изд-во РГУ им. И. Канта, 2008. - 214, [2] с. - Библиогр.: с.214 (6 назв.) . - ISBN 978-5-88874-862-6: 41.40, 41.40, р. Имеются экземпляры в отделах /There are copies in departments: всего /all 96: УБ(94), ч.з.N6(1), ИБО(1)

10. Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины (модуля).

- НЭБ Национальная электронная библиотека, диссертации и прочие издания
- eLIBRARY.RU Научная электронная библиотека, книги, статьи, тезисы докладов конференций
- Гребенников Электронная библиотека ИД журналы
- ЭБС Лань книги, журналы
- ЭБС Консультант студента
- ПРОСПЕКТ ЭБС
- ЭБС ZNANIUM.COM
- РГБ Информационное обслуживание по МБА
- БЕН РАН
- Электронно-библиотечная система (ЭБС) Кантитана (https://elib.kantiana.ru/)

11. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине.

Программное обеспечение обучения включает в себя:

- система электронного образовательного контента БФУ им. И. Канта – www.lms-3.kantiana.ru, обеспечивающую разработку и комплексное использование электронных образовательных ресурсов;
- серверное программное обеспечение, необходимое для функционирования сервера и связи с системой электронного обучения через Интернет;
- корпоративная платформа Microsoft Teams;
- установленное на рабочих местах студентов ПО: Microsoft Windows 7, Microsoft Office Standart 2010, антивирусное программное обеспечение Kaspersky Endpoint Security.

12. Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине.

Для проведения занятий лекционного типа, практических и семинарских занятий используются специальные помещения (учебные аудитории), оборудованные техническими средствами обучения – мультимедийной проекционной техникой. Для проведения занятий лекционного типа используются наборы демонстрационного оборудования.

Для проведения лабораторных работ, (практических занятий – при необходимости) используются специальные помещения (учебные аудитории), оснащенные специализированным лабораторным оборудованием: персональными компьютерами с возможностью выхода в интернет и с установленным программным обеспечением, заявленным в п.11.

Для проведения групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации используются специальные помещения (учебные аудитории), оборудованные специализированной мебелью (для обучающихся), меловой / маркерной доской.

Для организации самостоятельной работы обучающимся предоставляются помещения, оснащенные компьютерной техникой с возможностью подключения к сети «Интернет» и обеспечением доступа в электронную информационно-образовательную среду университета.

Для обучения инвалидов и лиц с ограниченными возможностями здоровья университетом могут быть представлены специализированные средства обучения, в том числе технические средства коллективного и индивидуального пользования.

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
федеральное государственное автономное образовательное учреждение высшего образования «Балтийский федеральный университет имени Иммануила Канта»
Институт физико-математических наук и информационных технологий

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

«БЕЗОПАСНОСТЬ ЖИЗНЕДЕЯТЕЛЬНОСТИ»

Шифр: 10.05.01
Специальность: «Компьютерная безопасность»
Специализация: «Математические методы защиты информации»
Квалификация (степень) выпускника: специалист по защите информации

Калининград
2022

Лист согласования

Составитель: старший преподаватель Института живых систем ***Судоплатов Константин Анатольевич***

Рабочая программа обсуждена и утверждена Ученым советом Института живых систем

Протокол №_____от «____»_____20__ г.

Председатель Ученого совета _____/О.О. Бабич/

Заместитель директора по учебной работе_____ /И.А. Ваколюк/

Рабочая программа одобрена на заседании Учебно-методического совета (УМС) ИФМНиИТ

Протокол № 1/22 от «01»февраля 2022 г.

Председатель УМС

Доцент, к.ф.-м.н. / А.А. Шпилевой

Руководитель ОПОП ВО / Е.П. Ставицкая

Содержание

1.Наименование дисциплины: «Безопасность жизнедеятельности».

Целью освоения дисциплины «Безопасность жизнедеятельности» является формирование представления о неразрывном единстве эффективной профессиональной деятельности с требованиями к безопасности и защищенности человека, формирование навыков безопасного поведения в повседневной жизни и в экстремальных условиях.

2. Перечень планируемых результатов обучения по дисциплине, соотнесенных с планируемыми результатами освоения образовательной программы

В результате изучения дисциплины студент должен овладеть следующими результатами обучения:

Код компетенции	Содержание компетенции	Результаты освоения образовательной программы (ИДК)	Перечень планируемых результатов обучения по дисциплине
УК-8	Способен создавать и поддерживать в повседневной жизни и в профессиональной деятельности и безопасные условия жизнедеятельности для сохранения природной среды, обеспечения устойчивого развития общества, в том числе при угрозе и возникновении чрезвычайных ситуаций и военных конфликтов	УК.8.1. Проводит идентификацию угроз (опасностей) природного и техногенного происхождения для жизнедеятельности человека и выбирает методы защиты человека и природной среды от угроз природного и техногенного характера. УК.8.2. Обеспечивает безопасные и /или комфортные условия труда на рабочем месте, в том числе с помощью средств защиты; выявляет и устраняет проблемы, связанные с нарушениями техники безопасности на рабочем месте. УК.8.3. Осуществляет действия по предотвращению возникновения чрезвычайных	**Знать:** • поражающие факторы стихийных бедствий, крупных производственных аварий и катастроф с выходом в атмосферу радиоактивных веществ (РВ) и аварийно-химически опасных веществ (АХОВ), современных средств поражения; • анатомо-физиологические последствия воздействия на человека травмирующих, вредных и опасных производственных факторов; • правовые, нормативно-технические и организационные основы «Безопасности жизнедеятельности»; **Уметь:** • проводить контроль параметров и уровня негативных воздействий на их соответствие нормативным требованиям; • эффективно применять средства защиты от негативных воздействий; • планировать мероприятия по защите производственного персонала и населения в чрезвычайных ситуациях и при необходимости принимать участие в проведении спасательных и других неотложных работ при ликвидации последствий чрезвычайных ситуаций. **Владеть:** • методами защиты в условиях чрезвычайных ситуаций; • методами прогнозирования чрезвычайных ситуаций и предотвращения их негативных

		ситуаций (природного и техногенного происхождения) на рабочем месте, в том числе с помощью средств защиты.	последствий; методами повышения стрессоустойчивос Способами управления эмоциями экстремальных ситуациях.

3. Место дисциплины в структуре образовательной программы

Дисциплина «Безопасность жизнедеятельности» относится к обязательной части Блока 1 Дисциплины (модули)в основной образовательной программе подготовки обучающихся.

4. Виды учебной работы по дисциплине

Виды учебной работы по дисциплине зафиксированы учебным планом основной профессиональной образовательной программы по указанному направлению и профилю, выражаются в академических часах. Часы контактной работы и самостоятельной работы обучающегося и часы, отводимые на процедуры контроля, могут различаться в учебных планах ОПОП по формам обучения. Объем контактной работы включает часы контактной аудиторной работы (лекции/практические занятия), контактной внеаудиторной работы (контроль самостоятельной работы), часы контактной работы в период аттестации. Контактная работа, в том числе может проводиться посредством электронной информационно-образовательной среды университета с использованием ресурсов сети Интернет и дистанционных технологий

5. Содержание дисциплины, структурированное по темам

Исходя из рамок, установленных учебным планом по трудоемкости и видам учебной работы по дисциплине, преподаватель самостоятельно выбирает тематику занятий по формам и количеству часов проведения контактной работы: лекции и иные учебные занятия, предусматривающие преимущественную передачу учебной информации преподавателем и (или) занятия семинарского типа (семинары, практические занятия, практикумы, и (или) групповые консультации, и (или) индивидуальную работу обучающихся с преподавателем. Рекомендуемая тематика занятий максимально полно реализуется в контактной работе с обучающимися очной формы обучения. В случае реализации образовательной программы в заочной / очно-заочной форме трудоемкость дисциплины сохраняется, однако объем учебного материала в значительной части осваивается обучающимися в форме самостоятельной работы. При этом требования к ожидаемым образовательным результатам обучающихся по данной дисциплине не зависят от формы реализации образовательной программы.

Содержание дисциплины

Тема № 1. Введение. Основные понятия, термины и определения.

Цель и содержание дисциплины, ее основные задачи, место и роль в подготовке специалиста. Основные понятия. Понятие опасности. Структура и состав опасности. Процесс идентификации опасности. Различные классификации опасностей. Аксиома о потенциальной опасности деятельности человека. Принципы достижения безопасности. Методы анализа опасности. Количественная характеристика опасности. Риск. Степень риска. Основные виды риска. Индивидуальный риск. Коллективный риск. Технический риск. Экологический риск. Социальный риск. Экономический риск. Потенциальный территориальный риск. Профессиональный риск. Оценка травматизма и профзаболеваний на производстве. Показатель сокращения продолжительности жизни. Концепция приемлемого риска и оценка безопасности профессиональной деятельности в РФ.

Тема № 2. Безопасность жизнедеятельности и природная среда. Экологические опасности. Классификация. Источники загрязнения среды обитания.

Экологическая безопасность. Критерии оценки качества окружающей среды, экологическое нормирование. Классификация нормативов качества природной среды. Основные принципы нормирования ОС. Государственные природоохранные органы РФ. Общественные природоохранные организации. Структура и краткая характеристика. Законодательство по охране природной среды РФ. Структура и основные документы. Система государственных стандартов «Охрана природы». Структура и описание. Экологическое законодательство и нормативные документы в области охраны окружающего воздуха. Основная характеристика загрязнителей атмосферного воздуха. Токсическая доза. Виды дозы. Виды ПДК для воздуха. Эффект суммации ПДК. ПДЭН. ВДК (ОБУВ). Определение и краткая характеристика понятий.

Комплексный индекс загрязнения КИЗА. Оценка рассеивающей способности атмосферы. Экологический мониторинг. Экологическая экспертиза. Принципы экологической экспертизы. Методы экологической экспертизы.

Ресурсные критерии оценки состояния поверхностных вод. Экологическое законодательство и нормативные документы в области водопользования, водосбережения и безопастности водных объектов. Нормирование качества воды.

Основная характеристика земельных ресурсов. Состав и структура почвы (почвенные фазы и горизонты). Минеральный состав почвы. Полидисперсность почвы. Гигиеническое и эпидемиологическое значение почвы. Антагонизм почвенной микрофлоры. Санитарная охрана почвы. Утилизация твердых и жидких бытовых отходов как экологический пример.

Тема № 3. Физиология и безопасность труда, обеспечение комфортных условий жизнедеятельности. Вредные и опасные произв. факторы

Структурно-функциональные системы восприятия и компенсации организмом человека изменений факторов среды обитания. Особенности структурно-функциональной организации человека. Естественные системы человека для зашиты от негативных воздействий. Характеристика нервной системы. Условные и безусловные рефлексы. Анализаторы, их строение, функции. Функциональные характеристики и роль во взаимодействии с внешней средой. Вегетативная нервная система, роль в защитных реакциях. Критические периоды в развитии ее отделов и суточном режиме.

Безопасность труда. Здоровье, определение. Виды здоровья. Профилактика нарушений состояния здоровья человека. Виды профилактики. Правовые и организационные основы производственной безопасности. Правовые и нормативно-методические документы по безопасности труда. Система государственных стандартов «Охрана труда». Структура и описание. Производственная среда. Классификация вредных и опасных производственных факторов в соответствие с ГОСТом 12.0.003-74. ПДУ вредного или опасного производственного фактора. Физиологические изменения в организме при физической и умственной нагрузке. Производственный травматизм.

Причины производственного травматизма. Профессиональные заболевания. Острые и хронические профзаболевания, их характеристика и примеры.

УФ-излучение. Характеристика, классификация. Бактерицидный и эритемный поток УФ. Виды доз облученности. Пороговая доза эритемной облученности: разовая и суточная. Биодоза. Производственные источники УФ. Биологическое действие УФ. Профилактические и защитные меры. СИЗ.

ИК-излучение. Характеристика, классификация. Биологическое действие. Основой закон термодинамики и расчет радиационных потерь организма.

Свет. Основные светотехнические характеристики и гигиенические требования по освещенности к рабочему месту. Основные зрительные функции. Механизм образования близорукости. Профилактика миопии.

Действие электрического тока на организм человека. Классификация видов тока по действию на человека. Факторы, влияющие на исход поражения электрическим током. Анализ опасности поражения электрическим током в различных электрических сетях (задание). Критерии электробезопасности и нормативные документы. Напряжение шага и прикосновения. Средства защиты, применяемые в электроустановках. Зануление и заземление принципиальная разница двух методов. Организация безопасности эксплуатации электроустановок. Оказание первой медицинской помощи при поражении электрическим током.

Шум. Гигиеническая классификация шума.

Нормирование контактного ультразвука. Вегетативно-сенсорная полиневропатия. Биологическое действие. Профилактика профессиональных заболеваний.

Электромагнитные волны. Источники электромагнитного излучения. Воздействие на организм человека. Нормирование электромагнитных полей. Напряженность ЭП и МП. Тепловой порог. Нормирование и профилактика профзаболеваний.

Механические колебания. Виды вибраций и их воздействие на человека. Нормирование вибраций. Вибрационная болезнь. Профилактика.

Лазерное излучение. Природа, источники и основные характеристики лазерного излучения, воздействие на организм человека и гигиеническое нормирование. Средства и методы защиты от лазерных излучений. Средства индивидуальной защиты (СИЗ).

Тема № 4. Принципы возникновения и классификация ЧС. Оценка, прогноз и мониторинг ЧС в РФ и за рубежом.

Общие сведения о чрезвычайных ситуациях, определение чрезвычайной ситуации, аварии, катастрофы, стихийного бедствия. Понятие аварийной и предаварийной ситуации, экстремальная ситуация, стадии чрезвычайной ситуации, классификация чрезвычайных ситуаций. Государственная концепция обеспечения безопасности в чрезвычайных ситуациях, разработка технических и организационных мероприятий, снижающих вероятность реализации поражающего потенциала современных технических систем. Подготовка объекта и обслуживающего персонала, служб МЧС и населения к действиям в условиях ЧС. Ликвидация последствий чрезвычайных ситуаций: разработка плана ликвидации последствий ЧС, спасательные и другие неотложные работы в очагах поражения: разведка очага поражения, локализация и тушение пожаров, розыск пострадавших, оказание пострадавшим первой помощи, санитарная обработка людей и техники, обеззараживание местности, неотложные аварийно-спасательные работы, спасательная техника и ее применение, определение материального ущерба, числа жертв и травм. Обучение персонала объекта и населения действиям в чрезвычайных ситуациях, психологическая подготовка персонала и населения к ЧС, структура МЧ Российской Федерации и их сил быстрого реагирования.

Организация систем мониторинга, цели и задачи мониторинга, виды мониторинга, экологический мониторинг, глобальный, национальный, региональный мониторинг.

Организация систем мониторинга в России, общегосударственная сеть наблюдения и контроля.

Тема № 5. ЧС природного и биолого-социального характера. Стихийные бедствия, виды, характеристика, основные повреждающие факторы. Действие человека при данных ЧС.

Классификация ЧС по источнику происхождения и масштабу. Классификация природных опасностей. Геологические. Гидрологические. Метеорологические. Природные пожары. Инфекции.

Наводнение, Половодье. Паводок, последствия. Классификация наводнений по признаку причин и по высоте подъема воды, ущербу и площади затопления. Защита и действие населения при угрозе и во время наводнения. Действия человека, оказавшегося в воде.

Ураганы, бури, смерчи, их происхождение и последствия. Меры по обеспечению безопасности населения. Шкала Бофорта. Шкала перевода из баллов в м/с.

Землетрясение. Основные параметры землетрясений, их последствия. Очаг, гипоцентр, эпицентр. Изосейсты. Характеристики землетрясений: Энергия (E), магнитуда (M), интенсивность (I), глубина гипоцентра (h). Шкала Рихтера. Шкала силы (интенсивности) землетрясений (Шкала MSK-64). Сейсмограммы. Фазы землетрясения, их отличия. Форшоки. Афтершоки. Правила безопасного поведения во время землетрясения.

Обвалы, оползни и сели, их происхождение, последствия и предотвращение данных событий. Классификация и профилактические мероприятия. Действия населения при угрозе схода оползней, селей и обвалов.

Лесные и торфяные пожары, их последствия и предотвращение. Классификация пожаров. Меры безопасности в зоне лесных и торфяных пожаров.

Извержение вулканов. Классификация и основные поражающие факторы. Снежные лавины. Классификация. Действие человека при данных стихийных бедствиях.

ЧС биолого-социального характера. Инфекционный процесс. Источник возбудителя инфекции. Эпидемический процесс. Эпидемический очаг инфекции. Эпидемия, пандемия. Старые. Новые и возвращающиеся инфекции, примеры. Механизм, факторы и основные пути передачи и проникновения возбудителя инфекции. Формы взаимодействия инфекционного агента с макроорганизмом. Острые и хронические формы. Реинфекция. Носительство инфекции. Субклиническая форма. Латентная форма. Медленная инфекция. Важнейшие свойства микроорганизмов, способных вызывать инфекционный процесс. Патогенность. Вирулентность. Адгезивность. Инвазивность. Токсигенность. Экзотоксины. Эндотоксины. Естественная классификация инфекционных болезней. Антропонозы и Зоонозы. Восприимчивый организм. Виды иммунитета. Естественный (специфический и неспецифический) и приобретенный. Иммунизация населения. Виды искусственного иммунитета.

Тема № 6. ЧС техногенного характера. Аварии, взрывы, пожары, и др. Основные повреждающие факторы. Действие человека при данных ЧС.

ЧС техногенного характера. Классификация. Аварии и катастрофы. Причины возникновения пожара в жилых и общественных зданиях. Меры пожарной безопасности в быту. Пожары и взрывы, их причины и возможные последствия. Горение. Возгорание. Воспламенение. Концентрационные пределы. Методы тушения пожаров. Огнегасительные вещества. Средства пожаротушения. Первичные, стационарные и передвижные. Зоны действия взрыва. Причины взрывов. Действие взрыва на человека (действие ударной волны). Правила безопасного поведения при пожаре и угрозе взрыва.

ХОО. Аварии на ХОО. АХОВ. Физико-химические свойства АХОВ влияющие на характер поражения. Поражающее действие АХОВ и пути проникновения в организм.

Классификация. Характеристики действия АХОВ: токсичность, дозы, токсодозы, концентрации. Клиническая классификация АХОВ. Развитие аварии при хранении АХОВ под давлением в виде жидкости. Зона химического заражения. Очаги поражения. Продолжительность заражения. Источники опасности при авариях на ХОО. Химическая обстановка и ее оценка. Задание метеоусловий. Количество АХОВ, обусловившее ЧС. Эквивалентное количество АХОВ. Коэффициенты, используемые при расчете эквивалентного количества АХОВ. Определение эквивалентного количества вещества в первичном облаке. Определение эквивалентного количества вещества во вторичном облаке и времени испарения. Расчет глубины зоны заражения при аварии на ХОО. Определение площади зоны заражения. Определение времени подхода зараженного воздуха к заданному объекту. Определение продолжительности заражения. Защитные мероприятия на химически опасных объектах. Средства индивидуальной защиты. Способы защиты от АХОВ. Медицинская помощь пострадавшим при авариях па ХОО. Свойства аммиака и хлора, учитываемые при оказании первой помощи. Способы и средства ликвидации последствий аварий на ХОО.

Радиационная безопасность. Виды и основная характеристика ионизирующих излучений. Корпускулярное и электромагнитное излучение. Источники радиационной опасности, естественные и искусственные. Радиоактивный распад. Изотопы. Радионуклиды. Период полураспада. Эффективный период полураспада. Характеристики радиационного излучения. Активность радионуклидов, виды активности. Доза излучения. Виды доз. Общая характеристика. Мощность доз. Коллективная эффективная эквивалентная доза. Полная коллективная эффективная эквивалентная доза. Понятие «уровень радиации» и «уровень (плотность) загрязнения» радионуклидом. Максимальные потенциальные эффективные и эквивалентные дозы, их МПД. Допустимая мощность годовой потенциальной дозы (ДМПД). Радиационная защита. РОО и зоны безопасности. Международная шкала тяжести событий на АС. Аварии на РОО. Классификация аварий. Зонирование территории при авариях на РОО. ЗРА и ЗРК. Типовые режимы радиационной защиты при авариях на АС. Эвакуация населения, ее предназначение, порядок проведения мероприятий при эвакуации.

Тема № 7. ЧС военного времени. Оружие массового поражения. Современная классификация. Действие населения при применении ОМП.

Чрезвычайные ситуации военного времени. Ядерное оружие, его поражающие факторы, зоны разрушения, степени разрушения зданий, сооружений, технических и транспортных средств. Возникновение и развитие пожаров в городах и на объектах экономики. Зоны радиоактивного заражения при наземных ядерных взрывах, воздействие радиации и электромагнитного импульса на технические средства. Возможные поражения людей при ядерном взрыве. Планируемые спасательные и другие неотложные работы в зонах очага ядерного поражения. Химическое оружие. Классификация и токсикологические характеристики отравляющих веществ. Зоны заражения и очаги поражения. Обычные средства поражения, их характеристики, профилактика последствий применения обычных средств поражения. Биологическое оружие. Основные характеристики и защита населения при использовании данного типа оружия МП.

Тема № 8. Защита населения в чрезвычайных ситуациях. Единая государственная система предупреждения и ликвидации чрезвычайных ситуациях (РСЧС). Структура. Задачи. ГО РФ и различных государств. МЧС РФ. Эвакуация. Особенности, задачи.

Единая государственная система предупреждения и ликвидации чрезвычайных ситуациях (РСЧС): задачи и структура. Территориальные подсистемы РСЧС. Функциональные подсистемы РСЧС. Уровни управления и состав органов по уровням. Координирующие органы, органы управления по делам ГО и ЧС, органы повседневного

управления. Гражданская оборона, ее место в системе общегосударственных мероприятий гражданской защиты. Структура ГО в РФ. Задачи ГО, руководство ГО, органы управления ГО, силы ГО, гражданские организации ГО. Структура ГО на промышленном объекте. Планирование мероприятий по гражданской обороне на объектах. Организация защиты в мирное и военное время, способы защиты, защитные сооружения, их классификация. Оборудование убежищ. Быстровозводимые убежища. Простейшие укрытия. Противорадиационные укрытия. Укрытие в приспособленных и специальных сооружениях. Организация укрытия населения в чрезвычайных ситуациях. Особенности и организация эвакуации из зон чрезвычайных ситуаций. Мероприятия медицинской защиты. Средства индивидуальной защиты и порядок их использования.

Тема № 9. Терроризм как реальная угроза безопасности в современном обществе

Причины терроризма. Социально-психологические характеристики террориста. Международный терроризм. Борьба с терроризмом. Правила поведения для заложников.

Тема № 10. Медико-биологические и психологические основы безопасности жизнедеятельности

Оказание первой медицинской помощи утопающему. Искусственная вентиляция легких. Ушиб. Признаки ушиба. Растяжения. Признаки растяжения. Вывих. Признаки. Перелом. Виды переломов. Признаки. Наиболее частые осложнения переломов. Первая медицинская помощь при растяжениях, переломах и вывихах. Иммобилизация и средства её достижения. Оказание первой медицинской помощи при термических и химических ожогах. Классификация ожогов. Оценка площади ожога. Ожоговая болезнь. Стадии. Ожоговый шок. Острая ожоговая токсемия, ожоговая септикотоксемия, реконвалесценция. Первая медицинская помощь при отравлении СДЯВ и ОВ. Классификация. Действие на организм человека. Первая медицинская помощь. Сердечно-сосудистая недостаточность – обморок, коллапс, шок. Оказание первой медицинской и доврачебной помощи. Кома. Первая медицинская и доврачебная помощь. Виды, классификация, диагностика и оказание первой помощи при кровотечениях. Кровопотеря. Наложение жгута. Раны. Правила и приемы наложения повязок. Первая медицинская помощь при отморожении. Физиологические изменения и признаки отморожения. Классификация поражений. Действие электрического тока на человека. Термическое. Электролитическое. Биологическое. Электрический ожог. Классификация и виды ожогов. Электрические знаки. Электрический удар. Классификация. Возможные пути тока через тело человека. Первая медицинская помощь при поражении электрическим током. Первая медицинская помощь при тепловом и солнечном ударах, признаки поражения. Понятие и определения здоровья. Общебиологическое здоровье. Популяционное. Индивидуальное. Факторы, влияющие на здоровье людей. Первичная, вторичная и третичная профилактика нарушений состояния здоровья.

Психологическая устойчивость в чрезвычайных ситуациях.

6. Рекомендуемая тематика учебных занятий в форме контактной работы

Рекомендуемая тематика учебных занятий *лекционного* типа (предусматривающих преимущественную передачу учебной информации преподавателями)

Тема № 1. Введение. Основные понятия, термины и определения.

Тема № 2. Безопасность жизнедеятельности и природная среда. Экологические опасности. Классификация. Источники загрязнения среды обитания.

Тема № 3. Физиология и безопасность труда, обеспечение комфортных условий жизнедеятельности. Вредные и опасные произв. факторы

Тема № 4. Принципы возникновения и классификация ЧС. Оценка, прогноз и мониторинг ЧС в РФ и за рубежом.

Тема № 5. ЧС природного и биолого-социального характера. Стихийные бедствия, виды, характеристика, основные повреждающие факторы. Действие человека при данных ЧС.

Тема № 6. ЧС техногенного характера. Аварии, взрывы, пожары, и др. Основные повреждающие факторы. Действие человека при данных ЧС.

Тема № 7. ЧС военного времени. Оружие массового поражения. Современная классификация. Действие населения при применении ОМП.

Тема № 8. Защита населения в чрезвычайных ситуациях. Единая государственная система предупреждения и ликвидации чрезвычайных ситуациях (РСЧС). Структура. Задачи. ГО РФ и различных государств. МЧС РФ. Эвакуация. Особенности, задачи.

Тема № 9. Терроризм как реальная угроза безопасности в современном обществе

Тема № 10. Медико-биологические и психологические основы безопасности жизнедеятельности

Тематика практических занятий

№ п/п	Темы практических занятий
1	Чрезвычайные ситуации природного характера
2	Чрезвычайные ситуации техногенного характера и защита от них
3	Принципы обеспечения безопасности населения и территорий в ЧС мирного и военного времени
4	Санитарно-гигиенические и противоэпидемические мероприятия в ЧС
5	Медицинская характеристика состояний, требующих оказания первой медицинской помощи, и методы оказания первой медицинской помощи
6	Чрезвычайные ситуации (ЧС) социального характера
7	Сущность и содержание информационной безопасности
8	Органы системы МЧС России в системе органов исполнительной власти
9	Терроризм как реальная угроза безопасности в современном обществе

Содержание *практических* занятий

Чрезвычайные ситуации природного характера	
1	Наводнение. Половодье. Паводок, последствия. Классификация наводнений по признаку причин и по высоте подъема воды, ущербу и площади затопления. Защита

	и действие населения при угрозе и во время наводнения. Действия человека, оказавшегося в воде.
2	Землетрясения, основные параметры землетрясений, их последствия. Гипоцентр, эпицентр. Магнитуда. Энергия. Интенсивность. Глубина гипоцентра. Шкала MSK-64, шкала Рихтера. Правила безопасного поведения во время землетрясения.
3	Ураганы, бури, смерчи, тайфуны их происхождение и последствия. Меры по обеспечению безопасности населения. Шкала Бофорта. Цунами. Причины возникновения. Характеристика природного явления. Действие человека при данном стихийном бедствии.
4	Извержение вулканов. Снежные лавины. Обвалы, оползни и сели, их происхождение, последствия и предотвращение данных событий. Действия населения.
Чрезвычайные ситуации техногенного характера и защита от них характера	
5	Пожары, их причины и возможные последствия. Основные поражающие факторы. Горение. Возгорание. Воспламенение. Методы тушения пожаров. Классификация средств. Огнегасительные вещества. Средства пожаротушения. Классификация. Первичные, стационарные и передвижные.
6	Меры пожарной безопасности в быту. Поведение человека в данной ситуации. Первая медицинская и доврачебная помощь. Лесные и торфяные пожары, их последствия и предотвращение. Классификация пожаров. Меры безопасности в зоне лесных и торфяных пожаров.
7	Взрывы и их последствия. Зоны действия взрыва. Действие взрыва на человека (действие ударной волны) и здания. Концентрационные пределы. Правила безопасного поведения при угрозе взрыва. Поведение человека в данной ситуации. Первая медицинская и доврачебная помощь.
8	Химически опасные объекты производства, возможные последствия при авариях на химически опасных объектах, правила поведения. Хронические и острые интоксикации. Первая медицинская и доврачебная помощь при отравлении СДЯВ (сильнодействующими ядовитыми веществами) и ОВ (отравляющими веществами). Поведение человека в данной ситуации.
9	Аварии на радиационно-опасных объектах, возможные последствия облучения людей, ОЛБ (острая лучевая болезнь). Профилактика лучевых поражений. Первая медицинская и доврачебная помощь. Виды ионизирующих излучений, их основные характеристики. Правила поведения при радиационных авариях.
10	Транспортные аварии и их последствия. Безопасное поведение человека. Оказание первой медицинской помощи. Действие пассажиров при аварии на железнодорожном транспорте. Аварийные и опасные ситуации в метрополитене. Безопасное поведение человека. Оказание первой медицинской помощи.
11	Опасные и аварийные ситуации на воздушном и водном транспорте. Действие пассажиров. Оказание первой медицинской помощи.
Принципы обеспечения безопасности населения и территорий в ЧС мирного и военного времени	
12	Ядерное оружие, его боевые свойства и поражающие факторы. Классификация поражающих факторов ядерного взрыва и защита от их действия человека. Виды ядерных взрывов. След от радиоактивного облака. Зоны поражения. Средства индивидуальной и коллективной защиты.
13	Химическое оружие. Классификация по характеру токсического действия ОВ. Нервнопаралитические. Кожно-нарывные. Удушающие. Общеядовитые. Психохимические. Раздражающие. Классификация отравляющих веществ в зависимости от характера поражающего действия. Защита. Средства индивидуальной и коллективной защиты.

14	Бактериологическое оружие. Защита от поражающих факторов. Способы применения. Эвакуация населения при ЧС, ее предназначение, порядок проведения мероприятий при эвакуации.
15	Современные и обычные средства поражения и защита от них. Классификация. Осколочные. Фугасные. Кумулятивные. Зажигательные. Объемного взрыва. Высокоточное оружие. Разведывательно-ударные комплексы. Управляемые авиационные бомбы. Средства индивидуальной и коллективной защиты.
16	Организация инженерной защиты населения от поражающих факторов. Виды убежищ. Размещение и правила поведения людей в защитном сооружении. Средства индивидуальной защиты (СИЗ). СИЗ кожи. Медицинские средства индивидуальной защиты. Аптечка индивидуальная АИ-2. Индивидуальные противохимические пакеты. Организация и проведение санитарной обработки людей.
Санитарно-гигиенические и противоэпидемические мероприятия в ЧС	
17	Иммунный статус человека. Органы иммунной системы. Понятия иммунная система и антигены. Вакцины, сыворотки. Иммунодефициты первичные и вторичные. Классификация. ВИЧ-инфекция как модель вторичного иммунодефицита. Профилактика СПИДа. Первая помощь.
18	Заболевания бронхолегочной системы (бронхит, плеврит, пневмония, рак легкого, пневмоторакс, пневмокониозы, эмфизема легких). Наблюдение и уход за больными с заболеваниями органов дыхания.
19	Туберкулез. Классификация. Клиническая характеристика. Вакцина БЦЖ Значение реакции Манту. Наблюдение и уход за больными.
20	Алкоголь и его влияние на физическое и психическое здоровье человека. Профилактика алкогольной зависимости. Курение и его влияние на здоровье курящего и окружающих (пассивное курение). Способы профилактики и отказа от курения.
21	Наркотические вещества и их влияние на физическое и психическое здоровье человека. Профилактика наркотической зависимости.
22	Функциональная анатомия органа зрения. Дальнозоркость и близорукость. Травмы глаза. Первая помощь. Профилактика заболеваний. Функциональная анатомия органа слуха. Основные нарушения. Профилактика.
23	Клинико-эпидемиологическая характеристика группы кишечных инфекций. Холера. Брюшной тиф. Сальмонеллез. Ботулизм. Дизентерия. Полиомиелит. Болезнь Боткина. Профилактика и оказание первой медпомощи.
24	Клинико-эпидемиологическая характеристика группы инфекций дыхательных путей. Грипп. Натуральная оспа. Эпидемический менингит. Эпидемический паротит (свинка). Энцефалиты вирусной этиологии. Профилактика и оказание первой медпомощи.
25	Клинико-эпидемиологическая характеристика группы инфекций дыхательных путей. Воспаление легких (пневмония). Ангина. Скарлатина. Дифтерия. Корь. Коклюш. ОРВИ. Профилактика и оказание первой медпомощи.
26	Клинико-эпидемиологическая характеристика группы кровяных инфекций. Сыпной тиф. Клещевой энцефалит, малярия. Профилактика и оказание первой медпомощи.
27	Детские инфекционные болезни. Корь и краснуха. Профилактика и оказание первой медпомощи. Профилактика и оказание первой медпомощи.
28	Клинико-эпидемиологическая характеристика группы инфекций наружных покровов. Бешенство. Столбняк. Сибирская язва. Ящур. Профилактика и оказание первой медпомощи.

Медицинская характеристика состояний, требующих оказания первой медицинской помощи, и методы оказания первой медицинской помощи	
29	Основные заболевания системы крови (анемия, лейкоз, лимфолейкоз, метгемоглобинемия). Первая помощь. Механизмы системы свертывания крови. Гемофилия. Первая помощь.
30	Раны. Виды ран. Повязка. Перевязка. Правила наложения и перевязки. Первая помощь при кровотечениях. Виды кровотечений. Методы остановки кровотечений. Наложение кровоостанавливающего жгута.
31	Сосудистая недостаточность. Обморок. Коллапс. Кома, виды комы. Атеросклероз. Вегетативно-сосудистая дистония. Артериальная гипертензия. Гипертонический криз. Диагностика. Характеристика и первая медицинская помощь при данных ситуациях.
32	Ишемическая болезнь сердца. Инфаркт миокарда. Стенокардия. Аритмия сердца Диагностика. Ушибы сердца. Диагностика. Первая помощь. Терминальное состояние. Агония. Клиническая и биологическая смерть.
33	Тепловой удар. Солнечный удар. Термические ожоги и ожоговая болезнь. Первая медицинская и доврачебная помощь.
34	Поражение электрическим током. Первая медицинская и доврачебная помощь. Действие электрического тока на человека. Термическое. Электролитическое. Биологическое. Электрический ожог. Классификация и виды ожогов. Электрические знаки. Электрический удар. Классификация. Возможные пути тока через тело человека. Первая медицинская помощь при поражении электрическим током.
35	Химические ожоги. Отморожение и общее замерзание. Первая медицинская и доврачебная помощь. Укусы ядовитых змей и насекомых. Первая медицинская и доврачебная помощь.
36	Острые и хронические отравления. Принципы оказания первой медицинской помощи при различных отравлениях.
37	Ушибы, растяжения и разрывы мягких тканей, переломы и вывихи. Первая медицинская и доврачебная помощь. Порядок наложения шины. Первая помощь. Инородные предметы в дыхательных путях. Острая дыхательная недостаточность. Наблюдение и уход за больными с заболеваниями органов дыхания. Оказание первой медицинской помощи при утоплении.
38	Понятие шока. Травматический шок. Фазы и степени шока. Первая медицинская и доврачебная помощь. Синдром длительного сдавливания. Клиническая картина. Первая медицинская и доврачебная помощь. Доврачебная реанимационная помощь. Искусственное дыхание. Непрямой массаж сердца. Методика. Прямой массаж сердца.
Чрезвычайные ситуации (ЧС) социального характера	
39	Массовые беспорядки их сущность и характер проявления. Город как среда повышенной опасности. Толпа, виды толпы. Паника. Массовые погромы. Массовые зрелища и праздники. Безопасность в толпе. Процесс воздействия субъекта социальной ЧС на Россию и ее регионы.
40	Чрезвычайные ситуации (ЧС) криминального характера и защита от них. Кража. Мошенничество. Правила поведения в случаях посягательства на жизнь и здоровье (нападение на улице, приставания пьяного, изнасилование, нападение в автомобиле, опасность во время ночной остановки). Предупреждение криминальных посягательств в отношении детей.
41	Необходимая самооборона в криминальных ситуациях (правовые основы

	самообороны, основные правила самообороны, средства самозащиты и их использование).
Сущность и содержание информационной безопасности	
42	Формы методы и способы обеспечения информационной безопасности. Основы защиты деловой информации и сведений, составляющих государственную и служебную коммерческую тайны. Методы и средства защиты электронной информации. Информационные технологии и здоровье. Сотовая радиотелефонная связь.
Экономическая безопасность социально-экономических систем	
43	Система обеспечения экономической безопасности личности. Государственная стратегия в сфере обеспечения экономической безопасности личности: сущность и комплекс мер по ее обеспечению. Основные направления обеспечения экономической безопасности личности: кредитование физических лиц, инвестирование, страхование человека и имущества, защита авторских прав, защита прав потребителей.
Биологические опасности	
44	Микроорганизмы. Виды патогенных микробов. Рост и размножение микроорганизмов. Бактериологическое нормирование. Грибы, растения и животные, представляющие опасность для человека.
Техногенные опасности	
45	Ионизирующие излучения (ИИ). Физика радиоактивности. Закон радиоактивного распада. Биологическое действие ионизирующих излучений. Дозиметрические величины и единицы их измерений. Источники излучения. Измерение ИИ. Нормирование радиационной безопасности. Защита от излучений.
Экологические опасности	
46	Состояние среды обитания. Критерии оценки качества окружающей среды. Экологическое нормирование. Источники экологических опасностей (тяжелые металлы, пестициды, диоксины, соединения серы, фосфора и азота, фреоны). Воздух как фактор среды обитания. Критерии оценки состояния загрязнения атмосферы. Комплексный индекс загрязнения атмосферы (КИЗА).
47	Вода как фактор среды обитания. Физиологическое и гигиеническое значение воды. Заболевания, связанные с изменением солевого и микроэлементного состояния воды. Вода как путь передачи инфекционных заболеваний. Влияние хозяйственно-бытовой и производственной деятельности человека н свойства природных вод. Показатели качества воды. Нормирование и нормативные акты в области охраны водной среды. Защита воды. Классификация водоемов и ПДК.
48	Государственные и общественные природоохранные организации. Стратегия экологического развития.
49	Почва как фактор среды обитания. Роль почвы в передаче инфекционных заболеваний. Процессы самоочищения почвы. Санитарная охрана почвы.
Органы системы МЧС России в системе органов исполнительной власти	
50	**МЧС**. Роль, место и задачи «**Министерства РФ по делам гражданской обороны, чрезвычайным ситуациям и ликвидации последствий стихийных бедствий**» (МЧС) в современных условиях. Общая организация МЧС РФ. **Единая государственная система предупреждения и ликвидации**

	чрезвычайных ситуаций (РСЧС). Задачи и структура. Территориальные подсистемы РСЧС, уровни управления и состав органов по уровням. **Гражданская оборона (ГО)**, ее место в системе общегосударственных мероприятий гражданской защиты. Структура, состав и задачи ГО РФ. **Государственная инспекция по маломерным судам (ГИМС)**. Главные задачи и структура ГИМС. **Государственная противопожарная служба (ГПС)**. Главные задачи и структура.

Практические занятия проводятся в интерактивной форме или в виде семинаров, где обсуждаются ключевые и наиболее сложные вопросы. Работа на практических занятиях оценивается преподавателем по итогам подготовки и выполнения студентами практических заданий, активности работы в группе и самостоятельной работе.

Пропуск практических занятий предполагает отработку по пропущенным темам (подготовка письменной работы, с ответами на вопросы, выносимые на семинар).

Неотработанный (до начала экзаменационной сессии) пропуск более 50% практических занятий по курсу является основанием для не допуска к итоговой аттестации по дисциплине.

Требования к самостоятельной работе обучающихся

Работа с лекционным материалом, предусматривающая проработку конспекта лекций и учебной литературы, по всем темам из п. 6 настоящей рабочей программы.

Руководствуясь положениями статьи 47 и статьи 48 Федерального закона от 29 декабря 2012 г. N 273-ФЗ «Об образовании в Российской Федерации» научно-педагогические работники и иные лица, привлекаемые университетом к реализации данной образовательной программы, пользуются предоставленными академическими правами и свободами в части свободы преподавания, свободы от вмешательства в профессиональную деятельность; свободы выбора и использования педагогически обоснованных форм, средств, методов обучения и воспитания; права на творческую инициативу, разработку и применение авторских программ и методов обучения и воспитания в пределах реализуемой образовательной программы и отдельной дисциплины.

Исходя из рамок, установленных учебным планом по трудоемкости и видам учебной работы по дисциплине, преподаватель самостоятельно выбирает тематику занятий по формам и количеству часов проведения контактной работы: лекции и иные учебные занятия, предусматривающие преимущественную передачу учебной информации преподавателем и (или) занятия семинарского типа (семинары, практические занятия, практикумы), и (или) групповые консультации, и (или) индивидуальную работу обучающихся с преподавателем.

Рекомендуемая тематика занятий максимально полно реализуется в контактной работе с обучающимися очной формы обучения. В случае реализации образовательной программы в заочной / очно-заочной форме трудоемкость дисциплины сохраняется, однако объем учебного материала в значительной части осваивается обучающимися в форме самостоятельной работы. При этом требования к ожидаемым образовательным результатам обучающихся по данной дисциплине не зависят от формы реализации образовательной программы.

7. Методические рекомендации по видам занятий

Лекционные занятия.

В ходе лекционных занятий обучающимся рекомендуется выполнять следующие действия. Вести конспектирование учебного материала. Обращать внимание на категории, формулировки, раскрывающие содержание тех или иных явлений и процессов, научные выводы и практические рекомендации по их применению. Задавать преподавателю уточняющие вопросы с целью уяснения теоретических положений, разрешения спорных ситуаций.

Желательно оставить в рабочих конспектах поля, на которых во внеаудиторное время можно сделать пометки из рекомендованной литературы, дополняющие материал прослушанной лекции, а также подчеркивающие особую важность тех или иных теоретических положений.

Практические и семинарские занятия.

На практических и семинарских занятиях в зависимости от темы занятия выполняется поиск информации по решению проблем, практические упражнения, контрольные работы, выработка индивидуальных или групповых решений, итоговое обсуждение с обменом знаниями, участие в круглых столах, разбор конкретных ситуаций, командная работа, представление портфолио и т.п.

Самостоятельная работа.

Самостоятельная работа осуществляется в виде изучения литературы, эмпирических данных по публикациям и конкретных ситуаций из практики, подготовке индивидуальных работ, работа с лекционным материалом, самостоятельное изучение отдельных тем дисциплины; поиск и обзор литературы и электронных источников; чтение и изучение учебника и учебных пособий.

Тематика самостоятельный работ:

№ п/п	Наименование темы	Тематика самостоятельных работ
1	Тема № 1. Введение. Основные понятия, термины и определения	Методы определения риска. Управление риском. Анализ риска. Качественные методы анализа опасностей и риска. Причинно-следственный анализ.
2	Тема № 2 Безопасность жизнедеятельности и природная среда. Экологические опасности. Классификация. Источники загрязнения среды обитания	Основная характеристика земельных ресурсов. Состав и структура почвы (почвенные фазы и горизонты). Минеральный состав почвы. Гигиеническое и эпидемиологическое значение почвы. Санитарная охрана почвы. Оценочная шкала опасности загрязнения почв. Утилизация твердых и жидких бытовых отходов как экологический пример.
3	Тема № 3. Физиология и безопасность труда, обеспечение комфортных условий жизнедеятельности. Вредные и опасные произв. факторы	Структурно-функциональные системы восприятия и компенсации организмом человека изменений факторов среды обитания. Естественные системы человека для зашиты от негативных воздействий. Характеристика нервной системы. Условные и безусловные рефлексы. Анализаторы, их строение, функции. Вегетативная нервная система, роль в защитных реакциях.

4	Тема № 4. Принципы возникновения и классификация ЧС. Оценка, прогноз и мониторинг ЧС в РФ и за рубежом	Организация систем мониторинга, цели и задачи мониторинга, виды мониторинга, экологический мониторинг, глобальный, национальный, региональный мониторинг. Организация систем мониторинга в России, общегосударственная сеть наблюдения и контроля.
5	Тема № 5. ЧС природного и биолого-социального характера. Стихийные бедствия, виды, характеристика, основные повреждающие факторы. Действие человека при данных ЧС	ЧС биолого-социального характера. Инфекционный процесс. Источник возбудителя инфекции. Эпидемический процесс. Эпидемический очаг инфекции. Эпидемия, пандемия. Старые. Новые и возвращающиеся инфекции, примеры. Механизм, факторы и основные пути передачи и проникновения возбудителя инфекции. Формы взаимодействия инфекционного агента с макроорганизмом.
6	Тема № 6. ЧС техногенного характера. Аварии, взрывы, пожары, и др. Основные повреждающие факторы. Действие человека при данных ЧС	ЧС техногенного характера. Классификация. Аварии и катастрофы. Причины возникновения пожара в жилых и общественных зданиях. Меры пожарной безопасности в быту. Пожары и взрывы, их причины и возможные последствия. Горение. Возгорание. Воспламенение. Концентрационные пределы. Методы тушения пожаров.
7	Тема № 7. ЧС военного времени. Оружие массового поражения. Современная классификация. Действие населения при применении ОМП	Биологическое оружие. Основные характеристики и защита населения при использовании данного типа оружия.
8	Тема № 8. Защита населения в чрезвычайных ситуациях. Единая государственная система предупреждения и ликвидации чрезвычайных ситуациях (РСЧС). Структура. Задачи. ГО РФ и различных государств. МЧС РФ. Эвакуация. Особенности, задачи	Единая государственная система предупреждения и ликвидации чрезвычайных ситуациях (РСЧС): задачи и структура. Территориальные подсистемы РСЧС. Функциональные подсистемы РСЧС. Уровни управления и состав органов по уровням.
9	Тема № 9. Управление безопасностью жизнедеятельности. Противодействие терроризму и экстремизму.	Вопросы безопасности жизнедеятельности в законах и подзаконных актах. Охрана окружающей среды. Нормативно-техническая документация по охране окружающей среды. Международное сотрудничество по охране окружающей среды. Мониторинг окружающей среды в РФ и за рубежом. Правила контроля состояния окружающей среды. Законодательство о труде. Противодействие терроризму и экстремизму.
10	Тема № 10. Медико-биологические и	Психологическая устойчивость в чрезвычайных ситуациях. Норма

	психологические основы безопасности жизнедеятельности	психологического здоровья, психология риска, регуляция психологического состояния, психологическое воздействие на людей обстановки чрезвычайной ситуации, идентифицирование личности, психологический портрет, социально-психологические отклонения в чрезвычайных ситуациях, дезадаптированность личности, посттравматические расстройства.

8. Фонд оценочных средств

8.1. Перечень компетенций с указанием этапов их формирования в процессе освоения образовательной программы в рамках учебной дисциплины

Основными этапами формирования указанных компетенций при изучении обучающимися дисциплины являются последовательное изучение содержательно связанных между собой тем учебных занятий. Изучение каждой темы предполагает овладение обучающимися необходимыми компетенциями. Результат аттестации обучающихся на различных этапах формирования компетенций показывает уровень освоения компетенций.

Контролируемые модули, разделы (темы) дисциплины	**Индекс контролируемой компетенции (или её части)**	**Оценочные средства по этапам формирования компетенций (текущий контроль по дисциплине)**
Тема № 1. Введение. Основные понятия, термины и определения	УК.8.1	Опрос, тестирование
Тема № 2 Безопасность жизнедеятельности и природная среда. Экологические опасности. Классификация. Источники загрязнения среды обитания	УК.8.1 УК.8.2 УК.8.3	Опрос, тестирование
Тема № 3. Физиология и безопасность труда, обеспечение комфортных условий жизнедеятельности. Вредные и опасные произв. факторы	УК.8.1 УК.8.2 УК.8.3	Опрос, тестирование
Тема № 4. Принципы возникновения и классификация ЧС. Оценка, прогноз и мониторинг ЧС в РФ и за рубежом	УК.8.1 УК.8.3	Опрос, тестирование

Тема № 5. ЧС природного и биолого-социального характера. Стихийные бедствия, виды, характеристика, основные повреждающие факторы. Действие человека при данных ЧС	УК.8.1 УК.8.3	Опрос, тестирование
Тема № 6. ЧС техногенного характера. Аварии, взрывы, пожары, и др. Основные повреждающие факторы. Действие человека при данных ЧС	УК.8.1 УК.8.2 УК.8.3	Опрос, тестирование
Тема № 7. ЧС военного времени. Оружие массового поражения. Современная классификация. Действие населения при применении ОМП	УК.8.1 УК.8.3	Опрос, тестирование
Тема № 8. Защита населения в чрезвычайных ситуациях. Единая государственная система предупреждения и ликвидации чрезвычайных ситуациях (РСЧС). Структура. Задачи. ГО РФ и различных государств. МЧС РФ. Эвакуация. Особенности, задачи	УК.8.1	Опрос, тестирование
Тема № 9. Управление безопасностью жизнедеятельности. Противодействие терроризму и экстремизму.	УК.8.1 УК.8.2 УК.8.3	Опрос, тестирование
Тема № 10. Медико-биологические и психологические основы безопасности жизнедеятельности	УК.8.1 УК.8.2 УК.8.3	Опрос, тестирование

8.2. Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений и навыков и (или) опыта деятельности процессе текущего контроля

Примеры тестовых задания для самоконтроля

Целью тестирования является закрепление, углубление и систематизация знаний студентов, полученных на лекциях и в процессе самостоятельной работы; проведение тестирования позволяет ускорить контроль за усвоением знаний и объективизировать процедуру оценки знаний студента.

Тема № 1. Введение. Основные понятия, термины и определения

1. Интегральным показателем безопасности жизнедеятельности является…
1) смертность людей;
2) продолжительность жизни человека;
3) уровень жизни человека;
4) здоровье людей.
2. Безопасность - это

1) состояние деятельности, при котором с определённой вероятностью исключено проявление опасности;

2) присутствие чрезмерной опасности;

3) защищённость человека от социальных опасностей;

4) отсутствие военных действий.

Тема № 2 Безопасность жизнедеятельности и природная среда. Экологические опасности. Классификация. Источники загрязнения среды обитания

1. Потенциальной опасностью называется возможность воздействия на человека _____ факторов.

1) личностных

2) производственных

3) неблагоприятных или несовместимых с жизнью

4) социальных

2. К непрогнозируемым внезапным относятся чрезвычайные ситуации _____ характера.

1) политического;

2) природного, техногенного;

3) социального, экологического;

4) индивидуального.

Тема № 3. Физиология и безопасность труда, обеспечение комфортных условий жизнедеятельности. Вредные и опасные произв. факторы

1. Вредный фактор – это фактор, воздействие которого на человека в определенных условиях вызывает:

1) смерть;

2) нарушения самочувствия;

3) травму;

4) снижение работоспособности или заболевание.

2. Вероятность реализации опасностей называется:

1) аварией;

2) риском;

3) катастрофой;

4) ущербом.

Тема № 4. Принципы возникновения и классификация ЧС. Оценка, прогноз и мониторинг ЧС в РФ и за рубежом

1. Безопасность жизнедеятельности – это…

1) состояние защищённости национальных интересов;

2) область научных знаний, изучающая опасности и способы защиты от них человека в любых условиях его обитания;

3) этапы развития человека;

4) расширения техносферы.

2. Опасность – это..

1) любые явления, процессы, объекты, угрожающие жизни и здоровью человека;

2) исключение нежелательных последствий;

3) неотъемлемая отличительная черта деятельности человека;

4) любые явления, вызывающие положительные эмоции.

Тема № 5. ЧС природного и биолого-социального характера. Стихийные бедствия, виды, характеристика, основные повреждающие факторы. Действие человека при

данных ЧС

1. Наука, изучающая землетрясения, называется …
1) Топографией;
2) Сейсмологией;
3) Гидрологией;
4) Геологией.
2. Ветер большой разрушительной силы, значительной продолжительности скоростью 32 м/с называется …
1) Ураганом;
2) Вихрем;
3) Торнадо;
4) Смерчем.

Тема № 6. ЧС техногенного характера. Аварии, взрывы, пожары, и др. Основные повреждающие факторы. Действие человека при данных ЧС

1. Неконтролируемый, стихийно развивающийся процесс горения, сопровождающийся уничтожением материальных ценностей и создающий опасность для жизни людей, называется …
1) Вспышкой;
2) Возгоранием;
3) Пожаром;
4) Огнем.
2. Вещества и смеси, поражающие высокой температурой, относятся к _____ оружию.
1) химическому;
2) биологическому;
3) инфразвуковому;
4) зажигательному.

Тема № 7. ЧС военного времени. Оружие массового поражения. Современная классификация. Действие населения при применении ОМП

1. В случае возникновения ЧС в школе учитель, в первую очередь, обязан …
1) ожидать дальнейших указаний;
2) эвакуировать учащихся;
3) собрать ценные документы и вещи;
4) укрыться в защитном сооружении.
2. Опасность определенного вида для отдельного индивидуума характеризует риск:
1) социальный;
2) инженерный;
3) индивидуальный;
4) модельный.

Тема № 8. Защита населения в чрезвычайных ситуациях. Единая государственная система предупреждения и ликвидации чрезвычайных ситуациях (РСЧС). Структура. Задачи. ГО РФ и различных государств. МЧС РФ. Эвакуация. Особенности, задачи

1. Катастрофа – это:
1) крупная авария с большим материальным ущербом;
2) авария с материальным ущербом и человеческими жертвами;
3) авария с человеческими жертвами;
4) внезапное событие, которое возникло в результате действий человека или

опасного природного явления…

2. В дисциплине «Безопасность жизнедеятельности» важнейшими понятиями являются:

1) среда обитания;

2) деятельность;

3) опасность и безопасность;

4) экология.

Тема № 9. Терроризм как реальная угроза безопасности в современном обществе

1. Правила поведения, которых следует придерживаться при захвате террористами:

1) выполнять команды террористов, не пытаться встать, покинуть свое место

2) не выполнять команды террористов, пытаться встать, покинуть свое место

3) злить террористов, впадать в истерику, кричать, звать на помощь

2. Совершение действий, создающих опасность гибели людей, причинения значительного имущественного ущерба либо наступления иных общественно опасных последствий, а также угроза совершения указанных действий в тех же целях называется …

1) терроризмом;

2) бандитизмом;

3) экстремизмом;

4) преступной акцией.

Тема № 10. Медико-биологические и психологические основы безопасности жизнедеятельности

1. Утомление – это…

1) напряжение, связанное с временным снижением работоспособности, вызванное длительной работой;

2) расстройство сенсорной области;

3) Профессиональное заболевание.

2. Здоровье – это…

1) полное физическое, психическое и социальное благополучие, а не только отсутствие болезней или физических дефектов;

2) главная функция живой материи;

3) отражение психических функций человека;

4) наука, изучающая строение тела человека.

8.3. Перечень вопросов и заданий для промежуточной аттестации по дисциплине

Вопросы для промежуточного контроля (зачета)

1. Предмет БЖД. Понятия: интегральный показатель БЖД, техносфера, среда безопасности, вредные и опасные факторы.

2. «Аксиома о потенциальной опасности», концепция приемлемого риска, экстремальная ситуация, безопасность труда.

3. Понятие терминов: техника безопасности, охрана труда, производственная санитария, естественные и антропогенные негативные факторы.

4. Понятия физических, химических, биологических и психофизических опасных и вредных факторов.

5. Принципы нормирования опасных и вредных факторов. Понятия ПДК, ДОК, ПДУ, ОБУВ, ПДВ, ПДС.

6. Биологически активные элементы. Макро-, микро- и следовые элементы. Биогеохимические провинции.

7. Источники антропогенных химических факторов.

8. Пути поступления вредных веществ в организм.

9. Комбинированное действие вредных веществ на организм. Формула А.А. Аверьянова.

10. Источники и уровни различных видов опасностей естественного, антропогенного и техногенного происхождения, их эволюция. Классификация опасностей и негативных факторов; травмирующие и вредные зоны.

11. Вероятность (риск) и уровни воздействия негативных факторов. Критерии безопасности. Интегративный характер безопасности. Опасность и риск. Способы определения степени риска. Индивидуальный риск. Концепция приемлемого риска.

12. Причины техногенных аварий и катастроф. Взрывы, пожары и другие чрезвычайные негативные воздействия на человека и среду обитания.

13. Негативное воздействие вредных веществ на среду обитания. Допустимые уровни воздействия вредных веществ на гидросферу, почву, животных и растительность, конструкционные и строительные материалы.

14. Ядерное оружие, его боевые свойства и поражающие факторы.

15. Химическое оружие. Виды отравляющих веществ. Защита от поражающих факторов.

16. Бактериологическое оружие. Защита от поражающих факторов. Современные обычные средства поражения и защита от них.

17. Ионизирующее излучение и его действие на организм. Лучевая болезнь. Нормы радиационной безопасности. Защита от ионизирующих излучений. Защитные свойства материалов. Радиационный (дозиметрический) контроль, его цели и виды. Дозиметрические приборы, их использование. Определение возможных доз облучения, получаемых людьми за время пребывания на загрязненной местности и при преодолении зон загрязнения; определение допустимого времени пребывания людей в зонах загрязнения.

18. Химически опасные объекты (ХОО), их группы и классы опасности. Основные способы хранения и транспортировки химически опасных веществ. Общие меры профилактики аварий на ХОО. Химический контроль и химическая защита. Способы защиты производственного персонала, населения и территорий от химически опасных веществ. Приборы химического контроля. Средства индивидуальной защиты, медицинские средства защиты.

19. Классификация пожаров и промышленных объектов по пожароопасности. Тушение пожаров, принципы прекращения горения. Огнетушащие вещества, технические средства пожаротушения.

20. Пожаро- и взрывоопасные объекты. Классификация взрывчатых веществ. Газовоздушные и пылевоздушные смеси.

21. Ударная волна и ее параметры. Особенности ее прямого и косвенного воздействия на человека, сооружения, технику, природную среду. Особенности ударной волны ядерного взрыва, при взрыве конденсированных взрывчатых веществ, газовоздушных смесей.

22. Ядерный взрыв. Факторы поражения ядерного взрыва. Защита.

23. Транспортные аварии и их последствия.

24. Гидродинамические аварии и их последствия. Защита и действие населения.

25. Характеристики и области возникновения опасных природных процессов: землетрясений, извержений вулканов, магнитных бурь, циклонов и антициклонов, тайфунов, смерчей, ураганов, цунами, оползней, селей, обвалов, осыпей, лавин, пыльных бурь, наводнений, лесных и степных пожаров, ураганов и эпидемий, эпизоотий, эпифитотий, массовых распространений вредителей лесного и сельского хозяйства. Особенности процессов развития стихийных явлений, их воздействие на население, объекты экономики и среды обитания.

26. Безопасность жизнедеятельности и окружающая природная среда. Источники загрязнения среды обитания. Источники загрязнения, виды и состав загрязнений, интенсивность их образования в основных технологических процессах современной промышленности

27. Характеристики основных газообразных загрязняющих веществ и механизм их образования - соединения серы, азота, углерода, высокотоксичные соединения; характеристики аэрозольных загрязнений.

28. Антропогенное воздействие на недра и почвы; методы и средства снижения техногенного воздействия на ландшафт и почву; охрана растительных ресурсов; загрязнение окружающей среды при авариях; экологический риск; малоотходные технологии и ресурсосберегающие технологии.

29. Допустимое воздействие вредных факторов на человека и среду обитания. Принципы определения допустимых воздействий вредных факторов.

30. Вредные вещества, классификация, агрегатное состояние, пути поступления в организм человека, распределение и превращение вредного вещества, действие вредных веществ и чувствительность к ним.

31. Хронические отравления, профессиональные и бытовые заболевания при действии токсинов.

32. Механические колебания. Виды вибраций и их воздействие на человека. Нормирование вибраций, вибрационная болезнь.

33. Функциональная анатомия органа зрения. Дальнозоркость и близорукость. Травмы глаза. Первая помощь. Профилактика заболеваний. Освещение. Требования к системам освещения. Естественное и искусственное освещение. Светильники, источники света.

34. Функциональная анатомия органа слуха. Основные нарушения. Профилактика.

35. Акустические колебания. Постоянный и непостоянный шум. Действие шума на человека. Аудиометрия.

36. Инфразвук, возможные уровни. Нормирование акустического воздействия. Профессиональные заболевания. Профилактика.

37. Ультразвук, контактное и акустическое действие ультразвука. Нормирование акустического воздействия.

38. Профессиональные заболевания от воздействия шума, инфразвука и ультразвука. Опасность их совместного воздействия.

39. Электромагнитные поля. Воздействие на человека статических электрических и магнитных полей, электромагнитных полей промышленной частоты, электромагнитных полей радиочастот.

40. Воздействие УКВ и СВЧ излучений на органы зрения, кожный покров, центральную нервную систему, состав крови и состояние эндокринной системы. Воздействие на организм электромагнитного излучения оптического диапазона.

41. Источники негативных факторов бытовой среды.

42. Атмосферное давление и его влияние на организм.

43. Микроклимат и комфортные условия жизнедеятельности. Терморегуляция и теплопродукция.

44. Организация укрытия населения в чрезвычайных ситуациях. Особенности и организация эвакуации из зон чрезвычайных ситуаций.

45. Мероприятия медицинской защиты. Средства индивидуальной защиты и порядок их использования.

46. Оборудование убежищ. Быстровозводимые убежища. Простейшие укрытия. Противорадиационные укрытия. Укрытие в приспособленных и специальных сооружениях.

47. Терроризм как реальная угроза безопасности в современном обществе. Причины терроризма. Социально-психологические характеристики террориста. Борьба с терроризмом. Взрыв как средство террора. Правила поведения для заложников.

48. Иммунный статус человека. Органы иммунной системы. Понятия иммунная система и антигены. Вакцины, сыворотки. Иммунодефициты первичные и вторичные. Классификация. ВИЧ-инфекция как модель вторичного иммунодефицита. Профилактика СПИДа. Первая помощь.

49. Заболевания бронхолегочной системы (бронхит, плеврит, пневмония, рак легкого, пневмоторакс, пневмокониозы, эмфизема легких). Наблюдение и уход за больными с заболеваниями органов дыхания.

50. Туберкулез. Классификация. Клиническая характеристика. Вакцина БЦЖ Значение реакции Манту. Наблюдение и уход за больными.

51. Алкоголь и его влияние на физическое и психическое здоровье человека. Профилактика алкогольной зависимости.

52. Курение и его влияние на здоровье курящего и окружающих (пассивное курение). Способы профилактики и отказа от курения.

53. Наркотические вещества и их влияние на физическое и психическое здоровье человека. Профилактика наркотической зависимости.

54. Клинико-эпидемиологическая характеристика группы кишечных инфекций. Холера. Брюшной тиф. Сальмонеллез. Ботулизм. Дизентерия. Полиомиелит. Болезнь Боткина. Профилактика и оказание первой медпомощи.

55. Клинико-эпидемиологическая характеристика группы инфекций дыхательных путей. Грипп. Натуральная оспа. Эпидемический менингит. Эпидемический паротит (свинка). Энцефалиты вирусной этиологии. Воспаление легких (пневмония). Ангина. Скарлатина. Дифтерия. Корь. Коклюш. ОРВИ. Профилактика и оказание первой медпомощи.

56. Клинико-эпидемиологическая характеристика группы кровяных инфекций. Сыпной тиф. Клещевой энцефалит, малярия. Профилактика и оказание первой медпомощи.

57. Детские инфекционные болезни. Корь и краснуха. Профилактика и оказание первой медпомощи. Профилактика и оказание первой медпомощи.

58. Клинико-эпидемиологическая характеристика группы инфекций наружных покровов. Бешенство. Столбняк. Сибирская язва. Ящур. Профилактика и оказание первой медпомощи.

59. Основные заболевания системы крови (анемия, лейкоз, лимфолейкоз, метгемоглобинемия). Первая помощь.

60. Механизмы системы свертывания крови. Гемофилия. Первая помощь.

61. Раны. Виды ран. Повязка. Перевязка. Правила наложения и перевязки. Первая помощь при кровотечениях. Виды кровотечений. Методы остановки кровотечений. Наложение кровоостанавливающего жгута.

62. Сосудистая недостаточность. Обморок. Коллапс. Кома, виды комы. Атеросклероз. Вегетативно-сосудистая дистония. Артериальная гипертензия. Гипертонический криз. Диагностика. Понятие шока. Фазы шока. Характеристика и первая медицинская помощь при данных ситуациях.

63. Ишемическая болезнь сердца. Инфаркт миокарда. Стенокардия. Аритмия сердца Диагностика. Ушибы сердца. Диагностика. Первая помощь. Терминальное состояние. Агония. Клиническая и биологическая смерть.

64. Тепловой удар. Солнечный удар. Термические ожоги и ожоговая болезнь. Первая медицинская и доврачебная помощь.

65. Травматический шок. Фазы и степени шока. Первая медицинская и доврачебная помощь.

66. Синдром длительного сдавливания. Клиническая картина. Первая медицинская и доврачебная помощь.

67. Поражение электрическим током. Электрический удар. Возможные пути тока через тело человека. Первая медицинская и доврачебная помощь. Действие электрического тока на человека. Термическое. Электролитическое. Биологическое. Электрический ожог. Электрические знаки. Первая медицинская помощь при поражении электрическим током.

68. Химические ожоги. Отморожение и общее замерзание. Первая медицинская и доврачебная помощь.

69. Укусы ядовитых змей и насекомых. Первая медицинская и доврачебная помощь.

70. Острые и хронические отравления. Принципы оказания первой медицинской помощи при различных отравлениях.

71. Ушибы, растяжения и разрывы мягких тканей, переломы и вывихи. Первая медицинская и доврачебная помощь. Порядок наложения шины. Первая помощь.

72. Реанимация. Искусственное дыхание. Инородные предметы в дыхательных путях. Острая дыхательная недостаточность. Наблюдение и уход за больными с заболеваниями органов дыхания. Оказание первой медицинской помощи при утоплении.

73. Доврачебная реанимационная помощь. Непрямой массаж сердца. Методика. Прямой массаж сердца.

74. Массовые беспорядки их сущность и характер проявления. Город как среда повышенной опасности. Толпа, виды толпы. Паника. Массовые погромы. Массовые зрелища и праздники. Безопасность в толпе. Процесс воздействия субъекта социальной ЧС на Россию и ее регионы.

75. Чрезвычайные ситуации (ЧС) криминального характера и защита от них. Кража. Мошенничество. Правила поведения в случаях посягательства на жизнь и здоровье (нападение на улице, приставания пьяного, изнасилование, нападение в автомобиле, опасность во время ночной остановки). Предупреждение криминальных посягательств в отношении детей. Необходимая самооборона в криминальных ситуациях (правовые основы самообороны, основные правила самообороны, средства самозащиты и их использование).

76. Сущность и содержание информационной безопасности. Формы методы и способы обеспечения информационной безопасности. Основы защиты деловой информации и сведений, составляющих государственную и служебную коммерческую тайны. Методы и средства защиты электронной информации. Информационные технологии и здоровье. Сотовая радиотелефонная связь.

77. Биологические опасности. Микроорганизмы. Виды патогенных микробов. Рост и размножение микроорганизмов. Бактериологическое нормирование. Грибы, растения и животные, представляющие опасность для человека.

78. Состояние среды обитания. Критерии оценки качества окружающей среды. Экологическое нормирование. Источники экологических опасностей (тяжелые металлы, пестициды, диоксины, соединения серы, фосфора и азота, фреоны). Воздух как фактор среды обитания. Критерии оценки состояния загрязнения атмосферы. Комплексный индекс загрязнения атмосферы (КИЗА).

79. Вода как фактор среды обитания. Физиологическое и гигиеническое значение воды. Заболевания, связанные с изменением солевого и микроэлементного состояния воды. Вода как путь передачи инфекционных заболеваний. Влияние хозяйственно-бытовой и производственной деятельности человека н свойства природных вод. Показатели качества воды. Нормирование и нормативные акты в области охраны водной среды. Защита воды. Классификация водоемов и ПДК.

80. Государственные и общественные природоохранные организации.

8.4. Планируемые уровни сформированности компетенций обучающихся и критерии оценивания

Уровни	Содержательное описание уровня	Основные признаки выделения уровня (этапы формирования компетенции, критерии оценки сформированности)	Пятибалльная шкала (академическая) оценка	Двухбалльная шкала, зачет	БРС, % освоения (рейтинговая оценка)
Повышенный	Творческая деятельность	*Включает нижестоящий уровень.* Умение самостоятельно принимать решение, решать проблему/задачу теоретического и прикладного характера на основе изученных методов, приемов, технологий	отлично	зачтено	90-100
Базовый	Применение знаний и умений в более широких контекстах учебной и профессиональной деятельности, нежели по образцу с большей степени самостоятельности и инициативы	*Включает нижестоящий уровень.* Способность собирать, систематизировать, анализировать и грамотно использовать информацию из самостоятельно найденных теоретических источников и иллюстрировать ими теоретические	хорошо		80-89

		положения или обосновывать практику применения			
Удовлетворительный (достаточный)	Репродуктивная деятельность	Изложение в пределах задач курса теоретически и практически контролируемого материала	удовлетворительно		70-79
Недостаточный	Отсутствие признаков удовлетворительного уровня		неудовлетворительно	не зачтено	Менее 70

9. Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины.

Основная литература:

1. Безопасность жизнедеятельности: учеб. пособие для вузов/ Т. А. Хван, П. А. Хван. - 11-е изд.. - Ростов-на-Дону: Феникс, 2014. - 443, [1] с.: ил., табл.. - (Высшее образование). - Соответствует Федеральному государственному образовательному стандарту (третьего поколения). - ISBN 978-5-222-22237-9: 445.00, 445.00, р. Имеются экземпляры в отделах: УБ(50).

2. Халилов, Ш. А. Безопасность жизнедеятельности : учебное пособие / Ш.А. Халилов, А.Н. Маликов, В.П. Гневанов ; под ред. Ш.А. Халилова. — Москва : ФОРУМ : ИНФРА-М, 2022. — 576 с. — (Высшее образование). - ISBN 978-5-8199-0905-8. - Текст : электронный. - URL: https://znanium.com/catalog/product/1841091 (дата обращения: 25.03.2022). – Режим доступа: по подписке.

Дополнительная литература:

1. Белов, С. В. Безопасность жизнедеятельности и защита окружающей среды (техносферная безопасность):: учеб. для бакалавров / С. В. Белов. - 4-е изд., перераб. и доп.. - Москва: Юрайт; Москва: Юрайт, 2013. - 681, [1] с.: ил.. - (Бакалавр. Базовый курс). - Библиогр.: с. 682 (10 назв.). - ISBN 978-5-9916-2771-9. - ISBN 978-5-9692-1461-3: 601.04, 601.04, р.Имеются экземпляры в отделах: всего 50: УБ(49), МБ(ЧЗ)(1).

10. Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины (модуля).

– НЭБ Национальная электронная библиотека, диссертации и прочие издания

- eLIBRARY.RU Научная электронная библиотека, книги, статьи, тезисы докладов конференций
- Гребенников Электронная библиотека ИД журналы
- ЭБС Лань книги, журналы
- ЭБС Консультант студента
- ПРОСПЕКТ ЭБС
- ЭБС ZNANIUM.COM
- РГБ Информационное обслуживание по МБА
- БЕН РАН
- Электронно-библиотечная система (ЭБС) Кантитана (https://elib.kantiana.ru/)
- Электронно-библиотечная система «Университетская библиотека онлайн» http://www.biblioclub.ru/

11. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине.

Программное обеспечение обучения включает в себя:

- система электронного образовательного контента БФУ им. И. Канта – www.lms-3.kantiana.ru, обеспечивающую разработку и комплексное использование электронных образовательных ресурсов;
- серверное программное обеспечение, необходимое для функционирования сервера и связи с системой электронного обучения через Интернет;
- корпоративная платформа Microsoft Teams;
- установленное на рабочих местах обучающихся ПО: Microsoft Windows 7/10, Microsoft Office Standart 2010, антивирусное программное обеспечение Kaspersky Endpoint Security.
- специализированное ПО не требуется.

12. Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине.

Для проведения занятий лекционного типа, практических и семинарских занятий используются специальные помещения (учебные аудитории), оборудованные техническими средствами обучения – мультимедийной проекционной техникой. Для проведения занятий лекционного типа используются наборы демонстрационного оборудования.

Для проведения групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации используются специальные помещения (учебные аудитории), оборудованные специализированной мебелью (для обучающихся), меловой / маркерной доской, персональными компьютерами с выходом в сеть «Интернет».

Для организации самостоятельной работы обучающимся предоставляются помещения, оснащенные компьютерной техникой с возможностью подключения к сети «Интернет» и обеспечением доступа в электронную информационно-образовательную среду университета.

Для обучения инвалидов и лиц с ограниченными возможностями здоровья университетом могут быть представлены специализированные средства обучения, в том числе технические средства коллективного и индивидуального пользования.

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ
федеральное государственное автономное образовательное учреждение высшего образования «Балтийский федеральный университет имени Иммануила Канта»
Институт физико-математических наук и информационных технологий

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

«Основы информационной безопасности»

Шифр: 10.05.01
Специальность: «Компьютерная безопасность»
Специализация: «Математические методы защиты информации»
Квалификация (степень) выпускника: Специалист по защите информации

Калининград
2022

Лист согласования

Составитель: Ветров Игорь Анатольевич, к.т.н., доцент

Рабочая программа утверждена на заседании учебно-методического совета института физико-математических наук и информационных технологий
Протокол № 01/22 от «01» февраля 2022 г.

Председатель учебно-методического совета института физико-математических наук и информационных технологий
Первый заместитель директора ИФМНиИТ, к. ф.-м. н., доцент — Шпилевой А. А

Ведущий менеджер — Е.П.Ставицкая

Содержание

1. Наименование дисциплины: «ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ»

Целью изучения дисциплины «**Основы информационной безопасности**» является теоретическая и практическая подготовка специалистов к деятельности, связанной с комплексным анализом возможных угроз и созданием адекватной модели нарушителя, постановкой конкретных задач заданной степени сложности в рамках модели для обеспечения информационной безопасности компьютерных систем, а также содействие фундаментализации образования и развитию системного мышления, овладение обучаемыми целостной системой знаний, необходимых для понимания роли и места информационной безопасности в системе национальной безопасности Российской Федерации, уяснения основных методов и средств обеспечения информационной безопасности государства и его информационной инфраструктуры

2. Перечень планируемых результатов обучения по дисциплине, соотнесенных с планируемыми результатами освоения образовательной программы

Код компетенции	Результаты освоения образовательной программы (ИДК)	Результаты обучения по дисциплине
ОПК-1: Способность оценивать роль информации, информационных технологий и информационной безопасности в современном обществе, их значение для обеспечения объективных потребностей личности, общества и государства	ОПК.1.1. Демонстрирует знания понятия информации, информационной безопасности, место и роль информационной безопасности в системе национальной безопасности Российской Федерации, основы государственной информационной политики; ОПК.1.2. Демонстрирует знание основных средств и способов обеспечения информационной безопасности, принципов построения систем защиты информации; ОПК.1.3. Классифицирует защищаемую информацию по видам тайны и степеням конфиденциальности; классифицирует и оценивает угрозы информационной безопасности для объекта информатизации	**Знать:** законодательство Российской Федерации, государственные стандарты и нормативные документы по защите информации, основные общеметодологические принципы теории информационной безопасности **Уметь**: систематизировать информацию, формулировать требования к защищаемым системам на основе требований нормативных и правовых документов **Владеть**: средствами поиска, методами обобщения нормативных и методических материалов в сфере своей профессиональной деятельности
ОПК-5: Способность применять нормативные правовые акты, нормативные и методические документы, регламентирующие деятельность по защите информации	ОПК-5.1. Демонстрирует знание нормативных правовых актов, нормативных и методических документов, регламентирующих деятельность по защите информации в организации; классифицирует и оценивает угрозы информационной безопасности для объекта информатизации. ОПК-5.2. Формулирует основные требования по защите конфиденциальной информации, персональных данных и охране результатов интеллектуальной	**Знать**: понятия информации, информационной безопасности, место и роль информационной безопасности в системе национальной безопасности Российской Федерации, основы государственной информационной политики; основные средства и способы обеспечения информационной безопасности, принципы построения систем защиты **Уметь**: классифицировать защищаемую информацию по видам тайны и степеням конфиденциальности; классифицировать и оценивать угрозы

	деятельности в организации ОПК-5.3. Анализирует и разрабатывает проекты локальных правовых актов, инструкций, регламентов и организационно-распорядительных документов, регламентирующих работу по обеспечению информационной безопасности в организации	информационной безопасности для объекта информатизации;информации **Владеть**: профессиональной терминологией в области информационной безопасности

3. Место дисциплины в структуре образовательной программы

Дисциплина ***«Основы информационной безопасности»*** **Б1.0.04** относится к обязательной части Блока 1 Дисциплины (модули) подготовки обучающихся.

4. Виды учебной работы по дисциплине

Виды учебной работы по дисциплине зафиксированы учебным планом основной профессиональной образовательной программы по указанному направлению и профилю, выражаются в академических часах. Часы контактной работы и самостоятельной работы обчающегося и часы, отводимые на процедуры контроля, могут различаться в учебных планах ОПОП по формам обучения. Объем контактной работы включает часы контактной аудиторной работы (лекции/практические занятия/ лабораторные работы), контактной внеаудиторной работы (контроль самостоятельной работы), часы контактной работы в период аттестации. Контактная работа, в том числе может проводиться посредством электронной информационно-образовательной среды университета с использованием ресурсов сети Интернет и дистанционных технологий.

5. Содержание дисциплины, в том числе практической подготовки в рамках дисциплины, структурированное по темам

Исходя из рамок, установленных учебным планом по трудоемкости и видам учебной работы по дисциплине, преподаватель самостоятельно выбирает тематику занятий по формам и количеству часов проведения контактной работы: лекции и иные учебные занятия, предусматривающие преимущественную передачу учебной информации преподавателем и (или) занятия семинарского типа (семинары, практические занятия, практикумы, лабораторные работы, коллоквиумы и иные аналогичные занятия), и (или) групповые консультации, и (или) индивидуальную работу обучающихся с преподавателем, в том числе индивидуальные консультации (по курсовым работам/проектам – при наличии курсовой работы/проекта по данной дисциплине в учебном плане). Рекомендуемая тематика занятий максимально полно реализуется в контактной работе с обучающимися очной формы обучения. В случае реализации образовательной программы в заочной / очно-заочной форме трудоемкость дисциплины сохраняется, однако объем учебного материала в значительной части осваивается обучающимися в форме самостоятельной работы. При этом требования к ожидаемым образовательным результатам обучающихся по данной дисциплине не зависят от формы реализации образовательной программы.

№ п/п	**Наименование темы**	**Содержание темы**
1	Информационная безопасность в системе	Стратегия национальной безопасности Российской Федерации до 2020 года. Стратегия развития информационного общества в РФ.

№ п/п	Наименование темы	Содержание темы
	национальной безопасности Российской Федерации. Отечественные и зарубежные стандарты в области защиты информации.	Виды информации, подлежащей защите. Лицензирование, сертификация и аттестация. Критерии оценки надежных компьютерных систем. Гармонизированные критерии Европейских стран. Особенности информационной безопасности компьютерных сетей. Рекомендации Х.800. Интерпретация "Оранжевой книги" для сетевых конфигураций. Международный стандарт "Общие критерии оценки безопасности информационных технологий". Классификация факторов, воздействующих на защищаемую информацию (ГОСТ Р 51275-2006). Практические правила управления информационной безопасностью (ГОСТ Р ИСО/МЭК 17799-2005). Задачи и функции подразделений по защите информации на предприятии. Защита электронного документооборота с использованием электронной подписи.
2	Информационная война и информационное оружие. Особенности технических средств информационной войны. Защита информации от утечки по техническим каналам.	Основные положения Доктрины информационной безопасности РФ. Национальные интересы РФ. Угрозы информационной безопасности РФ. Источники угроз информационной безопасности РФ. Государственная система защиты информации. Информационное оружие, понятие информационной войны. Информационное оружие и его классификация. Информационно-психологическая война. Технические каналы утечки информации. Характеристика канала утечки информации за счет ПЭМИН. Классификация электронных устройств перехвата информации, а том числе внедряемых в средства вычислительной техники. Средства и методы защиты от утечки по техническим каналам.
3	Виды информационных систем. Угрозы безопасности информационных систем, компьютерно-техническая экспертиза	Классификация информационных систем (обрабатывающих конфиденциальную информацию, персональные данные, государственных информационных систем, систем критической информационной инфраструктуры). Классификация угроз. Модели нарушителя и типичные атаки. Модель действий вероятного нарушителя и модель угроз. Классификация основных видов атак. Сетевая (компьютерная) разведка. Примеры сетевых атак. Троянские программы, люки, эксплойты. Следы в сети. Уникальные идентификаторы интернет-пользователей и электронные "отпечатки". Компьютерно-техническая экспертиза. Методы экспертизы. Проведение расследования компьютерных инцидентов. Исследование носителей компьютерной информации. Аппаратно-программные средства расследования компьютерных инцидентов.
4	Методы и средства защиты информационных систем.	Анализ рисков в области защиты конфиденциальной информации. Формирование политики информационной безопасности предприятия. Основные принципы создания комплексных систем защиты информации. Обзор средств и методов информационной/компьютерной безопасности. Модели управления доступом. Контроль прав доступа. Программные и программно-технические

№ п/п	Наименование темы	Содержание темы
		средства защиты информации от несанкционированного доступа. Возможности и ограничения антивирусных программ. Специализированные средства и методы выявления вредоносных программ. Межсетевое экранирование. Технологии построения виртуальных частных сетей. Системы обнаружения вторжений. Резервирование и резервное копирование. Средства контроля персонала.

6. Рекомендуемая тематика учебных занятий в форме контактной работы

Рекомендуемая тематика учебных занятий *лекционного* типа (предусматривающих преимущественную передачу учебной информации преподавателями):

№ п/п	Наименование темы	Содержание темы
1	Информационная безопасность в системе национальной безопасности Российской Федерации. Отечественные и зарубежные стандарты в области защиты информации.	Стратегия национальной безопасности Российской Федерации до 2020 года. Стратегия развития информационного общества в РФ. Виды информации, подлежащей защите. Лицензирование, сертификация и аттестация. Критерии оценки надежных компьютерных систем. Гармонизированные критерии Европейских стран. Особенности информационной безопасности компьютерных сетей. Рекомендации X.800. Интерпретация "Оранжевой книги" для сетевых конфигураций. Международный стандарт "Общие критерии оценки безопасности информационных технологий". Классификация факторов, воздействующих на защищаемую информацию (ГОСТ Р 51275-2006). Практические правила управления информационной безопасностью (ГОСТ Р ИСО/МЭК 17799-2005). Задачи и функции подразделений по защите информации на предприятии. Защита электронного документооборота с использованием электронной подписи.
2	Информационная война и информационное оружие. Особенности технических средств информационной войны. Защита информации от утечки по техническим каналам.	Основные положения Доктрины информационной безопасности РФ. Национальные интересы РФ. Угрозы информационной безопасности РФ. Источники угроз информационной безопасности РФ. Государственная система защиты информации. Информационное оружие, понятие информационной войны. Информационное оружие и его классификация. Информационно-психологическая война. Технические каналы утечки информации. Характеристика канала утечки информации за счет ПЭМИН. Классификация электронных устройств перехвата информации, а том числе внедряемых в средства вычислительной техники. Средства и методы защиты от утечки по техническим каналам.
3	Виды информационных	Классификация информационных систем (обрабатывающих кон-

№ п/п	Наименование темы	Содержание темы
	систем. Угрозы безопасности информационных систем, компьютерно-техническая экспертиза	фиденциальную информацию, персональные данные, государственных информационных систем, систем критической информационной инфраструктуры). Классификация угроз. Модели нарушителя и типичные атаки. Модель действий вероятного нарушителя и модель угроз. Классификация основных видов атак. Сетевая (компьютерная) разведка. Примеры сетевых атак. Троянские программы, люки, эксплойты. Следы в сети. Уникальные идентификаторы интернет-пользователей и электронные "отпечатки". Компьютерно-техническая экспертиза. Методы экспертизы. Проведение расследования компьютерных инцидентов. Исследование носителей компьютерной информации. Аппаратно-программные средства расследования компьютерных инцидентов.
4	Методы и средства защиты информационных систем.	Анализ рисков в области защиты конфиденциальной информации. Формирование политики информационной безопасности предприятия. Основные принципы создания комплексных систем защиты информации. Обзор средств и методов информационной/компьютерной безопасности. Модели управления доступом. Контроль прав доступа. Программные и программно-технические средства защиты информации от несанкционированного доступа. Возможности и ограничения антивирусных программ. Специализированные средства и методы выявления вредоносных программ. Межсетевое экранирование. Технологии построения виртуальных частных сетей. Системы обнаружения вторжений. Резервирование и резервное копирование. Средства контроля персонала.

Тематика практических занятий

№ п/п	Наименование Темы	Содержание темы
1	Информационная безопасность в системе национальной безопасности Российской Федерации. Отечественные и зарубежные стандарты в области защиты информации.	Получение актуальной информации с официального сайта ФСТЭК России (перечень органов по аттестации, реестр аккредитованных ФСТЭК России органов по сертификации и испытательных лабораторий и государственный реестр сертифицированных средств защиты информации). Перечень средств защиты информации, сертифицированных ФСБ России (сайт ФСБ России). Защита электронного документооборота с использованием электронной подписи для защиты электронного документооборота (издание самоподписанного сертификата, проверка сертификата). Разработка Политики информационной безопасности организации (по выбору).
2	Информационная война и информационное оружие. Особенности технических средств информационной	Работа с документом «Доктрина информационной безопасности РФ», конспект по основным информационным угрозам и направлениям обеспечения безопасности.

№ п/п	Наименование Темы	Содержание темы
	войны. Защита информации от утечки по техническим каналам.	
3	Виды информационных систем. Угрозы безопасности информационных систем. Компьютерно-техническая экспертиза	Работа с банком данных угроз безопасности информации (сайт ФСТЭК России). Групповая практическая работа: Разработка перечня актуальных угроз для информационной системы, обрабатывающей персональные данные организации. Групповая практическая работа: Составление перечня обязательных требований по безопасности информации в государственной информационной системе, обрабатывающей персональные данные. Уникальные идентификаторы интернет-пользователей и электронные "отпечатки".
4	Методы и средства защиты информационных систем.	Установка и первоначальная настройка рабочего места администратора антивирусного приложения (на примере антивируса Касперского). Удаленная установка клиентского антивирусного приложения с рабочего места администратора. Создание Политики работы антивирусного приложения с учетом специфики заданной сети. Установка и первоначальная настройка СЗИ от НСД (на примере Secret Net Studio). Настройка разграничения доступа к ресурсам средствами СЗИ от НСД. Использование персональных идентификаторов для аутентификации пользователей. Настройка замкнутой программной среды средствами СЗИ от НСД. Установка и первоначальная настройка межсетевого экрана (на примере TrustAccess). Групповая практическая работа: Разработка правил фильтрации IP-трафика для заданной конфигурации сети.

Тематика самостоятельных работ

№ п/п	Наименование темы	Тематика самостоятельных работ
1	Информационная безопасность в системе национальной безопасности Российской Федерации. Отечественные и зарубежные стандарты в области защиты информации.	Ознакомление с литературой по курсу. Работа с ресурсами сети Интернет. Выбор темы курсовой работы. Повторение теоретического материала.

№ п/п	Наименование темы	Тематика самостоятельных работ
2	Информационная война и информационное оружие. Особенности технических средств информационной войны. Защита информации от утечки по техническим каналам.	Повторение теоретического материала к практическим занятиям. Ознакомление с литературой по курсу. Работа с ресурсами сети Интернет. Подготовка раздела «Предварительные сведения» курсовой работы
3	Виды информационных систем. Угрозы безопасности информационных систем. Компьютерно-техническая экспертиза	Повторение теоретического материала к практическим занятиям. Ознакомление с литературой по курсу. Работа с ресурсами сети Интернет. Подготовка к выполнению групповых практических работ. Подготовка практической части курсовой работы.
4	Методы и средства защиты информационных систем.	Повторение теоретического материала к практическим занятиям. Ознакомление с литературой по курсу. Работа с ресурсами сети Интернет. Подготовка текста курсовой работы. Подготовка к выполнению групповой практической работы. Подготовка к итоговой аттестации по дисциплине (зачету). Защита курсовой работы.

Руководствуясь положениями статьи 47 и статьи 48 Федерального закона от 29 декабря 2012 г. N 273-ФЗ «Об образовании в Российской Федерации» научно-педагогические работники и иные лица, привлекаемые университетом к реализации данной образовательной программы, пользуются предоставленными академическими правами и свободами в части свободы преподавания, свободы от вмешательства в профессиональную деятельность; свободы выбора и использования педагогически обоснованных форм, средств, методов обучения и воспитания; права на творческую инициативу, разработку и применение авторских программ и методов обучения и воспитания в пределах реализуемой образовательной программы и отдельной дисциплины.

Исходя из рамок, установленных учебным планом по трудоемкости и видам учебной работы по дисциплине, преподаватель самостоятельно выбирает тематику занятий по формам и количеству часов проведения контактной работы: лекции и иные учебные занятия, предусматривающие преимущественную передачу учебной информации преподавателем и (или) занятия семинарского типа (семинары, практические занятия, практикумы, лабораторные работы, коллоквиумы и иные аналогичные занятия), и (или) групповые консультации, и (или) индивидуальную работу обучающихся с преподавателем, в том числе индивидуальные консультации (по курсовым работам/проектам – при наличии курсовой работы/проекта по данной дисциплине в учебном плане).

Рекомендуемая тематика занятий максимально полно реализуется в контактной работе с обучающимися очной формы обучения. В случае реализации образовательной программы в заочной / очно-заочной форме трудоемкость дисциплины сохраняется, однако объем учебного материала в значительной части осваивается обучающимися в форме самостоятельной работы. При этом требования к ожидаемым образовательным результатам обучающихся по данной дисциплине не зависят от формы реализации образовательной программы.

7. Методические рекомендации по видам занятий

Лекционные занятия.

В ходе лекционных занятий обучающимся рекомендуется выполнять следующие действия. Вести конспектирование учебного материала. Обращать внимание на категории, формулировки, раскрывающие содержание тех или иных явлений и процессов, научные выводы и практические рекомендации по их применению. Задавать преподавателю уточняющие вопросы с целью уяснения теоретических положений, разрешения спорных ситуаций.

Желательно оставить в рабочих конспектах поля, на которых во внеаудиторное время можно сделать пометки из рекомендованной литературы, дополняющие материал прослушанной лекции, а также подчеркивающие особую важность тех или иных теоретических положений.

Практические и семинарские занятия.

На практических и семинарских занятиях в зависимости от темы занятия выполняется поиск информации по решению проблем, практические упражнения, контрольные работы, выработка индивидуальных или групповых решений, итоговое обсуждение с обменом знаниями, участие в круглых столах, разбор конкретных ситуаций, командная работа, представление портфолио и т.п.

Самостоятельная работа.

Самостоятельная работа осуществляется в виде изучения литературы, эмпирических данных по публикациям и конкретных ситуаций из практики, подготовке индивидуальных работ, работа с лекционным материалом, самостоятельное изучение отдельных тем дисциплины; поиск и обзор литературы и электронных источников; чтение и изучение учебника и учебных пособий.

8. Фонд оценочных средств

8.1. Перечень компетенций с указанием этапов их формирования в процессе освоения образовательной программы в рамках учебной дисциплины

Основными этапами формирования указанных компетенций при изучении обучающимися дисциплины являются последовательное изучение содержательно связанных между собой тем учебных занятий. Изучение каждой темы предполагает овладение обучающимися необходимыми компетенциями. Результат аттестации обучающихся на различных этапах формирования компетенций показывает уровень освоения компетенций.

Контролируемые разделы (темы) дисциплины	Индекс контролируемой компетенции (или её части)	Оценочные средства по этапам формирования компетенций
		текущий контроль по дисциплине
Тема 1. Информационная безопасность в системе национальной безопасности Российской Федерации. Отечественные и зарубежные стандарты в области защиты информации.	ОПК-1	Устный опрос, выполнение практических заданий
Тема 2. Информационная война и информационное оружие. Особенности технических средств информационной войны. Защита информации от утечки по техническим каналам.	ОПК-5 ОПК-1	Устный опрос, выполнение практических заданий
Тема 3. Виды информационных систем. Угрозы безопасности информа-	ОПК-1 ОПК-5	Устный опрос, выполнение практических заданий

Контролируемые разделы (темы) дисциплины	Индекс контролируемой компетенции (или её части)	Оценочные средства по этапам формирования компетенций
		текущий контроль по дисциплине
ционных систем, компьютерно-техническая экспертиза		
Тема 4. Методы и средства защиты информационных систем.	ОПК-1 ОПК-5	Устный опрос, выполнение практических заданий

8.2. Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений и навыков и (или) опыта деятельности процессе текущего контроля

8.2.1. Типовые вопросы для устного опроса

	Вопрос
Оценка «зачтено» - пороговый уровень освоения компетенции	Перечислить основные законодательные акты и ведомства, регулирующие сферу информационной безопасности Российской Федерации.
Оценка «зачтено» - достаточный уровень освоения компетенции	Перечислить виды информации, подлежащей защите, основные законодательные акты по защите отдельных видов информации, перечислить области, подлежащие лицензированию и сертификации
Оценка «зачтено» - высокий уровень освоения компетенции	Перечислить виды информации, подлежащей защите, основные законодательные акты по защите отдельных видов информации, перечислить области, подлежащие лицензированию и сертификации, контролирующие органы и виды контрольных проверок

Тема 2. Информационная война и информационное оружие. Особенности технических средств информационной войны. Защита информации от утечки по техническим каналам.

	Вопрос
Оценка «зачтено» - пороговый уровень освоения компетенции	Перечислить основные угрозы информационной безопасности Российской Федерации и их источники
Оценка «зачтено» - достаточный уровень освоения компетенции	Перечислить основные угрозы информационной безопасности Российской Федерации и их источники, перечислить подразделения в государственной системе защиты информации, дать определение информационного оружия и информационной войны
Оценка «зачтено» - высокий уровень освоения компетенции	Перечислить основные угрозы информационной безопасности Российской Федерации и их источники, перечислить подразделения в государственной системе защиты информации, их функции и основные направления работы, представить классификацию информационного оружия, дать определение информационной войны и привести примеры

8.2.2. Курсовые работы

Курсовая работа – творческая исследовательская работа, включающая изучение и обзор определённого количества научной литературы по теме исследования, изложение предварительных сведений и основной части работы, в которую должен входить сравнительный анализ систем или методов защиты информации, предложен вариант выбора оптимального набора защитных механизмов для некоторой выбранной информационной системы.

Цель написания курсовой работы – привитие студенту первоначальных навыков работы с правовыми документами, технической литературой, источниками сети Интернет, в том числе официальными сайтами «регуляторов» в области защиты информации, краткого и лаконичного представления полученных результатов в соответствии с требованиями, предъявляемыми к научным отчетам, обзорам и статьям.

При написании курсовой работы необходимо:

- изучить источники по предмету исследования;
- в развернутом виде представить актуальность проблемы;
- отметить теоретическую и практическую значимость решения проблемы;
- обозначить цели и задачи исследования;
- проанализировать и детализировать известные результаты рассматриваемой области;
- сделать выводы по теме исследования;
- обозначить перспективу изучения проблемы;
- указать литературу по теме исследования.

Объем курсовой работы может достигать 13-20 стр. Подготовка курсовой работы подразумевает самостоятельное изучение студентом нескольких источников (монографий, научных статей, правовых документов и т.д.) по определённой теме, не рассматриваемой подробно на лекции, систематизацию материала и краткое его изложение.

Работа должна быть графически и методически грамотно оформлена. При написании курсовой работы необходимо: а) отобрать учебную и научную литературу по вопросу исследования; б) составить план курсовой, в котором следует отразить: введение с постановкой цели и задач исследования; описанием актуальности исследования, его теоретической и практической значимости; основную часть работы, включающую сравнительный анализ систем или методов защиты информации, вариант выбора оптимального набора защитных механизмов для некоторой выбранной информационной системы, а также перспективу дальнейшего развития темы, вопроса; список литературы, Интернет-ресурсы, приложение (при необходимости).

Темы курсовых работ

1. Средства защиты информации от несанкционированного доступа (СЗИ от НСД): принципы работы, обзор российского и мирового рынка, сравнительный анализ.
2. Системы контроля действий пользователей и системы поиска конфиденциальных данных в корпоративной сети (DLP, Discovery DLP): принципы работы, обзор российского и мирового рынка, сравнительный анализ.
3. Средства усиленной аутентификации (USB-токены, смарт-карты…): принципы работы, обзор российского и мирового рынка, сравнительный анализ.

4. SIEM-системы: принципы работы, обзор мирового и российского рынка, сравнительный анализ.

5. Биометрия в России: правовое регулирование и практика применения.

6. Системы и методы аутентификации пользователей.

7. Угрозы безопасности и риски промышленной автоматизации.

8. Системы Enterprise Single Sign-On (ESSO): принципы работы, обзор российского и мирового рынка, сравнительный анализ.

9. Системы Endpoint Detection and Response (EDR): принципы работы, обзор российского и мирового рынка, сравнительный анализ.

10. Угрозы и защита интернета вещей (IoT).

11. Современные угрозы для мобильных устройств и методы защиты.

12. Способы атак на банкоматы и их последствия, способы защиты.

13. VPN-сервисы и VPN-системы: принципы работы, обзор российского и мирового рынка

14. Безопасность мобильных мессенджеров.

15. Брокеры безопасного доступа в облако Cloud Access Security Broker (CASB): принципы работы, обзор рынка, сравнительный анализ.

16. Прокси-серверы Secure Web Gateways (SWG): принципы работы, обзор российского и мирового рынка, сравнительный анализ.

17. Угрозы безопасности при использовании браузера Tor (темного интернета).

18. Межсетевые экраны: принципы работы, типы, обзор российского и мирового рынка, сравнительный анализ.

19. Средства электронной подписи и шифрования документов): принципы работы, типы, требования, обзор российского рынка, сравнительный анализ.

20. Антивирусы: принципы работы, обзор российского и мирового рынка, сравнительный анализ.

21. Средств резервного копирования и восстановления данных: принципы работы, виды, обзор российского и мирового рынка, сравнительный анализ.

22. Систем обнаружения вторжений: принципы работы, обзор российского и мирового рынка

23. Угрозы безопасности и защита среды виртуализации.

24. Угрозы безопасности и защита облачных решений и технологий.

Тема курсовой работы также может быть индивидуально предложена студентом по согласованию с преподавателем.

Шкала оценивания компетенций по результатам проверки курсовой работы

Дескрипторы	**Минимальный ответ**	**Изложенный, раскрытый ответ**	**Законченный, полный ответ**	**Образцовый, примерный, достойный подражания ответ**
Раскрытие проблемы	Проблема не раскрыта. Отсутствуют выводы	Проблема раскрыта не полностью. Выводы не сделаны и/или выводы не обоснованы	Проблема раскрыта. Проведен анализ проблемы без привлечения дополнительной литературы.	Проблема раскрыта полностью. Проведен анализ проблемы с привлечением дополнительной литературы. Выводы обоснованы

Дескрипторы	Минимальный ответ	Изложенный, раскрытый ответ	Законченный, полный ответ	Образцовый, примерный, достойный подражания ответ
			Не все выводы сделаны и/или обоснованы	
Представ-ление	Представляемая информация логически не связана. Не использованы профессиональные термины	Представляемая информация не систематизирована и/или не последовательна. Использован 1-2 профессиональный термин	Представляемая информация систематизирована и последовательна. Использовано более 2 профессиональных терминов	Представляемая информация систематизирована, последовательна и логически связана. Использовано более 5 профессиональных терминов
Оформление	Оформление курсовой работы не соответствует стандарту. Много ошибок форматирования текста.	Оформление курсовой работы частично соответствует стандарту. Имеется 3-4 ошибки в форматировании представляемой информации	Оформление курсовой работы в основном соответствует стандарту. Не более 2 ошибок форматирования в представляемой информации	Оформление курсовой работы полностью соответствует стандарту. Отсутствуют ошибки в представляемой информации.
Итоговая оценка				

Дескрипторы для поэлементного оценивания курсовой работы

Уровень 5 – детерминирующая идея отражает глубокое понимание, содержание работы соответствует теме; работа оформлена с высоким качеством, оригинально.

Уровень 4 – основная идея содержательна; работа оформлена хорошо, традиционно.

Уровень 3 – идея ясна, но, возможно, шаблонна; работа оформлена некачественно, имеются методические и технические ошибки.

Уровень 2 – основная идея очевидна, но слишком проста или неоригинальна (вторична), методические и технические ошибки значительны.

Уровень 1 – основная идея поверхностна или заимствована; работа не обладает информационно-образовательными достоинствами.

Уровень 0 – основная идея отсутствует или о ней можно только догадываться.

Критерии и показатели при оценивании курсовой работы

Критерии	Показатели
Новизна	- актуальность проблемы и темы; - новизна и самостоятельность в постановке проблемы, в формулировании нового аспекта выбранной для анализа проблемы; - наличие авторской позиции, самостоятельность суждений.

Критерии	Показатели
Степень раскрытия сущности проблемы	- соответствие плана теме курсовой работы; - соответствие содержания теме и плану курсовой работы; - полнота и глубина раскрытия основных понятий проблемы; - обоснованность способов и методов работы с материалом; - умение работать с литературой, систематизировать и структурировать материал; - умение обобщать, сопоставлять различные точки зрения по рассматриваемому вопросу, аргументировать основные положения и выводы.
Обоснованность выбора источников	- круг, полнота использования литературных источников по проблеме; - привлечение новейших работ по проблеме (журнальные публикации, материалы сборников научных трудов и т.д.).
Соблюдение требований к оформлению	- правильное оформление ссылок на используемую литературу; - грамотность и культура изложения; - владение терминологией и понятийным аппаратом проблемы; - соблюдение требований к объему курсовой работы; - культура оформления: выделение абзацев.
Грамотность	- отсутствие орфографических и синтаксических ошибок, стилистических погрешностей; - отсутствие опечаток, сокращений слов, кроме общепринятых; - литературный стиль.

8.3. Перечень вопросов и заданий для промежуточной аттестации по дисциплине

Промежуточный контроль по дисциплине служит для оценки работы студента в течение семестра и призван выявить уровень, прочность и систематичность полученных им теоретических и практических знаний, приобретения навыков самостоятельной работы, развития творческого мышления, умение синтезировать полученные знания и применять их в решении практических задач.

Вопросы предполагают контроль общих методических знаний и умений, способность студентов проиллюстрировать их примерами, индивидуальными материалами, составленными студентами в течение курса.

Промежуточный контроль проводится в форме устного собеседования, по результатам которого ставится «зачтено» или «не зачтено» на основе следующих критериев: полноты, структурированности и правильности ответа по сути поставленных вопросов.

Вопросы для промежуточного контроля (зачета)

1. Стратегия национальной безопасности Российской Федерации до 2020 года
2. Стратегия развития информационного общества в РФ.
3. Виды информации, подлежащей защите
4. Понятия лицензирования, сертификации и аттестации
5. Угрозы информационной безопасности Российской Федерации

6. Источники угроз информационной безопасности Российской Федерации
7. Государственная система защиты информации
8. Информационное обеспечение оборонных мероприятий и боевых действий
9. Информационное оружие и его классификация
10. Понятие информационно-психологической войны
11. Свойства монитора обращений. Понятия произвольного т принудительного управления доступом, гарантированности операционной и технологической. («Оранжевая книга»).
12. Функции безопасности, понятия мощности механизмов (Гармонизированные критерии европейских стран)
13. Сетевые функции (сервисы) и механизмы безопасности (Рекомендации X.800)
14. Классификация факторов, воздействующих на защищаемую информацию
15. Анализ рисков в области защиты конфиденциальной информации
16. Политика информационной безопасности предприятия
17. Основные принципы создания комплексных систем защиты информации
18. Источники угроз информации информационных систем
19. Классификация угроз информационной безопасности автоматизированных систем
20. Классификация автоматизированных систем и средств защиты информации
21. Основные направления защиты информации в автоматизированной системе
22. Основные меры защиты автоматизированных систем
23. Этапы реализации защитных мероприятий по обеспечению безопасности информационных систем
24. Модели управления доступом в автоматизированных системах
25. Обзор средств защиты информации от несанкционированного доступа
26. Характеристика канала утечки информации за счет ПЭМИН. Методология защиты информации от утечки за счет ПЭМИН. Способы защиты информации от утечки за счет ПЭМИН
27. Защита электронного документооборота с использованием электронной подписи
28. Экранирование как метод защиты
29. Обзор технологий построения виртуальных частных сетей
30. Системы обнаружения вторжений
31. Организация антивирусной защиты
32. Резервирование и резервное копирование

8.4. Планируемые уровни сформированности компетенций обучающихся и критерии оценивания

Уровни	Содержательное описание уровня	Основные признаки выделения уровня (этапы формирования компетенции, критерии оценки сформированности)	Пятибалльная шкала (академическая) оценка	Двухбалльная шакала, зачет	БРС, % освоения (рейтинговая оценка)
Повышенный	Творческая деятельность	*Включает нижестоящий уровень.*	отлично	зачтено	86-100

		Умение самостоятельно принимать решение, решать проблему/задачу теоретического и прикладного характера на основе изученных методов, приемов, технологий			
Базовый	Применение знаний и умений в более широких контекстах учебной и профессиональной деятельности, нежели по образцу с большей степени самостоятельности и инициативы	*Включает нижестоящий уровень.* Способность собирать, систематизировать, анализировать и грамотно использовать информацию из самостоятельно найденных теоретических источников и иллюстрировать ими теоретические положения или обосновывать практику применения	хорошо		71-85
Удовлетворительный (достаточный)	Репродуктивная деятельность	Изложение в пределах задач курса теоретически и практически контролируемого материала	удовлетворительно		55-70
Недостаточный	Отсутствие признаков удовлетворительного уровня		неудовлетворительно	не зачтено	Менее 55

9. Перечень основной и дополнительной литературы, необходимой для освоения дисциплины

9.1. Основная литература

1. Белов, Е. Б. Основы информационной безопасности: Учебное пособие для вузов / Е.Б. Белов и др. - Москва : Гор. линия-Телеком, 2011. - 558 с.: ил.; . - (Специальность; Учебное пособие для высших учебных заведений). ISBN 5-93517-292-5, 100 экз. - Текст : электронный. - URL: https://znanium.com/catalog/product/405159 (дата обращения: 13.01.2022). – Режим доступа: по подписке.

2. Ковалев, Д. В. Информационная безопасность: Учебное пособие / Ковалев Д.В., Богданова Е.А. - Ростов-на-Дону:Южный федеральный университет, 2016. - 74 с.: ISBN 978-5-9275-2364-1. - Текст

: электронный. - URL: https://znanium.com/catalog/product/997105 (дата обращения: 13.01.2022). – Режим доступа: по подписке.
3. Краковский, Ю. М. Защита информации: Учебное пособие (ФГОС) / Краковский Ю.М. - Ростов-на-Дону :Феникс, 2016. - 347 с.ISBN 978-5-222-26911-4. - Текст : электронный. - URL: https://znanium.com/catalog/product/908844 (дата обращения: 13.01.2022). – Режим доступа: по подписке.

9.2. Дополнительная литература

1. Белоус, А. И. Кибероружие и кибербезопасность. О сложных вещах простыми словами : монография / А. И. Белоус, В. А. Солодуха. - Москва ; Вологда : Инфра-Инженерия, 2020. - 692 с. - ISBN 978-5-9729-0486-0. - Текст : электронный. - URL: https://znanium.com/catalog/product/1167736 (дата обращения: 13.01.2022). – Режим доступа: по подписке.
2. Защита информации : учебное пособие / А.П. Жук, Е.П. Жук, О.М. Лепешкин, А.И. Тимошкин. — 3-е изд. — Москва : РИОР : ИНФРА-М, 2021. — 400 с. — (Высшее образование). — DOI: https://doi.org/10.12737/1759-3. - ISBN 978-5-369-01759-3. - Текст : электронный. - URL: https://znanium.com/catalog/product/1210523 (дата обращения: 13.01.2022). – Режим доступа: по подписке.
3. Баранова, Е. К. Информационная безопасность и защита информации : учебное пособие / Е.К. Баранова, А.В. Бабаш. — 4-е изд., перераб. и доп. — Москва : РИОР : ИНФРА-М, 2021. — 336 с. — (Высшее образование). — DOI: https://doi.org/10.29039/1761-6. - ISBN 978-5-369-01761-6. - Текст : электронный. - URL: https://znanium.com/catalog/product/1189326 (дата обращения: 13.01.2022). – Режим доступа: по подписке.
4. Гришина, Н. В. Основы информационной безопасности предприятия : учебное пособие / Н. В. Гришина. - Москва : ИНФРА-М, 2021. - 216 с. - (Высшее образование: Специалитет). - ISBN 978-5-16-016534-9. - Текст : электронный. - URL: https://znanium.com/catalog/product/1178150 (дата обращения: 13.01.2022). – Режим доступа: по подписке.

9.3. Нормативные документы

Федеральный закон от 29 июля 2004 г. № 98-ФЗ «О коммерческой тайне».

Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации».

Федеральный закон от 27 июля 2006 г. №152 «О персональных данных».

Доктрина информационной безопасности Российской Федерации (утверждена Указом Президента РФ от 5 декабря 2016 г. № 646).

Стратегия развития информационного общества в Российской Федерации на 2017 - 2030 годы (утверждена Указом Президента РФ от 9 мая 2017 г. № 203).

Перечень сведений конфиденциального характера (утвержден указом Президента Российской Федерации от 6 марта 1997 года №188).

Постановление Правительства от 1 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».

10. Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины

- НЭБ Национальная электронная библиотека, диссертации и прочие издания
- eLIBRARY.RU Научная электронная библиотека, книги, статьи, тезисы докладов конференций
- Гребенников Электронная библиотека ИД журналы
- ЭБС Лань книги, журналы
- ЭБС Консультант студента
- ПРОСПЕКТ ЭБС
- ЭБС ZNANIUM.COM
- РГБ Информационное обслуживание по МБА
- БЕН РАН
- Электронно-библиотечная система (ЭБС) Кантитана (https://elib.kantiana.ru/)

11. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине

Программное обеспечение обучения включает в себя:

- система электронного образовательного контента БФУ им. И. Канта – www.lms-3.kantiana.ru, обеспечивающую разработку и комплексное использование электронных образовательных ресурсов;
- серверное программное обеспечение, необходимое для функционирования сервера и связи с системой электронного обучения через Интернет;
- корпоративная платформа Microsoft Teams;
- установленное на рабочих местах студентов ПО: Microsoft Windows 7, Microsoft Office Standart 2010, антивирусное программное обеспечение Kaspersky Endpoint Security.

12. Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине

Для проведения занятий лекционного типа, практических и семинарских занятий используются специальные помещения (учебные аудитории), оборудованные техническими средствами обучения – мультимедийной проекционной техникой. Для проведения занятий лекционного типа используются наборы демонстрационного оборудования.

Для проведения лабораторных работ, (практических занятий – при необходимости) используются специальные помещения (учебные аудитории), оснащенные специализированным лабораторным оборудованием: персональными компьютерами с возможностью выхода в интернет и с установленным программным обеспечением, заявленным в п.11.

Для проведения групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации используются специальные помещения (учебные аудитории), оборудованные специализированной мебелью (для обучающихся), меловой / маркерной доской.

Для организации самостоятельной работы обучающимся предоставляются помещения, оснащенные компьютерной техникой с возможностью подключения к сети «Интернет» и обеспечением доступа в электронную информационно-образовательную среду университета.

Для обучения инвалидов и лиц с ограниченными возможностями здоровья университетом могут быть представлены специализированные средства обучения, в том числе технические средства коллективного и индивидуального пользования.

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
федеральное государственное автономное образовательное учреждение высшего образования «Балтийский федеральный университет имени Иммануила Канта»
Институт физико-математических наук и информационных технологий

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

«Физическая культура и спорт»

Шифр: 10.05.01
Специальность: «Компьютерная безопасность»
Специализация: «Математические методы защиты информации»
Квалификация (степень) выпускника: специалист по защите информации

Калининград
2022

Лист согласования

Составитель: Томашевская О.Б. к.п.н, доцент; Доценты, к.п.н: Юшков.В.И., Семенив Д.А., Никитина А.А., Ст. преподаватели: Бекаури М.В., Барановский В.Н., Головина Е.А., Грудько Л.С, Долматов Б.В., Калягин В.И., Коваленко Т.А., Макиенко В.В., Маркелова Е.Б., Мартынова В.И., Моржухин А.Н., Кравченко И.А., Пасевина В.В., Писаренко Е.Г., Попова И.В., Покровская Н.В., Романов С.С., Румянцева О.В., Созинова Л.Л., Споденко С.В., Станчик Т.И., Тюпа П.И., , Ассистенты: Мусейчук С.В., Ястребова О.С., Сыч Р.К.

Рабочая программа утверждена на заседании учебно-методического совета института физико-математических наук и информационных технологий

Протокол № 01/22 от «01» февраля 2022 г.

Председатель учебно-методического
совета института физико-
математических наук и информационных
технологий

Первый заместитель директора Шпилевой А. А
ИФМНиИТ, к. ф.-м. н., доцент

Ведущий менеджер Е.П.Ставицкая

Содержание

1.Наименование дисциплины: ««Физическая культура и спорт».

Дисциплина «Физическая культура и спорт» как составная часть общей культуры и профессиональной подготовки студента в период обучения в университете, входит обязательным разделом в гуманитарный компонент образования, значимость которого проявляется через гармонизацию духовных и физических сил, формирование таких общечеловеческих ценностей, как здоровье, физическое и психическое благополучие, физическое совершенство.

Результатом образования в области физической культуры должно быть создание у студентов устойчивой мотивации и потребности в выборе здорового образа жизни, в физическом самосовершенствовании, приобретении личного опыта творческого использование средств и методов физической культуры, в достижении достаточного уровня психофизической подготовленности.

Реализация программы по модулям дисциплины «Физическая культура и спорт» направлена на:

- повышение уровня теоретических знаний студентов в формировании навыков здорового образа жизни;
- достижение целостности знаний в области физической культуры, направленных на профессионально-личностное развитие будущего специалиста, его профессиональной компетенции;
- ориентацию всех видов программного материала на решение задач обучения студентов умениям физической самоподготовки, самосовершенствованию средствами физической культуры;
- учет профессиональной направленности университета, кадрового потенциала преподавателей физической культуры, специфики организации учебного процесса и возможностей материально-технической базы.

2. Перечень планируемых результатов обучения по дисциплине, соотнесенных с планируемыми результатами освоения образовательной программы

Код компетенции	Результаты освоения образовательной программы (ИДК)	Результаты обучения по дисциплине
УК-7 Способен поддерживать должный уровень физической подготовленности для обеспечения полноценной социальной и профессиональной деятельности	УК.7.1. Поддерживает должный уровень физической подготовленности для обеспечения полноценной социальной и профессиональной деятельности и соблюдает нормы здорового образа жизни. УК.7.2. Использует основы физической культуры для осознанного выбора здоровьесберегающих технологий с учётом внутренних и внешних условий реализации конкретной	**Знать**: - Влияние физической культуры на укрепления здоровья, профилактику профессиональных заболеваний и вредных привычек. - Основные средства и методы физического воспитания; - Основы здорового образа жизни; - Методы оценки физического развития, физической подготовленности средствами физической культуры и спорта в студенческом возрасте. **Уметь:** -Использовать средства и методы физической культуры в регулировании своего

	профессиональной деятельности.	психофизического состояния;- выполнять комплексы упражнений оздоровительной и профессионально прикладной направленности; **Владеть:** -Навыком самостоятельно применять средства и методы физического воспитания в укреплении здоровья, методами контроля состояния организма при нагрузках; - Навыками ведения здорового образа жизни, участия в физкультурно-оздоровительной деятельности.

3. Место дисциплины в структуре образовательной программы

Дисциплина «Физическая культура и спорт» относится к обязательной части Блока 1 Дисциплины (модули).

4. Виды учебной работы по дисциплине.

Виды учебной работы по дисциплине зафиксированы учебным планом основной профессиональной образовательной программы по указанному направлению и профилю, выражаются в академических часах. Часы контактной работы и самостоятельной работы обучающегося и часы, отводимые на процедуры контроля, могут различаться в учебных планах ОПОП по формам обучения. Объем контактной работы включает часы контактной аудиторной работы (лекции/практические занятия/ лабораторные работы), контактной внеаудиторной работы (контроль самостоятельной работы), часы контактной работы в период аттестации. Контактная работа, в том числе может проводиться посредством электронной информационно-образовательной среды университета с использованием ресурсов сети Интернет и дистанционных технологий

5. Содержание дисциплины, структурированное по темам (разделам)

Исходя из рамок, установленных учебным планом по трудоемкости и видам учебной работы по дисциплине, преподаватель самостоятельно выбирает тематику занятий по формам и количеству часов проведения контактной работы: лекции и иные учебные занятия, предусматривающие преимущественную передачу учебной информации преподавателем и (или) занятия семинарского типа (семинары, практические занятия, практикумы, лабораторные работы, коллоквиумы и иные аналогичные занятия), и (или) групповые консультации, и (или) индивидуальную работу обучающихся с преподавателем, в том числе индивидуальные консультации (по курсовым работам/проектам – при наличии курсовой работы/проекта по данной дисциплине в учебном плане). Рекомендуемая тематика занятий максимально полно реализуется в контактной работе с обучающимися очной формы обучения. В случае реализации образовательной программы в заочной / очно-заочной форме трудоемкость дисциплины сохраняется, однако объем учебного материала в значительной части осваивается обучающимися в форме самостоятельной работы. При этом требования к ожидаемым

образовательным результатам обучающихся по данной дисциплине не зависят от формы реализации образовательной программы.

№	Наименование раздела	Содержание раздела
1	Тема 1. Физическая культура и спорт в общекультурной и профессиональной подготовке студентов.	Физическая культура и спорт как социальные феномены общества. Современное состояние физической культуры и спорта. Нормативно-правовая основа физической культуры и спорта. Федеральный закон «О физической культуре и спорте в Российской Федерации». Физическая культура личности. Ценности физической культуры. физическая культура как учебная дисциплина высшего профессионального образования и целостного развития личности. Основные положения организации физического воспитания в высшем учебном заведении, в БФУ им.И.Канта.
2	Тема 2. Универсиады. История комплексов ГТО и БГТО. Новый Всероссийский физкультурно-спортивный комплекс.	История становления и развития Олимпийского движения. Возникновение олимпийских игр. Возрождение олимпийской идеи. Олимпийское движение. Олимпийские комитеты в России. Универсиады. Универсиада в Казани. История комплексов ГТО и БГТО. Новый Всероссийский физкультурно-спортивный комплекс: цель, задачи, структура, основные требования.
3	Тема 3. Социально-биологические основы физической культуры.	Организма человека как единая саморазвивающаяся и саморегулирующаяся биологическая система. Воздействие природных и социально-экологических факторов на организм и жизнедеятельность человека. Средства физической культуры и спорта в управлении совершенствованием функциональных возможностей организма в целях обеспечения умственной и физической деятельности. Физиологические механизмы и закономерности совершенствования отдельных систем организма под воздействием направленной физической тренировки. Двигательная функция и повышение устойчивости организма человека к различным условиям внешней среды.
4	Тема 4. Основы здорового образа жизни студента.	Здоровье человека как ценность. Факторы, определяющие здоровье. Понятие «здоровье», его содержание и критерии. Основы здорового образа жизни студента. Роль физической культуры в обеспечении здоровья. Здоровый образ жизни и его составляющие. Личное отношение к здоровью как условие формирования здорового образа жизни. Образ жизни студентов и его влияние на здоровье. Основные требования к организации

		здорового образа жизни (ЗОЖ). Взаимосвязь общей культуры студента и его образа жизни. Структура жизнедеятельности студентов и ее отражение в образе жизни. Основные требования к организации здорового образа жизни. Физическое самовоспитание и самосовершенствование в здоровом образе жизни.
5	Тема 5. Лечебная Физическая культура и спорт как средство профилактики и реабилитации при различных заболеваниях.	Значение лечебной физической культуры. Клинико-физиологическое обоснование и механизмы лечебного действия физических упражнений. Средства лечебной физической культуры. Классификация и характеристика физических упражнений. Методика лечебного применения физических упражнений. Дозировка. Формы лечебной физической культуры. Лечебная физическая культура при заболеваниях сердечно-сосудистой системы. Механизмы лечебного действия физических упражнений при заболеваниях сердечно-сосудистой системы. Показания и противопоказания к применению лечебной физической культуры при заболеваниях сердечно-сосудистой системы. Роль физических упражнений в профилактике заболеваний сердечно-сосудистой системы. Лечебная физкультура при заболеваниях органов дыхания Механизмы лечебного действия физических упражнений при заболеваниях органов дыхания. Лечебная физкультура при заболеваниях органов пищеварения и нарушениях обмена веществ. Механизмы лечебного действия физических упражнений при заболеваниях органов пищеварения и нарушениях обмена веществ. Основы методики лечебной физкультуры органов пищеварения и нарушениях обмена веществ.
6	Тема 6. Психофизиологические основы учебного труда и интеллектуальной деятельности. Средства физической культуры в регулировании работоспособности.	Основные понятия. Работоспособность в умственном труде и влияние на нее внешних и внутренних факторов. Влияние периодичности ритмических процессов в организме на работоспособность студентов. Общие закономерности изменения работоспособности студентов в процессе обучения. Работоспособность студентов в период экзаменационной сессии. Здоровье и работоспособность студентов. Заболеваемость студентов в период учебы и ее профилактика. Средства физической культуры в регулировании умственной работоспособности, психоэмоционального и функционального состояния студентов. Физические упражнения как средство активного отдыха. Основные причины изменения состояния студентов в период

		экзаменационной сессии, критерии нервно-эмоционального и психофизического утомления. Особенности использованию средств физической культуры для оптимизации работоспособности, профилактики нервно-эмоционального и психофизического утомления студентов, повышения эффективности учебного труда.
7	Тема 7. Физическая подготовка в системе физического воспитания.	Характеристика физической подготовки студентов. Воспитание физических качеств. Формирование психических качеств в процессе физического воспитания. Общая физическая подготовка. Специальная физическая подготовка, цели и задачи. Спортивная подготовка. Структура подготовленности спортсмен. Зоны и интенсивность физических нагрузок. Значения мышечной релаксации. Возможность и условия коррекции физического развития, телосложения, двигательной и функциональной подготовленности средствами физической культуры и спорта в студенческом возрасте. Формы занятий физическими упражнениями. Учебно-тренировочное занятие как основная формы обучения физическим упражнениям. Структура и направленность учебно-тренировочного занятия.
8	Тема 8. Спорт. Классификация видов спорта. Особенности занятий индивидуальным видом спорта или системой физических упражнений.	Спорт. Многообразие видов спорта. Классификация. Краткая характеристика некоторых видов спорта. Особенности занятий избранным видом спорта или системой физических упражнений. Влияние избранного вида спорта или системы физических упражнений на физическое развитие, функциональную подготовленность и психические качества. Пути достижения физической, технической, тактической и психической подготовленности. Модельные характеристики спортсмена высокого класса. Планирование тренировки в избранном виде спорта или системе физических упражнений. Виды и методы контроля за эффективностью тренировочных занятий. Специальные зачетные требования и нормативы по годам (семестрам) обучения студентов. Система студенческих спортивных соревнований. Требования спортивной классификации и правил соревнований по избранному виду спорта. Спорт. Индивидуальный выбор видов спорта или систем физических упражнений. Студенческий спорт. Его организационные особенности. Олимпийские игры и Универсиады. Участие в спортивных соревнованиях.
9	Тема 9. Современные оздоровительные системы	Основные понятия и характеристика современных оздоровительных технологий. Их классификация.

	физических упражнений.	Требования. Современные оздоровительные системы:- атлетическая гимнастика, спортивная аэробика, гидроаэробика, стрейтчинг, шейпинг, калланетика, изотон, бодифлекс, велнес и др., системы дыхательной гимнастики оздоровительная методика фитнеса. Классификация фитнес программ по функциональной направленности.
10	Тема 10. Методические основы самостоятельных занятий физическими упражнениями.	Мотивация и целенаправленность самостоятельных занятий. Формы и содержание самостоятельных занятий. Организация самостоятельных занятий физическими упражнениями различной направленности. Характер содержания занятий в зависимости от возраста. Особенности самостоятельных занятий для студентов. Планирование и управление самостоятельными занятиями. Взаимосвязь между интенсивностью нагрузок и уровнем физической подготовленности. Гигиена самостоятельных занятий. Самоконтроль за эффективностью самостоятельных занятий.
11	Тема 11. Профессионально-прикладная физическая подготовка студентов. Физическая культура и спорт в профессиональной деятельности специалиста.	Личная и социально-экономическая необходимость специальной психофизической подготовки человека к труду. Определение понятия «профессионально-прикладная физическая подготовка» (ППФП), ее цели, задачи, средства. Место ППФП в системе физического воспитания студентов. Факторы, определяющие конкретное содержание ППФП. Особенности форм и подбора средств ППФП студентов, отнесенных к специальной медицинской группе. Понятие производственная физическая культура, ее содержание и составляющие. Роль нетрадиционной гимнастики в профессиональной деятельности специалиста. Особенности выбора форм, методов и средств физической культуры и спорта в рабочее и свободное время специалистов. Профилактика профессиональных заболеваний и травматизма средствами физической культуры. Влияние индивидуальных особенностей, географо-климатических условий и других факторов на содержание физической культуры специалистов. Роль будущих специалистов по внедрению физической культуры в производственный коллектив.
12	Тема 12. Основы судейства соревнований базовых видов спорта.	Виды физкультурно-спортивных массовых мероприятий и их значение. Цели, задачи, принципы, особенности организации и проведения физкультурно-спортивных массовых мероприятий. Правила поведения болельщиков на соревнованиях. Обязанности судейской бригады. Характеристика видов деятельности.

		Положения о соревнованиях.

6. Рекомендуемая тематика учебных занятий в форме контактной работы

Рекомендуемая тематика учебных занятий *лекционного* типа (предусматривающих преимущественную передачу учебной информации преподавателями):

№	Наименование раздела	Тема лекции
1	Тема 1. Физическая культура и спорт в общекультурной и профессиональной подготовке студентов.	Лекция 1. Физическая культура и спорт в общекультурной и профессиональной подготовке студентов.
2	Тема 2. Универсиады. История комплексов ГТО и БГТО. Новый Всероссийский физкультурно-спортивный комплекс.	Лекция 2. Универсиады. История комплексов ГТО и БГТО. Новый Всероссийский физкультурно-спортивный комплекс.
3	Тема 3. Социально-биологические основы физической культуры.	Лекция 3. Социально-биологические основы физической культуры.
4	Тема 4. Основы здорового образа жизни студента.	Лекция 4. Основы здорового образа жизни студента.
5	Тема 5. Лечебная Физическая культура и спорт как средство профилактики и реабилитации при различных заболеваниях.	Лекция 5. Лечебная Физическая культура и спорт как средство профилактики и реабилитации при различных заболеваниях.
6	Тема 6. Психофизиологические основы учебного труда и интеллектуальной деятельности. Средства физической культуры в регулировании работоспособности.	Лекция 6. Психофизиологические основы учебного труда и интеллектуальной деятельности. Средства физической культуры в регулировании работоспособности.
7	Тема 7. Физическая подготовка в системе физического воспитания.	Лекция 7. Физическая подготовка в системе физического воспитания.
8	Тема 8. Спорт. Классификация видов спорта. Особенности занятий индивидуальным видом спорта или системой физических	Лекция 8. Спорт. Классификация видов спорта. Особенности занятий индивидуальным видом спорта или системой физических упражнений.

	упражнений.	
9	Тема 9. Современные оздоровительные системы физических упражнений.	Лекция 9. Современные оздоровительные системы физических упражнений.
10	Тема 10. Методические основы самостоятельных занятий физическими упражнениями.	Лекция 10. Методические основы самостоятельных занятий физическими упражнениями.
11	Тема 11. Профессионально-прикладная физическая подготовка студентов. Физическая культура и спорт в профессиональной деятельности специалиста.	Лекция 11. Профессионально-прикладная физическая подготовка студентов. Физическая культура и спорт в профессиональной деятельности специалиста.
12	Тема 12. Основы судейства соревнований базовых видов спорта.	Лекция 12. Основы судейства соревнований базовых видов спорта.

Рекомендуемая тематика *практических* занятий:

№ п/п	Наименование темы	Содержание темы занятия
1.	Тема 6. Психофизиологические основы учебного труда и интеллектуальной деятельности. Средства физической культуры в регулировании работоспособности.	Комплексы упражнений для регулирования работоспособности с учетом учебной и интеллектуальной деятельности. Средства физической культуры для профилактики утомления, связанного с учебной и интеллектуальной деятельностью.
2.	Тема 7. Физическая подготовка в системе физического воспитания.	Двигательная и функциональная подготовленности средствами физической культуры и спорта в студенческом возрасте. Основы совершенствования двигательных действий и воспитание физических качеств средствами ОФП Формирование психических качеств в процессе физического воспитания студентов. Упражнения на воспитание выносливости, координации, силы, быстроты, гибкости: Общеразвивающие упражнений, упражнения с предметами, упражнения в парах, упражнения с отягощениями, собственным весом. Комплекс разминки для сдачи упражнений ВФСК ГТО.
3.	Тема 8. Спорт. Классификация видов спорта. Особенности занятий индивидуальным видом спорта или системой физических упражнений.	Легкая атлетика. Обучение и совершенствование техники легкоатлетических упражнений. Упражнения на воспитание выносливости: Бег и разновидности ходьбы на средние длинные дистанции. Обучение технике бега

		по дистанции: беговой цикл, постановка стопы, работа рук, дыхание. Кроссовая подготовка. Техника бега по дистанции, обгон, преодоление препятствий. Развитие общей и специальной выносливости (равномерный, переменный, повторный бег) Упражнения на воспитание скоростных качеств и координации: совершенствование двигательных реакций на различные сигналы, старты из различных исходных положений, ускорения, бег на короткие дистанции, обучение технике высокого и низкого старта и стартового ускорения, финиширования. Техника бега по дистанции. Челночный бег. Скоростно-силовые упражнения: техника прыжков и метаний. Спортивные игры. Подвижные игры и эстафеты. Основы спортивных игр. Правила соревнований. Подвижные игры на внимание, координацию, скорость и точность выполнения команд. Эстафетный бег: техника передачи и приема эстафетной палочки на месте и в движении, техника эстафетного бега по дистанции. Эстафеты с предметами и без, различные способы передвижений, преодоления препятствий. Способы передвижения и преодоления препятствий в командной эстафете. Передвижения с предметами, партнером. Преодоление препятствий, движение по заданной траектории. Выполнение заданий на станциях эстафеты.
4.	Тема 9. Современные оздоровительные системы физических упражнений.	Гимнастика. Техника гимнастических упражнений на развитие силы, координации и гибкости. Дыхательные упражнения, упражнения в расслаблении. Комплекс упражнений оздоровительной гимнастики с предметами (гимнастическая палка, мяч, скакалка, гантели, медицинболлы) Комплекс упражнений утренней гимнастики. Комплекс упражнений производственной гимнастики. Комплекс упражнений на растягивание и восстановление.
5.	Тема 10. Методические основы самостоятельных занятий физическими упражнениями.	Методика составление комплексов упражнений оздоровительной направленности. Терминология, основные принципы построения. Примеры. Показ комплексов.
6.	Тема 11. Профессионально-	Методика составление комплексов

	прикладная физическая подготовка студентов. Физическая культура и спорт в профессиональной деятельности специалиста.	упражнений профессионально-прикладной направленности. Особенности будущей профессиональной деятельности, профилактика профессиональных заболеваний средствами физической культуры. основные принципы построения. Примеры. Показ комплексов.

Требования к самостоятельной работе обучающихся

1. Работа с лекционным материалом, предусматривающая проработку конспекта лекций и учебной литературы.

2.

№ п/п	Наименование темы	Тематика самостоятельной работы
1.	Методические основы самостоятельных занятий физическими упражнениями.	Составление комплекса упражнений оздоровительной направленности.
2.	Профессионально-прикладная физическая подготовка студентов. Физическая культура и спорт в профессиональной деятельности специалиста.	Составление комплекса упражнений производственной гимнастики.

Руководствуясь положениями статьи 47 и статьи 48 Федерального закона от 29 декабря 2012 г. N 273-ФЗ «Об образовании в Российской Федерации» научно-педагогические работники и иные лица, привлекаемые университетом к реализации данной образовательной программы, пользуются предоставленными академическими правами и свободами в части свободы преподавания, свободы от вмешательства в профессиональную деятельность; свободы выбора и использования педагогически обоснованных форм, средств, методов обучения и воспитания; права на творческую инициативу, разработку и применение авторских программ и методов обучения и воспитания в пределах реализуемой образовательной программы и отдельной дисциплины.

Исходя из рамок, установленных учебным планом по трудоемкости и видам учебной работы по дисциплине, преподаватель самостоятельно выбирает тематику занятий по формам и количеству часов проведения контактной работы: лекции и иные учебные занятия, предусматривающие преимущественную передачу учебной информации преподавателем и (или) занятия семинарского типа (семинары, практические занятия, практикумы, лабораторные работы, коллоквиумы и иные аналогичные занятия), и (или) групповые консультации, и (или) индивидуальную работу обучающихся с преподавателем, в том числе индивидуальные консультации (по курсовым работам/проектам – при наличии курсовой работы/проекта по данной дисциплине в учебном плане).

Рекомендуемая тематика занятий максимально полно реализуется в контактной работе с обучающимися очной формы обучения. В случае реализации образовательной программы в заочной / очно-заочной форме трудоемкость дисциплины сохраняется, однако объем учебного материала в значительной части осваивается обучающимися в форме самостоятельной работы. При этом требования к ожидаемым образовательным результатам обучающихся по данной дисциплине не зависят от формы реализации образовательной программы.

7. Методические рекомендации по видам занятий

Лекционные занятия.

В ходе лекционных занятий обучающимся рекомендуется выполнять следующие действия. Вести конспектирование учебного материала. Обращать внимание на категории, формулировки, раскрывающие содержание тех или иных явлений и процессов, научные выводы и практические рекомендации по их применению. Задавать преподавателю уточняющие вопросы с целью уяснения теоретических положений, разрешения спорных ситуаций.

Желательно оставить в рабочих конспектах поля, на которых во внеаудиторное время можно сделать пометки из рекомендованной литературы, дополняющие материал прослушанной лекции, а также подчеркивающие особую важность тех или иных теоретических положений.

Практические и семинарские занятия.

На практических и семинарских занятиях в зависимости от темы занятия выполняется поиск информации по решению проблем, практические упражнения, контрольные работы, выработка индивидуальных или групповых решений, итоговое обсуждение с обменом знаниями, участие в круглых столах, разбор конкретных ситуаций, командная работа, представление портфолио и т.п.

Самостоятельная работа.

Самостоятельная работа осуществляется в виде изучения литературы, эмпирических данных по публикациям и конкретных ситуаций из практики, подготовке индивидуальных работ, работа с лекционным материалом, самостоятельное изучение отдельных тем дисциплины; поиск и обзор литературы и электронных источников; чтение и изучение учебника и учебных пособий.

8. Фонд оценочных средств

8.1. Перечень компетенций с указанием этапов их формирования в процессе освоения образовательной программы в рамках учебной дисциплины

Основными этапами формирования указанных компетенций при изучении обучающимися дисциплины являются последовательное изучение содержательно связанных между собой тем учебных занятий. Изучение каждой темы предполагает овладение обучающимися необходимыми компетенциями. Результат аттестации обучающихся на различных этапах формирования компетенций показывает уровень освоения компетенций.

Контролируемые модули, разделы (темы) дисциплины	**Индекс контролируемой компетенции (или ее части)**	**Оценочные средства по этапам формирования компетенций**			**Способ контроля**
		текущий контроль по дисциплине	**рубежный контроль по дисциплине**	**итоговый контроль по дисциплине**	
Тема 1. Физическая культура и спорт в общекультурной и профессиональной подготовке студентов.	УК - 7	1. Посещение лекций по дисциплине и/или прохождение	Тестирование	Тестирование	МООК (портал Stepik) Тестирование ФП

Тема 2. Универсиады. История комплексов ГТО и БГТО. Новый Всероссийский физкультурно-спортивный комплекс.		Онлайн-курсов, подтвержденное сертификатом 2.Учебные проекты 3. Тесты по темам теоретического раздела программы STEPIK			
Тема 3. Социально-биологические основы физической культуры.					
Тема 4. Основы здорового образа жизни студента.					
Тема 5. Лечебная Физическая культура и спорт как средство профилактики и реабилитации при различных заболеваниях.					
Тема 6. Психофизиологические основы учебного труда и интеллектуальной деятельности. Средства физической культуры в регулировании работоспособности.					
Тема 7. Физическая подготовка в системе физического воспитания.					
Тема 8. Спорт. Классификация видов спорта. Особенности занятий индивидуальным видом спорта или системой физических упражнений.					
Тема 9. Современные оздоровительные системы физических упражнений.					
Тема 10. Методические основы самостоятельных занятий физическими упражнениями.					
Тема 11. Профессионально-прикладная физическая подготовка студентов. Физическая культура и спорт в профессиональной					

деятельности специалиста.					
Тема 12. Основы судейства соревнований базовых видов спорта.					

8.2. Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений и навыков и (или) опыта деятельности процессе текущего контроля

Тестовые задания

Целью тестирования является закрепление, углубление и систематизация знаний студентов, полученных на лекциях и в процессе самостоятельной работы; проведение тестирования позволяет ускорить контроль за усвоением знаний и объективизировать процедуру оценки знаний студента.

Примерные тестовые задания

1. Вид культуры, специфический результат деятельности, средство и способ физического совершенствования людей и выполнения ими свои социальных обязанностей в обществе – это …
   а) Физическая культура и спорт;
   б) социология;
   в) спортивная культура;
   г) социология физической культуры;
   д) культура знаний по физическому воспитанию.

2. Педагогический процесс, направленный на системное освоение рациональных способов управления своими движениями, приобретение необходимых двигательных навыков, умений, а так же связанных с этим процессом знаний, называется…

   а) физическим воспитанием;
   б) физическим развитием;
   в) физической культурой;
   г) обучение движениям;
   д) физической рекреацией.

3. Спорт, обусловленный коммерческими интересами и являющийся источником существования спортсменов – это спорт …

   а) олимпийский;
   б) адаптивный;
   в) массовый;
   г) профессиональный;
   д) любительский.

4. Физическая культура и спорт в форме физических упражнений эффективно формирует необходимые …

а) умения и навыки;
б) физические способности;
в) оптимизирование состояния здоровья и работоспособности;
г) физические качества;
д) все ответы правильные.

5. К основным составляющим ЗОЖ относят: 1) режим труда и отдыха; 2) организацию сна; 3) режим питания; 4) организацию двигательной активности; 5) выполнение требований санитарии и гигиены; 6) профилактику вредных привычек; 7) занятие спортом.Выбери правильный ответ.
   а) 1, 2, 3, 4, 5, 6;
   б) 1, 3, 4, 6, 7;
   в) 1, 2, 4 ,5, 6;
   г) 2, 3, 4, 5, 6, 7;
   д) 1, 2, 3, 4, 6, 7.

6. После прохождения медицинского обследования студенты распределяются по следующим медицинским группам:

   а) основная, подготовительная, специальная;
   б) основная, специальная, лечебная;
   в) подготовительная, основная, спортивная;
   г) спортивная, специальная, подготовительная;
   д) спортивная, основная, специальная.

7. Процесс развития двигательных качеств и приобретения двигательных навыков это:

   а) физическое развитие;
   б) физическое воспитание;
   в) Физическая культура и спорт;
   г) комплекс физических упражнений;

8. К циклическим упражнениям относится

   а) спортивные игры;
   б) бокс;
   в) езда на велосипеде;
   г) прыжки в высоту;
   д) фигурное катание.

9. К ациклическим упражнениям относится:

   а) бег;
   б) плавание;
   в) езда на велосипеде;
   г) гребля;
   д) спортивные игры.

10. Физическим качеством человека не является

    а) сила;
    б) быстрота;
    в) ловкость;

г) уравновешенность;
д) выносливость.

11. Основатель отечественной системы физического образования:

а) П.Ф. Лесгафт;
б) Л.П. Матвеев;
в) М.В. Ломоносов;
г) Пьер де Кубертен;
д) С.П. Евсеев.

12. Выносливость – это способность:
а) человека выполнять упражнение с максимальным усилием;
б) организма противостоять внешним воздействиям окружающей среды;
в) организма быстро восстанавливаться после физических упражнений;
г) организма противостоять утомлению;
д) человека быстро приспосабливаться к различным видам деятельности.

13. Быстрота – это способность человека выполнять:
а) движения с минимальным усилием;
б) движения с максимальной амплитудой;
в) движения в минимальный промежуток времени;
г) движения в максимальный промежуток времени;
д) движения с максимальным усилием.

14. Гибкость – это способность человека выполнять:
а) движения с максимальной скоростью;
б) движения с максимальным усилием;
в) сложнокоординационные движения;
г) движения с большой амплитудой;
д) движения с минимальной затратой времени.

Практический раздел реализуется в виде учебно-тренировочных, методико – практических занятий. Критерием успешности освоения учебного материала являются тесты физической подготовленности для основной и подготовительной групп (Приложение 1), для специальной медицинской группы (Приложение 2).

Студенты, временно освобожденные по состоянию здоровья, выполняют индивидуальные проектные задания по темам:

1. Анкета студента 2 курса 4 функциональной группы.
2. Формы самостоятельных занятий физическими упражнениями. Утренняя гигиеническая гимнастика**.**
3. Организация соревнований по спортивным играм по круговой системе.

8.3. Перечень вопросов и заданий для промежуточной аттестации по дисциплине

Промежуточной формой контроля знаний, умений и навыков по дисциплине «Физическая культура и спорт» является зачет. Условием получения зачета является

оценки четырех блоков: практического, теоретического, физической подготовленности, в которых учитывается наличие медицинского осмотра, регулярность посещения занятий по расписанию, знание теоретического материала программы, достаточный уровень физической подготовленности и функционального состояния, участие в соревнованиях, научно-исследовательская деятельность.

Особенностью преподавания данной дисциплины является необходимость учета физиологических процессов организма обучающегося, поэтому важное значение имеет регулярность и систематичность занятий семестре. В итоговый показатель практического блока вводится количественная оценка за посещаемость занятий, которая выражается в величине 1 единица за учебное занятие. В конце каждого семестра, студент выполняет контрольные упражнения - задания. А также может получить бонусные баллы. (Положение бально -рейтингой оценки учебных достижений обучающихся в БФУ им.И.Канта)

8.4. Планируемые уровни сформированности компетенций обучающихся и критерии оценивания

Уровни	Содержательное описание уровня	Основные признаки выделения уровня (этапы формирования компетенции, критерии оценки сформированности)	Пятибалльная шкала (академическая) оценка	Двухбалльная шакала, зачет	БРС, % освоения (рейтинговая оценка)
Повышенный	Творческая деятельность	*Включает нижестоящий уровень.* Умение самостоятельно принимать решение, решать проблему/задачу теоретического и прикладного характера на основе изученных методов, приемов, технологий	отлично	зачтено	86-100
Базовый	Применение знаний и умений в более широких контекстах учебной и профессиональной деятельности, нежели по образцу с большей	*Включает нижестоящий уровень.* Способность собирать, систематизировать, анализировать и грамотно использовать информацию из самостоятельно найденных теоретических источников и иллюстрировать ими теоретические	хорошо		71-85

	степени самостоятельности и инициативы	положения или обосновывать практику применения			
Удовлетворительный (достаточный)	Репродуктивная деятельность	Изложение в пределах задач курса теоретически и практически контролируемого материала	удовлетворительно		55-70
Недостаточный	Отсутствие признаков удовлетворительного уровня		неудовлетворительно	не зачтено	Менее 55

9. Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины.

Основная литература

1.Чертов, Н. В. Физическая культура : учебное пособие / Н. В. Чертов. - Ростов-на-Дону : Издательство ЮФУ, 2012. - 118 с. - ISBN 978-5-9275-0896-9. - Текст : электронный. - URL: https://znanium.com/catalog/product/551007 (дата обращения: 29.03.2022). – Режим доступа: по подписке.

Дополнительная литература

1.Булгакова, Н. Ж. Теория и методика плавания [Электронный ресурс]: учеб. для высш. проф. образования/ Н. Ж. Булгакова, О. И. Попов, Е. А. Распопова ; под ред. Н. Ж. Булгаковой. - 2-е изд., стер.. - Москва: Академия, 2014. - 1 эл. опт. диск (CD-ROM), 318, [1] с.: ил.. - Библиогр. в конце гл... Имеются экземпляры в отделах: ЭБС Кантиана(1)

2.Петров, П. К. Информационные технологии в физической культуре и спорте [Электронный ресурс]: учебник/ П. К. Петров. - 4-е изд., стер.. - Москва: Академия, 2014. - 1 эл. опт. диск (CD-ROM), 288 с.: рис.. - (Высшее образование - бакалавриат). - Библиогр.: с. 278-283 (80 назв.). - Лицензия до 31.12.2020 г.. Имеются экземпляры в отделах: ЭБС Кантиана(1)

10. Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины (модуля).

- НЭБ Национальная электронная библиотека, диссертации и прочие издания
- eLIBRARY.RU Научная электронная библиотека, книги, статьи, тезисы докладов конференций
- Гребенников Электронная библиотека ИД журналы
- ЭБС Лань книги, журналы
- ЭБС Консультант студента
- ПРОСПЕКТ ЭБС
- ЭБС ZNANIUM.COM
- РГБ Информационное обслуживание по МБА
- БЕН РАН
- Электронно-библиотечная система (ЭБС) Кантитана (https://elib.kantiana.ru/)

11. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине.

Программное обеспечение обучения включает в себя:

- система электронного образовательного контента БФУ им. И. Канта – www.lms-3.kantiana.ru, обеспечивающую разработку и комплексное использование электронных образовательных ресурсов;
- серверное программное обеспечение, необходимое для функционирования сервера и связи с системой электронного обучения через Интернет;
- корпоративная платформа Microsoft Teams;
- установленное на рабочих местах обучающихся ПО: Microsoft Windows 7, Microsoft Office Standart 2010, антивирусное программное обеспечение Kaspersky Endpoint Security.
- специализированное ПО не требуется.

12. Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине.

Для осуществления образовательного процесса по дисциплине «Физическая культура и спорт» необходимо соответствующий аудиторных фонд и материально-спортивная база, которая продуктивно развивается в БФУ им. И. Канта. Учебные аудитории оснащены мультимедийным оборудованием, которые используются для лекционных и методико-практических занятий. К материально-техническому обеспечению относим также используемые мультимедийные средства обучения: электронные презентации к лекциям, иллюстрированные упражнения тестового типа, комплект дополнительных структурно-логических схем.

Характеристика материально-технического обеспечения практических занятий «Физическая культура и спорт»:

Материально- спортивная база	Обеспечение учебного процесса по дисциплине «Физическая культура и спорт»
Учебные аудитории в корпусах Институтов БФУ им. И. Канта	Мультимедийное оборудование, доска, компьютер.
Учебно-физкультурный корпус с бассейном, Корпус №22 236000 Калининградская область. г. Калининград ул. А. Невского, 14 Бассейн, Фитнес-зал, Тренажерный зал.	Бассейн: плавательные доски, плавательные ласты, нудлы, плавательные лопатки, Электронное табло, настенный секундомер, колобашки. Раздевалки. Фитнес – зал: Степы, Гимнастические палки, Гимнастические мячи, металлические обручи, коврики гимнастические, гантели 9 кг, 1,5 кг,3 кг, 2 кг, утяжелители для рук- ног 1,5, утяжелители для рук-ног 3 кг., скакалки, мини степы, гимнастические маты. Музыкальный центр.
Физкультурно-оздоровительный комплекс, корпус №9 Калининградская область. г. Калининград ул. А. Невского, 14	Гимнастические маты, баскетбольные щиты, волейбольные стойки, волейбольная сетка с креплениями, гимнастические палки, баскетбольные мячи, волейбольные мячи, ракетки для бадминтона, воланы. медицинболы, скакалки, раздевалки для мужчин и

	женщин, гимнастические скамейки,
Корпус №4 спортивный зал № 2236000 Калининградская обл., г. Калининград ул. Чернышевского, 56А	Гимнастические скамейки, гимнастические маты, шведская стенка, фишки, гимнастические палки деревянные, гимнастические палки пластиковые, скакалки, ракетки для бадминтона, воланы, теннисные мячи, волейбольные мячи, баскетбольные мячи, музыкальный центр, коврики гимнастические, медицинболы. Баскетбольные щиты, волейбольные стойки и сетка.
Спортивный зал №1 236000 Калининградская обл., г. Калининград ул. Чернышевского, 56А	Борцовский ковер, гимнастические маты, гимнастические брусья, бревно гимнастическое напольное, гимнастическое бревно постоянной высоты, мостик гимнастический пружинный, перекладина гимнастическая, брусья гимнастические разновысокие, конь гимнастический маховый, козел гимнастический, гимнастические скамейки, шведские стенки, зеркала, скакалки, теннисные мячи, гимнастические палки, обручи, медицинболы.
Корпус №15 236000 Калининградская обл., г. Калининград Адрес: ул. Соммера, 23.	Зал аэробики: степы, металлические обручи, гимнастические палки, гантели 1 кг, гимнастические мячи, музыкальный центр, гимнастические скамейки, коврики гимнастические.
Корпус № 15 Тренажерный зал 236000 Калининградская обл., г. Калининград Адрес: ул. Соммера, 23.	Кардиотренажеры, блочные тренажеры, рычажные , тренажер с собственным весом, Велотренажеры, железные блины 5, 10,15,20,25кг.; гантели от 1 кг – 3 кг.; резиновые блины 10, 15, 20,50 кг., гири.
Стадион «Кантиана» 236000 Калининградская обл., г. Калининград Адрес: ул. Озерова,57.	Беговые дорожки, сектор для прыжков, сектор для метаний, футбольное поле, футбольные мячи,
Учебная аудитория №125 236000 Калининградская обл., г. Калининград Адрес: ул. Озерова,57.	Плазменный телевизор Кафедра с персональным компьютером с LCD – монитором с сенсорным экраном Программы Microsoft Office 2007 или 2010: – MS Office Power Point, – MS Office Word, – MS Office Excel, – MS Internet Explorer (или любой другой Интернет-браузер).

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
федеральное государственное автономное образовательное учреждение высшего образования «Балтийский федеральный университет имени Иммануила Канта»
Институт физико-математических наук и информационных технологий

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

«История (история России, всеобщая история)»

Шифр: 10.05.01
Специальность: «Компьютерная безопасность»
Специализация: «Математические методы защиты информации»
Квалификация (степень) выпускника: специалист по защите информации

Калининград
2022

Лист согласования

Составитель: Жданович Людмила Николаевна, к.и.н., доцент

Рабочая программа утверждена на заседании учебно-методического совета института физико-математических наук и информационных технологий

Протокол № 01/22 от «01» февраля 2022 г.

Председатель учебно-методического
совета института физико-
математических наук и информационных
технологий

Первый заместитель директора Шпилевой А. А
ИФМНиИТ, к. ф.-м. н., доцент

Ведущий менеджер Е.П.Ставицкая

Содержание

1.Наименование дисциплины: «История (история России, всеобщая история)».

Целью освоения дисциплины «История (история России, всеобщая история)» является формирование систематизированных знаний об основных закономерностях и особенностях всемирно-исторического процесса, целостной картины отечественной и мировой истории, учитывающей взаимосвязь всех ее этапов, их значимость для понимания современного места и роли России в мире.

2. Перечень планируемых результатов обучения по дисциплине, соотнесенных с планируемыми результатами освоения образовательной программы

Код компетенции	Результаты освоения образовательной программы (ИДК)	Результаты обучения по дисциплине
ОПК-17. Способен анализировать основные этапы и закономерности исторического развития России, ее место и роль в контексте всеобщей истории, в том числе для формирования гражданской позиции и развития патриотизма.	ОПК-17.1. Знает базовые принципы исторической науки; видеть причинно-следственные связи; основные этапы и закономерности исторического развития России; понимать историческое своеобразие нашей страны. ОПК-17.2. Способен оценивать место и роль страны в современном мире, грамотно проводить исторические параллели. ОПК-17.3. Владеет методом анализа исторических закономерностей.	Знать: - важнейшие понятия и термины, основные события, явления и процессы отечественной и мировой истории; -ключевые методологические, исторические и источниковедческие проблемы отечественной истории; - признаки и характеристики, изучаемых в курсе политических, социальных, культурных процессов и явлений, связанных с отечественной и мировой историей; Уметь: - уметь ориентироваться в историческом и этнокультурном пространстве мировой истории; - использовать полученные знания для формирования собственной гражданской позиции и толерантно воспринимать социальные, этнические, конфессиональные и культурные различия; Владеть: - навыками ведения научной полемики; - методами критического анализа исторической информации;

3. Место дисциплины в структуре образовательной программы

Дисциплина «История (история России, всеобщая история)» относится к обязательной части Блока 1 Дисциплины (модули), входит в Модуль 1. Модуль общекультурных компетенций.

4. Виды учебной работы по дисциплине.

Виды учебной работы по дисциплине зафиксированы учебным планом основной профессиональной образовательной программы по указанному направлению и профилю, выражаются в академических часах. Часы контактной работы и самостоятельной работы обучающегося и часы, отводимые на процедуры контроля, могут различаться в учебных планах ОПОП по формам обучения. Объем контактной работы включает часы контактной аудиторной работы (лекции/практические занятия/ лабораторные работы), контактной внеаудиторной работы (контроль самостоятельной работы), часы контактной работы в период аттестации. Контактная работа, в том числе может проводиться посредством электронной информационно-образовательной среды университета с использованием ресурсов сети Интернет и дистанционных технологий

5. Содержание дисциплины, структурированное по темам (разделам)

Исходя из рамок, установленных учебным планом по трудоемкости и видам учебной работы по дисциплине, преподаватель самостоятельно выбирает тематику занятий по формам и количеству часов проведения контактной работы: лекции и иные учебные занятия, предусматривающие преимущественную передачу учебной информации преподавателем и (или) занятия семинарского типа (семинары, практические занятия, практикумы, лабораторные работы, коллоквиумы и иные аналогичные занятия), и (или) групповые консультации, и (или) индивидуальную работу обучающихся с преподавателем, в том числе индивидуальные консультации (по курсовым работам/проектам – при наличии курсовой работы/проекта по данной дисциплине в учебном плане). Рекомендуемая тематика занятий максимально полно реализуется в контактной работе с обучающимися очной формы обучения. В случае реализации образовательной программы в заочной / очно-заочной форме трудоемкость дисциплины сохраняется, однако объем учебного материала в значительной части осваивается обучающимися в форме самостоятельной работы. При этом требования к ожидаемым образовательным результатам обучающихся по данной дисциплине не зависят от формы реализации образовательной программы.

№	Наименование раздела	Содержание раздела
1	Раздел 1. История как наука.	Основы методологии исторической науки. Сущность, формы, функции исторического знания. Методы и источники изучения истории. Понятие и классификация исторического источника. Методология и теория исторической науки. Понятие истории России и его основные элементы (народ, территория, формы социальной общности). Связь отечественной истории с всеобщей историей. Мировой исторический процесс – единство и многообразие. Методология и теория исторической науки. История России - неотъемлемая часть всемирной истории. Главные особенности и факторы русского исторического процесса (природно-климатический, геополитический, религиозный, социальной организации). Общие сведения об историографии истории России. Ключевые проблемы курса

		истории России. Понятие и классификация исторического источника. Типы и виды источников. Роль вещественных, лингвистических и фольклорных источников в изучении истории России. Отечественная историография в прошлом и настоящем: общее и особенное.
2	Раздел 2. История России и мира в период древности и Средневековья.	Особенности становления государственности в России и мире. Древнейшие цивилизации человечества. Теории происхождения государства. Проблемы этногенеза и роль миграций в становлении народов. Восточный и античный типы цивилизационного развития. Древнейшие культуры Северной Евразии. Арии. Скифы. Древние империи Центральной Азии. Античное наследие в эпоху Великого переселения народов. Варварские королевства. Византийская империя. Проблема этногенеза восточных славян. Основные этапы становления государственности. Рождение варяжской теории, ее сторонники и противники. Современное состояние проблемы: вопрос о типологии древнерусского общества и государства. Вопрос о происхождении слова «Русь». Общий очерк образования Древнерусского государства. Политические институты Киевской Руси: формы правления и политическая система; центральные институты власти (киевский князь, дума – совет, специфика княжьего права в Киевской Руси). Вопрос о вече в Древней Руси. Роль церкви в политической системе Киевской Руси. Древняя Русь и кочевники. Византийско-древнерусские связи. Особенности социального строя Древней Руси. Этнокультурные и социально-политические процессы становления русской государственности. Принятие христианства. Международное положение Руси в начале XII века. Русские земли в XII - XV веках и европейское Средневековье. Общая характеристика политической раздробленности Руси домонгольского времени: сущность, причины и периодизация политической раздробленности. Средневековье как стадия исторического процесса в Западной Европе, на Востоке, России. Производственные отношения, политические системы, идеология и социальная психология. Роль религии и духовенства в средневековых обществах. Дискуссия о феодализме. Социально-политические изменения в русских землях в XIII в. Образование монгольской империи. Причины и направления монгольской экспансии. Социальная структура монголов. Русь и Орда: проблемы взаимовлияния. Монгольское нашествие на Русь. Масштабы разорения Руси. Иго и дискуссии о его роли в развитии Российского государства. Образование Золотой Орды и установление ее власти над Русью: система выдачи ярлыков, дань, повинности и система их сбора, баскаки. Политические, экономические и культурные последствия монгольского нашествия и золотоордынского ига. Борьба русского народа за безопасность западных границ. Россия в XVI – XVII веках в контексте развития европейской цивилизации. Россия и средневековые государства Европы и

		Азии. Эпоха Возрождения. Великие географические открытия. Эпоха Нового времени. Реформация. Первые буржуазные революции в Европе. Развитие капиталистических отношений. Торговый и мануфактурный капитализм. Абсолютизм в Европе. Восточные деспотии. Специфика формирования единого российского государства. Речь Посполитая. Возвышение Москвы. Характер и предпосылки объединения русских земель и княжеств. Борьба за Великое княжение Владимирское. Причины возвышения Москвы: вопрос о «выгоде» географического положения, роль внешнеполитических факторов. Роль церкви в возвышении Москвы. Иван Калита и политика его сыновей. Русь и Орда в 60-х – начале 80-х годов. Куликовская битва и ее историческое значение. Социально-экономические, внутриполитические и внешнеполитические условия развития единого Российского государства. Государственно-политический строй России в конце XV – начале XVI века. Усиление власти московских государей. Зарождение приказного управления. Судебник 1497 года. Начало оформления крепостного права в общегосударственном масштабе. Иван Грозный. Складывание сословно-представительной монархии. Опричнина. Основные направления внешней политики России в XVI веке. Присоединение Казани и Астрахани. Ливонская война. Политический кризис в России в начале XVII столетия. Смута и ее последствия. Земский собор 1613 года и начало правления Романовых. Территория и население страны в XVII веке. Развитие общественного разделения труда и рост товарного производства. Первые мануфактуры. Соборное уложение 1649 года. Завершение юридического оформления общегосударственной системы крепостного права и его значение в дальнейшей истории России. Усиление самодержавной власти, начало перехода к абсолютизму. Раскол, его социальная и идеологическая сущность. Конфликт государства и церкви. Причины массовых народных выступлений в «бунташном» столетии. Переяславская рада и воссоединение Украины с Россией. Русско-польская война 1654 – 1667 годов. Историческое значение воссоединения Украины с Россией.
3	Раздел 3. Отечественная и мировая история в период Нового и Новейшего времени.	Россия и мир в XVIII – XIX веках. XVIII век в европейской и мировой истории. Формирование колониальных империй. Первоначальное накопление капитала. Мануфактурное производство. Промышленный переворот в Европе и России: общее и особенное. Идеология Просвещения. Великая Французская революция и её влияние на развитие Европы. Американская революция и возникновения США. Предпосылки и особенности складывания российского абсолютизма. Личность Петра I, его роль в преобразованиях, в дипломатии, развитии военного искусства. Реформы Петра I. Превращение России в абсолютную монархию. Северная война и ее итоги. Формирование и развитие светской культуры, превращение ее в главное направление русской культуры. Век Екатерины II. Предпосылки и особенности складывания

		российского абсолютизма. «Просвещенный» абсолютизм в России, его сущность и особенности. Социальная политика и крепостническое законодательство. Крестьянская война под предводительством Е.И. Пугачева. Изменения во внутренней политике правительства. Развитие сословного строя, сословные дворянские организации и усиление власти дворянства на местах. Основные направления внешней политики Российской империи во второй половине XVIII века. Основные тенденции мирового развития в XIX веке. Европейский колониализм. Эпоха наполеоновских войн в Европе. Антифранцузские коалиции. Формирование национальных государств в Европе. Буржуазные революции середины XIX века. Секуляризация сознания. Романтизм. Реализм. Дарвинизм. Особенности и основные этапы экономического развития России. Личность Александра I и его ближайшее окружение. Политика правительства по крестьянскому вопросу. Реформа образования. Преобразование органов центрального управления. М.М. Сперанский, план преобразований и попытки его реализации. Отечественная война 1812 года и военные кампании 1813 – 1814 годов. Декабристы. Личность Николая I. Централизация и режим личной власти императора. Политика в области просвещения и печати. Восточный вопрос в 30 – 50-х годах. Крымская война 1853 – 1856 годов. Причины поражения России и последствия войны для нее. Эпоха Великих реформ (вторая половина XIX в.) Становление индустриального общества в России: общее и особенное. Общественная мысль и особенности общественного движения России XIX в. Революционные организации и кружки середины 60-х – начала 70-х годов. Цареубийство 1 марта 1881 года. Реформы и реформаторы в России. Отмена крепостного права. Реформы в области местного самоуправления: земская и городская. Состав и характер деятельности земских и городских выборных учреждений. Судебная реформа и судебные уставы 1864 года. Финансовые реформы. Реформы в области народного образования и печати. Цензурные правила. Военная реформа. Закон о всеобщей воинской повинности 1874 года. Соотношение буржуазных начал и крепостнических пережитков в реформах 60 – 70-х годов. Судьбы реформаторов. Русская культура XIX века и ее вклад в мировую культуру. Роль XX столетия в мировой истории. Глобализация общественных процессов. Проблема экономического роста и модернизации. Революции и реформы. Социальная трансформация общества. Столкновения тенденций интернационализма и национализма, интеграции и сепаратизма, демократии и авторитаризма. Объективная потребность в индустриальной модернизации России. Российские реформы в контексте общемирового развития в начале века. Россия в начале XX в. Николай II и его ближайшее окружение. Русско-японская война. Революция 1905 – 1907 годов. Изменения

		в государственном строе России после 17 октября 1905 года. Издание 23 апреля 1906 года «Основных государственных законов Российской империи» и их значение. Государственная дума в Российской империи. Основные политические партии и их программы. Сущность третьеиюньской политической системы. П.А. Столыпин как государственный деятель, его программа. Россия в Первой мировой войне. Экономическое и политическое положение России в годы войны. Кризис власти. Назревание политического кризиса к концу 1916 года. Февральская революция 1917 года. Отречение Николая II. Образование и состав Временного правительства. Складывание двоевластия. Политика Временного правительства. Большевики и их ориентация на развитие революции в условиях двоевластия. Кризисная ситуация в стране, углубление хозяйственной разрухи. Курс большевиков на вооруженный захват власти. Мятеж Корнилова. Провозглашение Российской республики. Демократическое совещание и создание Предпарламента. Создание третьего коалиционного правительства. Международные отношение на рубеже веков. Складывание военно-политических блоков. «Пробуждение Азии». Первая мировая война. Новая фаза европейского капитализма. Версальская система международных отношений. Октябрьское вооруженное восстание 1917 г. Первые декреты советской власти. Формирование Совета народных комиссаров во главе с В.И. Лениным. Создание Советского государства. Учредительное собрание и его судьба. Формирование однопартийного политического режима. Принятие первой советской Конституции. Гражданская война и иностранная интервенция. Основные этапы и решающие сражения. Экономические, социальные, демографические и политические последствия войны. Экономическая и социальная политика советской власти в годы Гражданской войны. Политика военного коммунизма. Российская эмиграция. Особенности международных отношений в межвоенный период. Лига Наций. Альтернативы развития западной цивилизации в 1920 – 1930-х годах. Социально-экономическое развитие Советской России и СССР в 1920-е голы. Ленинская концепция нэпа. X съезд РКП(б) и его решения. Социально-экономические противоречия и причины их углубления. Культурная жизнь страны в 20-е годы. Образование СССР. Внешняя политика. Национальный вопрос в программе большевиков. Проекты создания Советского многонационального государства, позиции лидеров (автономизация, федерация, конфедерация). I Всесоюзный съезд Советов. Декларация и Договор об образовании Союза ССР. Конституция СССР 1924 года. СССР в 30-е гг. Мировой экономический кризис 1929 г. Государственно-монополистический капитализм. Приход к власти фашистов в Германии. «Новый курс» Рузвельта. Дискуссия о тоталитаризме в современной научной литературе.

		Курс на строительство социализма в одной стране и его последствия. 1929 год - год «великого перелома». Социально-экономические преобразования в 30-е годы. Индустриализация в СССР. Коллективизация. Итоги индустриализации и коллективизации. Государственный аппарат. Конституция 1936 г. Усиление режима личной власти Сталина. Устранение политической оппозиции. Культ личности И.В. Сталина и тоталитарное государство. Вступление СССР в Лигу Наций. Фашизм и внешняя политика СССР. Война в Испании. Конфликт с Японией. Вторая мировая война: причины, этапы, итоги. СССР в годы Великой Отечественной войны и послевоенного развития: 1941-1953 гг. СССР накануне и в начальный период второй мировой войны. Народное хозяйство страны в годы третьей пятилетки. Социально-экономическое развитие, общественно-политическая жизнь, культура, внешняя политика СССР в послевоенные годы. Противоречивость общественной жизни страны. Меры по усилению режима личной власти Сталина. Политические процессы: «Ленинградское дело», «Дело врачей» и их жертвы. XIX съезд ВКП(б) и реформа высших партийных органов. Советский политический режим в последние годы жизни И.В. Сталина. Изменение соотношения сил в мире. Международные отношения в послевоенном мире. Крах колониальной системы. Новые международные организации. Трансформация капиталистической экономики. Развитие мировой экономики в 1945 – 1991 годах. Холодная война. Создание социалистического лагеря. Создание организации Варшавского договора. Достижение военного паритета между СССР и США. Трудности послевоенного переустройства: восстановление хозяйства. Ужесточение политического режима и идеологического контроля. Избрание Н.С. Хрущева первым секретарем ЦК КПСС. «Оттепель». XX съезд КПСС. Отставка Н.С. Хрущева. СССР в середине 60-х - 80-х годов: нарастание кризисных явлений. «Номенклатура» и «Застой» как явления советской бюрократической системы. «Неосталинизм». Попытки осуществления политических и экономических реформ. Реформы А.Н. Косыгина. Конституция 1977 г. Диспропорции в структуре единого народнохозяйственного комплекса страны. Советское общество в годы Перестройки: 1985-1991 гг. Приход к власти М.С. Горбачева. Перестройка и ее последствия. Изменения в государственном механизме СССР. Введение института президентской власти. Углубление противостояния общесоюзного центра и республиканских политических элит. Декларации республик о суверенитете. Провозглашение суверенитета РСФСР. Формирование массовых национальных движений - фронтов. Референдум 1991 года о судьбе Союза и позиция народа. Избрание Б.Н. Ельцина президентом РСФСР. Попытка государственного переворота 1991 г. и ее провал. Распад СССР. Беловежские соглашения. Образование СНГ.

		Многополярный мир в начале XXI века. Глобализация мирового, экономического и культурного пространства. Роль Российской Федерации в современно мировом сообществе. Становление новой российской государственности. Октябрьские события 1993 г. Ликвидация советской политической системы. Принятие Конституции РФ 12 декабря 1993 года. Россия на пути радикальной социально-экономической модернизации. Социальные последствия изменений в экономике страны. Социальные конфликты 90-х гг. Культура в современной России. Поиски новых духовных ориентиров. Положение конфессий в России. Внешнеполитическая деятельность в условиях новой геополитической ситуации. Расширение НАТО и ЕС на восток и проблема Калининградской области. Проблемы России в международной политике. Модернизация общественно-политических отношений. Социально-экономические отношения в начале XXI в. Региональные и глобальные интересы России на современном этапе.

6. Рекомендуемая тематика учебных занятий в форме контактной работы

Рекомендуемая тематика учебных занятий *лекционного* типа (предусматривающих преимущественную передачу учебной информации преподавателями):

№	Наименование раздела	Темы лекций
1	Раздел 1. История как наука.	Лекция 1. Основы методологии исторической науки.
2	Раздел 2. История России и мира в период древности и Средневековья.	Лекция 1. Особенности становления государственности в России и мире. Лекция 2. Русские земли в XII - XV веках и европейское Средневековье. Лекция 3. Россия в XVI – XVII веках в контексте развития европейской цивилизации.
3	Раздел 3. Отечественная и мировая история в период Нового и Новейшего времени.	Лекция 1. Россия и мир в XVIII – XIX веках. Лекция 2. Россия (СССР) и мир в первой половине XX века. Лекция 3. СССР и мир во второй половине XX века. Лекция 4. Россия и мир в XXI веке.

Рекомендуемая тематика *практических* занятий:

Тема 1. Социально-экономический и политический строй Киевской Руси по материалам Русской Правды

Тема 2. Древнерусская и европейская средневековая культура.

Тема 3. Крепостное право на Руси. История законодательства.

Тема 4. Петровские реформы и европейская модернизация.

Тема 5. «Восточный вопрос» в международной политике XIX века.

Тема 6. Реформы 60 – 70 – х гг. XIX века в России.

Тема 7. Россия в годы Первой мировой войны и революции.

Тема 8. Холодная война: причины, этапы, итоги.

На практических занятиях происходит обсуждение и изучение заявленных вопросов.

Требования к самостоятельной работе обучающихся

1. Работа с лекционным материалом, предусматривающая проработку конспекта лекций и учебной литературы, по следующим темам: Основы методологии исторической науки. Древнейшие цивилизации человечества. Особенности становления государственности в России и мире. Русские земли в XII - XV веках и европейское Средневековье. Россия в XVI – XVII веках в контексте развития европейской цивилизации. Россия и мир в XVIII – XIX веках. Россия (СССР) и мир в первой половине XX века. СССР и мир во второй половине XX века. Россия и мир в XXI веке.

2. Выполнение домашнего задания связано с подготовкой к темам практических занятий: Социально-экономический и политический строй Киевской Руси по материалам Русской Правды, Древнерусская и европейская средневековая культура, Крепостное право на Руси. История законодательства, Петровские реформы и европейская модернизация, «Восточный вопрос» в международной политике XIX века, Реформы 60 – 70 – х гг. XIX века в России, Россия в годы Первой мировой войны и революции, Индустриальная модернизация СССР в конце 1920-х – 1930-е годы, Холодная война: причины, этапы, итоги.

Руководствуясь положениями статьи 47 и статьи 48 Федерального закона от 29 декабря 2012 г. N 273-ФЗ «Об образовании в Российской Федерации» научно-педагогические работники и иные лица, привлекаемые университетом к реализации данной образовательной программы, пользуются предоставленными академическими правами и свободами в части свободы преподавания, свободы от вмешательства в профессиональную деятельность; свободы выбора и использования педагогически обоснованных форм, средств, методов обучения и воспитания; права на творческую инициативу, разработку и применение авторских программ и методов обучения и воспитания в пределах реализуемой образовательной программы и отдельной дисциплины.

Исходя из рамок, установленных учебным планом по трудоемкости и видам учебной работы по дисциплине, преподаватель самостоятельно выбирает тематику занятий по формам и количеству часов проведения контактной работы: лекции и иные учебные занятия, предусматривающие преимущественную передачу учебной информации преподавателем и (или) занятия семинарского типа (семинары, практические занятия, практикумы, лабораторные работы, коллоквиумы и иные аналогичные занятия), и (или) групповые консультации, и (или) индивидуальную работу обучающихся с преподавателем, в том числе индивидуальные консультации (по курсовым работам/проектам – при наличии курсовой работы/проекта по данной дисциплине в учебном плане).

Рекомендуемая тематика занятий максимально полно реализуется в контактной работе с обучающимися очной формы обучения. В случае реализации образовательной программы в заочной / очно-заочной форме трудоемкость дисциплины сохраняется, однако объем учебного материала в значительной части осваивается обучающимися в

форме самостоятельной работы. При этом требования к ожидаемым образовательным результатам обучающихся по данной дисциплине не зависят от формы реализации образовательной программы.

7. Методические рекомендации по видам занятий

Лекционные занятия.

В ходе лекционных занятий обучающимся рекомендуется выполнять следующие действия. Вести конспектирование учебного материала. Обращать внимание на категории, формулировки, раскрывающие содержание тех или иных явлений и процессов, научные выводы и практические рекомендации по их применению. Задавать преподавателю уточняющие вопросы с целью уяснения теоретических положений, разрешения спорных ситуаций.

Желательно оставить в рабочих конспектах поля, на которых во внеаудиторное время можно сделать пометки из рекомендованной литературы, дополняющие материал прослушанной лекции, а также подчеркивающие особую важность тех или иных теоретических положений.

Практические и семинарские занятия.

На практических и семинарских занятиях в зависимости от темы занятия выполняется поиск информации по решению проблем, практические упражнения, контрольные работы, выработка индивидуальных или групповых решений, итоговое обсуждение с обменом знаниями, участие в круглых столах, разбор конкретных ситуаций, командная работа, представление портфолио и т.п.

Самостоятельная работа.

Самостоятельная работа осуществляется в виде изучения литературы, эмпирических данных по публикациям и конкретных ситуаций из практики, подготовке индивидуальных работ, работа с лекционным материалом, самостоятельное изучение отдельных тем дисциплины; поиск и обзор литературы и электронных источников; чтение и изучение учебника и учебных пособий.

8. Фонд оценочных средств

8.1. Перечень компетенций с указанием этапов их формирования в процессе освоения образовательной программы в рамках учебной дисциплины

Основными этапами формирования указанных компетенций при изучении обучающимися дисциплины являются последовательное изучение содержательно связанных между собой тем учебных занятий. Изучение каждой темы предполагает овладение обучающимися необходимыми компетенциями. Результат аттестации обучающихся на различных этапах формирования компетенций показывает уровень освоения компетенций.

Контролируемые разделы (темы) дисциплины	Индекс контроли-руемой компетенции (или её части)	Оценочные средства по этапам формирования компетенций
		текущий контроль по дисциплине
1. Основы методологии исторической науки	ОПК-17	тестирование
2. Особенности становления государственности в	ОПК-17	Тестирование Опрос на практическом занятии

Контролируемые разделы (темы) дисциплины	Индекс контроли-руемой компетенции (или её части)	Оценочные средства по этапам формирования компетенций
		текущий контроль по дисциплине
России и мире		
3. Русские земли в XII - XV веках и европейское Средневековье	ОПК-17	Тестирование Опрос на практическом занятии
4. Россия в XVI – XVII веках в контексте развития европейской цивилизации	ОПК-17	Тестирование Опрос на практическом занятии
5. Россия и мир в XVIII – XIX веках	ОПК-17	Тестирование Опрос на практическом занятии
6. Россия (СССР) и мир в первой половине XX века	ОПК-17	Тестирование Опрос на практическом занятии
7. СССР и мир во второй половине XX века	ОПК-17	Тестирование Опрос на практическом занятии
8. Россия и мир XXI веке	ОПК-17	Тестирование реферат

8.2. Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений и навыков и (или) опыта деятельности процессе текущего контроля

Тестовые задания

Целью тестирования является закрепление, углубление и систематизация знаний студентов, полученных на лекциях и в процессе самостоятельной работы; проведение тестирования позволяет ускорить контроль за усвоением знаний и объективизировать процедуру оценки знаний студента.

Раздел 1. История как наука

Тип задания	***Текст вопроса***	***Варианты ответов***	***Правильные ответы***
Single Selection	Основной функцией исторической науки является:	Изучение прошлого Построение перспективных моделей развития общества. Хранение и классификация письменных исторических источников. Разработка научных методов для гуманитарных дисциплин.	1
Single Selection	Познавательная функция исторического знания заключается в:	Формировании гражданских, нравственных ценностей и качеств Идентификации общества, личности Выработке научно обоснованного политического курса Выявлении закономерностей исторического развития	4

Single Selection	Сравнительный метод в исторической науке позволяет:	Выявлять исторические законы Предсказывать будущее Пересматривать историю	1
Short Answer	Кого называют «отцом истории»?		Геродот
Short Answer	Как называют главный метод исторической науки?		Историзм
Short Answer	Автор «Истории государства Российского»?		Карамзин
Short Answer	Название теории происхождения древнерусского государства М.В. Ломоносова		Антинорманизм
Single Selection	Метод, рассматривающий исторические процессы в их развитии, взаимодействии и взаимовлиянии	исторический хронологический диалектический ретроспективный	1
Single Selection	Принцип исторической науки, требующий рассматривать исторический процесс таким, каким он был в действительности, а не таким, каким бы нам хотелось	историзма объективности социального подхода диалектический	2
Single Selection	Подход к исследованию исторических процессов, в основе которого лежит взаимодействие и взаимовлияние производительных сил, производственных отношений и классовой борьбы	исторический логический формационный цивилизационный	3
Single Selection	Принцип объективности в исторической науке подразумевает изучение исторической реальности	с точки зрения интересов определённого государства в соответствии с интересами одного социального слоя независимость от каких-либо установок и пристрастий сообразность политической конъюнктуре текущего момента	3
Multiple Selection	К вспомогательным историческим дисциплинам относятся:	сфрагистика палеография криптография мемуаристка	1,2

Раздел 2. История России и мира в период древности и Средневековья.

Тип задания	***Текст вопроса***	***Варианты ответов***	***Правильные ответы***
SingleSelection	Полюдье это	сбор дани, осуществляемый князем и дружиной во время объезда покорённых территорий Смотр древнерусского войска места, где приносились жертвы богам Места для сбора дани	1

SingleSelection	Что из перечисленного является причиной раздробленности древнерусских земель?	Пресечение династии Рюриковичей Наличие сильной великокняжеской власти Отсутствие тесных экономических связей между княжествами усиление внешнеполитической опасности	3
SingleSelection	Какое из перечисленных событий относится к правлению Ярослава Мудрого?	Крещение Руси Создание Русской правды Разгром Хазарского каганата Битва на Калке	2
SingleSelection	К заслугам княгини Ольги относится	Введение уроков и погостов Строительство Софийского собора в Киеве Объединение Киева и Новгорода в единое государство Проведение религиозной реформы	1
SingleSelection	Что из перечисленного свидетельствует о том, что распад Древней Руси не был полным?	Действие «Русской правды» Междоусобные войны Сохранение торговых связей Правление Рюриковичей	1
SingleSelection	Кто из перечисленных князей правил позже?	Ярослав Мудрый Владимир Мономах Андрей Боголюбский Всеволод Большое гнездо	4
Comparison	Соотнесите даты и события	862 — Крещение Руси 882 — Объединение Киева и Новгорода 988 — Призвание варягов на Русь 1097 — Любечский съезд	1-3,2-2,3-1,4-4
Comparison	Соотнесите имена великих князей и события	Разгром Хазарского каганата — Владимир Святославович Борьба с печенегами — Святослав Игоревич Расправа с древлянами — Ярослав Мудрый Крещение Руси — Ольга	1-2,2-3,3-4,4-1
Comparison	Соотнесите имена и даты	1238 — Битва на р. Калка 1223 — Битва на р. Сить 1240 — Ледовое побоище 1242 — Взятие монголами Киева	1-2,2-1,3-4,4-3
Comparison	Соотнесите события и даты	1648 — Переяславская Рада 1649 — Соляной бунт 1662 — Соборное Уложение 1654 — Медный бунт	1-2,2-3,3-4,4-1
SingleSelection	Какое событие произошло позже других?	Подвиг Ивана Сусанина Изгнание из Москвы поляков народным ополчением Соляной бунт Избрание на царство Михаила Романова	3
SingleSelection	Что из перечисленного является одной из причин Смуты?	Династический кризис Поражение в Ливонской войне Объявление Россией войны Польше Движение Ивана Болотникова	1

SingleSelection	Что из перечисленного произошло позже?	Избрание Романовых на престол Смоленская война Присоединение Левобережной Украины Вступление Священную лигу	4
SingleSelection	В период нахождения у власти какого правителя было открыто Славяно-греко-латинское училище?	Иван Грозный Михаил Романов Софья Алексеевна Борис Годунов	3
SingleSelection	Что из перечисленного стало результатом церковной реформы середины XVII в.?	Появление нестяжателей Появление иосифлян Появление ереси стригольников Появление старообрядцев	4
SingleSelection	Основным портом в России, через которой шла торговля с Европой в XVI в. был	Азов Архангельск Астрахань Санкт-Петербург	2

Раздел 3. Отечественная и мировая история в период Нового и Новейшего времени.

Тип задания	Текст вопроса	Варианты ответов	Правильные ответы
SingleSelection	Какая из перечисленных реформ была осуществлена Петром I	Открытие первого университета Уничтожение патриаршества Учреждение Верховного тайного совета Открытие Академии художеств	2
SingleSelection	Какое из сражений произошло раньше?	Гангутская битва Взятие Измаила Битва при Гросс-Егерсдорфе Полтавская битва	4
SingleSelection	Что из перечисленного относится к результатам реформ Петра I?	Создание новых отраслей промышленности Улучшение положения крепостных крестьян Превращение дворянства в привилегированное сословие Утрата позиций на международной арене	1
SingleSelection	Противником России в Северной войне была	Пруссия Швеция Речь Посполитая Дания	2
SingleSelection	Что из перечисленного относится к реформам Петра I?	Введение подушной подати Секуляризация церковных земель Генеральное межевание земель Жалованная грамота дворянству	1

Comparison	Соотнесите даты и события	1700 - 1721 — Русско-турецкая война 1756 - 1763 — Северная война 1773 - 1775 — Восстание Е. Пугачева 1768 - 1774 — Семилетняя война	1-2,2-4,4-1,3-3
Comparison	Соотнесите имена и события	Петр I — Открытие университета Екатерина II — Принятие табели о рангах Анна Иоанновна — Создание Уложенной комиссии Елизавета Петровна — Отказ принять кондиции	1-2,2-3,3-4,4-1
Comparison	Соотнесите имена и события	Михаил Ломоносов — Сподвижник Петра Великого Александр Радищев — Автор антинорманнской теории Василий Татищев — Автор первого труда по истории России Феофан Прокопович — Автор «Путешествия из Петербурга в Москву»	1-2,2-4,3-3,4-1
Comparison	Соотнесите термины и понятия	протекционизм — Форма правления, при которой вся власть принадлежит монарху рекрутчина — Изъятие материальных и земельных богатств у церкви Абсолютизм — Экономическая политика, направленная на защиту национальной промышленности секуляризация — Проведение регулярных наборов населения в постоянную армию	1-3,2-4,3-1,4-2
Comparison	Соотнесите даты и события	1803 — Восстание декабристов 1825 — Указ о вольных хлебопашцах 1861 — Создание Государственного совета 1810 — Отмена крепостного права	1-2,2-1,3-4,4-3
Comparison	Соотнесите имена современников	Александр I — А.М. Горчаков Николай I — М.М. Сперанский Александр II — Н.Х. Бенкендорф Александр III — К.П. Победоносцев	1-2,2-3,3-1,4-4
Comparison	Соотнесите события	Бородино — Отечественная война 1812 Оборона Шипки — Крымская война Оборона Севастополя — Русско-турецкая война 1877 - 1878 Присоединение Финляндии — Русско-шведская война 1807 – 1808 гг.	1-1,2-3,3-2,4-4
SingleSelection	Первым главой советского правительства являлся	В.И. Ленин И.В. Сталин Рыков Л.Д. Троцкий	1

SingleSelection	Москва стала столицей советской России в	1918 г. 1922 г. 1917 г. 1934 г.	1
SingleSelection	Что из перечисленного относится к политике военного коммунизма?	Запрет на ведение частной торговли Разрешение применения наемного труда Разрешение аренды земли Создание бирж труда	1
SingleSelection	Какое из перечисленных событий произошло раньше?	Заключение Брестского мира Принятие декрета о земле Образование СССР Вхождение СССР в Лигу наций	2
SingleSelection	Какое из перечисленных событий произошло позже?	Заключение пакта о ненападении с Германией Принятие первой конституции СССР Образование СНК Вступление СССР в Лигу наций	1

Примеры вопросов для устного опроса

1. **Раздел 2. История России и мира в период древности и Средневековья.**

1. Особенности становления государственности в мировой истории.
2. Роль мировых религий в истории.
3. Древнерусское законодательство: история и особенности.
4. Особенности древнерусской и средневековой европейской культуры.
5. Причины введения, основные этапы и значение крепостного права в России.
6. Истоки и особенности модернизации в России в XVII веке.

Раздел 3. Отечественная и мировая история в период Нового и Новейшего времени.

1. Особенности российской и европейской модернизации в XVIII веке.
2. Причины, сущность и значение «Восточного вопроса» в международных отношениях XVIII _ XIX веков.
3. Причины, особенности и значение «Великих реформ» в России в 1860-х – 1870-х годов.
4. Особенности национального вопроса в Российской империи.
5. Причины и итоги участия России в Первой мировой войне.
6. Особенности российских революций 1917 года.
7. Особенности социально-экономического развития СССР в 1920-х – 1930-х годах.
8. Истоки и уроки Холодной войн.
9. Основные кризисы Холодной войны.

Темы рефератов:

1. Великая Российская революция: истоки и уроки
2. Становление советского государства.
3. Трагедия Гражданской войны в России.

4. НЭП: опыт и уроки.
5. Индустриализация и коллективизация в Советской России: цели, методы, цена.
6. Складывание административно-командной системы: «Большой террор» и сопротивление сталинизму.
7. Международные отношения накануне Второй мировой войны.
8. Антигитлеровская коалиция во Второй мировой войне.
9. Культура СССР в годы Великой Отечественной войны.
10. Мир после войны: «холодная война» и противостояние двух политических систем.
11. Сталинские репрессии в послевоенном СССР.
12. Хрущевская «оттепель» и реформы 1950–1960-х годов.
13. Общественный протест и правозащитное движение в СССР.
14. «Разрядка» международной напряженности в 1970-е годы.
15. Афганская война 1979–1989 годов.
16. Задачи и противоречия Перестройки (1985–1991 гг.).
17. Духовное развитие СССР в годы Перестройки. Гласность.
18. Августовский путч 1991 года и «Дело ГКЧП»: события и версии.
19. Политические партии и движения современной России.
20. Россия и мировое сообщество в начале третьего тысячелетия: тревоги и надежды.
21. Национальный вопрос в современной России.
22. Калининградский эксклав в XXI веке: особенности развития.

8.3. Перечень вопросов и заданий для промежуточной аттестации по дисциплине

Вопросы для промежуточного контроля (зачета)

Проблемы методологии истории.
2. Древнейшие цивилизации человечества.
3. Особенности Древнерусской государственности.
4. Феномен политической раздробленности. Удельная Русь.
5. Образование монгольской империи и борьба Руси за независимость в XIII в.
6. Образование Российского централизованного государства.
7. Колонизация России и Великие географические открытия.
8. Россия в XVI - XVII вв. “Смута”.
9. Российское государство в XVII в.
10. Россия и мир на рубеже XVII – XVIII веков.
11. Россия в первой четверти XVIII столетия.
12. Россия во второй четверти XVIII в.
13. Просвещенный абсолютизм в Европе и России.
14. Внешняя политика России во второй половине XVIII в.
15. Европа в эпоху наполеоновских войн.
16. Либеральные реформы Александра I.
17. Отечественная война 1812 г. и последствия победы над наполеоновской Францией для России.
18. Декабристы.
19. Самодержавие Николая I.
20. Восточный вопрос в международных отношениях в XIX в.
21. Общественная мысль конца 30-40-х гг. о путях исторического развития России.
22. Крымская война.
23. Падение крепостного права в России.
24. Реформы в России в 60-70-х гг. XIX в.
25. Общественное движение в пореформенной России.

26. Внутренняя политика самодержавия в 80 - е гг. XIX- начале XX в.
27. Россия и мир в начале XX века: особенности развития.
28. Революция 1905 - 1907 гг. и Третьеиюньская монархия.
29. Мир и Россия накануне и в годы первой мировой войны.
30. Февральская буржуазно - демократическая революция.
31. Октябрьское вооружённое восстание и установление советской власти в стране.
32. Версальский мирный договор и послевоенный мир.
33. Гражданская война в России и иностранная военная интервенция.
34. Становление советского государства.
35. Форсированная индустриализация.
36. Сталинский “великий перелом” 1929 г.
37. Международные отношения между двумя мировыми войнами.
38. Вторая мировая война: причины, этапы и итоги.
39. Великая отечественная война: этапы и итоги.
40. Страна в 1950 - годы - первой половине 1960 - гг.
41. СССР в эпоху 1960-х – 1980-х гг.
42. Советское общество в годы перестройки (1985 - 1991).
43. Внешняя политика Советского Союза в годы перестройки.
44. Распад СССР.
45. Изменение политического и социально - экономического строя в 1991 – 1993 гг.
46. Особенности развития России на рубеже XX – XXI веков.
47. Территория и население России с древности до наших дней.
48. Основные теории происхождения государства.
49. Древнейшие культуры Северной Евразии.
50. Промышленный переворот в Европе и России.
51. Международные отношения в послевоенном мире.

8.4. Планируемые уровни сформированности компетенций обучающихся и критерии оценивания

Уровни	Содержательное описание уровня	Основные признаки выделения уровня (этапы формирования компетенции, критерии оценки сформированности)	Пятибалльная шкала (академическая) оценка	Двухбалльная шакала, зачет	БРС, % освоения (рейтинговая оценка)
Повышенный	Творческая деятельность	*Включает нижестоящий уровень.* Умение самостоятельно принимать решение, решать проблему/задачу теоретического и прикладного характера на основе изученных методов, приемов, технологий	отлично	зачтено	86-100
Базовый	Применение знаний и умений в более широких	*Включает нижестоящий уровень.* Способность собирать, систематизировать, анализировать и	хорошо		71-85

	контекстах учебной и профессиональной деятельности, нежели по образцу с большей степени самостоятельности и инициативы	грамотно использовать информацию из самостоятельно найденных теоретических источников и иллюстрировать ими теоретические положения или обосновывать практику применения			
Удовлетворительный (достаточный)	Репродуктивная деятельность	Изложение в пределах задач курса теоретически и практически контролируемого материала	удовлетворительно		55-70
Недостаточный	Отсутствие признаков удовлетворительного уровня		неудовлетворительно	не зачтено	Менее 55

9. Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины.

Основная литература

1. Фортунатов, В. В. История : учебное пособие / В. В. Фортунатов. - Санкт-Петербург: Питер, 2020. - 464 с. - (Учебное пособие). - ISBN 978-5-4461-1179-4. - Текст: электронный. - URL: https://znanium.com/catalog/product/1720878 (дата обращения: 06.03.2022). – Режим доступа: по подписке.

Дополнительная литература

1. Всемирная история: учебник для студентов вузов / под ред. Г.Б. Поляка, А.Н. Марковой. — 3-е изд., перераб. и доп. — М.: ЮНИТИ-ДАНА, 2017. - 887 с. - (Серия «Cogito ergo sum»). - ISBN 978-5-238-01493-7. - Текст: электронный. - URL: https://znanium.com/catalog/product/1028870 (дата обращения: 06.03.2022). – Режим доступа: по подписке.

2. Новейшая история стран Европы и Америки. XX век: учебник для студентов вузов : В 3 ч. / под ред. А. М. Родригеса и М. В. Пономарева. — Москва: Гуманитар, изд. центр ВЛАДОС, 2017. — Ч. 1: 1900-1945. - 463 с. - (Учебник для вузов). - ISBN 5-691-00607-X. - Текст: электронный. - URL: https://znanium.com/catalog/product/1053792 (дата обращения: 06.03.2022). – Режим доступа: по подписке.

10. Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины (модуля).

- НЭБ Национальная электронная библиотека, диссертации и прочие издания
- eLIBRARY.RU Научная электронная библиотека, книги, статьи, тезисы докладов конференций
- Гребенников Электронная библиотека ИД журналы

- ЭБС Лань книги, журналы
- ЭБС Консультант студента
- ПРОСПЕКТ ЭБС
- ЭБС ZNANIUM.COM
- РГБ Информационное обслуживание по МБА
- БЕН РАН
- Электронно-библиотечная система (ЭБС) Кантитана (https://elib.kantiana.ru/)

11. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине.

Программное обеспечение обучения включает в себя:

- система электронного образовательного контента БФУ им. И. Канта – www.lms-3.kantiana.ru, обеспечивающую разработку и комплексное использование электронных образовательных ресурсов;
- серверное программное обеспечение, необходимое для функционирования сервера и связи с системой электронного обучения через Интернет;
- корпоративная платформа Microsoft Teams;
- установленное на рабочих местах обучающихся ПО: Microsoft Windows 7, Microsoft Office Standart 2010, антивирусное программное обеспечение Kaspersky Endpoint Security.
- специализированное ПО не требуется.

12. Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине.

Для проведения занятий лекционного типа, практических занятий используются специальные помещения (учебные аудитории), оборудованные техническими средствами обучения – мультимедийной проекционной техникой. Для проведения занятий лекционного типа используются наборы демонстрационного оборудования.

Для проведения групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации используются специальные помещения (учебные аудитории), оборудованные специализированной мебелью (для обучающихся), меловой / маркерной доской.

Для организации самостоятельной работы обучающимся предоставляются помещения, оснащенные компьютерной техникой с возможностью подключения к сети «Интернет» и обеспечением доступа в электронную информационно-образовательную среду университета.

Для обучения инвалидов и лиц с ограниченными возможностями здоровья университетом могут быть представлены специализированные средства обучения, в том числе технические средства коллективного и индивидуального пользования.

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
федеральное государственное автономное образовательное учреждение высшего образования «Балтийский федеральный университет имени Иммануила Канта»
Институт физико-математических наук и информационных технологий

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

«Основы предпринимательской деятельности»

Шифр: 10.05.01
Специальность: «Компьютерная безопасность»
Специализация: «Математические методы защиты информации»
Квалификация (степень) выпускника: специалист по защите информации

Калининград
2022

Лист согласования

Составитель: Минкова Е.С., к.п.н., доцент

Рабочая программа утверждена на заседании учебно-методического совета института физико-математических наук и информационных технологий

Протокол № 01/22 от «01» февраля 2022 г.

Председатель учебно-методического совета института физико-математических наук и информационных технологий

Первый заместитель директора ИФМНиИТ, к. ф.-м. н., доцент — Шпилевой А. А

Ведущий менеджер — Е.П.Ставицкая

Содержание

1.Наименование дисциплины: «Основы предпринимательской деятельности»

Целью освоения дисциплины является формирование у обучающихся компетенций для организации и реализации предпринимательской деятельности в областях и сферах актуальных в рамках направления профессиональной подготовки.

2. Перечень планируемых результатов обучения по дисциплине, соотнесенных с планируемыми результатами освоения образовательной программы

Код компетенции	Результаты освоения образовательной программы (ИДК)	Результаты обучения по дисциплине
УК-1. Способен осуществлять критический анализ проблемных ситуаций на основе системного подхода, вырабатывать стратегию действий	УК.1.1. Анализирует проблемную ситуацию как систему, выявляя ее составляющие и связи между ними. УК.1.2. Критически оценивает надежность источников информации, работает с противоречивой информацией из разных источников. УК.1.3. Разрабатывает и содержательно аргументирует стратегию решения проблемной ситуации на основе системного и междисциплинарных подходов.	Студент, изучивший данный курс, должен: • Знать: критерии постановки задач в соответствии с целью • Уметь: анализировать информацию и работать с большим количеством источников информации • Владеть: технологиями поиска решений поставленной задачи и анализа последствий возможных решений задачи
УК-2. Способен управлять проектом на всех этапах его жизненного цикла	УК.2.1. Формулирует в рамках поставленной цели проекта совокупность задач, обеспечивающих ее достижение. УК.2.2. Осуществляет мониторинг хода реализации проекта, корректирует отклонения, вносит дополнительные изменения в план реализации проекта, уточняет зоны ответственности участников проекта. УК.2.3. Способен публично представлять результаты решения конкретной задачи в проекте.	Студент, изучивший данный курс, должен: • Знать основные правила и приемы работы в команде • Уметь выявлять, согласовывать и осуществлять социальное взаимодействие • Владеть практически средствами управления и работы в команде в различных ролях
УК-3. Способен организовывать и руководить	УК.3.1. Умеет организовать команду для достижения поставленной цели и	Студент, изучивший данный курс, должен:

работой команды, вырабатывая командную стратегию для достижения поставленной цели	взаимодействовать с другими участниками проекта для решения текущих задач. УК.3.2. Планирует последовательность шагов для достижения заданного результата; понимает эффективность использования стратегии сотрудничества для достижения поставленной цели, определяет свою роль в команде. УК.3.3. Осуществляет обмен информацией с другими членами команды, осуществляет презентацию результатов работы команды	• знать основы методов формирования команд для научно-исследовательских и опытно-конструкторских работ; • уметь самостоятельно определять ключевые задачи, формировать план действий с учетом общекомандных приоритетов; • владеть навыками гибкой разработки в условиях высокой неопределённости окружения.
УК-6. Способен определять и реализовывать приоритеты собственной деятельности и способы ее совершенствования на основе самооценки и образования в течение всей жизни	УК.6.1. Определяет свои личные ресурсы, возможности и ограничения для достижения поставленной цели УК.6.2. Создает и достраивает индивидуальную траекторию саморазвития при получении основного и дополнительного образования УК.6.3. Умеет обобщать и транслировать свои индивидуальные достижения на пути реализации задач саморазвития; умеет рационально распределять временные и информационные ресурсы.	Студент, изучивший данный курс, должен: • знать основы метода научного подхода к изучению и освоению новых профессиональных знаний; • уметь эффективно использовать современные образовательные и информационные технологии для исследования заданной темы; • владеть навыками формирования научных гипотез, их проверки и построения соответствующих научных выводов.
УК-9. Способен принимать обоснованные экономические решения в различных областях жизнедеятельности	УК-9.1. Понимает базовые принципы функционирования экономики и экономического развития, цели, роль и формы участия государства в экономике. УК-9.2. Способен производить оценку технико-экономических показателей проектных решений в профессиональной области. УК-9.3. Владеет навыками быстрой адаптации к изменениям экономических условий, решения задач,	Студент, изучивший данный курс, должен: • знать основные теории и методы работы экономических механизмов в рыночных условиях; • уметь самостоятельно осваивать новые методы работы хозяйствующих субъектов и адаптироваться к решению новых практических задач; • владеть навыками быстрой адаптации к изменениям экономических условий, решения задач, требованиями должностных обязанностей.

	требованиями должностных обязанностей.	
УК-10. Способен формировать нетерпимое отношение к коррупционному поведению	УК-10.1. Анализирует возможные последствия принимаемых экономических решений в профессиональной сфере УК-10.2. Анализирует и правильно применяет правовые нормы о противодействии коррупционному поведению. УК-10.3. Понимает, что формирование положительного морального облика имеет большое значение в выбранной профессиональной деятельности.	Студент, изучивший данный курс, должен: • знать основы действующей правовой системы в объеме необходимом для работы как по найму, так и в качестве самостоятельного хозяйствующего субъекта; • уметь самостоятельно контролировать свои действия в правовом аспекте; • владеть навыками поиска решений юридических вопросов.

3. Место дисциплины в структуре образовательной программы

Дисциплина «Основы предпринимательской деятельности» относится к дисциплинам обязательной части раздела «Дисциплины», входит в Модуль 1 «Модуль универсальных компетенций».

4. Виды учебной работы по дисциплине.

Виды учебной работы по дисциплине зафиксированы учебным планом основной профессиональной образовательной программы по указанному направлению и профилю, выражаются в академических часах. Часы контактной работы и самостоятельной работы обучающегося и часы, отводимые на процедуры контроля, могут различаться в учебных планах ОПОП по формам обучения. Объем контактной работы включает часы контактной аудиторной работы (лекции/практические занятия/ лабораторные работы), контактной внеаудиторной работы (контроль самостоятельной работы), часы контактной работы в период аттестации. Контактная работа, в том числе может проводиться посредством электронной информационно-образовательной среды университета с использованием ресурсов сети Интернет и дистанционных технологий

5. Содержание дисциплины, структурированное по темам (разделам)

Исходя из рамок, установленных учебным планом по трудоемкости и видам учебной работы по дисциплине, преподаватель самостоятельно выбирает тематику занятий по формам и количеству часов проведения контактной работы: лекции и иные учебные занятия, предусматривающие преимущественную передачу учебной информации преподавателем и (или) занятия семинарского типа (семинары, практические занятия, практикумы, лабораторные работы, коллоквиумы и иные аналогичные занятия), и (или) групповые консультации, и (или) индивидуальную работу обучающихся с преподавателем, в том числе индивидуальные консультации (по курсовым работам/проектам – при наличии курсовой работы/проекта по данной дисциплине в учебном плане). Рекомендуемая тематика занятий максимально полно реализуется в контактной работе с обучающимися очной формы обучения. В случае реализации образовательной программы в заочной / очно-

заочной форме трудоемкость дисциплины сохраняется, однако объем учебного материала в значительной части осваивается обучающимися в форме самостоятельной работы. При этом требования к ожидаемым образовательным результатам обучающихся по данной дисциплине не зависят от формы реализации образовательной программы.

№	**Наименование раздела**	Содержание раздела
1	Тема1. Бизнес-планирование и формирование команды	Содержание процессов генерирования бизнес-идей; алгоритм креативного рождения идеи бизнеса с ее последующим развитием в систему решений (бизнес-модель); базовые положения создания и применения бизнес-моделей: понятие и виды моделей бизнеса (бизнес-модель М. Джонсона, К. Кристенсена, Х. Кагерманна), ключевые этапы формирования бизнес-модели; механизм выбора бизнес-модели компании; ключевые элементы, функциональные блоки бизнес-модели; концепция ценностного предложения А. Остервальдера; переход от бизнес-модели к бизнес-плану. Понятие предпринимательской команды; эффективность команды; командное лидерство; мотивация команды; распределение командных ролей и функций; развитие команды; поддержание командного духа; учет психологических особенностей личности; технологии командообразования.
2	Тема 2. Разработка и выведение продукта на рынок	подходы к разработке продукта — метод водопада (каскадный метод) и метод гибкой разработки; теория решения изобретательских задач; теория ограничений; процесс улучшения характеристик существующих видов продукции; разработка новых видов продукции; техническое сопровождение проекта создания нового продукта (технологии) от предпроектных разработок до проектирования, создания и использования; инструменты современного процесса product development: анализ конкурентной среды, технический аудит, разработка технико-экономического обоснования, технической документации, управляющих программ. Основы понятия Customer development, по С. Бланку и Б. Дорфу; составляющие Customer development: выявление потребителей, верификация потребителей, расширение клиентской базы, выстраивание компании; изучение потребностей и запросов потребителей; методы моделирования потребностей потребителей; факторы поведения потребителя; приемы привлечения внимания потребителя; оценка эффективности проводимых мероприятий и оптимизация маркетинговой деятельности предприятия; специфика поведения индивидуальных и корпоративных потребителей.
3	Тема 3. Охрана интеллектуальной	Понятие интеллектуальной собственности, ее основные юридические свойства и система охраны, понятие и содержание интеллектуальных прав, их соотношение с

	собственности и трансфер технологий	понятием нематериальных активов; IP-стратегия инновационного проекта и ее составляющие; различия между двумя основными режимами правовой охраны результатов интеллектуальной деятельности — авторским правом и патентным правом; патентование, системы и процедуры патентования в России, за рубежом, на международном уровне; понятия «формула изобретения (полезной модели)», «приоритет», «уровень техники», «патентный поиск», «патентная чистота»; существующие правовые способы приобретения и коммерциализации интеллектуальной собственности; основные особенности секретов производства (ноу-хау) и средств индивидуализации юридических лиц, товаров, работ, услуг и предприятий. Понятия «трансфер технологий» и «лицензирование» как правовые институты в сфере интеллектуальной собственности; их соотношение; роль стратегии лицензирования как части IP-стратегии инновационного проекта; мотивы использования стратегии лицензирования; существующие виды лицензионных сделок; требования российского законодательства к форме и содержанию лицензионного договора; последствия их несоблюдения; определение стоимости объекта интеллектуальной собственности; основные методы расчета цены лицензионного договора; роялти и паушальный платеж; их сравнительные преимущества и недостатки, специфика применения; конкретные методики расчета роялти.
4	Тема 4. Оценка инвестиционной привлекательности и инструменты привлечения финансирования	Статические и динамические методы оценки экономической эффективности инновационных проектов; принципы оценки эффективности проектов; чистая прибыль инновационного проекта как критерий экономической эффективности; сравнительный анализ различных видов оценки: коммерческая, общественная, участия в проекте; система метрик инновационных проектов с учетом неприменимости критериев экономической эффективности на ранних стадиях развития проектов (до выхода на устойчивые продажи); критерии инвестиционной готовности проекта для венчурных инвестиций и их отличие от критериев для прямых инвестиций. Источники финансирования проекта: средства бюджета и внебюджетных фондов, государственных институтов развития, компаний, индивидуальных предпринимателей, частных, институциональных и иностранных инвесторов, кредитно-финансовых организаций, научных и образовательных учреждений; инструменты финансирования: инвестиции бизнес-ангелов и венчурных фондов, гранты, субсидии; выбор и обоснование источников финансирования инновационного проекта; финансовое моделирование проекта; технологии переговоров с инвесторами о финансировании проекта.

6. Рекомендуемая тематика учебных занятий в форме контактной работы

Рекомендуемая тематика учебных занятий *лекционного* типа (предусматривающих преимущественную передачу учебной информации преподавателями):

№	Наименование раздела	Темы лекций
1	Бизнес-планирование и формирование команды	Тема1. Бизнес-планирование и формирование команды
2	Разработка и выведение продукта на рынок	Тема 2. Разработка и выведение продукта на рынок
3	Охрана интеллектуальной собственности и трансфер технологий	Тема 3. Охрана интеллектуальной собственности и трансфер технологий
4	Оценка инвестиционной привлекательности и инструменты привлечения финансирования	Тема 4. Оценка инвестиционной привлекательности и инструменты привлечения финансирования

Рекомендуемая тематика *практических* занятий:

№ п/п	Наименование Темы	Содержание темы
1	Тема1. Бизнес-планирование и формирование команды	Работа с кейсом
2	Тема 2. Разработка и выведение продукта на рынок	Работа с кейсами
3	Тема 3. Охрана интеллектуальной собственности и трансфер технологий	Деловая игра
4	Тема 4. Оценка инвестиционной привлекательности и инструменты привлечения финансирования	Работа с кейсом

Требования к самостоятельной работе обучающихся

1. Работа с лекционным материалом, предусматривающая проработку конспекта лекций и учебной литературы, по всем темам из п. 6 настоящей рабочей программы.
2. Выполнение домашнего задания, предусматривающего решение задач, выполнение упражнений, выдаваемых на практических занятиях, по всем темам из п. 6 настоящей рабочей программы.

Руководствуясь положениями статьи 47 и статьи 48 Федерального закона от 29 декабря 2012 г. N 273-ФЗ «Об образовании в Российской Федерации» научно-педагогические работники и иные лица, привлекаемые университетом к реализации данной

образовательной программы, пользуются предоставленными академическими правами и свободами в части свободы преподавания, свободы от вмешательства в профессиональную деятельность; свободы выбора и использования педагогически обоснованных форм, средств, методов обучения и воспитания; права на творческую инициативу, разработку и применение авторских программ и методов обучения и воспитания в пределах реализуемой образовательной программы и отдельной дисциплины.

Исходя из рамок, установленных учебным планом по трудоемкости и видам учебной работы по дисциплине, преподаватель самостоятельно выбирает тематику занятий по формам и количеству часов проведения контактной работы: лекции и иные учебные занятия, предусматривающие преимущественную передачу учебной информации преподавателем и (или) занятия семинарского типа (семинары, практические занятия, практикумы, лабораторные работы, коллоквиумы и иные аналогичные занятия), и (или) групповые консультации, и (или) индивидуальную работу обучающихся с преподавателем, в том числе индивидуальные консультации (по курсовым работам/проектам – при наличии курсовой работы/проекта по данной дисциплине в учебном плане).

Рекомендуемая тематика занятий максимально полно реализуется в контактной работе с обучающимися очной формы обучения. В случае реализации образовательной программы в заочной / очно-заочной форме трудоемкость дисциплины сохраняется, однако объем учебного материала в значительной части осваивается обучающимися в форме самостоятельной работы. При этом требования к ожидаемым образовательным результатам обучающихся по данной дисциплине не зависят от формы реализации образовательной программы.

7. Методические рекомендации по видам занятий

Лекционные занятия.

В ходе лекционных занятий обучающимся рекомендуется выполнять следующие действия. Вести конспектирование учебного материала. Обращать внимание на категории, формулировки, раскрывающие содержание тех или иных явлений и процессов, научные выводы и практические рекомендации по их применению. Задавать преподавателю уточняющие вопросы с целью уяснения теоретических положений, разрешения спорных ситуаций.

Желательно оставить в рабочих конспектах поля, на которых во внеаудиторное время можно сделать пометки из рекомендованной литературы, дополняющие материал прослушанной лекции, а также подчеркивающие особую важность тех или иных теоретических положений.

Практические и семинарские занятия.

На практических и семинарских занятиях в зависимости от темы занятия выполняется поиск информации по решению проблем, практические упражнения, контрольные работы, выработка индивидуальных или групповых решений, итоговое обсуждение с обменом знаниями, участие в круглых столах, разбор конкретных ситуаций, командная работа, представление портфолио и т.п.

Самостоятельная работа.

Самостоятельная работа осуществляется в виде изучения литературы, эмпирических данных по публикациям и конкретных ситуаций из практики, подготовке индивидуальных работ, работа с лекционным материалом, самостоятельное изучение отдельных тем дисциплины; поиск и обзор литературы и электронных источников; чтение и изучение учебника и учебных пособий.

Тематика самостоятельных работ:

№	*Наименование темы*	*Содержание темы*
1	Тема1. Бизнес-планирование и формирование команды	Разработка бизнес-модели группового проекта
2	Тема 2. Разработка и выведение продукта на рынок	Выявление противоречий продукта по теории развития изобретательских задач. Выявление потребителей группового проекта
3	Тема 3. Охрана интеллектуальной собственности и трансфер технологий	Разработка плана управления интеллектуальной собственностью группового проекта
4	Тема 4. Оценка инвестиционной привлекательности и инструменты привлечения финансирования	Оценка инвестиционной привлекательности и разработка финансовой модели группового проекта

8. Фонд оценочных средств

8.1. Перечень компетенций с указанием этапов их формирования в процессе освоения образовательной программы в рамках учебной дисциплины

Основными этапами формирования указанных компетенций при изучении обучающимися дисциплины являются последовательное изучение содержательно связанных между собой тем учебных занятий. Изучение каждой темы предполагает овладение обучающимися необходимыми компетенциями. Результат аттестации обучающихся на различных этапах формирования компетенций показывает уровень освоения компетенций.

Контролируемые разделы (темы) дисциплины	Индекс контролируемой компетенции (или её части)	Оценочные средства по этапам формирования компетенций
		текущий контроль по дисциплине
Тема1. Бизнес-планирование и формирование команды	УК-1 УК-2 УК-3 УК-6 УК-9 УК-10	Тестирование
Тема 2. Разработка и выведение продукта на рынок	УК-1 УК-2 УК-3 УК-6 УК-9 УК-10	Тестирование
Тема 3. Охрана интеллектуальной собственности и трансфер технологий	УК-1 УК-2 УК-3 УК-6 УК-9 УК-10	Тестирование

Контролируемые разделы (темы) дисциплины	Индекс контролируемой компетенции (или её части)	Оценочные средства по этапам формирования компетенций
		текущий контроль по дисциплине
Тема 4. Оценка инвестиционной привлекательности и инструменты привлечения финансирования	УК-1 УК-2 УК-3 УК-6 УК-9 УК-10	Тестирование

8.2. Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений и навыков и (или) опыта деятельности процессе текущего контроля

Тема 1.
Тест

Тип задания	Текст вопроса	Варианты ответов		Правильные ответы	Сложность вопроса
MultipleSelection	Основные элементы бизнес-плана?	Риски		1,3	2
		Доходы			
		Компетенции			
		Продвижение			
Comparison	Сопоставьте основные элементы бизнес-модели:	Ценностное предложение	Скорость обращения ресурсов	1-4, 2-3, 3-1, 4-2	3
		Ключевые процессы	Информация		
		Формула прибыли	Размер возможностей для инвестиций (нормы)		
		Ключевые ресурсы	Предложения, удовлетворяющие потребности.		
Comparison	Сопоставьте названия структурных блоков с их определением (описанием):	Потоки поступления доходов	отражает те преимущества, которые получит клиент, воспользовавшись продуктом или услугой данной компании	1-3, 2-1, 3-4, 4-2	3
		Ценностное предложение	характер отношений с клиентами в зависимости от		

			решаемых компанией задач: приобретение клиентов; удержание клиентов; увеличение продаж.		
		Структура издержек	материальная прибыль, которую компания получает от каждого потребительского сегмента.		
		Взаимоотношения с клиентами	это расходы, связанные с функционированием бизнес-модели.		
Shortanswer	Бизнес-модели, относящиеся к предложению товаров широкого потребления, не делают различий между … сегментами.			Потребительскими	2
SingleSelection	Что НЕ относится к основным видам ресурсов?	Интеллектуальные ресурсы Финансы Энергетические ресурсы Материальные ресурсы		3	1

Тема 2.
Тест

Тип задания	Текст вопроса	Варианты ответов	Правильные ответы	Сложность вопроса

MultipleSelection	Основные элементы бизнес-плана?	Риски		1,3	2
		Доходы			
		Компетенции			
		Продвижение			
Comparison	Сопоставьте основные элементы бизнес-модели:	Ценностное предложение	Скорость обращения ресурсов	1-4, 2-3, 3-1, 4-2	3
		Ключевые процессы	Информация		
		Формула прибыли	Размер возможностей для инвестиций (нормы)		
		Ключевые ресурсы	Предложения, удовлетворяющие потребности.		
Comparison	Сопоставьте названия структурных блоков с их определением (описанием):	Потоки поступления доходов	отражает те преимущества, которые получит клиент, воспользовав-шись продуктом или услугой данной компании	1-3, 2-1, 3-4, 4-2	3
		Ценностное предложение	характер отношений с клиентами в зависимости от решаемых компанией задач: приобретение клиентов; удержание клиентов; увеличение продаж.		
		Структура издержек	материальная прибыль, которую компания получает от каждого потребительского сегмента.		

		Взаимоотношения с клиентами	это расходы, связанные с функционированием бизнес-модели.		
Shortanswer	Бизнес-модели, относящиеся к предложению товаров широкого потребления, не делают различий между … сегментами.			Потребительскими	2
SingleSelection	Что НЕ относится к основным видам ресурсов?	Интеллектуальные ресурсы Финансы Энергетические ресурсы Материальные ресурсы		3	1

Тема 3.
Тест

Тип задания	Текст вопроса	Варианты ответов	Правильные ответы	Сложность вопроса
SingleSelection	Выберите верную расшифровку аббревиатуры ИС:	Информационная система Интеллектуальная система Интеллектуальная собственность Интеллектуальная система	3	1
SingleSelection	Выберите верное утверждение:	Интеллектуальная собственность – это права на те или иные нематериальные результаты человеческого труда.	1	1

		Интеллектуальная собственность – это важнейшее понятие патентного права. Интеллектуальная собственность – это права на те или иные материальные результаты человеческого труда. Интеллектуальная собственность – это интеллектуальные права на произведения науки, музыки, литературы.		
MultipleSelection	Виды систем патентирования:	Традиционная (национальная) система Европейская система Региональная система Нетрадиционная система Евразийская система Международная система	1, 3, 6	2
MultipleSelection	Укажите верные отличия авторских прав от патентных:	Авторское право охраняет результат литературного, научного, художественного творчества. Патентное право охраняет результат литературного, научного, художественного творчества. Презумпция авторства: автором в авторском праве	1, 2, 3	3

		считается тот, кто указа на оригинале или экземпляре произведения, пока не доказано обратное Авторское право охраняет не все творческие результаты, а лишь те, которые являются оригинальными, не повторяющимися при параллельном творчестве Презумпция авторства: автором в патентном праве считается тот, кто указан в патенте, пока не доказано обратное		
MultipleSelection	Какая из процедур длится 30 месяцев?	Парижская процедура Процедура PTT Процедура PCT Международная процедура	1, 3	2

Примеры кейсов

Тема 1. Бизнес-планирование и формирование команды

Кейс «Цветочный рай»

Компания «Цветочный рай» — это стартап, представляющий собой интернет-платформу по продаже цветов, цветочных композиций, фруктовых букетов и т. п. Платформа работает с сегментами B2C (покупатели, частные производители/дизайнеры/флористы) и B2B (организации). Численность стартапа — три человека, находится в Санкт-Петербурге. Бизнес-идея стартапа — предоставление сервиса для покупки уникальных дизайнерских композиций из цветов и фруктов. Для частных заказов сервис будет бесплатным, для мастеров-изготовителей — платным.

Задание:

Опираясь на кейс компании «Цветочный рай», сформируйте шаблон бизнеса. Построение бизнес-модели мы начинаем справа налево, двигаясь от потребительских сегментов к структуре издержек и доходов, последовательно прорабатывая каждый блок канвы. Необходимо ответить на вопросы таблицы 1, формируя каждый блок бизнес-модели,

ориентируясь на таблицу и заполняя шаблон бизнес-модели, приведенный в теоретической части. Блоки шаблона бизнес-модели, необходимые для заполнения:

1. Потребительские сегменты.
2. Ценностное предложение.
3. Каналы сбыта.
4. Взаимоотношения с клиентами.
5. Потоки поступления дохода.
6. Ключевые ресурсы.
7. Ключевые виды деятельности.
8. Ключевые партнеры.
9. Структура издержек.

Тема 2. Разработка и выведение продукта на рынок

Кейс «Роботикум»

На этапе финальной полировки при производстве турбинных лопаток во всем мире используется ручной труд. Это связано с тем, что задача программирования робота, способного учитывать различные факторы (гибкость полировочной ленты, исходные шероховатости поверхности и пр.) для адаптивного управления обработкой, в мире пока не решена. Санкт-Петербургская компания «Роботикум» разработала сложные нелинейные алгоритмы обратной связи, которые позволяют создать роботизированную ячейку для полировки турбинных лопаток. В настоящее время работоспособность алгоритмов продемонстрирована на примере модели «бабочка» — управление удержанием шарика на поверхности сложной формы, с которой шарик скатывается.

Задание: Определите, какой из способов разработки продукта предпочтителен для компании «Роботикум».

Тема 4. Оценка инвестиционной привлекательности и инструменты привлечения финансирования

Кейс «Обоснование экономической целесообразности реализации проекта»

Известный профессор в области лазерной физики изобрел новый подход к производству игл для микроскопов. Вместе со своим учеником они обдумывают возможность начать инновационный проект, ориентированный на организацию производства данного изобретения. Затраты на патентование, по их оценкам, составят 300 тысяч рублей. Команда предполагает, что предприятие займет стабильное финансовое положение, рентабельность активов от текущей деятельности по их расчетам должна составить в среднем 20%. Профессор предполагает привлечь к продвижению данной продукции своего коллегу (маркетолога), имеющего опыт провижения данной продукции на рынок. Профессор пообещал своему коллеге-маркетологу 5% от доли компании в качестве опциона в случае достижения прогнозируемого ниже объема продаж.Проведенный маркетинговый анализ рынка дает следующий прогноз продаж на первые три года освоения рынка

ПРОГНОЗ ПРОДАЖ ПРОДУКЦИИ

Годы реализации проекта Прогнозируемые объемы продаж, тыс. шт.

1-й 30
2-й 35
3-й 45

Опыт деятельности предприятия показывает, что цена на подобную продукцию в среднем может составить 600 рублей. Со второго года прогнозируется появление на рынке конкурентов, что вынудит снизить исходную цену на 5%, но позволит сохранить планируемые объемы продаж.

Для организации производства планируется приобрести технологическое оборудование общей стоимостью 600 тысяч рублей и оборотные средства в размере 100 тысяч рублей. Производство планируется организовать на арендуемых площадях. При этом арендная плата составит 100 тысяч рублей в месяц. Для текущего производства продукции необходимы следующие затраты:

сырье и материалы — 200 рублей/шт.;

основная зарплата производственного персонала — 150 рублей/шт.;

накладные расходы — 2 000 тысяч рублей в год;

оплата торгового персонала — 50 рублей за единицу реализованной продукции.

В последний год проекта планируется продать технологическое оборудование по остаточной стоимости. Размер амортизационных отчислений определяется из условий эксплуатации оборудования в течение пяти лет. Величина отчислений во внебюджетные фонды составляет 30,2%.В расчет принимается только налог на прибыль в размере, установленном законодательными актами на период выполнения расчетов по проекту (на настоящий момент — 20% от налогооблагаемой прибыли). Все инвестиции предполагается провести на предынвестиционной стадии проекта до начала производства новой продукции.

Для осуществления производственной деятельности необходимо определить состав и величину производственно-сбытовых затрат, формирующих себестоимость выпускаемой продукции. При этом выделить две группы затрат: переменные и постоянные. Общая величина затрат на производство и сбыт продукции формирует полную себестоимость, которая может быть рассчитана на единицу и на объем выпуска продукции по годам расчетного периода проекта. Для определения доходной части проекта рассчитывается выручка от реализации продукции как произведение цены за единицу продукции на объем продаж в количественном выражении.

Цена первого года проекта устанавливается в размере 600 рублей. По результатам маркетингового прогноза со второго года проекта предполагается появление на рынке конкурентов с аналогичной продукцией. Для сохранения планируемого объема продаж предприятие предполагает снизить исходную цену на 5% и сохранить эту величину на второй и третий год реализации проекта.

На основе проведенных оценок инвестиционных единовременных затрат, текущих производственно-сбытовых затрат и выручки от продажи реализованной продукции составляется план денежных потоков, который отражает реальные поступления и выплаты денежных средств по проекту, осуществляемые в установленные интервалы времени, в данном проекте — по годам расчетного периода. Расчет показателей плана денежных потоков проводится по видам деятельности, которые осуществляет каждое предприятие — операционной, инвестиционной и финансовой. Разница между поступлениями и выплатами формирует чистый денежный поток — сальдо реальных денежных средств. В таблице денежных потоков поступления отражаются в виде положительной величины, а выплаты денежных средств — в виде отрицательной величины.

При расчете показателей денежного потока необходимо учесть налоговые выплаты. В данном проекте учитывается только налог на прибыль. Налогооблагаемая прибыль рассчитывается как разница между поступлениями (выручкой) по проекту и выплатами (себестоимостью продукции). Чистая прибыль рассчитывается как разность между

налогооблагаемой прибылью и налогом на прибыль. Отдельной строкой в плане денежных потоков выделяется величина амортизационных отчислений. Это связано с тем, что эти средства реально не покидают предприятие, а формируют амортизационный фонд, который может быть использован в дальнейшем как источник для финансирования инвестиций. Сумма чистой прибыли и амортизационных отчислений и формирует чистый денежный поток по проекту, т. е. тот доход, который и остается в распоряжении предприятия.

Показатели, которые используются для расчета денежных потоков, являются исходной информационной базой для оценки коммерческой эффективности проекта.

Экономический эффект на ранних стадиях проработки проекта оценивается путем анализа следующих показателей: критического объема производства (точки безубыточности), рентабельности инвестиций, срока окупаемости. Оценка экономической эффективности в динамике предполагает расчет и анализ следующих показателей: чистой текущей стоимости, индекса доходности, дисконтированного срока окупаемости, внутренней нормы рентабельности проекта. Для расчета этих показателей нужно определить минимально требуемую норму доходности (норму дисконта — R), которую должен приносить проект, по мнению инициаторов или предполагаемых инвесторов проекта. Эта норма дисконта может учитывать величину риска по проекту. На окончательном этапе оценки готовится ана-

литическое заключение по всем рассчитанным показателям эффективности, выявляются возможные противоречия между ними и принимается окончательное решение о целесообразности реализации проекта.

Вопросы для обсуждения по кейсу «Обоснование экономической целесообразности реализации проекта»

1. Определите состав и величину инвестиционных затрат по проекту.
2. Какие еще виды затрат, кроме указанных в описании, можно отнести к инвестиционным?
3. Рассчитайте производственно-сбытовые затраты по проекту, определите себестоимость в расчете на единицу продукции и по годам расчетного периода проекта.
4. Проведите расчеты выручки от продажи продукции проекта, основываясь на прогнозах продаж и конъюнктуре цен.
5. Назовите факторы окружающей среды проекта, которые могут повлиять на величину выручки от реализации продукции.
6. Проведите расчеты денежных потоков поступлений и выплат за весь период реализации проекта.
7. Как вы оцениваете жизнеспособность проекта по результатам прогноза денежных потоков? Какой показатель является критерием экономической целесообразности проекта на данном этапе его оценки?
8. Проведите расчеты показателей эффективности проекта методами статической оценки. Охарактеризуйте полученные значения. Насколько полно эти показатели характеризуют инвестиционную привлекательность проекта?
9. Рассчитайте дисконтированные показатели эффективности проекта. С каких позиций они характеризуют проект? Объясните наличие возможных противоречий между ними.
10. На основании проведенных расчетов показатлей эффективности определите экономическую целесообразность и инвестиционную привлекательность реализации проекта. Аргументируйте свои выводы.

Деловая игра

Тема 3. Охрана интеллектуальной собственности и трансфер технологий

Деловая игра «Подготовка сделки по лицензированию разработки, лежащей в основе группового проекта»

В данной игре ваша задача — проработка возможности использования бизнес-модели «Лицензирование» для вашего проекта. Игра состоит из двух этапов. 1-й этап игры — подготовительный

На первом этапе должно пройти распределение ролей и подготовка к основному этапу в соответствии с распределением. Все слушатели в группе делятся на три команды:

1. Команда правообладателя инновационной технологии, т. е. команда потенциального «продавца» разработки (лицензиара).
2. Команда потенциального «покупателя» разработки (лицензиата).
3. Команда техноброкера.

В качестве смыслового центра игры выбирается одна разработка: в частности, это может быть технология вашего группового проекта.

На подготовительном этапе каждая из команд самостоятельно (независимо от других команд) формулирует справедливые (на ее взгляд) условия лицензионного договора (оферту, коммерческое предложение) по всем обязательным

пунктам, а также по тем факультативным пунктам, по которым она считает необходимым, с мотивировкой каждого из предлагаемых условий. Помимо материалов данной темы при проведении подготовительной работы командам рекомендуется пользоваться поиском в сети Интернет отраслевых ставок роялти и подобрать оптимальную ставку в зависимости от предметной фокусировки проекта.

2 этап представляет собой двусторонние переговоры команды лицензиара и команды лицензиата. В ходе переговоров стороны оглашают свои условия (выработанные на этапе подготовки к игре) и мотивируют их. Техноброкер и его команда выполняют роль посредника (медиатора и модератора переговоров), основной задачей которого является достижение общей игровой цели за счет

8.3. Перечень вопросов и заданий для промежуточной аттестации по дисциплине

Вопросы для промежуточного контроля (зачета)

1. Инновация — это конечный результат инновационной деятельности, получивший воплощение в виде:
2. Сопоставьте классификации инновации:
3. Сопоставьте классификации инновации:
4. Какие инновации исключают выполнение какой-либо операции или даже этапов производственного процесса и не заменяют ее новой операцией или процессом?
5. К обязательным свойствам инноваций НЕ относится:
6. Какие этапы не обязательно должна пройти придуманная вами идея, чтобы превратиться в готовый инновационный продукт?
7. К механизмам работы компании по принципу «открытых инноваций» НЕ относится:
8. … инновации создают такие значительные изменения в процессах, продуктах или услугах, что приводят к трансформации существующих рынков или отраслей или же создают новые рынки и отрасли.
9. Что относится к примерам «подрывных инноваций»?
10. Сопоставьте примеры инновации по уровню новизны:
11. Командный дух предполагает:
12. Сопоставьте этапы формирования проектной команды:
13. Почему лучше работать в команде?

14. Командный лидер — это умелый …, способный и готовый формировать команду единомышленников, не предполагающую безусловное подчинение или однозначное согласие с его мнением.
15. Что из нижеперечисленного НЕ относится к малой группе:
16. Что относится к командному лидеру:
17. При формировании команды НЕ нужно:
18. Группа (малая группа) — немногочисленная … людей, обладающая структурой и объединенная общей целью деятельности, члены которой взаимодействуют друг с другом.
19. Основные черты малой группы:
20. К заповедям формирования командного духа относятся:
21. Лидер появляется и формируется в группе, лишь … с другими людьми.
22. Работа в команде имеет следующее преимущество:
23. Основные элементы бизнес-плана?
24. Сопоставьте основные элементы бизнес-модели:
25. Сопоставьте названия структурных блоков с их определением (описанием):
26. Бизнес-модели, относящиеся к предложению товаров широкого потребления, не делают различий между … сегментами.
27. Что НЕ относится к основными видам ресурсов?
28. Бизнес-модель – это:
29. Что НЕ относится к основным методам генерирования бизнес-идей:
30. Основные элементы любой бизнес-модели:
31. Сопоставьте названия структурных блоков с основными вопросами, на которые они отвечают:
32. Что НЕ относится к методам сбора качественных данных?
33. Сопоставьте основные виды маркетинговых исследований с их сутью:
34. Сопоставьте основные элементы микросреды с их описанием:
35. Как называются фирмы, которые оказывают услуги в продвижении, сбыте, распространении товаров среди клиентуры?
36. Что относится с параметрам привлекательности сегмента?
37. К этапам маркетингового исследования НЕ относятся:
38. Специфика подхода к организации продаж (и в том числе к коммуникационной политике) обусловлена следующими факторами:
39. Комплекс маркетинга — это набор поддающихся контролю … факторов маркетинга, совокупность которых фирма использует в стремлении вызвать желательную ответную реакцию со стороны целевого рынка.
40. Классический комплекс маркетинга включает составляющие:
41. Сопоставьте элементы микросреды с их определением:
42. Задача продажи абсолютно нового продукта в сегменте … рассматривается в двух аспектах: продажа дистрибьютору (оптовику, рознице) и действия, направленные на конечного потребителя.
43. Стадии жизненного цикла товара (вычеркните ненужное):
44. Расставьте в правильном порядке стадии традиционного жизненного цикла продукта:
45. Сопоставьте основные элементы микросреды с их описанием:
46. Как называются фирмы, которые оказывают услуги в продвижении, сбыте, распространении товаров среди клиентуры?
47. Что относится с параметрам привлекательности сегмента?
48. К этапам маркетингового исследования НЕ относятся:
49. Специфика подхода к организации продаж (и в том числе к коммуникационной политике) обусловлена следующими факторами:

50. Комплекс маркетинга — это набор поддающихся контролю … факторов маркетинга, совокупность которых фирма использует в стремлении вызвать желательную ответную реакцию со стороны целевого рынка.
51. Классический комплекс маркетинга включает составляющие:
52. Сопоставьте элементы микросреды с их определением:
53. Задача продажи абсолютно нового продукта в сегменте … рассматривается в двух аспектах: продажа дистрибьютору (оптовику, рознице) и действия, направленные на конечного потребителя.
54. Расставьте в правильном порядке стадии традиционного жизненного цикла продукта:
55. Стадии жизненного цикла товара (выберите лишнее):
56. Взаимодействие рынка и продукта описывается следующим циклом (расставьте стадии в правильном порядке):
57. Преимуществами модели водопада являются (выберите лишний ответ)
58. Недостатками метода гибкой разработки являются (выберите лишнее)
59. Роль изобретательской идеи при разработке состоит в том, чтобы (выберите правильный ответ):
60. Основным принципом теории ограничений является (выберите правильный ответ):
61. Теория сложного сечения (выберите верный ответ):
62. Теория ограничений оперирует термином «_», при этом это может быть поток сырья, финансов, продукции, и т. п.
63. ТРИЗ как методология изобретательства была предложена __ (1926–1998). Это советский (а позднее российский) инженер-изобретатель, писатель-фантаст, который разработал ТРИЗ, используя собственный изобретательский опыт и наблюдения за работой других изобретателей
64. Потребность (с точки зрения психологии) – это:
65. Расположите формы потребности в порядке развития
66. Какой из барьеров на пути осуществления запроса относится к внутренним?
67. Алгоритм Customer Development (расположите в нужном порядке):
68. Как эффективнее всего снизить высоту барьера неплатежеспособности (товар – 3-комнатная квартира):
69. Что такое функциональная ценность товара в соответствии с подходом Шета, Ньюмана и Гросса?
70. Расположите в «классическом» порядке стадии потребительского процесса (процесс покупки)
71. В какой ситуации наиболее сильно влияние референтных групп на выбор индивидуальным потребителем товарной группы и товарной марки
72. __ -препятствия, не позволяющие субъекту сформировать и предъявить запрос.
73. Внешние барьеры (дальнего окружения). Выберите лишнее:
74. Выберите верную расшифровку аббревиатуры ИС:
75. Выберите верное утверждение:
76. Виды систем патентирования:
77. Укажите верные отличия авторских прав от патентных:
78. Какая из процедур длится 30 месяцев?
79. Процедура патентирования. Поставьте в правильном порядке шаги:
80. Патентный поиск - это
81. __ чистота — важнейшее условие конкурентоспособности продукта, обеспечивающее возможность свободного использования объекта в какой-либо стране без нарушения действующих на ее территории исключительных прав третьих лиц.

82. Ноу-хау является самым специфическим объектом ИС. Охрана разработки в режиме ноу-хау может являться предпочтительной в случае, когда: (выберите верные варианты)
83. Для того чтобы извлекать преимущества из имущественных интеллектуальных прав, их надо сначала получить. Какими юридическими способами приобретаются и коммерциализируются эти права? Существует два возможных направления коммерциализации ИС:
84. Что понимают под трансфером технологий?
85. Выберите верные классификации лицензий по форме правовой охраны объекта интеллектуальной собственности:
86. Выберите верные утверждения:
87. Выберите верные классификации лицензий по условиям предоставления прав:
88. Верны ли следующие утверждения?
89. Неисключительная лицензия может предполагать N лицензиатов.
90. Исключительная лицензия предполагает единственного лицензиата.
91. Выберите верное определение.
92. Перекрестные лицензии — это
93. Ключевые методы определения стоимости разработки для формирования цены лицензионного договора:
94. __ платёж – как правило, твердая сумма, величина которой не поставлена в зависимость от каких-либо переменных, в том числе от экономических результатов использования лицензиатом объекта интеллектуальной собственности, выплачиваемая в один или несколько приемов на ранней стадии действия лицензионного договора.
95. __ - как правило, лицензионное вознаграждение, величина которого привязана к какой-либо переменной и выплата которого осуществляется с определенной периодичностью в течении всего срока действия лицензионного договора.
96. Выберите формулу расчета лицензии с использованием роялти:
97. что такое бутстреппинг - ?
98. распределите стадии развития инновационной компании
99. …- это привлечение финансовых ресурсов от практически неограниченного числа людей для реализации продукта или услуги, проведения различных мероприятий, социальных, креативных или бизнес-проектов и др
100. Гранты не облагаются налогом на прибыль, если соблюдаются следующие условия:
101. В формуле денежного потока соотнесите величины и их значения:
102. NCF = CIF – COF
103. что относится к доступным способам первоначального финансировании при использовании бутсреппинга ?
104. Оптимальными источниками финансирования инновационной компании с точки зрения доступности на стадии создания являются:
105. Расставьте основные источники финансирования инновационной деятельности в порядке возрастания доступного объем финансирования:
106. венчурное финансирование относится:
107. Что из перечисленного не является особенностью бизнес-ангельского финансирования инновационной деятельности?
108. Какой показатель отражает экономический интерес инвестора, вкладывающего средства в инновационный проект?
109. Что понимается под нормой дохода, приемлемой для инвестора?
110. Укажите первый этап оценки экономической эффективности для проекта, который имеет общественную значимость.

111. Суммарное сальдо трех потоков по шагам расчетного периода составляет: 0, 100, 300, –200, 500. Соответствует ли такой поток денежных средств условиям финансовой реализуемости проекта? (да/нет)
112. Рентабельность инвестиций определяется как отношение:
113. Дисконтирование представляет собой:
114. в формуле денежного потока соотнесите величину и ее значение :
115. промежуток времени от момента начала реализации проекта до его завершения, за который рассчитываются планируемые затраты и результаты проекта при определении его эффективности.
116. разность между притоком (поступлением) и оттоком (выплатами) денежных средств на каждом шаге расчета2.
117. характеризует соотношение дисконтированных денежных потоков поступлений и выплат в течение расчетного периода проекта.
118. Анализ рисков инновационного проекта представляет собой:
119. Риски забастовок персонала предприятия следует отнести к:
120. Неправильное определение целевой аудитории, неудачная рекламная кампания, неправильный прогноз спроса на услуги следует отнести к:
121. Технические неполадки используемого на производстве электрооборудования, бытовых приборов, сантехнического оборудования следует отнести к:
122. Возникновение недовольства среди жителей района расположением гостиницы, которую вы построили, следует отнести к:
123. Риск роста темпов инфляции, сопровождающий ваш проект, следует отнести к:
124. это процедуры выявления, определения, идентификации и приоритизации, сопровождаемые эффективным использованием ресурсов с тем, чтобы: (1) контролировать и минимизировать вероятность и/или воздействие неприятного события или (2) максимизировать реализацию возможностей.
125. возможность того, что какое-либо событие произойдет и негативно скажется на достижении цели.
126. соотнесите риски с предложенными примерами
127. сопоставьте процедуры управления рисками с порядком их выполнения
128. Чем отличаются лифтовая презентация, презентация идеи и презентация для привлечения инвестиций?
129. Какие главные критерии используют инвесторы для оценки проектов?
130. Каковы должны быть основные требования к презентации, чтобы слушатели не уснули?
131. Какое основное действие должен осуществлять маркетолог во время проведения проблемного интервью?
132. Наиболее сильные акценты необходимо расставить при представлении:
133. С чего начинать построение структуры презентации?
134. Краткая презентация идеи, проекта, команды и т. д.
135. соотнесите название презентации и ее описание
136. соотнесите структуры презентации и примеры
137. Какая информация является ключевой для лиц, принимающих решения:
138. К внутренней среде субъектов инновационного процесса относится:
139. Одним из элементов инновационного потенциала является:
140. сеть институтов частного и общественного секторов, чья деятельность и взаимосвязи направлены на инициацию, импорт, модификацию и диффузию новых технологий1.
141. это часть национальной инновационной системы, которая содействует пере-воду научных знаний в коммерчески привлекательные продукты.
142. соотнесите подсистемы инновационной инфраструктуры с их описанием
143. соотнесите подсистемы инновационной инфраструктуры с примерами

144. сеть институтов частного и общественного секторов, чья деятельность и взаимосвязи направлены на инициацию, импорт, модификацию и диффузию новых технологий1.
145. Кому принадлежит лидирующая роль в концепции «тройной спирали»?
146. К внешним условиям, благоприятствующим инновационному развитию, относится:
147. соотнесите название бизнес-акселератора с его описанием
148. составная часть социально-экономической политики, которая выражает отношение государства
149. Ведомство Российской Федерации, ответственное за реализацию государственной политики в сфере инноваций — это:
150. Какие цели следует закладывать в государственную инновационную политику:
151. В СИР 2020 НЕ заложены следующие приоритеты:
152. В программе повышения конкурентоспособности российских университетов среди ведущих мировых научно-образовательных центров (имеет название «Проект 5–100») участвуют:
153. Программы инновационного развития запущены в следующих компаниях:
154. Институт технологических платформ можно отнести к:
155. долгосрочная комплексная программа по созданию условий для обеспечения лидерства российских компаний на новых высокотехнологичных рынках, которые будут определять структуру мировой экономики в ближайшие 15–20 лет.
156. катализаторы частных инвестиций в приоритетных секторах и отраслях экономики, создающие условия для формирования инфраструктуры, обеспечивающей доступ предприятиям, функционирующим в приоритетных сферах экономики, к необходимым финансовым и информационным ресурсам.
157. это коммуникационный инструмент, направленный на активизацию усилий по созданию перспективных коммерческих технологий, новых продуктов (услуг), на привлечение дополнительных ресурсов для проведения исследований и разработок, совершенствование нормативно-правовой базы в области научно-технологического, инновационного развития.

8.4. Планируемые уровни сформированности компетенций обучающихся и критерии оценивания

Уровни	Содержательное описание уровня	Основные признаки выделения уровня (этапы формирования компетенции, критерии оценки сформированности)	Пятибалльная шкала (академическая) оценка	Двухбалльная шакала, зачет	БРС, % освоения (рейтинговая оценка)
Повышенный	Творческая деятельность	*Включает нижестоящий уровень.* Умение самостоятельно принимать решение, решать проблему/задачу теоретического и прикладного характера на основе изученных методов, приемов, технологий	отлично	зачтено	86-100
Базовый	Применение знаний и умений в более широких	*Включает нижестоящий уровень.* Способность собирать, систематизировать, анализировать и	хорошо		71-85

	контекстах учебной и профессиональной деятельности, нежели по образцу с большей степени самостоятельности и инициативы	грамотно использовать информацию из самостоятельно найденных теоретических источников и иллюстрировать ими теоретические положения или обосновывать практику применения			
Удовлетворительный (достаточный)	Репродуктивная деятельность	Изложение в пределах задач курса теоретически и практически контролируемого материала	удовлетворительно		55-70
Недостаточный	Отсутствие признаков удовлетворительного уровня		неудовлетворительно	не зачтено	Менее 55

9. Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины.

Основная литература

1. Забродская Н. Г. Предпринимательство. Организация и экономика малых предприятий : учебник / Н. Г. Забродская. - Москва : Вузовский учебник : ИНФРА-М, 2019. - 263 с. - ISBN 978-5-9558-0367-8. - Текст : электронный. - URL:

2. Бизнес-планирование : учебник / под ред. проф. Т.Г. Попадюк, проф. В.Я. Горфинкеля. — Москва : Вузовский учебник : ИНФРА-М, 2021. — 296 с. - ISBN 978-5-9558-0270-1. - Текст : электронный. - URL: https://znanium.com/catalog/product/1222076

Дополнительная литература

1. Линц К. Радикальное изменение бизнес-модели: адаптация и выживание в конкурентной среде / Карстен Линц, Гюнтер Мюллер-Стивенс, Александр Циммерман ; пер. с англ. - Москва : Альпина Паблишер, 2019. - 311 с. - ISBN 978-5-96142-170-5. - Текст : электронный. - URL: https://znanium.com/catalog/product/1078433
2. Иванов Г. Г. Коммерческая деятельность : учебник / Г.Г. Иванов, Е.С. Холин. - М. : ИД ФОРУМ : ИНФРА-М, 2020. - 384 с.: ил. - (Высшее образование). - ISBN 978-5-8199-0498-5
.

10. Перечень ресурсов информационно-телекоммуникационной сети «Интернет», - необходимых для освоения дисциплины (модуля).

– НЭБ Национальная электронная библиотека, диссертации и прочие издания
– eLIBRARY.RU Научная электронная библиотека, книги, статьи, тезисы докладов конференций
– Гребенников Электронная библиотека ИД журналы
– ЭБС ZNANIUM.COM
– РГБ Информационное обслуживание по МБА
– БЕН РАН

э
л
е
к

– Электронно-библиотечная система (ЭБС) Кантитана (https://elib.kantiana.ru/)

11. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине.

Программное обеспечение обучения включает в себя:

- система электронного образовательного контента БФУ им. И. Канта – www.lms-3.kantiana.ru, обеспечивающую разработку и комплексное использование электронных образовательных ресурсов;
- серверное программное обеспечение, необходимое для функционирования сервера и связи с системой электронного обучения через Интернет;
- корпоративная платформа Microsoft Teams;
- установленное на рабочих местах обучающихся ПО: Microsoft Windows 7, Microsoft Office Standart 2010, антивирусное программное обеспечение Kaspersky Endpoint Security.
- специальных программных продуктов не требуется.

12. Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине.

Для проведения занятий лекционного типа, практических и семинарских занятий используются специальные помещения (учебные аудитории), оборудованные техническими средствами обучения – мультимедийной проекционной техникой. Для проведения занятий лекционного типа используются наборы демонстрационного оборудования.

Для проведения лабораторных работ, (практических занятий – при необходимости) используются специальные помещения (учебные аудитории), оснащенные специализированным лабораторным оборудованием: персональными компьютерами с возможностью выхода в интернет и с установленным программным обеспечением, заявленным в п.11.

Для проведения групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации используются специальные помещения (учебные аудитории), оборудованные специализированной мебелью (для обучающихся), меловой / маркерной доской.

Для организации самостоятельной работы обучающимся предоставляются помещения, оснащенные компьютерной техникой с возможностью подключения к сети «Интернет» и обеспечением доступа в электронную информационно-образовательную среду университета.

Для обучения инвалидов и лиц с ограниченными возможностями здоровья университетом могут быть представлены специализированные средства обучения, в том числе технические средства коллективного и индивидуального пользования.

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
федеральное государственное автономное образовательное учреждение высшего образования «Балтийский федеральный университет имени Иммануила Канта»
Институт физико-математических наук и информационных технологий

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

«Философия»

Шифр: 10.05.01
Специальность: «Компьютерная безопасность»
Специализация: «Математические методы защиты информации»
Квалификация (степень) выпускника: специалист по защите информации

Калининград
2022

Лист согласования

Составитель: доцент кафедры философии, кандидат философских наук Вячеслав Игоревич Савинцев, ассистент кафедры философии Игорь Александрович Горьков

Рабочая программа утверждена на заседании учебно-методического совета института физико-математических наук и информационных технологий

Протокол № 01/22 от «01» февраля 2022 г.

Председатель учебно-методического совета института физико-математических наук и информационных технологий
Первый заместитель директора ИФМНиИТ, к. ф.-м. н., доцент — Шпилевой А. А

Ведущий менеджер — Е.П.Ставицкая

Содержание

1.Наименование дисциплины: «Философия»

Цель изучения дисциплины «Философия» - дать целостное представление о философии как самостоятельной области духовной культуры и теоретических исследований

2. Перечень планируемых результатов обучения по дисциплине, соотнесенных с планируемыми результатами освоения образовательной программы

Код компетенции	Результаты освоения образовательной программы (ИДК)	Результаты обучения по дисциплине
УК-5. Способен анализировать и учитывать разнообразие культур в процессе межкультурного взаимодействия	УК.5.1. Выявление общего и особенного в историческом развитии России. УК.5.2. Анализирует современное состояние общества на основе знания истории. УК.5.3. Способен использовать основы философских знаний для формирования мировоззренческой позиции.	Знать - основные этапы развития и современное состояние философской мысли; - основные понятия и проблемы философских исследований основные концепции, родившиеся при решении наиболее значимых философских проблем Уметь: - анализировать философские тексты - ставить и решать собственные перспективные исследовательские задачи Владеть: - навыками использования фундаментальных философских категорий и знаний, необходимых для решения научно-исследовательских и практических задач

3. Место дисциплины в структуре образовательной программы

«Философия» относится к обязательной части Блока 1 Дисциплины (модули), входит в Модуль 1. Модуль универсальных компетенций направления подготовки обучающихся.

4. Виды учебной работы по дисциплине.

Виды учебной работы по дисциплине зафиксированы учебным планом основной профессиональной образовательной программы по указанному направлению и профилю, выражаются в академических часах. Часы контактной работы и самостоятельной работы обучающегося и часы, отводимые на процедуры контроля, могут различаться в учебных планах ОПОП по формам обучения. Объем контактной работы включает часы контактной аудиторной работы (лекции/практические занятия/ лабораторные работы), контактной внеаудиторной работы (контроль самостоятельной работы), часы контактной работы в период аттестации. Контактная работа, в том числе может проводиться посредством электронной информационно-образовательной среды университета с использованием ресурсов сети Интернет и дистанционных технологий

5. Содержание дисциплины, структурированное по темам (разделам)

Исходя из рамок, установленных учебным планом по трудоемкости и видам учебной работы по дисциплине, преподаватель самостоятельно выбирает тематику занятий по формам и количеству часов проведения контактной работы: лекции и иные учебные занятия, предусматривающие преимущественную передачу учебной информации преподавателем и (или) занятия семинарского типа (семинары, практические занятия, практикумы, лабораторные работы, коллоквиумы и иные аналогичные занятия), и (или) групповые консультации, и (или) индивидуальную работу обучающихся с преподавателем, в том числе индивидуальные консультации (по курсовым работам/проектам – при наличии курсовой работы/проекта по данной дисциплине в учебном плане). Рекомендуемая тематика занятий максимально полно реализуется в контактной работе с обучающимися очной формы обучения. В случае реализации образовательной программы в заочной / очно-заочной форме трудоемкость дисциплины сохраняется, однако объем учебного материала в значительной части осваивается обучающимися в форме самостоятельной работы. При этом требования к ожидаемым образовательным результатам обучающихся по данной дисциплине не зависят от формы реализации образовательной программы.

№	Наименование раздела	Содержание раздела
1	Тема 1. Предмет и метод философии. Специфика философского знания	Предмет философии: Человек и мир как два полюса мировоззрения. Эмпирическая и трансцендентная реальность. Философия как рациональная форма целостного мировоззрения. «Вечные вопросы». Теоретический и прикладной характер философского знания. Сомнение как методологическая предпосылка философского рассуждения. Феномен философской веры, её отличие от веры религиозной. Структура философского знания.
2	Тема 2. Роль философии в жизни человека и общества	Мировоззренческие и методологические функции философии. Философия как способ личностного самоопределения. Философия как судьба и образ жизни. Философская культура личности. Место и роль философии в культуре. Философия как квинтэссенция и самосознание духовной культуры.
3	Тема 3. От мифа к логосу: генезис и становление философии	Особенности мифосознания. Время, место и предпосылки появления индивидуальной рациональности. Становление философии. Основные направления, школы философии и этапы ее исторического развития. Первые философские школы в Др. Греции, Др. Индии и Др. Китае. Концепция осевого времени К. Ясперса.
4	Тема 4. Основные этапы истории западной философии	Периодизация и основные особенности античной философии. Сократ и антропологический переворот в древнегреческой философии. Платонизм и аристотелизм. Этические школы эллинизма (киники, скептики, эпикурейцы, стоики). Основные проблемы и особенности средневековой философии. Новые тенденции в философии эпохи Возрождения. Наука и философия в Новое Время. Спор эмпириков и

		рационалистов. Философский проект Просвещения. Немецкая классическая философия. Трансцендентальный идеализм И.Канта и «коперниканский переворот» в философии. Марксизм. Критика классической философии (Шопенгауэр, Ницше, Кьеркегор). сциентизм и антисциентизм, иррационализм и рационализм в современной западной философии.
5	Тема 5. Духовные основы и особенности русской философии	Дискуссии о хронологических рамках русской философии. Взаимодействие с западной философской мыслью. Самобытность русской философии. Русская философия как феномен национального самосознания, её историософичность. Русский духовный ренессанс, религиозность русской философии. Преображение (спасение) как базовая ценность русской философии. Мессианизм и революционизм в русской философии. Онтологизм русской религиозной философии и концепция всеединства. Значение интуитивистской гносеологии в русской религиозной философии. Соборность как социальный идеал русской религиозной философии. Судьба философии в России.
6	Тема 6. Проблема сознания в философии	Психика, сознание, мышление: соотношение понятий. Основные характеристики сознания. Сознание и мозг. Структура сознания. Сознание и бессознательное. Сознание и познание. Сознание, самосознание и личность. Действительность, мышление, логика и язык.
7	Тема 7. Возможности и границы познания	Место гносеологии в структуре философского знания. Сущность познания. Субъект и объект познания. Вера и знание. Основные познавательные способности. Рациональное и иррациональное в познавательной деятельности. Познание, творчество, практика. Понимание и объяснение. Проблема истины. Основные гносеологические модели: познавательный оптимизм, скептицизм и критицизм. Эмпиризм, рационализм, интуитивизм.
8	Тема 8. Научное познание и знание	Понятие науки. Научное и вненаучное знание. Критерии научности. Структура научного познания, его методы и формы. Рост научного знания. Научные революции и смены типов рациональности. Наука и техника.
9	Тема 9. Основы онтологии	Место онтологии в структуре философского знания. Учение о бытии. Субстанция и акциденция. Материя и дух. Монистические и плюралистические концепции бытия, самоорганизация бытия. Понятия материального и идеального. Пространство, время.

		Движение и развитие. Диалектика и синергетика. Детерминизм и индетерминизм. Динамические и статистические закономерности.
10	Тема 10. Научная, философская и религиозная картины мира	Научные, философские и религиозные картины мира: общее и особенное. Особенности мифологической картины мира. Содержательное различие и взаимодействие между научными, философскими и религиозными парадигмами. Космоцентризм, теоцентризм и антропоцентризм в истории философии. Основные модели соотношения Бога и мира: теизм, деизм, пантеизм. «Атеистические религии». Механицизм в науке Нового времени. Эволюционизм и органицизм. Новые представления о мире в теории относительности и квантовой механике. Становление системно-синергетической парадигмы.
11	Тема 11. Природа и сущность человека	Биологическое и социальное, телесное и духовное в человеческой природе. Открытость человеческой природы. Представления о совершенном человеке в различных культурах. Проблема антропогенеза. Основные феномены человеческого бытия.
12	Тема 12. Мотивы, нормы и ценности человеческой деятельности	Потребности, интересы, цели. Понятие социальной нормы. Основные виды социальных норм. Обычаи, право, мораль. Человек как оценивающий субъект. Понятие ценности. Ценности, идеалы, смыслы. Смысл человеческого бытия. Основные виды ценностей. Аксикреация и девальвация. Насилие и ненасилие. Свобода и ответственность. Мораль, справедливость, право. Нравственные ценности. Представления о совершенном человеке в различных культурах. Эстетические ценности и их роль в человеческой жизни. Религиозные ценности и свобода совести.
13	Тема 13. Природа и сущность социальности	Человек и природа. Деятельность как способ человеческого бытия и субстанция социальности. Человек, общество, культура. Общество и его структура. Гражданское общество и государство.
14	Тема 14. Общество и личность. Проблема свободы и ответственности	Человек, индивид, личность. Личность и индивидуальность. Проблема отчуждения и самореализации личности. Человек в системе социальных связей. Социализация и инкультурация. Личность и массы. Конформизм и нонконформизм. Свобода и необходимость в общественной жизни.
15	Тема 15. Основы философии истории	Человек и исторический процесс. Единство и многообразие истории. Случайное и необходимое,

		субъективное и объективное в истории. Субъекты исторического процесса. Дискуссии о смысле и направленности истории. Основные парадигмы социальной динамики: циклическая, прогрессивистская, синергетическая. Формационная и цивилизационная концепции общественного развития.
16	Тема 16. Проблемы и перспективы современной цивилизации	Будущее человечества. Основные тенденции развития современной цивилизации: глобализация, унификация, рост национального самосознания, «ускорение времени». Современное общество как постиндустриальное, информационное, технократическое, потребительское. Кризис современной цивилизации. Глобальные проблемы современности. Взаимодействие цивилизаций и сценарии будущего.

6. Рекомендуемая тематика учебных занятий в форме контактной работы

Рекомендуемая тематика учебных занятий *лекционного* типа (предусматривающих преимущественную передачу учебной информации преподавателями):

№	Наименование раздела	Содержание раздела
1	Предмет и метод философии. Специфика философского знания.	Лекция 1. Предмет и метод философии. Специфика философского знания
2	Роль философии в жизни человека и общества	Лекция 1. Роль философии в жизни человека и общества
3	От мифа к логосу: генезис и становление философии	Лекция 2. От мифа к логосу: генезис и становление философии
4	Основные этапы истории западной философии	Лекция 2. Основные этапы истории западной философии
5	Духовные основы и особенности русской философии	Лекция 3. Духовные основы и особенности русской философии
6	Проблема сознания в философии	Лекция 3. Проблема сознания в философии
7	Возможности и границы познания	Лекция 4. Возможности и границы познания
8	Научное познание и знание	Лекция 4. Научное познание и знание
9	Основы онтологии	Лекция 5. Основы онтологии
10	Научная, философская и религиозная картины мира	Лекция 5. Научная, философская и религиозная картины мира
11	Природа и сущность человека	Лекция 6. Природа и сущность человека

12	Мотивы, нормы и ценности человеческой деятельности	Лекция 6. Мотивы, нормы и ценности человеческой деятельности
13	Природа и сущность социальности	Лекция 7. Природа и сущность социальности
14	Общество и личность. Проблема свободы и ответственности	Лекция 7. Общество и личность. Проблема свободы и ответственности
15	Основы философии истории	Лекция 8. Основы философии истории
16	Проблемы и перспективы современной цивилизации	Лекция 8. Проблемы и перспективы современной цивилизации

Рекомендуемая тематика *практических* занятий:

№ п/п	Наименование Темы	Содержание темы
1	Роль философии в жизни человека и общества	План: 1) Философия и обыденное сознание. 2) Философия и наука. 3) Философия и религия. 4) Философия и искусство. Задания: 1. Подготовить сообщения по вопросам. Методические указания. Цель занятия – соотнести философское знание со знаниями обыденным, научным, религиозным, искусствоведческим, политическим, на основании чего – узреть общее и различия этих знаний. Важно отметить, что на всех этапах становления философской мысли философия развивалась в контакте с иными формами знания, реализуя не только собственные исследовательские программы, но и проявляя эвристическую, мировоззренческую, методологическую функции, способствующие развитию науки, религиозным доктринам, политическим и экономическим программам, обыденному мировосприятию. Занятие проводится в форме дискуссии по заданным реферативным темам. Литература для подготовки к занятию: 1. Абаньяно Н. Мудрость философии и проблемы нашей жизни. СПб., 1998. 2. Ахутин А.В. Дело философии // Ахутин А.В. Тяжба о бытии. Сборник философских работ. М., 1997. С.16-71. 3. Бранский В.П. Искусство и философия. Калининград, 2003. 4. Бубер М. Затмение Бога. Мысли по поводу взаимоотношений философии и религии. // Бубер М. Два образа веры. М., 1995. 5. Ильенков Э.В. Философия и культура. М., 1991. 6. Митрохин Л.Н. Философия и религия // Философские науки, 1989. №9. 7. Никифоров А.Л. Является ли философия наукой?// Философские науки, 1989, №6. 8. Рассел Б. Мудрость Запада: Историческое исследование западной философии в связи с общественными и политическими обстоятельствами. М., 1998.

2	Основные этапы истории западной философии	2.1. Основные этапы истории философии до XVII в. План: 1. Особенности древнегреческого мировоззрения и мировосприятия. 2. Библия и её влияние на историю западной философии. 3. Основные особенности философии эпохи Возрождения. 4. Последствия секуляризации культуры для общественного сознания западной Европы Нового Времени. 5. Эмпиризм и рационализм в философии Нового Времени. 6. Философия эпохи Просвещения. Задания: 1. Подготовить сообщения по вопросам. Методические указания. Цель занятия – проследить основные вехи трансформации философской мысли, связанных с удовлетворением социокультурных «вызовов» цивилизации. При подготовке презентаций, следует учитывать специфику миропонимания, выраженную в типичных мировоззренческих установках, соответствующих эпохам развития философской мысли: космоцентризм, теоцентризм, пантеизм, деизм, позитивизм, атеизм, плюрализм и пр., что отобразилось в проблематике и методологии философского мышления. Необходимо также давать четкие формулировки и объяснения базовым концепциям, характеризующим философские направления. Литература для подготовки к занятию: 1. Антисери Д., Реале Дж. Западная философия от истоков до наших дней. В 6 т. / Пер. с итал. С. Мальцевой. СПб.: Петрополис, I994-I996. 2. Виндельбанд В. История философии. Киев, 1997. 3. Мир философии: книга для чтения: В 2 ч. / Сост. П. С. Гуревич, В. И. Столяров. М. : Политиздат, 1991. 4. Рассел Б. Мудрость Запада: Историческое исследование западной философии в связи с общественными и политическими обстоятельствами. М., 1998. 5. Ясперс К. Всемирная история философии. Введение. Спб., 2000.
3	Основные этапы истории западной философии	2.2 Философия XVIII – XX вв. План 1) Феномен Немецкой классической философии; его предпосылки и влияние на мировую культуру. 2) Основные проблемы философии И. Канта. 3) Культурные и социальные предпосылки кризиса классической философии. 4) Основные направления в философии XIX века. 5) Основные направления философской мысли XX века. 6) Постмодернизм как феномен культуры 20 века. Задания: 1. Подготовить сообщения с презентациями.

		Методические указания. Данное занятие состоит из трех условно выделенных тематических блоков: Немецкая классика, философия XIX века, философия XX века. При подготовке к семинарскому занятию следует обратить внимание на многообразие направлений, концепций и проблем в указанных временных рамках. Рекомендуется подготовить сообщение, посвященное одной персоналии, однако при этом не забывать соотнести его философию с более общим контекстом: с идеями предшественников и последователей. Также следует обратить внимание на культурно-исторические обстоятельства, при которых развивались те или иные идеи. Литература для подготовки к занятию: 1. Антисери Д., Реале Дж. Западная философия от истоков до наших дней. В 6 т. / Пер. с итал. С. Мальцевой. СПб.: Петрополис, I994-I996. 2. Библер В.С. История философии как философия. // На гранях логики культуры. Книга избранных очерков. М., 1997. 3. Брикмон Ж., Сокал А. Интеллектуальные уловки: Критика современной философии постмодерна / Ин-т "Открытое общество" (Фонд Сороса); Пер.с англ. А. Костиковой и Д. Кралечкина. М., 2002. 4. Гулыга А. В. Кант. 4-е изд., испр. и доп.. М., 2005. 5. Ильин В.В. История философии. Спб., 2003. 6. Ильин И.П. Постструктурализм. Деконструктивизм. Постмодернизм.. М., 1996. 7. Пассмор Дж. Сто лет философии. М., 1998.
4	Проблема сознания в философии	План: 1. Дискуссии о генезисе и эволюции сознания 2. Индивидуальное и коллективное сознание. 3. Сознание и коммуникация. 4. Взаимосвязь сознательного и бессознательного. Задания: 1. Подготовить сообщения с презентациями; составить конспект источников по вопросам. Методические указания. Следует иметь в виду, что сознание является объектом изучения многих наук. Философия интерпретирует феномен сознание как источник и инструмент миропознания. При подготовке сообщений следует опираться не широкий спектр трактовок сознания, реализованных не только в классической, но и постклассической философиях, раскрывающих многообразие духовно-душевной жизни. Литература для подготовки к занятию: 1. Бескова Н.А. Эволюция и сознание: новый взгляд. М., 2002. 2. Иванов Е. М. Онтология субъективного. Саратов: 2007. 3. Дубровский Д. И. Информация, сознание, мозг. М., 1980. 4. Леонтьев А.Н. Эволюция психики. М., Воронеж, 1999. 5. Лурия А.Р. Язык и сознание. Ростов-на-Дону, 1998. 6. Мамардашвили М. К. Символ и сознание: Метафизические рассуждения о сознании, символике и языке / Под общ. ред. Ю. П. Сенокосова. М., 1997, 1999.

		7. Михайлов Ф.Т. Общественное сознание и самосознание индивида. М., 1990. 8. Молчанов В. И. Исследования по феноменологии сознания / В. И. Молчанов. - М.: Территория будущего, 2007. 9. Патнэм Х. Философия сознания / Пер.с англ. Макеевой Л.Б., Назаровой О.А., Никифорова А.Л.; Предисл. Макеевой Л.Б. М., 1999. 10. Прист С. Теории сознания. М., 2000. 11. Проблема сознания в современной западной философии: критика некоторых концепций: Сб. статей. Под ред. Т.А. Кузьмина. М., 1999. 12. Поппер К. Знание и психофизическая проблема. В защиту взаимодействия / пер. с англ. и послесл. И. В. Журавлева. М., 2008. 13. Райл Г. Понятие сознания. М., 1999. 14. Рубинштейн С. Л. Бытие и сознание. Человек и мир. СПб., 2003. 15. Сёрл Ж. Открывая сознание заново. М., 2000. 16. Субботский Е. В. Строящееся сознание. М., 2007. 17. Фрейд З. Психология бессознательного. М., 1989. 18. Эволюция, язык, познание: Когнитивная зволюция. Развитие научного знания. Эволюция мышления./ ИФ РАН. Под ред. Меркулова И.П. М., 1999. 19. Юнг К.Г. Психология бессознательного. М., 2003.
5	Возможности и границы познания	План: 1) Вера и знание 2) Социальная (коммуникативная) природа познания. 3) Специфика социального познания. 4) Критерии истины. 5) Основные концепции истины. Задания: 1. Подготовить сообщения по вопросам для обсуждения. 2. Составить конспект текстов. Методические указания. Проблема познания, в связи с развитием новых научных направлений (когнитивистика, неклассическая эпистемология, эволюционная эпистемология, философия науки), обрела новое звучание. При подготовке к занятию следует задействовать как классический, так и неклассический опыт разработки темы познания в философии. Особое значение, в связи с развитием эпистемологии социально-гуманитарных наук, приобрела концепция истины. Важно отметить различия в критериях истины естественных и гуманитарных наук. Литература для подготовки к занятию: 1. Джеймс У. Воля к вере. М., 1997. 2. Илларионов, С. В. Теория познания и философия науки. М., 2007. 3. Ильин В.В. Теория познания. Введение. Общие проблемы. М., 1993. 4. Когнитивный подход / РАН, Ин-т философии; отв. ред. В. А. Лекторский. М., 2008. 5. Лекторский В.А. Эпистемология классическая и неклассическая. М., 2001.

		6. Микешина А.А., Опенков М.Ю. Новые образы познания и реальности. М., 1997. 7. Микешина Л.А. Философия познания: полемические главы. М., 2002. 8. Микешина, Л. А. Эпистемология ценностей. М., РОССПЭН, 2007. 9. Основы теории познания. Под ред. Б.Н. Липского. Спб., 2000. 10.Поппер К. Знание и психофизическая проблема. В защиту взаимодействия / пер. с англ. и послесл. И. В. Журавлева. М., 2008. 11.Рассел Б. Человеческое познание: его сфера и границы. М., Киев, 2001. 12.Теория познания. В 4-х тт.. М., 1991. 13.Эволюционная эпистемология: проблемы и перспективы. М., 1996.
6	Научное познание и знание	План: 1) Критерии научности знания. 2) Научные революции и смена типов рациональности. 3) Многообразие вненаучных форм познания. Задания: 1. Подготовить сообщения с презентациями. Методические указания. Цель занятия – выявить специфику научного познания, его отличие от познания обыденного, художественного, философского и пр. Следует учитывать то, когда и почему стало формироваться научное познание, каковы его уровни и возможности. Способно ли научное познание оказать влияние на иные разновидности познания. Следует также обратить внимание на то, что научное познание, при наличии устойчивых критериев (поиск объективной истины, продуцирование транссубъективного знания о мире, набор методологических процедур), видоизменялось в истории, что связано со сменой научных парадигм. При подготовке презентаций следует учитывать мнения как представителей классической науки и философии, так и мнения неклассической и постнеклассической науки и философии. Литература для подготовки к занятию: 1. Альтернативные миры знания. Под ред. В.Н. Поруса и Е.Л. Чертковой. Спб., 2000. 2. Заблуждающийся разум? Многообразие вненаучного знания / Отв. ред. и сост. И.Т. Касавин. М., 1990. 3. Илларионов С. В. Теория познания и философия науки. М., 2007. Философия науки. Общий курс: учеб. пособие для вузов / Под ред. С. А. Лебедева. - 3-е изд., перераб. и доп.. М., 2006. 4. Кун Т. Структура научных революций. М., 2003. 5. Лакатос И. Фальсификация и методология научно-исследовательских программ. История науки и ее рациональные реконструкции // В кн. Кун Т. Структура научных революций. М., 2003. 6. Лекторский В.А. Эпистемология классическая и неклассическая. М., 2001.

		7. Никифоров, А. Л. Философия науки: история и теория. М., 2006. 8. Поппер К. Логика и рост научного знания. М.: Прогресс, 1993. 9. Стёпин В.С. Горохов В.Г., Розов М.А. Философия науки и техники. М., 1995. 10. Стёпин В.С. Теоретическое знание. М., 2000. 11. Теория познания. В 4-х тт.. М., 1991. 12. Фейерабенд, П. Против методологического принуждения: очерк анархистской теории познания. Благовещенск, 1999. 13. Швырёв В.С. Анализ научного познания: основные направления, формы, проблемы. М., 1988. 14. Эволюция, язык, познание: Когнитивная зволюция. Развитие научного знания. Эволюция мышления./ ИФ РАН. Под ред. Меркулова И.П. М., 1999.
7	Основы онтологии	План: 1) Виды бытия. 2) Материализм и идеализм. 3) Дискуссии о природе пространства и времени. Задания: 1. Подготовить сообщения с презентациями. Методические указания. Цель занятия – раскрыть основные философские представления об устройстве мира. Онтология – одна из дисциплин, входящих в состав метафизики, занимающейся изучением предельных оснований бытия. Тем не менее, современный философский обобщающий подход должен базироваться на сведениях, получаемых из научной среды. Задача философии состоит не в том, чтобы предоставить человеку единственно правильное видение мироустройства, но показать спектр обоснованных (имеющих свою логику и концептуальную выраженность) подходов понимания бытия. При подготовке к занятию, следует понимать разницу между метафизическим и физикалистским способом интерпретации устройства мира, учитывать, что философия осуществляет познания мира не непосредственно (обращаясь к объектам как таковым), но опосредованно, через систему «мир-человек». Кроме того, за длительный период своего существования, философия выработала множество способов понимания бытия, многие из которых противоречат друг другу, но их следует учитывать, чтобы уйти от догматизма в мышлении. Литература для подготовки к занятию: 1. Анисов А. М. Темпоральный универсум и его познание / РАН, Ин-т философии. М., 2000. 2. Аронов Р.А., Терентьев В.В. Существуют ли нефизические формы пространства и времени? // Вопросы философии, 1988, №1. С.71-84. 3. Ахундов М. Д. Пространство и время в физическом познании. М., 1982. 4. Горин Д. Г. Пространство и время в динамике российской цивилизации. М., 2003. 5. Доброхотов А Л. Категория бытия в классической западноевропейской философии. М., 1986.

		6. Купцов В.И. Детерминизм и вероятность. М., 1976. (в калининрадской областной библиотеке) 7. Проблемы пространства и времени в современном естествознании. Л., 1991. 8. Рейхенбах Г. Философия пространства и времени / пер. с англ. общ. ред. А.А. Логунова, Ю.Б. Молчанова. - 2-е, стер. М., 2003. 9. Уитроу Д. Естественная философия времени / пер. с англ., общ. ред. М.Э. Омельяновского. - 2-е, стереотип. М., 2003. 10. Уранос и Кронос : Хронотоп человеческого мира / Под ред. И.Т. Касавина; РАН, Ин-т философии. М., 2001.
8	Научная, философская и религиозная картины мира	План: 1) Современные космогонические представления. 2) Особенности синергетической картины мира. 3) Религия и наука в современном мире Задания: 1. Подготовить сообщения с презентациями. 2. Составить развернутый конспект по вопросам плана. Методические указания. При подготовке к занятию следует учитывать историческое своеобразие формирования картин мира, заключающееся в пересмотре и трансформации основ миропонимания. На занятии основное внимание следует уделить современным концепциям мировоззренческим концепциям, раскрывающим передовые положения в исследовании природы, космоса, человека. В вопросе, посвященном синергетике, следует обратить внимание на освещение универсальности метода. Учение о саморазвивающихся системах ныне реализуется как в естественных науках, так и социально-гуманитарных (естественнонаучная синергетика, социально-гуманитарная синергетика). В вопросе о взаимосвязи религии и науки следует отметить мировоззренческие изменения в современных религиозных концепциях и пути контакта религии и науки. Литература для подготовки к занятию: 9. Азимов А. В начале. М., 1989. 10. Барбур И. Религия и наука: история и современность. М., 2000. 11. Гейзенберг, В. Избранные философские работы. Шаги за горизонт. Часть и целое (Беседы вокруг атомной физики). СПб., 2006. 12. Готт В.С. Философские вопросы современной физики. М., 1988. 13. Карнап Р. Философские основания физики: введение в философию науки. М., 2003. 14. Койре А. От замкнутого мира к бесконечной вселенной. М., 2001. 15. Культура, человек и картина мира / АН СССР. Ин-т философии; Отв.ред. А.И. Арнольдов, В.А.Кругликов. М., 1987. 16. Пригожин И., Стенгерс И. Порядок из хаоса: новый диалог человека с природой. М., 1986.

		17. Рузавин Т. Н. Концепции современного естествознания. М., 1997. 18. Синергетическая парадигма. Многообразие поисков и подходов: Сборник / Редкол.: В.С.Стерин, С.П.Курдюмов, В.Д.Поремский и др. М., 2000.
9	Природа и сущность человека	План: 1) Сущностные различия между человеком и животным. 2) Дискуссии о происхождении человека. 3) Смысл жизни и смерти как философская проблема. 4) Дискуссии вокруг «права на смерть». 5) Феномен пола и его философское осмысление. Пол и гендер. Задания: 1. Подготовить сообщения с презентациями по каждому из вопросов. 2. Составить развернутый конспект. Методические указания. Цель занятия – рассмотреть базовые философские представления о человеке, его сущности и формах существования. Следует обратить внимание на современные (неклассические) подходы в понимании эволюции человека, его гендерной спецификации, представлении о значимости жизни и смерти. При подготовке презентаций, важно осмыслить такие понятия как «эволюция», «природа человека», «сущность человека», «существование», «жизнь», «смерть», «гендер», «смысл жизни», «экзистенциал», «забота», «страх», «страдание», «бытие-в- мире» («присутствие»). Литература для подготовки к занятию: 1. Андреев И.Л. Происхождение человека и общества. М., 1988. 2. Арьес Ф. Человек перед лицом смерти. М.,1992. 3. Бородай Ю.М. Эротика. Смерть. Табу: Трагедия человеческого сознания. М., 1996. 4. Бубер М. Проблема человека // Бубер М. Два образа веры. М., 1995. 5. Введение в гендерные исследования. Ч. 1: Учеб. пособие / Под ред. И. А. Жеребкиной. Харьков, Спб., 2001. 6. Вейнингер О. Пол и характер: Принцип, исследование. М., 1992. 7. Губин В., Некрасова Е.. Философская антропология : Учеб. пособие. М., 2000. 8. Гуревич П.С. Философия человека: В 2 ч. М., 2001. 9. Демидов А.Б. Феномены человеческого бытия: Учеб. пособие. Минск, 1999. 10. О человеческом в человеке / Под ред. И.Т. Фролова М., 1991. 11. Поршнев Б.Ф. О начале человеческой истории: проблемы палеопсихологии / Науч. ред. Олег Вите; Фонд исслед. им. Б. Поршнева "Общественный человек и человеческое о-во" (Поршневскйи Фонд). СПб., 2007. 12. Проблема человека в западной философии М., 1988. 13. Трубников Н.Н. О смысле жизни и смерти. М., 1996. 14. Франкл В. Человек в поисках смысла. М., 1990. 15. Фукуяма Ф. Конец истории и последний человек / пер.с

		англ. М.Б. Левина. М, 2005. 16. Человек: Мыслители прошлого и настоящего о его жизни, смерти и бессмертии. Древний мир — эпоха Просвещения / Редкол.: И. Т. Фролов и др.; Сост. П. С. Гуревич. — М., 1991. 17. Шаронов В.В. Основы социальной антропологии. СПб., 1997. 18. Энгельс Ф. Роль труда в процессе превращения обезьяны в человека. // Маркс К., Энгельс Ф. Собр. соч., 2-е изд., т.20. 19. Янкелевич В. Смерть. М., 1999.
10	Мотивы, нормы и ценности человеческой деятельности	План: 1) Человек как высшая ценность. Золотое правило морали и категорический императив И.Канта. 2) Нравственные ценности и их роль в жизни общества. 3) Эстетические ценности и их роль в жизни общества. 4) Религиозные ценности и свобода слова. 5) Ненасилие и толерантность как ценности. Задания: 1. Подготовить сообщение. 2. Подготовить конспекты по вопросам. Методические указания. Цель занятия – познакомить студентов с учениями о ценностях. Важно проследить особенности формирования аксиологических концепций в классической и неклассической философиях. Отдельно рассматриваются нравственные, эстетические и религиозные ценности. При подготовке темы, посвященной проблемам ненасилия и толерантности, следует привлечь материалы из смежных областей – социологии, культурологии, политологии, конкретизирующие отдельные философские размышления. Литература для подготовки к занятию: 1. Адорно Т.В. Проблемы философии морали. М., 2000. 2. Апресян Р.Г. Идея морали. М., 1995. 3. Борев Ю. Б. Эстетика: учебник для вузов. М., 2002. 4. Голубева О. Ю., Попов Л. М., Устин П. Н. Добро и зло в этической психологии личности / РАН, Ин-т психологии. М., 2008. 5. Гуревич П. С. Этика: учеб. для вузов. М., 2006. 6. Гусейнов А.А., Апресян Р.Г. Этика. М., 2004. 7. Каган М.С. Философская теория ценностей. Спб., 1997. 8. Кант И. Наблюдения над чувством прекрасного и возвышенного // Кант И. Сочинения: В 8 т. М., 1994. Т. 2. 9. Кант И. Основоположения метафизики нравов // Кант И. Сочинения: В 8 т. М., 1994. Т. 4. 10. Микешина Л. А. Эпистемология ценностей. М., 2007. 11. Ненасилие: Философия, этика, политика / А.А.Гусейнов и др.; отв. ред. А.А. Гусейнов; РАН, Ин-т философии. М., 1993. 12. Никитина И. П. Эстетика: учеб. пособие. М., 2008. 13. Пейдж Г. Д. Общество без убийства: Возможно ли это? СПб., 2005. 14. Столович Л.Н. Красота. Добро. Истина. М., 1994. 15. Толерантность / Общ. ред. М.П. Мчедлова; Ин-т комплексных соц.исследований РАН; Исслед.центр "Религия в современном обществе"; Моск. гос. соц. ун-т. М., 2004.

		16. Тоффлер Э., Тоффлер Х. Война и антивойна. Что такое война и как с ней бороться. Как выжить на рассвете XXI века. М., 2005. 17. Франкл В. Человек в поисках смысла. М., 1990. 18. Швейцер А. Культура и этика. М., 1973.
11	Природа и сущность социальности	План: 1) Информационная специфика деятельности. 2) Адаптивная специфика деятельности. 3) Подсистемы, элементы, компоненты общества. Задания: 1. Подготовить сообщения с презентациями по первым двум вопросам. Методические указания. Одной из существенных и «прорывных» тем отечественной философии середины XX века стала тема деятельности. Деятельность в философии рассматривается как осмысленное, целенаправленное действие человека (людей) по преобразованию мира. Огромную роль в формировании деятельности играет социальная среда (социум), способствующий формированию у субъекта (ов) критериев (норм, идеалов, ценностей, мотивов), приемов, видов и способов деятельности. Цель занятия – рассмотреть многостороннюю специфику деятельности вне отрыва от общества. При подготовке презентаций, следует учитывать как классические модели философского осмысления общества, так и современные. Немаловажным является и вопрос о разнообразии подходов в осмыслении общества(эволюционный, формационный, структурно-ситстемный и пр.) Литература для подготовки к занятию: 1. Андреев И.Л. Происхождение человека и общества. М., 1988. 2. Барулин В.С. Социальная философия. Учебное пособие для студентов вузов. М., 2002. 3. Кемеров В.Е. Введение в социальную философию. Учебное пособие для гуманитарных вузов. М., 1996. 4. Крапивенский С. Э. Социальная философия: учебник для студ. гуманит.-соц. спец. вузов. - 4-е изд., испр. М., 2004 5. Момджян К.Х. Введение в социальную философию: Учебное пособие для студентов вузов. М., 1997. 6. Парсонс Т. О социальных системах. М., 2002. 7. Парсонс Т. О структуре социального действия. М., 2000. 8. Пигров К.С. Социальная философия: учебник для гуманитарных вузов. СПб., 2005. 9. Сильверстов В.В. Культура. Деятельность. Общение. М., 1998. (в калининрадской областной библиотеке) 10. Соколов С. В. Социальная философия: Учебное пособие для студентов вузов. М., 2003. 11. Сорокин П. Человек. Цивилизация. Общество. М., 1992. 12. Социальная философия. Учебник / Под ред. И.А. Гобозова. М., 2003.

		13. Социальная философия: словарь / Под общ. ред. В.Е. Кемерова, Т.Х. Керимова. М.: Акад. Проект, 2003. 14. Франк С.Л. Духовные основы общества. М., 1992.

Требования к самостоятельной работе обучающихся

1. Работа с лекционным материалом, предусматривающая проработку конспекта лекций и учебной литературы, по всем темам из п. 6 настоящей рабочей программы.

2. Выполнение домашнего задания, предусматривающего решение задач, выполнение упражнений, выдаваемых на практических занятиях, по всем темам из п. 6 настоящей рабочей программы.

Руководствуясь положениями статьи 47 и статьи 48 Федерального закона от 29 декабря 2012 г. N 273-ФЗ «Об образовании в Российской Федерации» научно-педагогические работники и иные лица, привлекаемые университетом к реализации данной образовательной программы, пользуются предоставленными академическими правами и свободами в части свободы преподавания, свободы от вмешательства в профессиональную деятельность; свободы выбора и использования педагогически обоснованных форм, средств, методов обучения и воспитания; права на творческую инициативу, разработку и применение авторских программ и методов обучения и воспитания в пределах реализуемой образовательной программы и отдельной дисциплины.

Исходя из рамок, установленных учебным планом по трудоемкости и видам учебной работы по дисциплине, преподаватель самостоятельно выбирает тематику занятий по формам и количеству часов проведения контактной работы: лекции и иные учебные занятия, предусматривающие преимущественную передачу учебной информации преподавателем и (или) занятия семинарского типа (семинары, практические занятия, практикумы, лабораторные работы, коллоквиумы и иные аналогичные занятия), и (или) групповые консультации, и (или) индивидуальную работу обучающихся с преподавателем, в том числе индивидуальные консультации (по курсовым работам/проектам – при наличии курсовой работы/проекта по данной дисциплине в учебном плане).

Рекомендуемая тематика занятий максимально полно реализуется в контактной работе с обучающимися очной формы обучения. В случае реализации образовательной программы в заочной / очно-заочной форме трудоемкость дисциплины сохраняется, однако объем учебного материала в значительной части осваивается обучающимися в форме самостоятельной работы. При этом требования к ожидаемым образовательным результатам обучающихся по данной дисциплине не зависят от формы реализации образовательной программы.

7. Методические рекомендации по видам занятий

Лекционные занятия.

В ходе лекционных занятий обучающимся рекомендуется выполнять следующие действия. Вести конспектирование учебного материала. Обращать внимание на категории, формулировки, раскрывающие содержание тех или иных явлений и процессов, научные выводы и практические рекомендации по их применению. Задавать преподавателю уточняющие вопросы с целью уяснения теоретических положений, разрешения спорных ситуаций.

Желательно оставить в рабочих конспектах поля, на которых во внеаудиторное время можно сделать пометки из рекомендованной литературы, дополняющие материал прослушанной лекции, а также подчеркивающие особую важность тех или иных теоретических положений.

Практические и семинарские занятия.

На практических и семинарских занятиях в зависимости от темы занятия выполняется поиск информации по решению проблем, практические упражнения, контрольные работы, выработка индивидуальных или групповых решений, итоговое обсуждение с обменом знаниями, участие в круглых столах, разбор конкретных ситуаций, командная работа, представление портфолио и т.п.

Самостоятельная работа.

Самостоятельная работа осуществляется в виде изучения литературы, эмпирических данных по публикациям и конкретных ситуаций из практики, подготовке индивидуальных работ, работа с лекционным материалом, самостоятельное изучение отдельных тем дисциплины; поиск и обзор литературы и электронных источников; чтение и изучение учебника и учебных пособий.

8. Фонд оценочных средств

8.1. Перечень компетенций с указанием этапов их формирования в процессе освоения образовательной программы в рамках учебной дисциплины

Основными этапами формирования указанных компетенций при изучении обучающимися дисциплины являются последовательное изучение содержательно связанных между собой тем учебных занятий. Изучение каждой темы предполагает овладение обучающимися необходимыми компетенциями. Результат аттестации обучающихся на различных этапах формирования компетенций показывает уровень освоения компетенций.

Контролируемые разделы (темы) дисциплины	Индекс контролируемой компетенции (или её части)	Оценочные средства по этапам формирования компетенций
		текущий контроль по дисциплине
Тема 1. Предмет и метод философии. Специфика философского знания	УК-5	Тестирование
Тема 2. Роль философии в жизни человека и общества	УК-5	Тестирование
Тема 3. От мифа к логосу: генезис и становление философии	УК-5	Тестирование
Тема 4. Основные этапы истории западной философии	УК-5	Тестирование Опрос на семинарском занятии
Тема 5. Духовные основы и особенности русской философии	УК-5	Тестирование
Тема 6. Проблема сознания в философии	УК-5	Тестирование Опрос на семинарском занятии
Тема 7. Возможности и границы познания	УК-5	Тестирование Опрос на семинарском занятии
Тема 8. Научное познание и знание	УК-5	Тестирование Опрос на семинарском занятии
Тема 9. Основы онтологии	УК-5	Тестирование Опрос на семинарском занятии

Контролируемые разделы (темы) дисциплины	Индекс контролируемой компетенции (или её части)	Оценочные средства по этапам формирования компетенций
		текущий контроль по дисциплине
Тема 10. Научная, философская и религиозная картины мира	УК-5	Тестирование Опрос на семинарском занятии
Тема 11. Природа и сущность человека	УК-5	Тестирование Опрос на семинарском занятии
Тема 12. Мотивы, нормы и ценности человеческой деятельности	УК-5	Тестирование Опрос на семинарском занятии
Тема 13. Природа и сущность социальности	УК-5	Тестирование Опрос на семинарском занятии
Тема 14. Общество и личность. Проблема свободы и ответственности	УК-5	Тестирование
Тема 15. Основы философии истории	УК-5	Тестирование
Тема 16. Проблемы и перспективы современной цивилизации	УК-5	Тестирование

8.2. Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений и навыков и (или) опыта деятельности процессе текущего контроля

Тестовые задания:

Тема 1. Предмет и метод философии. Специфика философского знания
Тема 2. Роль философии в жизни человека и общества

- Наиболее общие вопросы бытия в философии исследует …

1) *онтология* 2) гносеология 3) диалектика 4) логика

- Гносеология – это философское учение о …

1) природе 2) бытии 3) человеке 4) *познании*.

- Философское учение о ценностях называется …

1) теологией 2)гносеологией 3) онтологией 4)*аксиологией*.

- Философия, исследуемая в процессе её предистории, возникновения, становления и развития, есть …

1) культурология 2) эпистемология 3) *история философской мысли* 4) онтология

- Философская антропология – это философское учение о …

1) обществе 2) цивилизации 3) природе 4) *человеке.*

- Социальная философия – это максимально обобщенное знание об …

1) культуре 2) человеке 3) природе 4) *обществе.*

- Постижением закономерностей процесса развития общества во времени занимается …

1) *философия истории* 2) философии человека 3) истории философии 4) философия культуры

- Учение, не являющееся разделом философии, - это …

1) *искусствознание*; 2) онтология; 3)этика; 4) логика

- Исследованием сущности и происхождения морали, значения нравственных норм в жизни человека занимается

1) аксиология; 2) эстетика; 3) идеология; 4) *этика*

- Теоретическим ядром духовной культуры человека и общества называют …

1) религию; 2) *философию*; 3) мифологию; 4) искусство

- Миссию формирования целостной картины мира и бытия человека в нем выполняет _____функция философии …

1) методологическая; 2) *мировоззренческая*; 3) гносеологическая; 4) эвристическая

- Содержание _____функции философии составляет формирование у человека и общества ценностных ориентаций и идеалов …

1) критической; 2) *аксиологической*; 3) логической; 4) интегральной

- Философия, помогая индивиду обрести позитивный и глубинный смысл жизни, ориентироваться в кризисных ситуациях, реализует свою _____функцию …

1) *гуманистическую*; 2) аксиологическую; 3) критическую; 4) теоретическую

Когда философия учит, ничего сразу не принимать и не отвергать без глубокого и самостоятельного размышления и анализа, то её деятельность связана с _____ функцией …

1) гносеологической; 2) *критической*; 3) мировоззренческой; 4) прогностической

- _____функция философии базируется на её способности в союзе с наукой предсказывать общий ход развития бытия …

1) прогностическая; 2) *эвристическая*; 3) отражательно-информационная; 4) аксиологическая

- Обоснование ценности человека и его свободы, решение вопроса о смысле жизни связано с _____ функцией

1) *гуманистической*; 2) аксиологической; 3) идеологической; 4) критической

- Философия представляет собой ….

1) сложившуюся картину мира, принятую специалистами;
2) систему взглядов на мир в целом и на отношение человека к этому миру;
3) мировоззрение, основу которого составляют фантазии, легенды, вымыслы;
4) набор разнообразных знаний, обслуживающих повседневную жизнь людей

- Предметом _____ является всеобщее в системе «человек –мир» …

1) науки; 2) психологии; 3) философии; 4) искусства

- Основной вопрос философии формулируется как вопрос об отношении…

1) человека к миру; 2) общества к природе; 3) *мышления к бытию;* 4) цивилизации к культуре

- Философия была и остается…

1) то единой, то нет; 2) дуалистической, раздвоенной; 3) единой, монолитной;
4) *плюралистической, многообразной*

- Характерной чертой _____ проблем признают их вечность, открытость …

1) религиозных; 2) научных; 3) *философских*; 4) глобальных

- Наиболее ранней формой духовно-практического освоения мира человечеством считается

1) философия; 2) *мифология*; 3) религия; 4) наука.

- В искусстве, в отличие от философии, опыт транслируется в

1) гипотезах; 2) *образах*; 3) экспериментах; 4) теориях

- Философским может быть назван вопрос

1) «Возможны ли небелковые формы жизни»?; 2) «*Как отличить истину от заблуждения*?»; 3) «Является ли Плутон планетой?»; 4) «Обусловлена ли нравственность человека генетикой?»

- Проблемы, решаемые философией

1) могут быть решены в рамках конкретной научной дисциплины; 2) не имеют ничего общего с жизнью конкретных людей; 3) имеют отношение к сверхъестественному нереальному миру; 4) *имеют всеобщий, предельный характер*

Тема 3. От мифа к логосу: генезис и становление философии

- Философия возникла в период …

1) 1-2 вв. н.э. 2) 5-4 вв. н.э. 3) *7 – 6 вв. до н.э.* 4) 9-8 вв. до н.э.

- Согласно легенде, первым, кто отказался называть себя мудрецом, но лишь любомудром, т.е. философом, был …

1) Фалес 2) *Пифагор*. 3) Платон 4) Сократ

- Философия родилась через преодоление …

1) язычества 2) *мифа*. 3) логоса 4) рационализма

Тема 4. Основные этапы истории западной философии

АНТИЧНАЯ ФИЛОСОФИЯ:

- Принято считать, что создателями древнегреческой философии являются три мыслителя, жившие в Милете: …

1) Протагор, Горгий, Продик 2) Ксенофан, Парменид, Зенон 3) Сократ, Платон, Аристотель
4) *Фалес, Анаксимен, Анаксимандр.*

- Исторически первой попыткой постижения количественной стороны мироздания является учение

1) Гераклита; 2) Аристотеля; 3) Пифагора; 4) *Парменида*

- Согласно Пармениду, бытие есть

1) иллюзия; 2) чувственно воспринимаемый мир; 3) процесс непрерывного изменения и становления; 4) *то, что неподвижно, неизменно, непостигаемо*

- Автором знаменитых апорий «Ахиллес и черепаха», «Стрела» является

1) Аристотель; 2) Сократ; 3) Платон; 4) *Зенон Элейский*

- Переориентация античной философии с темы природы на тему человека связана с именем …

1) Парменида 2) *Сократа*. 3) Демокрита 4) Эпикура

- Греческая мысль зародилась в городах Ионии (побережье Малой Азии) и Южной Италии, а своего расцвета достигла в …

1) Эретрии 2) *Афинах* 3) Спарте 4) Дельфах

- Античный философ _____ связал добродетель со знанием, создав концепцию этического интеллектуализма

1) Парменид; 2) Платон; 3) Аристотель; 4) *Сократ*

- Разработка «майевтики» как способа достижения истины связана с именем

1) Диогена; 2) Гераклита;) Аристотеля; 4) *Сократа*

- Софисты и Сократ вошли в историю Античной философии своей ориентацией на

1) историю 2) космос 3) государство 4) *человека*.

- Древнегреческий философ, ставший символом грубой откровенности

1) Сократ; 2) *Диоген*; 3) Эпикур; 4) Протагор

- Истинное бытие, по Платону, есть

1) *мир эйдосов*; 2) мир чувственно воспринимаемых вещей; 3) космос; 4) мир человеческой души

- Философское учение Платона, утверждающее, что мир вещей зависит от мира идей называется …

1)материализмом 2) субъективным идеализмом 3) рационализмом 4)*объективным идеализмом*.

- Философ, полагавший, что в основе бытия лежит материя и форма

1) *Аристотель*; 2) Демокрит; 3) Сократ; 4) Платон

- Античный философ, создавший логику как науку -

1) Сократ; 2) Платон; 3) *Аристотель*; 4) Парменид

- Теория, исследующая первые начала и причины, была названа у Аристотеля …

1) *метафизикой* 2) философией 3) физикой 4) топикой.

- К Эллинистическому периоду древнегреческой философии относятся школа:

1) милетская; 2) пифагорейцев; 3) *эпикурейцев*; 4) элеатов

- Господствующим типом философского мировоззрения Античной эпохи признается …

1) теоцентризм 2) *космоцентризм* 3) социоцентризм 4)антропоцентризм .

- Создателем первой философской теории Античности является…

1) Пифагор; 2) *Фалес*; 3) Платон; 4) Диоген

- Первым европейским философом, поставившим вопрос о первоначале мира является

1) Платон; 2) *Фалес*; 3) Аристотель; 4) Демокрит

ФИЛОСОФИЯ СРЕДНИХ ВЕКОВ

- Философия в Средние века занимала подчиненное положение по отношению к ….

1) науке 2) этике 3) *богословию* 4) эстетике

- Господствующим типом философского мировоззрения в эпоху Средневековья признается …

1) антропоцентризм 2) космоцентризм 3) наукоцентризм 4) *теоцентризм*.

- Учение о сотворении мира Богом, сразу и из Ничего называется …

1)теизмом 2) *креационизмом*. 3) провиденцианизмом 4) томизмом

- Христианская философия неразрывно связана с ….., согласно которому все в истории и судьбах людей предопределено волей Бога

1) теоцентризмом 2) креационизмом 3) *провиденциализмом*. 4) интуитивизмом

- Основные положения христианской религии были сформулированы мыслителями эпохи «отцов Церкви», т.е. …

1) рационализма 2) эллинизма 3) *патристики* 4) схоластики

- Пять рациональных доказательств существования Бога сформулированы основателем томизма …

1)Ансельмом Кентерберийским 2) Пьером Абеляром 3) *Фомой Аквинским.* 4) Аврелием Августином

- Согласно Фоме Аквинскому бытие и сущность

1) совпадают в человеке; 2) совпадают в творении Божьем в мире; 3) *совпадают в Боге*;
4) никогда не совпадают

- Вековой спор средневековых мыслителей об «универсалиях», т.е. общих понятиях, разделил их на два основных лагеря: …

1) диалектиков и метафизиков 2) *реалистов и номиналистов*;
3)монистов и дуалистов; 4) эмпириков и рационалистов.

- «Бритва Оккама» отражает содержание принципа

1) «*не следует умножать сущности сверх необходимости»;* 2) «нет ничего, помимо Бога, и Бог есть бытие»; 3) все сущее – благо; 4) « возлюби ближнего своего, как самого себя»

9-14 века в средневековой европейской философии называются этапом

1) *схоластики*; 2) софистики; 3) апологетики; 4) патристики

- Средневековая схоластика ориентирована на учение…

1) *Аристотеля*; 2) Сократа; 3) Протагора; 4) Платона

- Выдающимся представителем эпохи патристики является

1) У. Оккам, Ф. Аквинский, *Августин Аврелий;* Р. Бэкон

ФИЛОСОФИЯ РЕНЕССАНСА

Эпохой восстановления идеалов античности в Европе считается …
1) Средние века; 2) Новое время; 3) *Ренессанс*; 4) Реформация

Умонастроение, преобладавшее в эпоху Возрождения, - …
1) интуитивизм; 2) космизм; 3) теизм; 4) *гуманизм*;

Для эпохи Возрождения характерен ….
1) природоцентризм; 2) теоцентризм; 3) культуроцентризм; 4)*антропоцентризм*

Внимание мыслителей Возрождения направлено преимущественно на …
1)Бога; 2) Космос; 3)*человека*; 4) язык.

Доминирующая тема философии Ренессанса …
1)знание; 2) мораль; 3) Бог; 4) *творчество человека*

Земля и Солнце – рядовые небесные тела в бесконечной, одушевленной, деятельной, наполненной разумной жизнью Вселенной, - утверждал мыслитель Ренессанса …
1) Мишель Монтень; 2) *Джордано Бруно*; 3) Франческо Петрарка; 4) Данте Алигьери

Пантеизм, основы которого были заложены философом-кардиналом Н.Кузанским, объединяет и отождествляет ….
1) человека и природу; 2) Бога и человека; 3) *Бога и природу*; 4) конечное и бесконечное

Вопросы философии политики в период Возрождения разрабатывались …
1) Галилео Галилием; 2) Леонардо да Винчи; 3) *Никколо Макиавелли*; 4) Николаем Коперником

В философии позднего Возрождения наблюдается разочарование в принципах …
1) космоцентризма; 2)*антропоцентризма*; 3) антропоморфизма; 4) теоцентризма

Родоначальник гуманистического движения, поэт и мыслитель раннего Возрождения …
1) Лоренцо Вала; 2) Джованни Боккаччо; 3) Данте Алигьери; 4) *Франческа Петрарка.*

Создатель первой литературной утопии, написанной по – латыни, нарисовавший картину идеального общества без частной собственности – это
1) Аврелий Августин; 2) Платон; 3) Томазо Компанелла;4) *Томас Мор*

Автором работы «Государь», обосновавшим принцип политического искусства является
1) Т. Мор; 2) *Н. Макиавелли;* 3) Л. Вала; 4) Т. Кампанелла

Главной целью Реформации XVI в. являлось

1) *преображение католической церкви*; 2) реформация церковной православной власти; 3) распространение идеологии католической церкви; 4) сближение католической и православной церкви

Автор «Опытов» и создатель нового литературного жанра - эссе
1) Данте; 2) Н. Макиавелли; *М. Монтень*; Э. Роттердамский

В основе философии Дж.Бруно лежит
1) *пантеизм*; б) натурализм; 3) деизм; 4) гедонизм

Немецкий кардинал, учение которого совпадение противоположностей способствовало отказу от геоцентрической модели мира
1) Дж.Бруно; 2) Г.Галилей; 3) *Н.Кузанский;* 4) Н.Коперник

Выдающийся деятель Возрождения, автор сочинения «Похвала глупости»
1) Т. Мор; 2) Н. Кузанский; 3) *Э. Роттердамский;* 4) М. Монтень

В основе натурфилософии Возрождения лежит
1) теизм; 2) эстетизм; 3) *пантеизм*; 4) гуманизм

Возрождение как движение в европейской культуре возникло в (во)
1) Франции; 2) Германии; 3) *Италии*; 4) Англии

Тезис Джордано Бруно «…Природа есть …не что иное, как Бог в вещах» выражает позицию
1) *пантеизма*; 2) панлогизма; 3) деизма; 4) атеизма

ФИЛОСОФИЯ НОВОГО ВРЕМЕНИ

Родоначальником эмпиризма как философского направления эпохи Нового времени явился...
1) Джон Локк; 2) *Френсис Бэкон*; 3)Томас Гоббс; 4) Декарт

Проблемы теории познания, поиска научного метода, противостояния эмпиризма и рационализма становятся центральными в европейской философии ...
1) XIX в.; 2) XVIII в.; 3) XVI в.; 4) *XVII в.*

Главной познавательной способностью человека и его судьей является разум
- утверждали представители рационализма XVII века ...
1) П. Гассенди, П. Бейль, Н. Мальбранш; 2) *Р. Декарт, Б. Спиноза, Г. Лейбниц;* 3) Ф. Бэкон, Т. Гоббс, Д. Локк; 4) Д. Дидро, К. Гельвеции, П. Гольбах

Все из опыта, - доказывали сторонники эмпиризма XVII века ...
1) П. Гассенди, П. Бейль, Н. Мальбранш; 2) Р. Декарт, Б. Спиноза, Г. Лейбниц; 3) *Ф. Бэкон, Т. Гоббс, Д. Локк;* 4) Д. Дидро, К. Гельвеции, П. Гольбах

Критическое отношение философии к церкви и религии является отличительной чертой эпохи ...
1) Ренессанса; 2) Античности; 3) Средневековья; 4) *Просвещения*

Идеи философии Просвещения ярко воплощены в первой в мире «Энциклопедии, или Толковом словаре наук, искусств и ремесел», написанной в ...
1) Германии; 2) *Франции*; 3) Италии; 4) Англии

Философская позиция Дж. Беркли и Д. Юма характеризуется как
1) абсолютный идеализм; 2) объективный идеализм; 3) *субъективный идеализм*; 4) материализм

Родоначальником немецкой классической философии считают ...
1) Л. Фейербаха; 2) *И. Канта;* 3) И. Фихте; 4) Г. Гегеля

Центральное понятие философии Гегеля
1) Бог; 2) Всеединство; 3) *Абсолютная идея;* 4) Мировая воля

Учение Л.Фейербаха характеризуется как..
1) *антропологический материализм;* 2) механический материализм; 3) стихийный материализм; 4) наивный материализм

Переход от классической к неклассической, иррационалистической философии связан с именами
1) *А. Шопенгауэра и Ф. Ницше;* 2) Ч. Пирса и У. Джемса; 3) К. Маркса и Ф. Энгельса
4) О. Конта и Г. Спенсера

Учение К.Маркса и Ф. Энгельса характеризуется как
1) субъективный идеализм; 2) наивный и стихийный материализм; 3) вульгарный материализм; 4) *диалектический и исторический материализм*

Философ-автор учения о множественности субстанций
1) *Г. Лейбниц;* 2) Г. В. Гегель; 3) Б. Спиноза; 4) Дж. Бруно

Центральная проблема философии Канта – это …
1) *нахождение всеобщих и необходимых оснований познания и гуманистических ценностей*; 2) исследование движущихся сил развития истории; 3) исследование предельных основ бытия; 4) анализ саморазвития абсолютной идеи.

СОВРЕМЕННАЯ ФИЛОСОФИЯ

СОВРЕМЕННАЯ ФИЛОСОФИЯ ЗАПАДА

Влиятельное направление в современной философии, связанное с именем Эдмунда Гуссерля, ...
1) постмодернизм; 2) *феноменология*; 3) герменевтика; 4) неотомизм

Идеи свободы, приоритета индивидуального бытия над социальным характерны для ...
1) позитивизма; 2) марксизма; 3) структурализма; 4) *экзистенциализма*

Экстравагантная, по мнению многих, философия, «современный вариант релятивизма и скептицизма» ...
1) экзистенциализм; 2) *постмодернизм*; 3) интуитивизм; 4) неопозитивизм

По мнению теоретиков популярного в США течения, философия призвана спуститься с «небес на землю» для решения жизненных проблем человека
1) консерватизма; 2) прагматизма; 3)*персонализма*; 4) марксизма

Проблемы языка, науки, логики занимают центральное место в ...

1) прагматизме; 2) фрейдизме; 3) *аналитической философии;* 4) экзистенциализме

Способом существования человека в мире объявляет понимание, связанное с языком, текстом, диалогом
1) *структурализм* ; 2) герменевтика; 3)номинализм; 4) персонализм

Характерной чертой философии постмодернизма является…
1) исторический оптимизм; 2) *замена объективной реальности знаково-символическими картинами мира*; 3) исследование предельных основ бытия; 4) рационализм

Исчезновение Я как результат коммуникативных взаимодействий провозглашается в
1) неофрейдизме; 2) феноменологии; 3) позитивизме; 4) *постмодернизме*

Возникновение психоанализа связано с именем
1) А. Шопенгауэра; 2) Ф. Ницше; 3) Э. Гуссерля; 4) *З. Фрейда*

Направление современной западной философии, обосновывавшее понимание как метод познания называется
1) номинализмом; 2) структурализмом; 3) *герменевтикой*; 4) персонализмом

Тема 5. Духовные основы и особенности русской философии

Ключевой проблемой в русской философии является...
1) пути достижения научного знания; 2) *смысл жизни и призвание человека;*
3) происхождение и сущность сознания; 4) защита собственности и свободы

Идеализация русских самобытных начал, проповедь национальной исключительности России принадлежит ...
1) народникам; 2) марксистам; 3) *славянофилам*; 4) западникам

Создателем религиозно-философского учения о всеединстве в русской философии был ...
1) Герцен А.И.; 2) Чернышевский Н.Г.; 3)Бакунин М.А.; 4) *Соловьев В.С.*

Представитель русского космизма, учения русской философии конца XIX- начала XX века о неразрывном единстве человека, Земли и космоса,
1) Хомяков А.С.; 2) Чаадаев П.Я.; 3) *Вернадский В.И.* ; 4) Бердяев Н.А.

Представителем марксизма в русской философии является ..,
1) Федоров Н.Ф.; 2) *Плеханов Г.В.;* 3) Чижевский А.Л.; 4) Флоренский П.А..

Философ русского зарубежья, автор исследования «О сопротивлении злу силой», перезахороненный в 2005 г. на Родине ...
1) Сорокин П.А.; 2) Бердяев Н.А.; 3) Карсавин Л.П.; 4) *Ильин И.А.*

8.3. Перечень вопросов и заданий для промежуточной аттестации по дисциплине

Вопросы для промежуточного контроля (зачета)

1. Предмет и метод философии. Специфика философского знания.
2. Смысл и назначение философии. Основные функции философии.
3. Философия и наука.

4. Философия и искусство.
5. Философия и религия.
6. Философия и обыденное сознание.
7. Философия и идеология.
8. Философия и мировоззрение.
9. Философия и культура. Философская культура личности.
10. Генезис философии. От мифа к логосу.
11. Даосизм и конфуцианство
12. Основные особенности, школы и понятия древнеиндийской философии.
13. Античная философия: общая характеристика.
14. Основные проблемы и школы досократической философии.
15. Платон и Аристотель о бытии, душе и познании.
16. Этические школы эллинизма (киники, эпикурейцы, стоики, скептики)
17. Основные этапы, проблемы и особенности средневековой христианской мысли.
18. Новые тенденции в философии эпохи Возрождения.
19. Наука и философия в Новое Время.
20. Немецкая классическая философия: общая характеристика.
21. Основные особенности современной философии. Постмодернизм.
22. Сциентизм и антисциентизм в философии 20 в.
23. Духовные основания и особенности русской философии.
24. Сознательное и бессознательное в человеческой психике. Основные характеристики сознания.
25. Понятие идеального. Сознание и мозг. Идеалистическая и материалистическая трактовки сознания.
26. Структура сознания. Предметное сознание и самосознание.
27. Сознание и язык.
28. Сущность познавательного процесса. Основные гносеологические модели.
29. Познавательные способности человека. Эмпиризм, рационализм, иррационализм.
30. Проблема истины и её критериев.
31. Познание и общение. Объяснение и понимание.
32. Научное знание, его структура, критерии, методы получения и обоснования. Роль научного знания в культуре.
33. Знание и вера.
34. Специфика социального познания.
35. Ценности: понятие, основные виды, роль в человеческой жизни и культуре.
36. Категория бытия. Виды бытия.
37. Единство и многообразие мира. Понятие субстанции. Монизм, дуализм, плюрализм.
38. Пространство и время.
39. Детерминизм и индетерминизм. Типы причинных связей и взаимодействий. Случайность и необходимость. Динамические и статистические закономерности.
40. Системность бытия. Методологический принцип системности.
41. Понятия движения и развития. Прогресс и регресс. Основные закономерности развития.
42. Человек, его природа и сущность.
43. Основные гипотезы и факторы антропогенеза.
44. Мотивы человеческой деятельности.
45. Проблема жизни и смерти в духовном опыте человека. Смысл жизни и «экзистенциальный вакуум». Проблема смерти в современных этических дискуссиях.
46. Феномен пола и его философское осмысление. Пол и гендер.

47. Социальное и природное. Деятельность как субстанция социального.
48. Общество: понятие и структура.
49. Общество как саморазвивающаяся система.
50. Общество, культура, цивилизация: соотношение понятий.
51. Единство и многообразие культур. Россия, Восток, Запад в диалоге культур.
52. Понятие личности. Социализация личности. Личность и масса.
53. Социальные нормы. Проблема свободы и ответственности.
54. Человек в технократическом обществе. Антропологический кризис.
55. Единство и многообразие исторического процесса. Случайное и необходимое в истории.
56. Проблема смысла истории. Направленность и формы исторического процесса.
57. Формационный и цивилизационный подходы к рассмотрению истории.
58. Культурно-исторический прогресс: понятие, движущие силы, критерии. Проблема гуманистического измерения прогресса.
59. Глобальные проблемы современности. Понятие, классификация и перспективы решения.
60. Перспективы человеческой цивилизации. Основные футурологические концепции

8.4. Планируемые уровни сформированности компетенций обучающихся и критерии оценивания

Уровни	Содержательное описание уровня	Основные признаки выделения уровня (этапы формирования компетенции, критерии оценки сформированности)	Пятибалльная шкала (академическая) оценка	Двухбалльная шакала, зачет	БРС, % освоения (рейтинговая оценка)
Повышенный	Творческая деятельность	*Включает нижестоящий уровень.* Умение самостоятельно принимать решение, решать проблему/задачу теоретического и прикладного характера на основе изученных методов, приемов, технологий	отлично	зачтено	86-100
Базовый	Применение знаний и умений в более широких контекстах учебной и профессиональной деятельности, нежели по	*Включает нижестоящий уровень.* Способность собирать, систематизировать, анализировать и грамотно использовать информацию из самостоятельно найденных теоретических источников и	хорошо		71-85

	образцу с большей степени самостоятельности и инициативы	иллюстрировать ими теоретические положения или обосновывать практику применения			
Удовлетворительный (достаточный)	Репродуктивная деятельность	Изложение в пределах задач курса теоретически и практически контролируемого материала	удовлетворительно		55-70
Недостаточный	Отсутствие признаков удовлетворительного уровня		неудовлетворительно	не зачтено	Менее 55

9. Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины.

Основная литература

1. Данильян, О. Г. Философия : учебник / О.Г. Данильян, В.М. Тараненко. — 2-е изд., перераб. и доп. — Москва : ИНФРА-М, 2021. — 432 с. — (Высшее образование: Бакалавриат). - ISBN 978-5-16-005473-5. - Текст : электронный. - URL: https://znanium.com/catalog/product/1228788 (дата обращения: 30.03.2022). – Режим доступа: по подписке.

Дополнительная литература

2. Спиркин, А. Г. Философия: Учеб.для студ.вузов/ Спиркин А.Г.. - 2-е изд.. - М.: Гардарики, 2002, 2004, 2005, 2006, 2001. - 735 с. - Имеются экземпляры в отделах: УБ(188), НА(1), ч.з.N7(1), ч.з.N10(1)

10. Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины (модуля).

- НЭБ Национальная электронная библиотека, диссертации и прочие издания
- eLIBRARY.RU Научная электронная библиотека, книги, статьи, тезисы докладов конференций
- Гребенников Электронная библиотека ИД журналы
- ЭБС ZNANIUM.COM
- РГБ Информационное обслуживание по МБА
- БЕН РАН
- Электронно-библиотечная система (ЭБС) Кантитана (https://elib.kantiana.ru/)

11. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине.

Программное обеспечение обучения включает в себя:

- система электронного образовательного контента БФУ им. И. Канта – www.lms-3.kantiana.ru, обеспечивающую разработку и комплексное использование электронных образовательных ресурсов;
- серверное программное обеспечение, необходимое для функционирования сервера и связи с системой электронного обучения через Интернет;
- корпоративная платформа Microsoft Teams;

- установленное на рабочих местах обучающихся ПО: Microsoft Windows 7, Microsoft Office Standart 2010, антивирусное программное обеспечение Kaspersky Endpoint Security.
- Специального программного обеспечения не требуется.

12. Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине.

Для проведения занятий лекционного типа, практических и семинарских занятий используются специальные помещения (учебные аудитории), оборудованные техническими средствами обучения – мультимедийной проекционной техникой. Для проведения занятий лекционного типа используются наборы демонстрационного оборудования.

Для проведения лабораторных работ, (практических занятий – при необходимости) используются специальные помещения (учебные аудитории), оснащенные специализированным лабораторным оборудованием: персональными компьютерами с возможностью выхода в интернет и с установленным программным обеспечением, заявленным в п.11.

Для проведения групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации используются специальные помещения (учебные аудитории), оборудованные специализированной мебелью (для обучающихся), меловой / маркерной доской.

Для организации самостоятельной работы обучающимся предоставляются помещения, оснащенные компьютерной техникой с возможностью подключения к сети «Интернет» и обеспечением доступа в электронную информационно-образовательную среду университета.

Для обучения инвалидов и лиц с ограниченными возможностями здоровья университетом могут быть представлены специализированные средства обучения, в том числе технические средства коллективного и индивидуального пользования.

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
федеральное государственное автономное образовательное учреждение высшего образования «Балтийский федеральный университет имени Иммануила Канта»
Институт физико-математических наук и информационных технологий

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

«Основы деловых коммуникаций»

Шифр: 10.05.01
Специальность: «Компьютерная безопасность»
Специализация: «Математические методы защиты информации»
Квалификация (степень) выпускника: специалист по защите информации

Калининград
2022

Лист согласования

Составитель: к.ф.н., доцент Института гуманитарных наук Суворова Наталья Алексеевна

Рабочая программа утверждена на заседании учебно-методического совета института физико-математических наук и информационных технологий

Протокол № 01/22 от «01» февраля 2022 г.

Председатель учебно-методического совета института физико-математических наук и информационных технологий
Первый заместитель директора ИФМНиИТ, к. ф.-м. н., доцент — Шпилевой А. А

Ведущий менеджер — Е.П.Ставицкая

Содержание

1.Наименование дисциплины: «Основы деловых коммуникаций»

Целью освоения дисциплины «Основы деловых коммуникаций» являются формирование научного представления о коммуникации, ее моделях, уровнях и видах, структуре коммуникационного процесса, специфике массовой коммуникации как вида деятельности, развитие умения грамотно использовать возможности коммуникации в профессиональной деятельности математика; развитие у студентов личностных качеств, направленных на создание эффективной коммуникации, а также формирование общекультурных компетенций в соответствии с требованиями образовательного стандарта.

2. Перечень планируемых результатов обучения по дисциплине, соотнесенных с планируемыми результатами освоения образовательной программы

Код компетенции	Результаты освоения образовательной программы (ИДК)	Результаты обучения по дисциплине
УК-4. Способен применять современные коммуникативные технологии, в том числе на иностранном(ых) языке(ах), для академического и профессионального взаимодействия	УК.4.1. Демонстрирует умение вести обмен профессиональной информацией в устной и письменной формах в том числе и на иностранном языке. УК.4.2. Использует современные информационно-коммуникативные технологии для академического взаимодействия и с соблюдением этики делового общения; Использует современные информационно-коммуникативные технологии для взаимодействия в профессиональной сфере. УК.4.3. Способен осуществлять деловую коммуникацию в устной и письменной формах на государственном языке РФ.	Студент, изучивший курс аналитических методов в задачах защиты информации, должен: • **Знать** особенности деловой коммуникации как вида коммуникации, средства реализации делового общения, свойства устной и письменной деловой коммуникации как на русском языке, так и иностранных • **Уметь** определить характер делового общения, построить деловую коммуникацию с помощью вербальных и невербальных средств. • **Владеть** навыками, составляющими коммуникативную компетентность личности.
УК-5. Способен анализировать и учитывать разнообразие культур в процессе межкультурного взаимодействия	УК.5.1. Выявление общего и особенного в историческом развитии России. УК.5.2. Анализирует современное состояние общества на основе знания истории. УК.5.3. Способен использовать основы	• **Знать** особенности коммуникации в разных социальных группах, принципы и способы коммуникативного взаимодействия в группе, команде; • **Уметь** исполнять коммуникативную роль, связанную с социальным статусом коммуниканта в условиях

	философских знаний для формирования мировоззренческой позиции.	совместной коммуникации, разрабатывать коммуникативные способы решения конфликтных ситуаций; • **Владеть** навыками оценивания коммуникативной компетентности коммуникатора и коммуниканта, в том числе и в отношении собственной личности.

3. Место дисциплины в структуре образовательной программы

«Основы деловых коммуникаций» относится к обязательной части Блока 1 Дисциплины (модули), входит в Модуль 1. Модуль универсальных компетенций направления подготовки обучающихся.

4. Виды учебной работы по дисциплине.

Виды учебной работы по дисциплине зафиксированы учебным планом основной профессиональной образовательной программы по указанному направлению и профилю, выражаются в академических часах. Часы контактной работы и самостоятельной работы обучающегося и часы, отводимые на процедуры контроля, могут различаться в учебных планах ОПОП по формам обучения. Объем контактной работы включает часы контактной аудиторной работы (лекции/практические занятия/ лабораторные работы), контактной внеаудиторной работы (контроль самостоятельной работы), часы контактной работы в период аттестации. Контактная работа, в том числе может проводиться посредством электронной информационно-образовательной среды университета с использованием ресурсов сети Интернет и дистанционных технологий

5. Содержание дисциплины, структурированное по темам (разделам)

Исходя из рамок, установленных учебным планом по трудоемкости и видам учебной работы по дисциплине, преподаватель самостоятельно выбирает тематику занятий по формам и количеству часов проведения контактной работы: лекции и иные учебные занятия, предусматривающие преимущественную передачу учебной информации преподавателем и (или) занятия семинарского типа (семинары, практические занятия, практикумы, лабораторные работы, коллоквиумы и иные аналогичные занятия), и (или) групповые консультации, и (или) индивидуальную работу обучающихся с преподавателем, в том числе индивидуальные консультации (по курсовым работам/проектам – при наличии курсовой работы/проекта по данной дисциплине в учебном плане). Рекомендуемая тематика занятий максимально полно реализуется в контактной работе с обучающимися очной формы обучения. В случае реализации образовательной программы в заочной / очно-заочной форме трудоемкость дисциплины сохраняется, однако объем учебного материала в значительной части осваивается обучающимися в форме самостоятельной работы. При этом требования к ожидаемым образовательным результатам обучающихся по данной дисциплине не зависят от формы реализации образовательной программы.

№ п/п	**Наименование раздела**	**Содержание раздела**
1	Введение в теорию коммуникации. Узкое и широкое понимание	Актуальность знаний основ коммуникации. Определения коммуникации. Разные научные подходы в определении коммуникации. Основные факторы, определяющие процесс

	коммуникации. Структура коммуникативного акта.	коммуникации: коммуникатор, аудитория, канал коммуникации, сообщение. Понятия узкого определения коммуникации: социальный субъект, эффективное синхронное и диахронное взаимодействие, информация, имеющая смысл для коммуникантов. Понятия широкого определения коммуникации: субъект из мира живой природы, способный к автономному поведению; эффективное синхронное и диахронное взаимодействие, информация, имеющая смысл для коммуникантов. Трехкомпонентная, четырехкомпонентная структуры коммуникации, структура Шеннона-Якобсона, Е. Клюева, Лассуэлла.
2	Современные модели коммуникации, их особенности. Виды коммуникации.	20-ый век в науке о коммуникации: модели математическая, кибернетическая, социально-психологическая, трансакционная. Модели массовой коммуникации. Виды коммуникации: вербальная и невербальная, контактная и дистантная, непосредственная и опосредованная, монологическая, диалогическая, полилогическая; межличностная, групповая, массовая.
3	Вербальная и невербальная коммуникация	Цель и средства вербальной коммуникации. Особенности речевой деятельности на основе вербальной коммуникации. Цель и средства невербальной коммуникации. Особенности речевой деятельности на основе невербальной коммуникации: особенности невербальных сообщений, характеристики невербальной коммуникации, функции невербальной коммуникации. Классификация невербальных средств: симптомы, символы, знаки (виды знаков).
4	Коммуникативные стратегии и тактики.	Определение коммуникативной стратегии, тактики и приемов или средств в реализации стратегии. Классификация тактических приемов Т.А. ван Дейка.
5	Успешная и эффективная коммуникация.	Эффективная и успешная коммуникация. Содержание понятия успешной коммуникации. Условия успешности. Коммуникативные качества речи как условия успешной коммуникации. Коммуникативный кодекс Грайса и Лича. Относительность правил кодекса. Особенности письменной и устной деловой коммуникации.
6	Деловая коммуникация: особенности, формы, виды. Система деловых документов	Определение деловой коммуникации. Участники деловой коммуникации, ее формы, официально-деловой стиль как инструмент деловой коммуникации. Регламентированность, ролевая обусловленность деловой коммуникации, система управления в деловой коммуникации, этический аспект.
7	Деловое общение в сфере математики.	Конфликтные речевые ситуации в спорте: понятие конфликта, его признаки. Поведение в конфликте и коммуникативные стратегии в конфликтной ситуации.

6. Рекомендуемая тематика учебных занятий в форме контактной работы

Рекомендуемая тематика учебных занятий *лекционного* типа (предусматривающих преимущественную передачу учебной информации

преподавателями):

№	Наименование раздела	Содержание раздела
1	Тема 1. Введение в теорию коммуникации. Узкое и широкое понимание коммуникации. Структура коммуникативного акта.	Лекция 1. Введение в теорию коммуникации. Узкое и широкое понимание коммуникации. Структура коммуникативного акта.
2	Тема 2 Современные модели коммуникации, их особенности. Виды коммуникации.	Лекция 2 Современные модели коммуникации, их особенности. Виды коммуникации.
3	Тема 3. Вербальная и невербальная коммуникация	Лекция 3. Вербальная и невербальная коммуникация
4	Тема 4. Коммуникативные стратегии и тактики.	Лекция 4. Коммуникативные стратегии и тактики.
5	Тема 5. Успешная и эффективная коммуникация.	Лекция 5. Успешная и эффективная коммуникация.
6	Тема 6. Деловая коммуникация: особенности, формы, виды. Система деловых документов	Лекция 6. Деловая коммуникация: особенности, формы, виды. Система деловых документов
7	Тема 7. Деловое общение в профессиональной сфере математика	Лекция 7. Деловое общение в профессиональной сфере математика

Рекомендуемая тематика *практических* занятий:

№ п/п	Наименование Темы	Содержание темы
1	Введение в теорию коммуникации. Узкое и широкое понимание коммуникации. Структура коммуникативного акта.	Широкое и узкое определение коммуникации: сопоставление на основе общих критериев, примеры реальной коммуникации. Анализ структуры коммуникации Шеннона-Якобсона: референт, референция, сообщение на примерах реальной коммуникации.
2	Современные модели коммуникации, их особенности. Виды коммуникации.	Математическая модель коммуникации: виды шумов, их присутствие в отношении к разным компонентам коммуникации, анализ различных ситуаций коммуникации согласно этой модели. Виды коммуникации применительно к конкретным примерам коммуникации.
3	Вербальная и невербальная коммуникация	Функции невербальной коммуникации по отношению к вербальной коммуникации на примерах. Симптомы, символы и знаки в

		ежедневной коммуникации. Невербальная коммуникация в отражении отношений коммуникантов, отношения к содержанию коммуникации и как самохарактеристика.
4	Коммуникативные стратегии и тактики.	Планирование стратегии и применение в профессиональной коммуникации с помощью тактик и приемов. Вопросы как коммуникативные тактики в интервью с известными персонами.
5	Успешная и эффективная коммуникация.	Достижение успешной коммуникации с помощью коммуникативных качеств речи.
6	Деловая коммуникация: особенности, формы, виды. Система деловых документов	Проектная работа в группе: моделирование реальной ситуации в условиях деловой коммуникации на основе документа.
7	Деловое общение в сфере математики.	Проектная работа в группе: моделирование реальной ситуации в условиях профессиональной коммуникации на основе документа.

Требования к самостоятельной работе обучающихся

1. Работа с лекционным материалом, предусматривающая проработку конспекта лекций и учебной литературы, по всем темам из п. 6 настоящей рабочей программы.
2. Выполнение домашнего задания, предусматривающего решение задач, выполнение упражнений, выдаваемых на практических занятиях, по всем темам из п. 6 настоящей рабочей программы.

Руководствуясь положениями статьи 47 и статьи 48 Федерального закона от 29 декабря 2012 г. N 273-ФЗ «Об образовании в Российской Федерации» научно-педагогические работники и иные лица, привлекаемые университетом к реализации данной образовательной программы, пользуются предоставленными академическими правами и свободами в части свободы преподавания, свободы от вмешательства в профессиональную деятельность; свободы выбора и использования педагогически обоснованных форм, средств, методов обучения и воспитания; права на творческую инициативу, разработку и применение авторских программ и методов обучения и воспитания в пределах реализуемой образовательной программы и отдельной дисциплины.

Исходя из рамок, установленных учебным планом по трудоемкости и видам учебной работы по дисциплине, преподаватель самостоятельно выбирает тематику занятий по формам и количеству часов проведения контактной работы: лекции и иные учебные занятия, предусматривающие преимущественную передачу учебной информации преподавателем и (или) занятия семинарского типа (семинары, практические занятия, практикумы, лабораторные работы, коллоквиумы и иные аналогичные занятия), и (или) групповые консультации, и (или) индивидуальную работу обучающихся с преподавателем, в том числе индивидуальные консультации (по курсовым работам/проектам – при наличии курсовой работы/проекта по данной дисциплине в учебном плане).

Рекомендуемая тематика занятий максимально полно реализуется в контактной работе с обучающимися очной формы обучения. В случае реализации образовательной программы в заочной / очно-заочной форме трудоемкость дисциплины сохраняется, однако объем учебного материала в значительной части осваивается обучающимися в форме самостоятельной работы. При этом требования к ожидаемым образовательным результатам

обучающихся по данной дисциплине не зависят от формы реализации образовательной программы.

7. Методические рекомендации по видам занятий

Лекционные занятия.

В ходе лекционных занятий обучающимся рекомендуется выполнять следующие действия. Вести конспектирование учебного материала. Обращать внимание на категории, формулировки, раскрывающие содержание тех или иных явлений и процессов, научные выводы и практические рекомендации по их применению. Задавать преподавателю уточняющие вопросы с целью уяснения теоретических положений, разрешения спорных ситуаций.

Желательно оставить в рабочих конспектах поля, на которых во внеаудиторное время можно сделать пометки из рекомендованной литературы, дополняющие материал прослушанной лекции, а также подчеркивающие особую важность тех или иных теоретических положений.

Практические и семинарские занятия.

На практических и семинарских занятиях в зависимости от темы занятия выполняется поиск информации по решению проблем, практические упражнения, контрольные работы, выработка индивидуальных или групповых решений, итоговое обсуждение с обменом знаниями, участие в круглых столах, разбор конкретных ситуаций, командная работа, представление портфолио и т.п.

Самостоятельная работа.

Самостоятельная работа осуществляется в виде изучения литературы, эмпирических данных по публикациям и конкретных ситуаций из практики, подготовке индивидуальных работ, работа с лекционным материалом, самостоятельное изучение отдельных тем дисциплины; поиск и обзор литературы и электронных источников; чтение и изучение учебника и учебных пособий.

8. Фонд оценочных средств

8.1. Перечень компетенций с указанием этапов их формирования в процессе освоения образовательной программы в рамках учебной дисциплины

Основными этапами формирования указанных компетенций при изучении обучающимися дисциплины являются последовательное изучение содержательно связанных между собой тем учебных занятий. Изучение каждой темы предполагает овладение обучающимися необходимыми компетенциями. Результат аттестации обучающихся на различных этапах формирования компетенций показывает уровень освоения компетенций.

Контролируемые разделы (темы) дисциплины	Индекс контролируемой компетенции (или её части)	Оценочные средства по этапам формирования компетенций
		текущий контроль по дисциплине
Тема 1. Введение в теорию коммуникации. Узкое и широкое понимание коммуникации. Структура коммуникативного акта.	УК-4, УК-5	Выполнение практических заданий www.lms-2.kantiana.ru (не менее 60% правильных решений)
Тема 2. Современные модели коммуникации, их	УК-4, УК-5	Письменная работа (не менее 60% правильных ответов)

Контролируемые разделы (темы) дисциплины	Индекс контролируемой компетенции (или её части)	Оценочные средства по этапам формирования компетенций
		текущий контроль по дисциплине
особенности. Виды коммуникации.		
Тема 3. Вербальная и невербальная коммуникация	УК-4, УК-5	Выполнение практических заданий www.lms-2.kantiana.ru (не менее 60% правильных решений)
Тема 4. Коммуникативные стратегии и тактики.	УК-4, УК-5	Деловая игра: погружение в реальную коммуникацию (результативность моделируемой коммуникации)
Тема 5. Успешная и эффективная коммуникация.	УК-4, УК-5	Деловая игра: погружение в реальную коммуникацию (результативность моделируемой коммуникации)
Тема 6. Деловая коммуникация: особенности, формы, виды. Система деловых документов	УК-4, УК-5	Выполнение практических заданий www.lms-2.kantiana.ru (не менее 60% правильных решений)
Тема 7. Деловое общение в сфере математики.	УК-4, УК-5	Проектная работа в группе: моделирование реальной ситуации в условиях деловой коммуникации на основе документа.

8.2. Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений и навыков и (или) опыта деятельности процессе текущего контроля

Типовые тестовые задания

1. Чем отличается узкий подход к пониманию коммуникации от широкого подхода?
А) представлением о субъекте коммуникации
Б) представлением о структуре коммуникативного акта
В) представлением о характере протекания процесса

2. «*Коммуникация* - перевод текста с языка моего «я» на язык твоего «ты». Какой аспект процесса коммуникации акцентирует это определение?
А) содержание сообщений
Б) процесс кодирования и декодирования информации
В) характер отношений субъектов
Г) включенность шумов в процесс

3. К факторам, определяющим процесс коммуникации относятся:
А) коммуникатор
Б) канал коммуникации
В) технические средства коммуникации
Г) сообщение

4. Какой компонент структуры коммуникативного акта особо выделен в математической модели Шеннона – Уивера:
А) сообщение,

Б) приемник,
В) шумы
Г) адресат

5. Суть какой модели коммуникации отражает определение безупречной коммуникации: *объем информации, переданной* источником, равен *объему информации, полученной* адресатом?

А) социально-психологической модели
Б) математической модели
В) кибернетической модели
Г) модели интегрированных коммуникаций

6. Согласно какой модели в коммуникации есть эффект, если проводится контроль над всеми ее звеньями?

А) социально-психологической модели
Б) математической модели
В) кибернетической модели
Г) трансакционной модели

7. Какое значение имеет объект для коммуникации согласно социально-психологической модели?

А) необходим как компонент воздействия,
Б) необходим как средство коммуникации,
В) выступает как ценностный ориентир
Г) является причиной коммуникации

8. По используемым средствам коммуникация бывает:

А) межличностная,
Б) вербальная и невербальная
В) фатическая и информационная
Г) групповая

9. Личные и неличные коммуникации различаются:

А) по отношению коммуникантов к месту коммуникации
Б) по характеру личного контакта субъектов
В) по отношению к одной сфере деятельности
Г) по отношению коммуникантов ко времени контакта

10. Электронные коммуникации отличаются:

А) скоростью передачи информации
Б) безусловной опосредованностью
В) обязательной анонимностью субъектов
Г) масштабом распространения информации

11. Какие основные цели могут преследоваться в коммуникации?

А) фатическая
Б) информационная
В) воздействующая
Г) повествовательная

12. Какие средства языка сохраняют базовое значение в вербальной коммуникации при создании как письменной, так и устной формы речи?
А) буквы, знаки препинания
Б) звуки, ударные слоги
В) лексемы, фразеологизмы
Г) словосочетания, предложения

13. Какие средства языка приобретают особую значимость в **письменной** форме коммуникации?
А) звуки речи
Б) буквы в составе слов
В) стилистически окрашенная лексика
Г) знаки препинания

14. Вербальная коммуникация с точки зрения видов деятельности может быть представлена как:
А) повествование
Б) убеждение
В) говорение
Г) чтение

15. Вербальная коммуникация с точки зрения количества участников и ее направленности бывает:
А) монологом
Б) полилогом
В) слушанием
Г) рассуждением

16. Какие названные средства относятся к единицам невербальной коммуникации?
А) сигналы
Б) морфемы
В) поведение говорящего (пишущего)
Г) символы

17. Особенностями невербальных сообщений являются:
А) контекстуальность
Б) подготовленность
В) ненамеренность
Г) однозначность

18. Какие функции невербальной коммуникации по отношению к вербалике известны в практике общения?
А) замещения
Б) дополнения
В) воздействия
Г) опровержения

19. С помощью каких знаков субъект может демонстрировать сильное волнение?
А) симптома
Б) манипуляции предметом

В) изменения положения тела
Г) дотрагивания до кончика носа

20. Какие сигналы невербальной коммуникации могут контролироваться субъектом?
А) симптом радости
Б) симптом злобы
В) рукопожатие
Г) открытая поза

Письменная работа

Выберите из любого СМИ интервью (в основе 7-10 вопросов) и проанализируйте по критериям:

1. Какие типы вопросов заданы интервьюером?
2. Какой вывод о коммуникативной компетентности интервьюера можно сделать на основе созданной вопросной структуры интервью?
3. Какие ответы давал интервьюируемый? Как данные ответы были определены типам заданных вопросов?
4. Какая связь вопросов и ответов возникла в интервью?
5. Можно ли выявить коммуникативную стратегию интервьюера, реализованную с помощью вопросов-тактик?
6. Согласуется ли эта стратегия со стратегией интервьюируемого? Какие ответы были даны на поставленные вопросы?

Деловая игра на тему «Пресс-коференция со специалистом-математиком по защите информации»

Сценарий:

Перед участниками игры создается следующая ситуация: известный специалист по защите информации работает в новом проекте. В связи с этим организуется пресс-конференция, на которую приглашены журналисты, работающие в научных журналах, профессиональное математическое сообщество. Некоторые в*опросы для обсуждения:*

1. Кто стал инициатором Вашего нового проекта?
2. В чем особенности его реализации?
3. Как Вы считаете, возможно ли решение сложных задач по защите информации без специалиста-математика?
4. Какова роль специалиста по компьютерной безопасности в защите информации?
5. Какую роль играет специалист по защите информации в жизни социума и решении его проблем?

Журналисты придумывают название изданию, которое представляют, или могут воспользоваться названием реального издания.

Задания для журналистов отличается только подзаголовком. Журналисты представляют в статье разные моменты обсуждаемой темы. После того, как журналисты сделали заготовку, они возвращаются на свои места в центре аудитории.

Журналистам раздаются полоски с вопросами, которые пронумерованы. Желающий задать вопрос поднимает руку, после разрешения называет свое издание, называет имя того спортсмена, кому задает вопрос и озвучивает вопрос. Для записи ответов журналистам предоставляются рабочие листы с заготовками вопросов, которыми они будут пользоваться при написании статьи. Их задача кратко записать услышанный ответ, самую суть. Если что-то не понятно, то можно переспрашивать.

После обсуждения всех вопросов организуется написание статьи (доклада). Все участники игры делятся таким образом, чтобы за компьютером работало два человека. Трем журналистам в помощь предоставляется по одному математику, остальные журналисты делятся на пары.

На *четвертом этапе* происходит представление каждой парой своей работы. Другие участники могут дополнять и задавать вопросы.

На *завершающем этапе* подводятся итоги игры, анализ усвоенных знаний, обмен мнениями по поводу проведения игры, дисциплины, удачных и неудачных выступлений.

Назначение игры: В данном случае игра ориентирована на успешность и эффективность коммуникации, ее также можно проводить по другой теме, связанной с профессиональной деятельностью математика. Для этого в исходной ситуации представители компании меняют тему и сферу

Творческий проект

Проект 1 «Резюме для трудоустройства»

Вы – временно не работающий. Перед Вами поставлена задача – написать резюме для устройства на открывшуюся вакансию. Пройти собеседование после подачи резюме.

Основная исходная информация:

- Информация о специалисте по компьютерной безопасности для оформления резюме
- Данные о вакантном рабочем месте
- Знание процедуры собеседования для приема на работу

Представить результаты проекта в виде презентации.

Проект 2 «Информатика безопасность под контролем специалиста-математика»

Вы – специалист по компьютерной безопасности, в чьих компетенциях создание программ по защите информации. В проекте поставлена задача – популяризировать актуальность на современном рынке труда квалификацию специалиста по компьютерной безопасности.

Основная исходная информация:

- Информация о проблеме, которая требует решение
- Информация о компетенциях консультируемого в сфере компьютерной безопасности
- Данные об оформлении документа

Представить результаты проекта в виде презентации.

8.3. Перечень вопросов и заданий для промежуточной аттестации по дисциплине

Вопросы для промежуточного контроля (зачета)

1. Понятие коммуникации. Коммуникативное взаимодействие. Вопрос о типе взаимодействия.
2. Коммуникационный процесс и его структура.
3. Субъекты коммуникации. Проблема типов объектов коммуникации.
4. Виды коммуникации и основания для их классификации.
5. Понятие и особенности массовой коммуникации: специфика адресанта, каналов, информации, эффекта.
6. Характеристика массового адресата.
7. Место массовой коммуникации в ряду социальных коммуникаций.
8. Основные функции массовой коммуникации.
9. Математическая модель коммуникации К. Шеннона и У. Уивера. Кибернетическая модель коммуникации Н. Винера.
11. Социально-психологическая модель Т. Ньюкомба.
12. Интегральная обобщенная модель коммуникации Б. Вестли и М. Маклина.
13. Трансакционная модель коммуникации.
14. Модель интегрированных социальных коммуникаций. Модель интегрированных маркетинговых коммуникаций.
15. Уровни коммуникации: технический, семантический и уровень эффективности.
16. Виды коммуникации.
17. Основные характеристики вербальной коммуникации.
18. Невербальная речевая коммуникация: основная функция, средства.
19. Коммуникативное соотношение вербальных и невербальных речевых средств.
20. Виды невербальных знаков.
21. Коммуникативные стратегии: структура и реализация.
22. Коммуникативные тактики ван Дейка.
23. Успешность и эффективность коммуникации.
24. Коммуникативный кодекс и его критерии.
25. Принцип кооперации Г. Грайса.
26. Принцип вежливости Дж. Лича.
27. Особенности письменной деловой коммуникации.
28. Особенности устной деловой коммуникации.
29. Деловые письма как письменная форма деловой коммуникации.
30. Интернет-общение как особая текстовая и стилевая форма коммуникации.

8.4. Планируемые уровни сформированности компетенций обучающихся и критерии оценивания

Уровни	Содержательное описание уровня	Основные признаки выделения уровня (этапы формирования компетенции, критерии оценки сформированности)	Пятибалльная шкала (академическая) оценка	Двухбалльная шакала, зачет	БРС, % освоения (рейтинговая оценка)
Повышенный	Творческая деятельность	*Включает нижестоящий уровень.* Умение самостоятельно принимать решение, решать проблему/задачу теоретического и	отлично	зачтено	86-100

		прикладного характера на основе изученных методов, приемов, технологий			
Базовый	Применение знаний и умений в более широких контекстах учебной и профессиональной деятельности, нежели по образцу с большей степени самостоятельности и инициативы	*Включает нижестоящий уровень.* Способность собирать, систематизировать, анализировать и грамотно использовать информацию из самостоятельно найденных теоретических источников и иллюстрировать ими теоретические положения или обосновывать практику применения	хорошо		71-85
Удовлетворительный (достаточный)	Репродуктивная деятельность	Изложение в пределах задач курса теоретически и практически контролируемого материала	удовлетворительно		55-70
Недостаточный	Отсутствие признаков удовлетворительного уровня		неудовлетворительно	не зачтено	Менее 55

9. Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины.

Основная литература

1. Кулагина, Н. В. Деловые коммуникации / Кулагина Н.В. - Москва :Вузовский учебник, НИЦ ИНФРА-М, 2016. - 234 с.ISBN 978-5-9558-0515-3. - Текст : электронный. - URL: https://znanium.com/catalog/product/557755 (дата обращения: 30.03.2022). – Режим доступа: по подписке.

Дополнительная литература

1. Сахнюк, Т. И. Деловые коммуникации [Электронный ресурс] : учебное пособие / сост. Т.И. Сахнюк. - Ставрополь: СтГАУ, 2013. - 92 с. - Текст : электронный. - URL: https://znanium.com/catalog/product/514137 (дата обращения: 30.03.2022). – Режим доступа: по подписке.

10. Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины (модуля).

- НЭБ Национальная электронная библиотека, диссертации и прочие издания
- eLIBRARY.RU Научная электронная библиотека, книги, статьи, тезисы докладов конференций

- Гребенников Электронная библиотека ИД журналы
- ЭБС ZNANIUM.COM
- РГБ Информационное обслуживание по МБА
- БЕН РАН
- Электронно-библиотечная система (ЭБС) Кантитана (https://elib.kantiana.ru/)

11. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине.

Программное обеспечение обучения включает в себя:

- система электронного образовательного контента БФУ им. И. Канта – www.lms-3.kantiana.ru, обеспечивающую разработку и комплексное использование электронных образовательных ресурсов;
- серверное программное обеспечение, необходимое для функционирования сервера и связи с системой электронного обучения через Интернет;
- корпоративная платформа Microsoft Teams;
- установленное на рабочих местах обучающихся ПО: Microsoft Windows 7, Microsoft Office Standart 2010, антивирусное программное обеспечение Kaspersky Endpoint Security.
- Специального программного обеспечения не требуется.

12. Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине.

Для проведения занятий лекционного типа, практических и семинарских занятий используются специальные помещения (учебные аудитории), оборудованные техническими средствами обучения – мультимедийной проекционной техникой. Для проведения занятий лекционного типа используются наборы демонстрационного оборудования.

Для проведения лабораторных работ, (практических занятий – при необходимости) используются специальные помещения (учебные аудитории), оснащенные специализированным лабораторным оборудованием: персональными компьютерами с возможностью выхода в интернет и с установленным программным обеспечением, заявленным в п.11.

Для проведения групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации используются специальные помещения (учебные аудитории), оборудованные специализированной мебелью (для обучающихся), меловой / маркерной доской.

Для организации самостоятельной работы обучающимся предоставляются помещения, оснащенные компьютерной техникой с возможностью подключения к сети «Интернет» и обеспечением доступа в электронную информационно-образовательную среду университета.

Для обучения инвалидов и лиц с ограниченными возможностями здоровья университетом могут быть представлены специализированные средства обучения, в том числе технические средства коллективного и индивидуального пользования.

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ
федеральное государственное автономное образовательное учреждение высшего образования «Балтийский федеральный университет имени Иммануила Канта»
Институт физико-математических наук и информационных технологий

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

«Математический анализ»

Шифр: 10.05.01
Специальность: «Компьютерная безопасность»
Специализация: «Математические методы защиты информации»
Квалификация (степень) выпускника: специалист по защите информации

Калининград
2022

Лист согласования

Составители: Худенко Владимир Николаевич, к.ф.-м.н., профессор

Рабочая программа утверждена на заседании учебно-методического совета института физико-математических наук и информационных технологий

Протокол № 01/22 от «01» февраля 2022 г.

Председатель учебно-методического совета института физико-математических наук и информационных технологий

Первый заместитель директора ИФМНиИТ, к. ф.-м. н., доцент — Шпилевой А. А

Ведущий менеджер — Е.П.Ставицкая

Содержание

1.Наименование дисциплины: «Математический анализ».

Целью освоения дисциплины «Математический анализ» является изложение классических основ математического анализа и методики решения задач в указанной области, подготовка студентов к чтению математической и прикладной научной литературы, где широко применяется язык этой математической дисциплины, выработка у студентов умения использовать методы математического анализа в своей исследовательской деятельности.

2. Перечень планируемых результатов обучения по дисциплине, соотнесенных с планируемыми результатами освоения образовательной программы

Код компетенции	**Результаты освоения ООП Содержание компетенций**	**Перечень планируемых результатов обучения по дисциплине**
ОПК-3 Способен на основании совокупности математических методов разрабатывать, обосновывать и реализовывать процедуры решения задач профессиональной деятельности.	ОПК-3.1. Знает необходимые математические методы для решения задач обеспечения защиты информации. ОПК-3.2. Применяет совокупность необходимых математических методов для решения задач обеспечения защиты информации. ОПК-3.3. Разрабатывает, обосновывает и реализует на практике процедуры решения задач обеспечения защиты информации.	*знать* корректные постановки классических задач; математический аппарат, применяемый при решении прикладных задач; -*уметь* строго доказывать математическое утверждение; определять возможности применения методов математического анализа; -*владеть практическими навыками* использования стандартных методов и моделей математического анализа и их применения к решению прикладных задач

3. Место дисциплины в структуре образовательной программы

Дисциплина «Математический анализ» относится к обязательной части Блока 1 Дисциплины (модули), входит в Модуль 2. Фундаментальная математика и информатика направления подготовки обучающихся.

4. Виды учебной работы по дисциплине.

Виды учебной работы по дисциплине зафиксированы учебным планом основной профессиональной образовательной программы по указанному направлению и профилю, выражаются в академических часах. Часы контактной работы и самостоятельной работы обчающегося и часы, отводимые на процедуры контроля, могут различаться в учебных планах ОПОП по формам обучения. Объем контактной работы включает часы контактной аудиторной работы (лекции/практические занятия/ лабораторные работы), контактной внеаудиторной работы (контроль самостоятельной работы), часы контактной работы в период аттестации. Контактная работа, в том числе может проводиться посредством элек-

тронной информационно-образовательной среды университета с использованием ресурсов сети Интернет и дистанционных технологий

5. Содержание дисциплины, структурированное по темам (разделам)

№	Наименование раздела	Содержание раздела
1	Введение в математический анализ.	Предмет математического анализа. Множества. Отображения множеств. Эквивалентность множеств. Числовые множества. Непрерывность множества действительных чисел. Ограниченные множества. Верхние и нижние грани числовых множеств. Множество комплексных чисел.
2	Числовые функции одного действительного переменного.	Понятие функции. Способы задания. Основные характеристики поведения функции. Сложная функция, обратная функция. Основные элементарные функции и их графики. Функции, заданные параметрически и в полярных координатах.
3	Пределы числовых последовательностей	Числовая последовательность и ее предел. Признаки сходимости числовых последовательностей. Предельные точки последовательностей, нижний и верхний пределы. Критерий Коши сходимости последовательности. Вычисление пределов числовых последовательностей.
4	Предел функции и его свойства	Понятие предела функции. Общие свойства пределов функций. Свойства пределов, связанные с неравенствами. Бесконечно малые и бесконечно большие функции. Свойства бесконечно малых функций. Основные теоремы о пределах. Замечательные пределы. Критерий Коши существования предела функции. Предел монотонных функций. Сравнение асимптотического поведения функций. Основные приемы раскрытия неопределенностей. Общая теория предела
5	Непрерывность функции в точке и на множестве	Непрерывность функции в точке и на множестве. Точки разрыва функции и их классификация. Локальные свойства непрерывных функций. Действия над непрерывными функциями**.** Свойства функций, непрерывных на отрезке. Равномерная непрерывность функции.
6	Дифференцирование функции одной переменной. Производная.	Понятие производной функции. Механический и геометрический смысл производной. Дифференцируемость функции. Дифференциал функции. Производная и дифференциал сложной функции. Инвариантность формы дифференциала. Правила дифференцирования. Производные и дифференциалы основных элементарных функций. Производная обратной функции. Производные и дифференциалы обратных тригонометрических функций. Производные и дифференциалы гиперболических функций. Таблица производных основных элементарных функций. Дифференцирование неявных функций.

		Логарифмическое дифференцирование. Производная степенно-показательной функции. Дифференцирование функций, заданных параметрически. Производные высших порядков. Дифференциалы высших порядков. Теоремы о среднем. Правило Лопиталя. Формула Тейлора. Разложение по формуле Маклорена некоторых элементарных функций. Приложения формулы Тейлора.
7	Приложение производной	Возрастание и убывание функций. Точки локального экстремума функции. Необходимые и достаточные условия существования экстремума функции. Абсолютные экстремумы функции на отрезке. Исследование функций на выпуклость и вогнутость. Точки перегиба. Асимптоты графика функции. Общая схема исследования функции. Интерполирование функций. Приближенное решение уравнений.
8	Неопределенный интеграл и методы интегрирования	Первообразная функции и неопределенный интеграл. Основные свойства неопределенного интеграла. Таблица основных правил и формул интегрирования. Основные методы интегрирования. Рациональные дроби. Интегрирование простейших рациональных дробей. Интегрирование рациональных дробей. Интегрирование тригонометрических выражений. Интегрирование некоторых иррациональных функций.
9	Определённый интеграл и способы его вычисления	Интегральная сумма. Понятие определенного интеграла. Геометрический и физический смысл определенного интеграла. Условия интегрируемости функций. Классы интегрируемых функций. Основные свойства определенного интеграла. Определенный интеграл с переменным верхним пределом интернирования. Формула Ньютона-Лейбница. Основные методы вычисления определенного интеграла. Несобственные интегралы. Приближенные методы вычисления определенных интегралов.
10	Приложения определённого интеграла в геометрии и физике	Площадь плоской фигуры. Вычисление площадей плоских фигур в прямоугольной системе координат. Вычисление площадей плоских фигур в полярной системе координат. Вычисление длины кривой. Вычисление площади поверхности вращения. Вычисление объемов пространственных тел. Вычисление работы переменной силы. Вычисление силы давления жидкости. Вычисление статических моментов, моментов инерции и координат центра масс.
11	Функции нескольких независимых переменных. Дифференциальное исчисление функций нескольких переменных.	Пространство R^n. Понятие функции нескольких переменных. Открытые и замкнутые множества в метрических пространствах. Понятие функции нескольких переменных. Понятие предела функции нескольких переменных. Непрерывность функции нескольких переменных. Основные свойства непрерывных функций. Дифференцирование функций нескольких переменных. Дифференцируемость функ-

		ции нескольких переменных. Необходимое и достаточное условие дифференцируемости. Полный дифференциал функции нескольких переменных. Дифференцирование сложной функции. Касательная плоскость и нормаль к поверхности. Геометрический смысл полного дифференциала функции двух независимых переменных. Частные производные и дифференциалы высших порядков. Формула Тейлора для функции двух переменных. Локальные экстремумы функции двух переменных. Условный экстремум функции нескольких переменных. Наибольшее и наименьшее значения (глобальные экстремумы) функции двух переменных в замкнутой области. Эмпирические формулы. Определение параметров эмпирических формул методом наименьших квадратов. Функции нескольких переменных, заданные неявно. Неявные функции нескольких переменных. Отображения из R^n в R^m. Дифференцируемые отображения
12	Числовые ряды и их приложения	Основные понятия. Простейшие свойства сходящихся рядов. Необходимый признак сходимости числового ряда. Ряды с неотрицательными членами. Интегральный признак Коши. Признаки сходимости рядов с положительными членами. Признаки Куммера. Признаки Раабе, Бертрана, Гаусса. Знакочередующиеся ряды. Знакопеременные ряды. Умножение абсолютно сходящихся рядов. Повторные и двойные ряды. Бесконечные произведения.
13	Функциональные ряды.	Основные понятия. Признаки равномерной сходимости. Свойства равномерно сходящихся рядов. Почленное дифференцирование и интегрирование функциональных рядов. Степенные ряды
14	Разложение функций в степенные ряды.	Ряды Тейлора и Маклорена. Условия разложимости функций в степенной ряд. Примеры разложения элементарных функций в степенные ряды. Методы разложения функций в ряд Тейлора. Приложение рядов. Степенные ряды комплексной переменной. Показательные и тригонометрические функции в комплексной области. Равномерное приближение непрерывных функций многочленами.
15	Собственные интегралы, зависящие от параметра.	Определение интегралов, зависящих от параметра. Предельный переход под знаком интеграла. Непрерывность интеграла как функции параметра. Дифференцирование интегралов по параметру. Интегрирование интегралов по параметру. Пределы интегрирования, зависящие от параметра.
16	Несобственные интегралы, зависящие от параметра.	Определение равномерной сходимости. Непрерывность интеграла как функции параметра. Интегрирование по параметру под знаком интеграла. Дифференцирование по параметру под знаком интеграла
17	Обобщенные функции.	Бета-функция (интеграл Эйлера 1 рода). Свойства

		Бета-функции. Гамма-функция. Основные понятия. Основные свойства Гамма-функции.
18	Ряды Фурье.	Предварительные сведения о периодических функциях и постановка задачи. Ортогональные и ортонормированные системы функций. Разложение в ряд Фурье по ортонормированной системе функций. Разложение функций в тригонометрические ряды Фурье. Теоремы о сходимости рядов Фурье. Ряды Фурье функций с периодом $2l$ и непериодических функций. Комплексная форма ряда Фурье. Интеграл Фурье. Преобразования Фурье.
19	Двойные интегралы.	Задачи, приводящие к понятию двойного интеграла. Определение двойного интеграла. Условия существования двойного интеграла. Классы интегрируемых функций. Свойства двойных интегралов. Вычисление двойного интеграла в случае прямоугольной области. Вычисление двойного интеграла в случае криволинейной области. Замена переменных в двойном интеграле. Геометрические приложения двойного интеграла. Приложения двойных интегралов в механике.
20	Тройной интеграл.	Понятие тройного интеграла. Вычисление тройного интеграла. Замена переменных в тройном интеграле.
21	Криволинейные интегралы первого рода.	Криволинейные интегралы первого рода. Вычисление криволинейных интегралов первого рода. Механические приложения криволинейного интеграла 1 рода
22	Криволинейные интегралы второго рода.	Криволинейные интегралы второго рода. Вычисление криволинейных интегралов второго рода. Криволинейные интегралы второго рода по замкнутому контуру. Формула Грина. Независимость криволинейных интегралов от пути интегрирования. Интегрирование полных дифференциалов.
23	Поверхностные интегралы первого рода	Понятие поверхностного интеграла первого рода. Площадь поверхности. Вычисление поверхностного интеграла первого рода. Приложения поверхностного интеграла первого рода.
24	Поверхностные интегралы второго рода	Поверхностные интегралы второго рода и их вычисление. Формула Остроградского. Формула Стокса.
25	Элементы теории поля	Постановка задачи векторного анализа. Скалярные поля и их характеристики. Векторное поле. Ротор и поток векторного поля. Специальные виды векторных полей.

6. Рекомендуемая тематика учебных занятий в форме контактной работы

Рекомендуемая тематика учебных занятий *лекционного* типа (предусматривающих преимущественную передачу учебной информации преподавателями):

№	Наименование раздела	Темы лекций

1	Введение в математический анализ.	**Лекция 1.** Предмет математического анализа. Множества. **Лекция 2.** Ограниченные множества.
2	Числовые функции одного действительного переменного.	**Лекция 3.** Понятие функции. **Лекция 4.** Основные элементарные функции. Функции, заданные параметрически и в полярных координатах.
3	Пределы числовых последовательностей	**Лекция 5.** Числовая последовательность и ее предел. **Лекция 6.** Вычисление пределов числовых последовательностей.
4	Предел функции и его свойства	**Лекция 9.** Понятие предела функции. Общие свойства пределов функций. **Лекция 10.** Свойства пределов, связанные с неравенствами. **Лекция 11.** Предел монотонных функций. Основные приемы раскрытия неопределенностей.
5	Непрерывность функции в точке и на множестве	**Лекция 12.** Непрерывность функции в точке и на множестве. Точки разрыва функции и их классификация. **Лекция 13** Действия над непрерывными функциями.
6	Дифференцирование функции одной переменной. Производная.	**Лекция 14.** Понятие производной функции. Механический и геометрический смысл производной. Дифференцируемость функции. Дифференциал функции. **Лекция 15.** Производные и дифференциалы основных элементарных функций. Производные высших порядков.
6	Приложение производной	**Лекция 16.** Возрастание и убывание функций. Точки локального экстремума функции. Необходимые и достаточные условия существования экстремума функции. **Лекция 17.** Интерполирование функций. Приближенное решение уравнений.
7	Неопределенный интеграл и методы интегрирования	**Лекция 18.** Первообразная функции и неопределенный интеграл. Таблица основных правил и формул интегрирования. **Лекция 19.** Основные методы интегрирования. **Лекция 20.** Интегрирование рациональных дробей. **Лекция 21.** Интегрирование тригонометрических выражений. Интегрирование некоторых иррациональных функций.
8	Определённый интеграл и способы его вычисления	**Лекция 22.** Интегральная сумма. Понятие определенного интеграла. **Лекция 23.** Основные свойства определенного интеграла. Формула Ньютона-Лейбница. **Лекция 24.** Основные методы вычисления определенного интеграла. Приближенные методы вычисления определенных интегралов.
9	Приложения определённого интеграла в геомет-	**Лекция 25.** Вычисление площадей плоских фигур в прямоугольной системе координат.

	рии и физике	**Лекция 26.** Вычисление объемов пространственных тел. **Лекция 27.** Физические приложения определенного интеграла.
10	Функции нескольких независимых переменных. Дифференциальное исчисление функций нескольких переменных.	**Лекция 28.** Понятие функции нескольких переменных. **Лекция 29.** Понятие предела функции нескольких переменных. Непрерывность функции нескольких переменных. Основные свойства непрерывных функций. **Лекция 30.** Дифференцирование функций нескольких переменных. **Лекция 31.** Полный дифференциал функции нескольких переменных. Дифференцирование сложной функции **Лекция 32.** Экстремумы функции двух переменных. **Лекция 33.** Неявные функции нескольких переменных.
11	Числовые ряды и их приложения	**Лекция 34.** Простейшие свойства сходящихся рядов. Ряды с неотрицательными членами. Интегральный признак Коши. **Лекция 35.** Знакочередующиеся ряды.
12	Функциональные ряды.	**Лекция 36.** Основные понятия. Признаки равномерной сходимости. **Лекция 37** Свойства равномерно сходящихся рядов.. **Лекция 38.** Степенные ряды
13	Разложение функций в степенные ряды.	**Лекция 39.** Ряды Тейлора и Маклорена. пенной ряд. **Лекция 40.** Методы разложения функций в ряд Тейлора. Приложение рядов.
14	Собственные интегралы, зависящие от параметра.	**Лекция 41.** Определение интегралов, зависящих от параметра. **Лекция 42**. Дифференцирование интегралов по параметру. Интегрирование интегралов по параметру.
15	Несобственные интегралы, зависящие от параметра.	**Лекция 43.** Интегрирование по параметру под знаком интеграла. Дифференцирование по параметру под знаком интеграла
16	Обобщенные функции.	**Лекция 44.** Бета-функция (интеграл Эйлера 1 рода). **Лекция 45.** Гамма-функция. Основные понятия. Основные свойства Гамма-функции.
17	Ряды Фурье.	**Лекция 46**. Ортогональные и ортонормированные системы функций. **Лекция 47.** Разложение в ряд Фурье по ортонормированной системе функций. **Лекция 48.** Теоремы о сходимости рядов Фурье. **Лекция 49.** Интеграл Фурье. Преобразования Фурье.
18	Двойные интегралы.	**Лекция 50.** Определение двойного интеграла. Условия существования двойного интеграла. **Лекция 51.** Вычисление двойного интеграла в случае криволинейной области. **Лекция 52.** Геометрические приложения двойного интеграла. Приложения двойных интегралов в меха-

		нике.
19	Тройной интеграл.	**Лекция 53.** Понятие тройного интеграла. **Лекция 54.** Вычисление тройного интеграла. **Лекция 55.** Замена переменных в тройном интеграле.
20	Криволинейные интегралы первого рода.	**Лекция 56.** Криволинейные интегралы первого рода. Вычисление криволинейных интегралов первого рода. **Лекция 57.** Механические приложения криволинейного интеграла 1 рода
21	Криволинейные интегралы второго рода.	**Лекция 58.** Криволинейные интегралы второго рода. Вычисление криволинейных интегралов второго рода. **Лекция 59.** Криволинейные интегралы второго рода по замкнутому контуру. Формула Грина. Независимость криволинейных интегралов от пути интегрирования.
22	Поверхностные интегралы первого рода	**Лекция 60.** Понятие поверхностного интеграла первого рода. Площадь поверхности. **Лекция 61.** Вычисление поверхностного интеграла первого рода. Приложения поверхностного интеграла первого рода.
23	Поверхностные интегралы второго рода	**Лекция 62.** Поверхностные интегралы второго рода и их вычисление. **Лекция 63-64.** Формула Остроградского. Формула Стокса.
24	Элементы теории поля	**Лекция 65.** Постановка задачи векторного анализа. Скалярные поля и их характеристики. **Лекция 66.** Векторное поле. Ротор и поток векторного поля. **Лекция 67-68.** Специальные виды векторных полей.

Рекомендуемая тематика *практических* занятий:

№	Наименование раздела	Темы практических занятий
1	Введение в математический анализ.	**Занятие 1.** Множества и операции над ними. **Занятие 2.** Ограниченные множества.
2	Числовые функции одного действительного переменного.	**Занятие 3.** Понятие функции. **Занятие 4.** Основные элементарные функции. Функции, заданные параметрически и в полярных координатах.
3	Пределы числовых последовательностей	**Занятие 5.** Числовая последовательность и ее предел. **Занятие 6.** Вычисление пределов числовых последовательностей.
4	Предел функции и его свойства	**Занятие 9.** Понятие предела функции. Общие свойства пределов функций. **Занятие 10.** Свойства пределов, связанные с неравенствами. **Занятие 11.** Предел монотонных функций. Основные приемы раскрытия неопределенностей.

5	Непрерывность функции в точке и на множестве	**Занятие 12.** Непрерывность функции в точке и на множестве. Точки разрыва функции и их классификация. **Занятие 13** Действия над непрерывными функциями.
6	Дифференцирование функции одной переменной. Производная.	**Занятие 14.** Понятие производной функции. Механический и геометрический смысл производной. Дифференцируемость функции. Дифференциал функции. **Занятие 15.** Производные и дифференциалы основных элементарных функций. Производные высших порядков.
6	Приложение производной	**Занятие 16.** Возрастание и убывание функций. Точки локального экстремума функции. Необходимые и достаточные условия существования экстремума функции. **Занятие 17.** Интерполирование функций. Приближенное решение уравнений.
7	Неопределенный интеграл и методы интегрирования	**Занятие 18.** Первообразная функции и неопределенный интеграл. Таблица основных правил и формул интегрирования. **Занятие 19.** Основные методы интегрирования. **Занятие 20.** Интегрирование рациональных дробей. **Занятие 21.** Интегрирование тригонометрических выражений. Интегрирование некоторых иррациональных функций.
8	Определённый интеграл и способы его вычисления	**Занятие 22.** Интегральная сумма. Понятие определенного интеграла. **Занятие 23.** Основные свойства определенного интеграла. Формула Ньютона-Лейбница. **Занятие 24.** Основные методы вычисления определенного интеграла. Приближенные методы вычисления определенных интегралов.
9	Приложения определённого интеграла в геометрии и физике	**Занятие 25.** Вычисление площадей плоских фигур в прямоугольной системе координат. **Занятие 26.** Вычисление объемов пространственных тел. **Занятие 27.** Физические приложения определенного интеграла.
10	Функции нескольких независимых переменных. Дифференциальное исчисление функций нескольких переменных.	**Занятие 28.** Понятие функции нескольких переменных. **Занятие 29.** Понятие предела функции нескольких переменных. Непрерывность функции нескольких переменных. Основные свойства непрерывных функций. **Занятие 30.** Дифференцирование функций нескольких переменных. **Занятие 31.** Полный дифференциал функции нескольких переменных. Дифференцирование сложной функции **Занятие 32.** Экстремумы функции двух переменных.

		Занятие 33. Неявные функции нескольких переменных.
11	Числовые ряды и их приложения	**Занятие 34.** Простейшие свойства сходящихся рядов. Ряды с неотрицательными членами. Интегральный признак Коши. **Занятие 35.** Знакочередующиеся ряды.
12	Функциональные ряды.	**Занятие 36.** Основные понятия. Признаки равномерной сходимости. **Занятие 37** Свойства равномерно сходящихся рядов.. **Занятие 38.** Степенные ряды
13	Разложение функций в степенные ряды.	**Занятие 39.** Ряды Тейлора и Маклорена. пенной ряд. **Занятие 40.** Методы разложения функций в ряд Тейлора. Приложение рядов.
14	Собственные интегралы, зависящие от параметра.	**Занятие 41.** Определение интегралов, зависящих от параметра. **Занятие 42**. Дифференцирование интегралов по параметру. Интегрирование интегралов по параметру.
15	Несобственные интегралы, зависящие от параметра.	**Занятие 43.** Интегрирование по параметру под знаком интеграла. Дифференцирование по параметру под знаком интеграла
16	Обобщенные функции.	**Занятие 44.** Бета-функция (интеграл Эйлера 1 рода). **Занятие 45.** Гамма-функция. Основные понятия. Основные свойства Гамма-функции.
17	Ряды Фурье.	**Занятие 46**. Ортогональные и ортонормированные системы функций. **Занятие 47.** Разложение в ряд Фурье по ортонормированной системе функций. **Занятие 48.** Теоремы о сходимости рядов Фурье. **Занятие 49.** Интеграл Фурье. Преобразования Фурье.
18	Двойные интегралы.	**Занятие 50.** Определение двойного интеграла. Условия существования двойного интеграла. **Занятие 51.** Вычисление двойного интеграла в случае криволинейной области. **Занятие 52.** Геометрические приложения двойного интеграла. Приложения двойных интегралов в механике.
19	Тройной интеграл.	**Занятие 53.** Понятие тройного интеграла. **Занятие 54.** Вычисление тройного интеграла. **Занятие 55.** Замена переменных в тройном интеграле.
20	Криволинейные интегралы первого рода.	**Занятие 56.** Криволинейные интегралы первого рода. Вычисление криволинейных интегралов первого рода. **Занятие 57.** Механические приложения криволинейного интеграла 1 рода
21	Криволинейные интегралы второго рода.	**Занятие 58.** Криволинейные интегралы второго рода. Вычисление криволинейных интегралов второго рода. **Занятие 59.** Криволинейные интегралы второго ро-

		да по замкнутому контуру. Формула Грина. Независимость криволинейных интегралов от пути интегрирования.
22	Поверхностные интегралы первого рода	**Занятие 60.** Понятие поверхностного интеграла первого рода. Площадь поверхности. **Занятие 61.** Вычисление поверхностного интеграла первого рода. Приложения поверхностного интеграла первого рода.
23	Поверхностные интегралы второго рода	**Занятие 62.** Поверхностные интегралы второго рода и их вычисление. **Занятие 63-64.** Формула Остроградского. Формула Стокса.
24	Элементы теории поля	**Занятие 65.** Постановка задачи векторного анализа. Скалярные поля и их характеристики. **Занятие 66.** Векторное поле. Ротор и поток векторного поля. **Занятие 67-68.** Специальные виды векторных полей.

На практических занятиях решаются задачи по теме занятия.

Требования к самостоятельной работе обучающихся

1. Работа с лекционным материалом, предусматривающая проработку конспекта лекций и учебной литературы, по всем темам из п. 6 настоящей рабочей программы.

2. Выполнение домашнего задания, предусматривающего решение задач, выполнение упражнений, выдаваемых на практических занятиях, по всем темам из п. 6 настоящей рабочей программы.

7. Методические рекомендации по видам занятий

Лекционные занятия.

В ходе лекционных занятий обучающимся рекомендуется выполнять следующие действия. Вести конспектирование учебного материала. Обращать внимание на категории, формулировки, раскрывающие содержание тех или иных явлений и процессов, научные выводы и практические рекомендации по их применению. Задавать преподавателю уточняющие вопросы с целью уяснения теоретических положений, разрешения спорных ситуаций.

Желательно оставить в рабочих конспектах поля, на которых во внеаудиторное время можно сделать пометки из рекомендованной литературы, дополняющие материал прослушанной лекции, а также подчеркивающие особую важность тех или иных теоретических положений.

Практические и семинарские занятия.

На практических и семинарских занятиях в зависимости от темы занятия выполняется поиск информации по решению проблем, практические упражнения, контрольные работы, выработка индивидуальных или групповых решений, итоговое обсуждение с обменом знаниями, участие в круглых столах, разбор конкретных ситуаций, командная работа, представление портфолио и т.п.

Самостоятельная работа.

Самостоятельная работа осуществляется в виде изучения литературы, эмпирических данных по публикациям и конкретных ситуаций из практики, подготовке индивидуальных работ, работа с лекционным материалом, самостоятельное изучение отдельных тем дисциплины; поиск и обзор литературы и электронных источников; чтение и изучение учебника и учебных пособий.

8. Фонд оценочных средств

8.1. Перечень компетенций с указанием этапов их формирования в процессе освоения образовательной программы в рамках учебной дисциплины

Основными этапами формирования указанных компетенций при изучении обучающимися дисциплины являются последовательное изучение содержательно связанных между собой тем учебных занятий. Изучение каждой темы предполагает овладение обучающимися необходимыми компетенциями. Результат аттестации обучающихся на различных этапах формирования компетенций показывает уровень освоения компетенций.

Контролируемые модули, разделы (темы) дисциплины	Индекс контролируемой компетенции (или её части)	Оценочные средства по этапам формирования компетенций
		текущий контроль по дисциплине
Раздел 1. Введение в математический анализ.	***ОПК-3***	Решение задач, Устный опрос
Раздел 2. Числовые функции одного действительного переменного	***ОПК-3***	Решение задач, Устный опрос
Раздел 3. Пределы числовых последовательностей	***ОПК-3***	Решение задач, Устный опрос
Раздел 4 Предел функции и его свойства.	***ОПК-3***	Решение задач, Устный опрос
Раздел 5 Непрерывность функции в точке и на множестве	***ОПК-3***	Решение задач, Устный опрос
Раздел 6. Дифференцирование функции одной переменной	***ОПК-3***	Решение задач, Устный опрос
Раздел 6. Приложение производной	***ОПК-3***	Решение задач, Устный опрос
Итог 1 семестра	***ОПК-3***	
Раздел 8 Неопределенный интеграл и	***ОПК-3***	Решение задач, Устный опрос

методы интегрирования		
Раздел 9 Определённый интеграл и способы его вычисления	***ОПК-3***	Решение задач, Устный опрос
Раздел 10 Приложения определённого интеграла в геометрии и физике.	***ОПК-3***	Решение задач, Устный опрос
Раздел 11 Интеграл Стилтьеса	***ОПК-3***	Решение задач, Устный опрос
Раздел 12 . Функции нескольких независимых переменных. Дифференциальное исчисление	***ОПК-3***	Решение задач, Устный опрос
Контроль 2 семестра	***ОПК-3***	
Раздел 13 Числовые ряды и их приложения	***ОПК-3***	Решение задач, Устный опрос
Раздел 14 Функциональные ряды	***ОПК-3***	Решение задач, Устный опрос
Раздел 15 Разложение функций в степенные ряды	***ОПК-3***	Решение задач, Устный опрос
Раздел 16. Собственные интегралы, зависящие от параметра	***ОПК-3***	Решение задач, Устный опрос
Раздел 17 Несобственные интегралы, зависящие от параметра	***ОПК-3***	Решение задач, Устный опрос
Раздел 18. Обобщенные функции	***ОПК-3***	Решение задач, Устный опрос
Раздел 19 Ряды Фурье	***ОПК-3***	Решение задач, Устный опрос
Контроль 3 семестра	***ОПК-3***	
Раздел 20 Двойные интегралы.	***ОПК-3***	Решение задач, Устный опрос
Раздел 21 Тройной интеграл.	***ОПК-3***	Решение задач, Устный опрос
Раздел 22 Криволинейные интегралы первого рода	***ОПК-3***	Решение задач, Устный опрос
Раздел 23 Криволинейные интегралы второго рода	***ОПК-3***	Решение задач, Устный опрос

24-25 Поверхностные интегралы	***ОПК-3***	Решение задач
26 Элементы теории поля	***ОПК-3***	
Промежуточный контроль	***ОПК-3***	

8.2. Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений и навыков и (или) опыта деятельности процессе текущего контроля

Примеры вопросов для устного опроса:

- Определить декартово произведение множеств;

Тема 2. Числовые функции одного действительного переменного

- Понятие функции;
- Перечислить основные элементарные функции:
- Изобразить график основных элементарные функции;
- Определить возрастающую функцию;
- Дать определение периодической функции;
- Дать определение ограниченной на множестве функции;

Тема 3. Пределы числовых последовательностей

- Дать определение числовой последовательности;
- Дать определение убывающей числовой последовательности;
- Дать определение возрастающей числовой последовательности;
- Дать определение ограниченной числовой последовательности;
- Дать определение предела числовой последовательности на языке «ε» - «δ»;
- Привести пример ограниченной, но не сходящейся числовой последовательности;
- Дать определение, на языке «ε» - «δ», бесконечно малой последовательности;
- Дать определение, на языке «ε» - «δ», бесконечно большой последовательности:
- Привести графическую интерпретацию предела числовой последовательности;

Тема 4. Предел функции и его свойства. Замечательные пределы и их приложения

- Дать определение предела функции в смысле Гейне;
- Дать определение предела функции в смысле Коши;
- Дать определение левого одностороннего предела функции;

- Изобразить графическую интерпретацию предела функции в смысле Коши;
- Изобразить графическую интерпретацию левого одностороннего предела функции;
- Дать определение правого одностороннего предела функции;
- Изобразить графическую интерпретацию правого одностороннего предела функции;
- Перечислить основные приемы раскрытия неопределённостей;
- Перечислить основные типы неопределённостей;

Тема 5. Непрерывность функции в точке и на множестве

- Дать определение непрерывной функции в точке;
- Дать определение непрерывной функции на множестве;
- Дать определение непрерывной функции в точке на языке «ε» - «δ»;
- Дать определение непрерывной функции в точке с использованием приращений аргумента и функции;
- Сформулировать определение точки разрыва первого рода;
- Сформулировать определение точки разрыва второго рода;
- Дать определение понятия «устранимый разрыв»;

Тема 6. Дифференцирование функции одной переменной. Производная

- Сформулировать определение дифференцируемой в точке функции;
- Сформулировать теорему о необходимом условии дифференцирования функции;
- Сформулировать теорему о достаточных условиях дифференцирования функции;
- Определить алгоритм для определения производной;
- Дать определение односторонних производных;
- Вывести формулу вычисления производной логарифмической функции;

- Вывести формулу вычисления производной степенной функции;
- Вывести формулу вычисления производной показательной функции;
- Вывести формулу вычисления производной тригонометрических функций;
- Вывести формулу вычисления производной гиперболических функций;
- Вывести формулу вычисления производной обратных тригонометрических функций;
- Описать вычисление производной неявных функций;
- Описать вычисление производной функций, заданных параметрически;

Тема 7. Приложение производной

- Определить алгоритм вычисления угла между кривыми;
- Определить алгоритм исследования функции на возрастание и убывание;
- Определить алгоритм исследования функции на экстремум;
- Определить алгоритм исследования функции на выпуклость и вогнутость;
- Определить алгоритм нахождения точек перегиба графика функции;
- Определить алгоритм нахождения асимптот графика функции;
- Определить формулу касательной;
- Вывести формулу нормали к графику функции;
- Описать алгоритм нахождения наибольшего и наименьшего значений функции на отрезке;
- Описать метод касательных приближенного решения уравнений;
- Описать метод хорд приближенного решения уравнений;
- Описать комбинированный метод приближенного решения уравнений;
- Описать приемы применения дифференциалов для приближенного вычисления функций;

Тема 8. Неопределенный интеграл и методы интегрирования

- Дать определение первообразной функции;
- Дать определение неопределённого интеграла;
- Записать формулу взаимосвязи различных первообразных одной функции;
- Кому принадлежит авторство определения понятия «неопределённый интеграл»;
- Перечислить основные свойства неопределённого интеграла;
- Записать подстановки, применяемые при вычислении интегралов от тригонометрических функций;
- Записать подстановки, применяемые при вычислении интегралов от иррациональных функций;
- Перечислить типы элементарных дробей;
- Описать алгоритм интегрирования рациональных дробей;
- Перечислить подстановки Эйлера;
- Назвать достоинства и недостаток подстановок Эйлера;
- Перечислить подстановки Чебышёва;
- Назвать отечественных математиков, внесших вклад в развитие теории интегрирования;

Тема 9. Определённый интеграл и способы его вычисления

- Дать определение интегральной суммы Римана;
- Дать определение сумм Дарбу;
- Дать определение определенного интеграла;
- Сформулировать свойства линейности определенного интеграла;
- Сформулировать основные свойства определенного интеграла;
- Сформулировать теорему о среднем в определенном интеграле;
- Описать алгоритм непосредственного интегрирования в определенном интеграле;
- Сформулировать теорему о замене переменной в определенном интеграле;
- Записать формулу вычисления по частям в определенном интеграле;
- Перечислить приближенные методы вычисления определенного интеграла;

- Описать графическую интерпретацию определенного интеграла;

Тема 10. Приложения определённого интеграла в геометрии и физике

- Дать определение квадрируемой фигуры;
- Описать алгоритм вычисления площадей плоских фигур в прямоугольной декартовой системе координат;
- Описать алгоритм вычисления площадей плоских фигур в полярной системе координат;
- Описать алгоритм вычисления площадей плоских фигур в случае параметрического задания кривых;
- Дать определение спрямляемой кривой;
- Описать алгоритм вычисления длины кривой в прямоугольной декартовой системе координат;
- Описать алгоритм вычисления длины кривой в случае параметрического задания;
- Описать алгоритм вычисления длины кривой в полярной системе координат;
- Описать алгоритм вычисления объема фигуры по поперечному сечению;
- Описать алгоритм вычисления объема фигуры вращения;
- Написать формулы для вычисления центра масс плоской фигуры;
- Написать формулы для вычисления центра масс пространственного тела;
- Дать определение момента вращения относительно оси;
- Дать определение момента инерции относительно оси;

Тема 11. Функции нескольких независимых переменных. Дифференциальное исчисление функций нескольких переменных

- Дать определение метрического пространства;
- Дать определение функции нескольких переменных;
- Дать определение предела функции нескольких переменных в смысле Гейне;
- Дать определение предела функции нескольких переменных в смысле Коши;

- Изобразить графическую интерпретацию предела функции нескольких переменных в смысле Коши;
- Дать определение непрерывности функции двух переменных;
- Сформулировать Теорему Вейерштрасса для функции двух переменных;
- Дать определение частных приращений функции нескольких переменных;
- Дать определение полного приращения функции нескольких переменных;
- Дать определение частной производной функции нескольких переменных;
- Объяснить графическую интерпретацию частной производной функции нескольких переменных;
- Вывести формулу частной производной сложной функции нескольких переменных;
- Дать определение дифференцируемости функции нескольких переменных;
- Сформулировать достаточные условия дифференцируемости функции нескольких переменных;
- Вывести формулу полного дифференциала функции нескольких переменных;
- Дать определение локального минимума функции нескольких переменных;
- Дать определение локального максимума функции нескольких переменных;
- Сформулировать теорему о достаточных условиях существования экстремума функции нескольких переменных;
- Описать алгоритм нахождения глобальных экстремумов функции нескольких переменных в замкнутой ограниченной области;

Тема 12. Кратные и криволинейные интегралы

- Дать определение геометрической фигуры;
- Описать различные меры геометрической фигуры;
- Описать алгоритм построения интеграла по фигуре;
- Перечислить частные случаи интеграла по фигуре;
- Дать определение криволинейного интеграла 1 рода;
- Дать определение двойного интеграла;
- Дать определение поверхностного интеграла 1 рода;

- Дать определение тройного интеграла;
- Объяснить, как вычисляется двойной интеграл;
- Объяснить, как вычисляется тройной интеграл;
- Объяснить, как вычисляется криволинейный интеграл 1 рода;
- Объяснить, как вычисляется поверхностный интеграл 1 рода;
- Записать формулу перехода к полярным координатам в двойном интеграле;
- Записать формулу перехода к цилиндрическим координатам в тройном интеграле;
- Записать формулу перехода к сферическим координатам в тройном интеграле;
- Определить сферу применения двойного интеграла;
- Определить сферу применения тройного интеграла;
- Определить сферу применения криволинейного интеграла;
- Определить сферу применения поверхностного интеграла;

Типовые контрольные задания:

1 семестр

Тема №1. Предел последовательности.

Задача 1. Используя определение предела, доказать, что $\lim\limits_{n\to\infty} a_n = a$ (указать $N(\varepsilon)$).

1.1. $a_n = \frac{3n-2}{2n-5}, \quad a = \frac{3}{2}$.

Задача 2. Вычислить предел числовой последовательности.

2.1. $\lim\limits_{n\to\infty} \frac{(3-n)^2+(3+n)^2}{(4-n)^2+(4+n)^2}$

Задача 3. Вычислить предел числовой последовательности.

3.1. $\lim\limits_{n\to\infty} \frac{n\sqrt[3]{n^2}+\sqrt[4]{n^8-1}}{(n+\sqrt{n})\sqrt{2-2n+n^2}}$

Задача 4. Вычислить предел числовой последовательности.

4.1. $\lim\limits_{n\to\infty} n\left(\sqrt{n^2+2}-\sqrt{n^2-1}\right)$

Задача 5. Вычислить предел числовой последовательности.

5.1. $\lim\limits_{n\to\infty}\left(\frac{1}{n^2}+\frac{2}{n^2}+\frac{3}{n^2}+\cdots+\frac{n+2}{n^2}\right)$

Задача 6. Вычислить предел числовой последовательности.

6.1. $\lim\limits_{n\to\infty}\left(\frac{n+2}{n-2}\right)^n$

Тема №2. Предел функции.

Задача 1. Используя определение предела функции по Коши, доказать $\lim\limits_{x\to x_0} f(x)=A$ (указать $\delta(\varepsilon)$).

1.1. $f(x)=\frac{2x^2-2}{x+1},\quad x_0=-1,\quad A=-4.$

Задача 2. Доказать по определению, что функция $f(x)$ непрерывна в точке x_0.

$f(x)=2x^2-3x+1,\quad x_0=-2,$

Задача 3. Вычислить предел функции.

$$\lim_{x\to 1}\frac{x^3+x^2-x-1}{x^3-x-x^2+1}$$

Задача 4. Вычислить предел функции.

4.1. $\lim\limits_{x\to 4}\frac{\sqrt{1+2x}-3}{\sqrt{x}-2}.$

Задача 5. Вычислить предел функции.

5.1. $\lim\limits_{x\to 0}\frac{\ln(1+\sin x)}{\sin 4(x-\pi)}$

Задача 6. Вычислить предел функции.

6.1. $\lim\limits_{x\to 1}\frac{\ln x}{x^2-1}.$

Задача 7. Вычислить предел функции.

7.1. $\lim\limits_{x\to \pi/2}\frac{2^{\cos^2 x}-1}{\ln\sin x}$

Задача 8. Вычислить предел функции:

$$\lim_{x\to 0}\frac{2^{2x}-e^{2x}}{x\cdot\arcsin(3x)+\operatorname{arctg}(2x)-x\cdot\log_2(1+x)-x\cdot\left(\sqrt{1+x}-1\right)}$$

Задача 9. Вычислить предел функции:

$$\lim_{x\to 0}\frac{\ln(2+x)+\ln(2-x)-2\ln 2}{\cos(2x)-1}$$

Задача 10. Вычислить предел функции, используя метод логарифмирования:

$$\lim_{x\to 0}\left(\frac{1+\sin x\cos x}{1+\sin x\cos(3x)}\right)^{\operatorname{ctg}^3 x}$$

Задача 11. Вычислить предел функции, используя метод логарифмирования:

$$\lim_{x\to 0}\left(\frac{3^{x+1}+4^{x+1}+5^{x+1}}{12}\right)^{\frac{1}{x}}$$

Задача 12. Вычислить предел функции.

$$\lim_{x\to\infty}\frac{(x+3)^{x+3}(x+1)^{x+1}}{(x+4)^{2x+4}}$$

Задача 13. Исследовать функцию на точки разрыва:

$$f(x)=\begin{cases}\dfrac{1}{x+2}, & x\in(-\infty;-2)\cup(-2;\ 0],\\ x^x, & x\in\{-2\}\cup(0;\ 1),\\ \left[\dfrac{3}{2x}\right], & x\in[1;+\infty).\end{cases}$$

В ответе к заданию построить таблицу:

№	Точка разрыва x_0	Левосторонний предел в x_0	$f(x_0)$	Правосторонний предел в x_0	Род точки разрыва x_0
1.	…	…	…	…	…

Тема №4. Дифференцирование и построение графиков.

1. Вычислить приближённо $\sqrt[4]{17}$.
2. Найти дифференциал функции, заданной неявно: $y=e^{-\frac{x}{y}}$.
3. Используя правило Лопиталя, найти предел $\lim\limits_{x\to 1}\left[\dfrac{1}{x-1}-\dfrac{1}{\ln x}\right]$.
4. Найти предел $\lim\limits_{x\to 0}\dfrac{e^x-e^{-x}-2x}{\sin x-x}$.
5. Провести исследование и построить график функции: $y=\dfrac{x^3}{x^2-1}$.

8.3. Перечень вопросов и заданий для промежуточной аттестации по дисциплине

Вопросы для промежуточного контроля:

Первый семестр

1) Множества. Подмножества. Операции над множествами.
2) Функция, график функции, композиция отображений, сюръекция, инъекция и биекция, обратное отображение.
3) Бинарные отношения. Отношение эквивалентности. Отношение порядка.
4) Аксиоматика множества вещественных чисел. Аксиомы действительных чисел: аксиомы сложения, умножения и порядка. Аксиома Архимеда. Натуральные числа. Принцип индукции.
5) Грани числовых множеств.
6) Теорема Коши-Кантора о вложенных отрезках, теорема Бореля-Лебега о конечном покрытии, теорема Больцано-Вейерштрасса о предельной точке.
7) Понятие о мощности множества. Счетные множества. Континуум.
8) Понятие числовой последовательности и ее предела. Теорема о единственности предела. Ограниченность сходящихся последовательностей.
9) Свойства пределов последовательностей. Предельный переход в неравенствах.
10) Арифметические операции со сходящимися последовательностями.
11) Критерий Коши существования предела числовой последовательности.
12) Монотонные последовательности. Признак сходимости монотонной последовательности.
13) Число e.
14) Подпоследовательности. Теорема Больцано - Вейерштрасса.
15) Бесконечно большие и бесконечно малые последовательности. Основные свойства бесконечно малых и бесконечно больших последовательностей.
16) Предел функции в точке. Эквивалентность определения предела по Гейне и Коши. Единственность предела. Односторонние пределы.
17) Свойства пределов функций. Бесконечно малые и бесконечно большие функции. Пределы монотонных функций.
18) База. Предел функции по базе.
19) Критерий Коши существования предела функции.
20) Предел композиции функций. Второй замечательный предел.
21) Сравнение асимптотического поведения функций. O и o символика. Эквивалентные функции. Выделение главной части функции в точке.
22) Непрерывность функции в точке. Локальные свойства непрерывных функций. Точки разрыва. Классификация точек разрыва.
23) Непрерывность сложной функции.
24) Свойства функций, непрерывных на отрезке (теоремы Вейерштрасса). Теорема Коши о промежуточном значении.
25) Критерий непрерывности монотонной функции.
26) Существование и непрерывность обратной функции.
27) Равномерная непрерывность функции. Теорема Кантора.
28) Непрерывность элементарных функций.
29) Замечательные пределы
30) Определение производной. Геометрический и физический смысл производной. Односторонние производные. Необходимое условие дифференцируемости.
31) Правила дифференцирования.
32) Производная сложной функции. Производная обратной функции. Производная функции, заданной параметрически.
33) Производные элементарных функций.
34) Дифференциал функции, его геометрический смысл. Инвариантность формы первого дифференциала.
35) Производные и дифференциалы высших порядков. Формула Лейбница.
36) Теорема Ферма.
37) Теорема Ролля.

38) Теорема Лагранжа о среднем.
39) Теорема Коши о среднем.
40) Раскрытие неопределенностей по правилу Лопиталя.
41) Теорема Тейлора.
42) Локальный и глобальный варианты формулы Тейлора. Формула Тейлора с остаточным членом в общей форме, в форме Лагранжа, Коши и Пеано.
43) Многочлен Тейлора как многочлен наилучшего приближения функции в окрестности данной точки.
44) Формулы Тейлора для основных элементарных функций (с оценкой остатка).
45) Вычисление пределов с помощью формулы Тейлора (метод выделения главной части).
46) Применение производной к исследованию функции на монотонность и экстремум.
47) Необходимое условие экстремума функции. Достаточные условия экстремума на языке производных высших порядков.
48) Выпуклые функции. Критерии выпуклости. Точки перегиба. Построение графиков.

Второй семестр

49) Первообразная и неопределенный интеграл. Свойства неопределенного интеграла. Таблица основных интегралов.
50) Основные методы интегрирования: замена переменной и интегрирование по частям неопределенного интеграла
51) Интегрирование дробно-рациональных функций. Метод Остроградского.
52) Интегрирование квадратичных иррациональностей посредством подстановок Эйлера.
53) Интегралы от дифференциальных биномов. Теорема Чебышева.
54) Интегрирование некоторых трансцендентных функций.
55) Задачи, приводящие к понятию определенного интеграла. Определение интеграла Римана. Необходимое условие интегрируемости.
56) Верхние и нижние суммы Дарбу. Интеграл Дарбу.
57) Необходимые и достаточные условия интегрируемости.
58) Интегрируемость непрерывной функции, монотонной функции и ограниченной функции с конечным числом точек разрыва.
59) Критерии интегрируемости.
60) Свойства интегрируемых функций. Свойства определенного интеграла.
61) Теоремы о среднем.
62) Определенный интеграл с переменным верхним пределом.
63) Формула Ньютона Лейбница.
64) Формулы замены переменной и интегрирования по частям в определённом интеграле.
65) Понятие площади и квадрируемости плоской фигуры.
66) Понятие площади и квадрируемости плоской фигуры.
67) Геометрические приложения определенного интеграла.
68) Некоторые физические приложения определенного интеграла.
69) Теорема о представлении функции ограниченной вариации и основные свойства.
70) Признаки существования интеграла Стилтьеса и его вычисление.
71) Понятие функции нескольких переменных
72) Понятия n - мерного координатного пространства и n -мерного евклидова пространства.
73) Основные метрические и топологические характеристики точечных множеств евклидова пространства.

74) Предельное значение функции нескольких переменных. Сходящиеся последовательности точек n - мерного евклидова пространства. Критерий Коши сходимости последовательности.
75) Некоторые свойства ограниченных последовательностей точек n - мерного евклидова пространства.
76) Предел функции нескольких переменных. Пределы повторный и кратный. Бесконечно малые функции. Необходимое и достаточное условие существования предела функции.
77) Непрерывность функции нескольких переменных. Основные свойства непрерывных функций нескольких переменных.
78) Равномерная непрерывность функции нескольких переменных.
79) Частные производные. Понятие дифференцируемости. Дифференциал. Инвариантность формы первого дифференциала.
80) Достаточные условия дифференцируемости функции нескольких переменных. Дифференцирование сложной функции.
81) Производная по направлению. Градиент.
82) Касательная плоскость и нормаль к поверхности.
83) Частные производные и дифференциалы высших порядков. Свойства смешанных производных.
84) Формула Тейлора для функции нескольких переменных.
85) Отображения из R^n в R^m, их дифференцирование.Матрица производной. Якобиан
86) Экстремумы функции нескольких переменных. Необходимые условия экстремума.
87) Достаточные условия экстремума функции нескольких переменных.
88) Понятие неявной функции. Теорема о существовании и дифференцируемости неявной функции и некоторые ее применения.
89) Вычисление частных производных неявно заданной функции.
90) Понятие зависимости функций. Достаточное условие независимости.
91) Функциональные матрицы и их приложения.
92) Задачи, приводящие к понятию экстремума. Необходимые условия условного экстремума.
93) Метод неопределенных множителей Лагранжа.
94) Достаточные условия условного экстремума.

Третий семестр

95) Понятие числового ряда. Ряд и его частичные суммы. Сходящиеся и расходящиеся ряды.
96) Критерий Коши сходимости ряда. Свойства, сходящихся рядов.
97) Арифметические операции над сходящимися рядами.
98) Ряды с положительными членами. Необходимое и достаточное условие сходимости ряда с положительными членами.
99) Признаки сравнения. Признаки Даламбера и Коши.
100) Интегральный признак Коши—Маклорена. Признаки Раабе и Гаусса.
101) Абсолютно и условно сходящиеся ряды. Теоремы о перестановке членов условно сходящегося ряда и о перестановке членов абсолютно сходящегося ряда.
102) Знакочередующиеся ряды. Признаки Лейбница. Абсолютная и условная сходимость.
103) Сходимость произвольных рядов. Признаки Дирихле и Абеле.
104) Двойные и повторные ряды.
105) Бесконечные произведения. Связь между сходимостью бесконечных произведений и рядов.

106) Понятие функциональной последовательности и функционального ряда. Сходимость функциональной последовательности в точке и на множестве.
107) Равномерная сходимости на множестве. Критерий Коши.
108) Достаточные признаки равномерной сходимости функционального ряда: признаки Вейерштрасса, Дирихле и Абеля.
109) Непрерывность суммы равномерно сходящегося ряда.
110) Почленное интегрирование и почленное дифференцирование функциональных последовательностей и рядов.
111) Степенной ряд и область его сходимости.
112) Формула Коши—Адамара для радиуса сходимости степенного ряда.
113) Равномерная сходимость и непрерывность суммы степенного ряда.
114) Почленное интегрирование и почленное дифференцирование степенного ряда.
115) Ряд Тейлора. Разложение функций в степенные ряды. Достаточное условие.
116) Разложение некоторых элементарных функций в ряд Тейлора.
117) Применение рядов к приближённым вычислениям.
118) Теоремы Вейерштрасса о равномерном приближении непрерывной функции многочленами.
119) Ряды с комплексными членами. Формулы Эйлера.
120) Интегралы, зависящие от параметра. Непрерывность, дифференцирование и интегрирование по параметру.
121) Несобственные интегралы первого и второго рода. Признаки сходимости.
122) Абсолютная и условная сходимость несобственного интеграла.
123) Признаки Дирихле и Абеля сходимости несобственного интеграла.
124) Замена переменных под знаком несобственного интеграла и формула интегрирования по частям.
125) Несобственные интегралы, зависящие от параметра. Равномерная сходимость.
126) Свойства непрерывности, интегрируемости и дифференцируемости несобственных интегралов, зависящих от параметра.
127) Применение теории несобственных интегралов к вычислению некоторых интегралов. Интегралы Пуассона и Дирихле.
128) Г- и B-функции Эйлера. Интегралы Эйлера.
129) Ортогональные системы функций. Понятие об общем ряде Фурье, минимальном свойстве его коэффициентов.
130) Тригонометрическая система. Тригонометрические ряды. Ряд Фурье. Коэффициенты ряда Фурье.
131) Сходимость ряда Фурье. Неравенство Бесселя.
132) Равномерная сходимость ряда Фурье. Равенство Парсеваля.
133) Сходимость в среднем.
134) Образ Фурье и его простейшие свойства.
135) Интеграл Фурье. Условия разложимости функции в интеграл Фурье.
136) Понятие о прямом и обратном преобразованиях Фурье.
137) Некоторые дополнительные свойства преобразования Фурье.
138) Преобразование Лапласа. Понятие об операционном исчислении.

Четвёртый семестр

139) Определение и существование двойного интеграла.
140) Основные свойства двойного интеграла.
141) Вычисление двойного интеграла. Сведение двойного интеграла к повторному.

142) Понятие криволинейных координат на плоскости.
143) Замена переменных в двойном интеграле. Полярная система координат.
144) Геометрические и физические приложения двойных интегралов.
145) Тройные интегралы. Их определение, вычисление и простейшие свойства.
146) Замена переменных в тройном интеграле. Цилиндрическая и сферическая система координат.
147) Приложения тройных интегралов.
148) Несобственные кратные интегралы.
149) Определения криволинейного интеграла 1-го рода. Его свойства.
150) Вычисление криволинейного интеграла 1-го рода. Сведение криволинейного интеграла 1-го рода к определенному интегралу.
151) Определения криволинейного интеграла 2-го рода. Его свойства.
152) Вычисление криволинейного интеграла 2-го рода. Сведение криволинейного интеграла 2-го рода к определенному интегралу.
153) Приложения криволинейных интегралов.
154) Связь криволинейных интегралов 1-го и 2-го рода.
155) Формула Грина. Вычисление площадей с помощью криволинейных интегралов.
156) Условия независимости криволинейного интеграла второго рода от пути интегрирования.
157) Понятие поверхности. Задание поверхности с помощью векторных функций. Касательная плоскость и нормаль к поверхности.
158) Сторона поверхности. Ориентация. Односторонние и двусторонние поверхности.
159) Понятие площади поверхности. Квадрируемость гладких поверхностей.
160) Поверхностный интеграл первого рода. Его существование и свойства.
161) Поверхностный интеграл второго рода. Его существование и свойства.
162) Приложения поверхностных интегралов.
163) Формула Стокса.
164) Формула Остроградского.

8.4. Планируемые уровни сформированности компетенций обучающихся и критерии оценивания

Уровни	Содержательное описание уровня	Основные признаки выделения уровня (этапы формирования компетенции, критерии оценки сформированности)	Пятибалльная шкала (академическая) оценка	Двухбалльная шакала, зачет	БРС, % освоения (рейтинговая оценка)
Повышенный	Творческая деятельность	*Включает нижестоящий уровень.* Умение самостоятельно принимать решение, решать проблему/задачу теоретического и прикладного характера на основе изученных методов,	отлично	зачтено	86-100

		приемов, технологий			
Базовый	Применение знаний и умений в более широких контекстах учебной и профессиональной деятельности, нежели по образцу с большей степени самостоятельности и инициативы	*Включает нижестоящий уровень.* Способность собирать, систематизировать, анализировать и грамотно использовать информацию из самостоятельно найденных теоретических источников и иллюстрировать ими теоретические положения или обосновывать практику применения	хорошо		71-85
Удовлетворительный (достаточный)	Репродуктивная деятельность	Изложение в пределах задач курса теоретически и практически контролируемого материала	удовлетворительно		55-70
Недостаточный	Отсутствие признаков удовлетворительного уровня		неудовлетворительно	не зачтено	Менее 55

9. Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины.

Основная литература

1. Тер-Крикоров, А. М. Курс математического анализа : учебное пособие / А.М. Тер-Крикоров, М.И. Шабунин, 2-е изд. - Москва : ФИЗМАТЛИТ, 2001. - 669 с.ISBN 5-9221-0008-3. - Текст : электронный. - URL: https://znanium.com/catalog/product/544563 (дата обращения: 06.04.2022). – Режим доступа: по подписке.
2. Кудрявцев, Л. Д. Краткий курс математического анализа. Т. 1. Дифференциальное и интегральное исчисления функций одной переменной. Ряды: Учебник / Кудрявцев Л.Д., - 4-е изд. - Москва :ФИЗМАТЛИТ, 2015. - 444 с.: ISBN 978-5-9221-1585-8. - Текст : электронный. - URL: https://znanium.com/catalog/product/854332 (дата обращения: 06.04.2022). – Режим доступа: по подписке.
3. Кудрявцев, Л. Д. Краткий курс математического анализа. Т. 2. Дифференциальное и интегральное исчисления функций многих переменных. Гармонический анализ / Кудрявцев Л.Д., - 3-е изд. - Москва :ФИЗМАТЛИТ, 2003. - 424 с.: ISBN 5-9221-0185-4. - Текст : электронный. - URL: https://znanium.com/catalog/product/944781 (дата обращения: 06.04.2022). – Режим доступа: по подписке.

Дополнительная литература

1. Виноградов, О. Л. Математический анализ: учебник / О. Л. Виноградов. - Санкт-Петербург: БХВ-Петербург, 2017. - 752 с. - (Учебная литература для вузов). - ISBN 978-5-9775-3815-2. - Текст: электронный. - URL: https://znanium.com/catalog/product/1861364

2. Туганбаев, А. А. Высшая математика. Основы математического анализа. Задачи с решениями и теория: учебник / А. А. Туганбаев. - Москва: ФЛИНТА, 2018. - 316 с. - ISBN 978-5-9765-3503-9. - Текст: электронный. - URL: https://znanium.com/catalog/product/1859863

3. Демидович Б. П. Сборник задач и упражнений по математическому анализу [Текст] : учеб. пособие для вузов / Б. П. Демидович, 2010. 558 с. (УА 90 экз)

10. Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины (модуля).

- НЭБ Национальная электронная библиотека, диссертации и прочие издания
- eLIBRARY.RU Научная электронная библиотека, книги, статьи, тезисы докладов конференций
- https://lms-3.kantiana.ru/course/view.php?id=1004
- Гребенников Электронная библиотека ИД журналы
- https://www.youtube.com/channel/UCICd1ydh1XxiW_wyCjbp81A (визуализации автора по анализу на канале you tube)
- ЭБС Консультант студента
- ПРОСПЕКТ ЭБС
- ЭБС ZNANIUM.COM
- РГБ Информационное обслуживание по МБА
- БЕН РАН
- Электронно-библиотечная система (ЭБС) Кантитана (https://elib.kantiana.ru/)

11. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине.

Программное обеспечение обучения включает в себя:

- система электронного образовательного контента БФУ им. И. Канта – www.lms-3.kantiana.ru, обеспечивающую разработку и комплексное использование электронных образовательных ресурсов;
- серверное программное обеспечение, необходимое для функционирования сервера и связи с системой электронного обучения через Интернет;
- корпоративная платформа Microsoft Teams;
- установленное на рабочих местах обучающихся ПО: Microsoft Windows 7, Microsoft Office Standart 2010, антивирусное программное обеспечение Kaspersky Endpoint Security.
- специализированное ПО не требуется.

12. Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине.

Для проведения занятий лекционного типа, практических и семинарских занятий используются специальные помещения (учебные аудитории), оборудованные техническими средствами обучения – мультимедийной проекционной техникой. Для проведения занятий лекционного типа используются наборы демонстрационного оборудования.

Для проведения лабораторных работ, (практических занятий – при необходимости) используются специальные помещения (учебные аудитории), оснащенные специализированным

лабораторным оборудованием: персональными компьютерами с возможностью выхода в интернет и с установленным программным обеспечением, заявленным в п.11.

Для проведения групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации используются специальные помещения (учебные аудитории), оборудованные специализированной мебелью (для обучающихся), меловой / маркерной доской.

Для организации самостоятельной работы обучающимся предоставляются помещения, оснащенные компьютерной техникой с возможностью подключения к сети «Интернет» и обеспечением доступа в электронную информационно-образовательную среду университета.

Для обучения инвалидов и лиц с ограниченными возможностями здоровья университетом могут быть представлены специализированные средства обучения, в том числе технические средства коллективного и индивидуального пользования.

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
федеральное государственное автономное образовательное учреждение высшего образования «Балтийский федеральный университет имени Иммануила Канта»
Институт физико-математических наук и информационных технологий

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

«Алгебра»

Шифр: 10.05.01
Специальность: «Компьютерная безопасность»
Специализация: «Математические методы защиты информации»
Квалификация (степень) выпускника: специалист по защите информации

Калининград
2022

Лист согласования

Составитель: Скрыдлова Елена Викторовна, к.ф.-м.н., доцент

Рабочая программа утверждена на заседании учебно-методического совета института физико-математических наук и информационных технологий

Протокол № 01/22 от «01» февраля 2022 г.

Председатель учебно-методического
совета института физико-
математических наук и информационных
технологий

Первый заместитель директора Шпилевой А. А
ИФМНиИТ, к. ф.-м. н., доцент

Ведущий менеджер Е.П.Ставицкая

Содержание

1.Наименование дисциплины: «Алгебра».

Цель дисциплины: целью освоения дисциплины «Алгебра» является фундаментальная подготовка обучающихся в области алгебры.

2. Перечень планируемых результатов обучения по дисциплине, соотнесенных с планируемыми результатами освоения образовательной программы

Код компетенции	Результаты освоения образовательной программы (ИДК)	Результаты обучения по дисциплине
ОПК-3. Способен на основании совокупности математических методов разрабатывать, обосновывать и реализовывать процедуры решения задач профессиональной деятельности.	ОПК-3.1. Знает необходимые математические методы для решения задач обеспечения защиты информации. ОПК-3.2. Применяет совокупность необходимых математических методов для решения задач обеспечения защиты информации. ОПК-3.3. Разрабатывает, обосновывает и реализует на практике процедуры решения задач обеспечения защиты информации.	- **знать** основные понятия алгебры и основные типы задач, возникающих в алгебре; - **уметь** использовать полученные теоретические знания для решения конкретных прикладных задач, производить математические расчеты в стандартных постановках, производить содержательный анализ результатов вычислений; использовать полученные знания в профессиональной деятельности; - **владеть** практическими навыками формализации различных задач алгебраическими методами; составления алгоритмов решения, пригодных для последующего программирования; анализа оценки эффективности применяемых методов.

3. Место дисциплины в структуре образовательной программы

Дисциплина «Алгебра» представляет собой дисциплину обязательной части Блока 1 Дисциплины (модули) подготовки обучающихся.

4. Виды учебной работы по дисциплине.

Виды учебной работы по дисциплине зафиксированы учебным планом основной профессиональной образовательной программы по указанному направлению и профилю, выражаются в академических часах. Часы контактной работы и самостоятельной работы обчающегося и часы, отводимые на процедуры контроля, могут различаться в учебных планах ОПОП по формам обучения. Объем контактной работы включает часы контактной аудиторной работы (лекции/практические занятия/ лабораторные работы), контактной внеаудиторной работы (контроль самостоятельной работы), часы контактной работы в период аттестации. Контактная работа, в том числе может проводиться посредством электронной информационно-образовательной среды университета с использованием ресурсов сети Интернет и дистанционных технологий.

5. Содержание дисциплины, структурированное по темам (разделам)

Исходя из рамок, установленных учебным планом по трудоемкости и видам учебной работы по дисциплине, преподаватель самостоятельно выбирает тематику занятий по формам и количеству часов проведения контактной работы: лекции и иные учебные занятия, предусматривающие преимущественную передачу учебной информации преподавателем и (или) занятия семинарского типа (семинары, практические занятия, практикумы, лабораторные работы, коллоквиумы и иные аналогичные занятия), и (или) групповые консультации, и (или) индивидуальную работу обучающихся с преподавателем, в том числе индивидуальные консультации (по курсовым работам/проектам – при наличии курсовой работы/проекта по данной дисциплине в учебном плане). Рекомендуемая тематика занятий максимально полно реализуется в контактной работе с обучающимися очной формы обучения. В случае реализации образовательной программы в заочной / очно-заочной форме трудоемкость дисциплины сохраняется, однако объем учебного материала в значительной части осваивается обучающимися в форме самостоятельной работы. При этом требования к ожидаемым образовательным результатам обучающихся по данной дисциплине не зависят от формы реализации образовательной программы.

№	Наименование раздела	Содержание раздела
1	Матрицы и определители	Понятие матрицы. Линейные операции над матрицами. Умножение матриц. Перестановки из n элементов. Подстановки степени n. Четность подстановок. Понятие определителя порядка n. Определители порядка 2 и 3. Свойства определителей. Теоремы о разложении определителя по элементам строки. Теорема Лапласа. Формулы Крамера решения системы линейных уравнений. Теорема об определителе произведения матриц. Обратная матрица. Матричные уравнения. Элементарные преобразования матриц. Метод Гаусса решения систем линейных уравнений.
2	Поле комплексных чисел	Построение поля комплексных чисел. Действия с комплексными числами. Комплексно сопряженные числа. Тригонометрическая форма комплексного числа. Умножение и деление комплексных чисел в тригонометрической форме. Возведение комплексных чисел в степень. Формула Муавра. Извлечение корня из комплексного числа. Корни степени n из единицы. Первообразные корни.
3	Кольцо многочленов от одной переменной	Построение кольца многочленов от одной переменной. Действия над многочленами. Теорема деления многочленов с остатком. Делимость многочленов. Наибольший общий делитель. Алгоритм Евклида. Взаимно простые многочлены. Теорема Безу. Схема Горнера. Корни многочленов. Кратность корня и её связь со значениями производных. Основная теорема алгебры многочленов, следствие из нее. Формулы Виета. Многочлены с действительными коэффициентами и их корни. Приводимость многочленов над полем. Разложение многочленов на неприводимые множители над полями действительных и комплексных чисел. Многочлены с рациональными коэффициентами и их корни. Поле рациональных дробей. Разложение рациональной дроби на простейшие
4	Векторные пространства и системы линейных	Понятие векторного пространства. Линейная зависимость векторов. Свойства линейной зависимости. Базис пространства. Координаты вектора. Теоремы о базисах. Размерность

	уравнений	пространства. Формулы преобразования базиса. Формулы преобразования координат. Изоморфизм векторных пространств одинаковой конечной размерности. Подпространства. Признак подпространства. Сумма и пересечение подпространств. Прямая сумма. Ранг системы векторов. Линейная оболочка векторов. Ранг матрицы (основная теорема). Теоремы о ранге матрицы. Критерий совместности системы линейных уравнений. Подпространство решений системы линейных однородных уравнений. Фундаментальные решения системы линейных однородных уравнений. Обзор методов исследования и решения систем линейных уравнений.
5	Линейные операторы векторных пространств	Понятие линейного отображения и линейного оператора. Матрица линейного оператора. Связь матриц оператора в разных базисах. Действия над линейными операторами. Обратные операторы, условие существования. Образ и ядро линейного оператора. Теоремы о ранге и дефекте линейного оператора. Собственные векторы и собственные значения линейного оператора. Условия приводимости матрицы линейного оператора к диагональному виду. Характеристический многочлен линейного оператора. Характеристические корни и собственные значения линейного оператора. Инвариантные подпространства линейного оператора. Разложение векторного пространства в прямую сумму инвариантных подпространств.
6	Евклидовы пространства	Понятие евклидова и унитарного пространства. Скалярное произведение векторов. Процесс ортогонализации векторов. Длина вектора и угол между векторами. Неравенство Коши-Буняковского. Ортонормированные базисы. Ортогональные матрицы. Изоморфизм евклидовых пространств одинаковой размерности. Ортогональное дополнение подпространства. Симметрические операторы, их свойства. Критерий симметричности оператора, существование собственного ортонормированного базиса. Ортогональные операторы, их свойства. Канонический базис и каноническая матрица ортогонального оператора.
7	Квадратичные формы	Линейные формы. Квадратичные формы. Ранг квадратичной формы. Приведение квадратичной формы к каноническому виду. Метод Лагранжа. Метод элементарных преобразований. Приведение квадратичной формы в евклидовом пространстве к каноническому виду ортогональным преобразованием переменных. Нормальный вид квадратичной формы над полем вещественных и комплексных чисел. Закон инерции квадратичных форм. Положительно определённые квадратичные формы. Критерий Сильвестра. Распадающиеся квадратичные формы.
8	Основные алгебраические структуры	Внутренние и внешние операции на множестве. Понятие алгебраической структуры. Понятие группы. Примеры. Свойства элементов группы. Группа подстановок. Группа невырожденных матриц. Циклические группы. Конечные группы. Подгруппы. Признаки подгрупп. Теорема Лагранжа. Группы ортогональных и унимодулярных матриц. Кольца, тела, поля. Примеры. Кольцо матриц. Кольцо классов вычетов. Подкольца. Идеалы. Подполя.
9	Элементы общей алгебры	Отношение эквивалентности на множестве. Фактор множество. Разложение группы на смежные классы по подгруппе. Нормальный делитель группы. Конечные группы. Теорема Лагранжа. Фактор-группа. Гомоморфизм и изоморфизм групп. Ядро гомоморфизма. Изоморфизм циклических групп. Основная

		теорема о гомоморфизмах групп. Гомоморфизм и изоморфизм колец и полей. Ядро гомоморфизма. Факторкольцо. Теорема о расширении колец и полей. Простое алгебраическое расширение поля. Алгебраически замкнутые поля.

6. Рекомендуемая тематика учебных занятий в форме контактной работы

Рекомендуемая тематика учебных занятий *лекционного* типа (предусматривающих преимущественную передачу учебной информации преподавателями):

№	Наименование раздела	Темы лекций
1	Матрицы и определители	Лекция 1. Понятие матрицы. Линейные операции над матрицами. Умножение матриц. Лекция 2. Перестановки из n элементов. Подстановки n элементов. Четность подстановок. Лекция 3. Понятие определителя порядка n. Определители порядка 2 и 3. Свойства определителей. Лекция 4. Теоремы о разложении определителя по элементам строки. Лекция 5. Формулы Крамера решения системы линейных уравнений. Лекция 6. Теорема об определителе произведения матриц. Обратная матрица. Лекция 7. Матричные уравнения. Элементарные преобразования матриц. Метод Гаусса решения систем линейных уравнений.
2	Поле комплексных чисел	Лекция 8. Построение поля комплексных чисел. Действия с комплексными числами. Комплексно сопряженные числа. Лекция 9. Тригонометрическая форма комплексного числа. Умножение и деление комплексных чисел в тригонометрической форме. Лекция 10. Возведение комплексных чисел в степень. Формула Муавра. Извлечение корня из комплексного числа. Корни степени n из единицы. Первообразные корни.
3	Кольцо многочленов от одной переменной	Лекция 11. Построение кольца многочленов от одной переменной. Действия над многочленами. Теорема деления многочленов с остатком. Лекция 12. Делимость многочленов. Наибольший общий делитель. Алгоритм Евклида. Взаимно простые многочлены. Лекция 13. Теорема Безу. Схема Горнера. Корни многочленов. Кратность корня и её связь со значениями производных. Основная теорема алгебры многочленов, следствие из нее. Лекция 14. Формулы Виета. Многочлены с действительными коэффициентами и их корни. Приводимость многочленов над полем. Разложение многочленов на неприводимые множители над полями действительных и комплексных чисел. Лекция 15. Многочлены с рациональными коэффициентами и их корни. Поле рациональных дробей. Разложение рациональной дроби на простейшие
4	Векторные пространства и системы линейных	Лекция 16. Понятие векторного пространства. Линейная зависимость векторов. Свойства линейной зависимости. Лекция 17. Базис пространства. Координаты вектора. Теоремы о базисах. Размерность пространства.

	уравнений	Лекция 18. Формулы преобразования базиса. Формулы преобразования координат. Изоморфизм векторных пространств одинаковой конечной размерности. Лекция 19. Подпространства. Признак подпространства. Сумма и пересечение подпространств. Прямая сумма. Лекция 20. Ранг системы векторов. Линейная оболочка векторов. Ранг матрицы (основная теорема). Лекция 21. Теоремы о ранге матрицы. Критерий совместности системы линейных уравнений. Лекция 22. Подпространство решений системы линейных однородных уравнений. Фундаментальные решения системы линейных однородных уравнений. Обзор методов исследования и решения систем линейных уравнений.
5	Линейные операторы векторных пространств	Лекция 23. Понятие линейного отображения и линейного оператора. Матрица линейного оператора. Связь матриц оператора в разных базисах. Лекция 24. Действия над линейными операторами. Обратные операторы, условие существования. Образ и ядро линейного оператора. Теоремы о ранге и дефекте линейного оператора. Лекция 26. Собственные векторы и собственные значения линейного оператора. Условия приводимости матрицы линейного оператора к диагональному виду. Лекция 27. . Характеристический многочлен линейного оператора. Характеристические корни и собственные значения линейного оператора. Лекция 28. Инвариантные подпространства линейного оператора. Разложение векторного пространства в прямую сумму инвариантных подпространств.
6	Евклидовы пространства	Лекция 29. Понятие евклидова и унитарного пространства. Скалярное произведение векторов. Процесс ортогонализации векторов. Длина вектора и угол между векторами. Неравенство Коши-Буняковского. Лекция 30. Ортонормированные базисы. Ортогональные матрицы. Изоморфизм евклидовых пространств одинаковой размерности. Ортогональное дополнение подпространства. Лекция 31. Симметрические операторы, их свойства. Критерий симметричности оператора, существование собственного ортонормированного базиса. Ортогональные операторы, их свойства. Канонический базис и каноническая матрица ортогонального оператора.
7	Квадратичные формы	Лекция 32. Квадратичные формы. Ранг квадратичной формы. Приведение квадратичной формы к каноническому виду. Метод Лагранжа. Лекция 33. Метод элементарных преобразований. Приведение квадратичной формы в евклидовом пространстве к каноническому виду ортогональным преобразованием переменных. Нормальный вид квадратичной формы над полем вещественных и комплексных чисел. Лекция 34. Закон инерции квадратичных форм. Положительно определённые квадратичные формы. Критерий Сильвестра. Распадающиеся квадратичные формы.
8	Основные алгебраические структуры	Лекция 35. Внутренние и внешние операции на множестве. Понятие алгебраической структуры. Понятие группы. Примеры. Свойства элементов группы. Группа подстановок. Группа невырожденных матриц. Лекция 36. Циклические группы. Конечные группы. Подгруппы. Признаки подгрупп. Теорема Лагранжа. Группы ортогональных

		и унимодулярных матриц. Лекция 37. Кольца, тела, поля. Примеры. Кольцо матриц. Кольцо классов вычетов. Подкольца. Идеалы. Подполя.
9	Элементы общей алгебры	Лекция 38. Отношение эквивалентности на множестве. Фактор множество. Разложение группы на смежные классы по подгруппе. Лекция 39. Нормальный делитель группы. Конечные группы. Теорема Лагранжа. Фактор-группа. Гомоморфизм и изоморфизм групп. Ядро гомоморфизма. Изоморфизм циклических групп. Основная теорема о гомоморфизмах групп. Лекция 40. Гомоморфизм и изоморфизм колец и полей. Ядро гомоморфизма. Факторкольцо. Лекция 41. Теорема о расширении колец и полей. Простое алгебраическое расширение поля. Алгебраически замкнутые поля.

Рекомендуемая тематика *практических* занятий:

Первый семестр

1. Перестановки. Подстановки. Четность подстановки.
2. Матрицы и действия над ними. Самостоятельная работа.
3. Понятие определителя n-го порядка. Основные свойства определителей.
4. Вычисление определителей. Правило Крамера. Самостоятельная работа.
5. Обратная матрица. Матричные уравнения. Матричный метод решения систем линейных уравнений. Самостоятельная работа.
6. Метод Гаусса решения систем линейных уравнений.
7. Поле комплексных чисел. Действия над комплексными числами в алгебраической форме.
8. Извлечение корня квадратного из комплексных чисел в алгебраической форме. Решение квадратных уравнений.
9. Тригонометрическая форма комплексного числа. Самостоятельная работа.
10. Деление многочленов с остатком. Наибольший общий делитель многочленов.
11. Схема Горнера. Корни многочленов. Кратность корней. Самостоятельная работа.
12. Обобщенная теорема Виета.
13. Разложение многочлена на неприводимые множители над полем действительных и комплексных чисел.
14. Нахождение рациональных корней полинома. Самостоятельная работа.
15. Разложение правильной рациональной дроби на простейшие.

Второй семестр

1. Векторные пространства. Линейная зависимость векторов. Базис.
2. Формулы преобразования базиса. Формулы преобразования координат. Самостоятельная работа.
3. Ранг матрицы. Ранг системы векторов. Линейная оболочка векторов.
4. Исследование системы линейных неоднородных уравнений на совместность.
5. Фундаментальная система решений. Самостоятельная работа.
6. Подпространства векторного пространства.
7. Сумма и пересечения подпространств, определение их базисов. Самостоятельная работа.
8. Линейные операторы векторных пространств. Матрица линейного оператора.

9. Действия над линейными операторами. Самостоятельная работа.
10. Образ и ядро линейного оператора.
11. Характеристические корни и собственные векторы. Самостоятельная работа.
12. Евклидовы пространства. Процесс ортогонализации векторов.
13. Ортогональное дополнение подпространства. Ортогональная проекция и ортогональная составляющая вектора. Самостоятельная работа.
14. Приведение квадратичной формы к каноническому виду методом элементарных преобразований.
15. Приведение квадратичной формы к каноническому виду методом Лагранжа.
16. Приведение квадратичной формы к каноническому виду ортогональным преобразованием переменных.
17. Положительно определенные квадратичные формы.
18. Группы. Кольца. Поля.
19. Кольцо классов вычетов.
20. Отношение эквивалентности на множестве. Фактор-множество.
21. Разложение группы по подгруппе. Нормальный делитель. Факторгруппа.
22. Изоморфизм и гомоморфизм групп.
23. Конечные группы. Группа подстановок.
24. Идеал кольца. Факторкольцо.
25. Расширения колец и полей. Простое алгебраическое расширение поля.

На практических занятиях решаются задачи по теме занятия.

Требования к самостоятельной работе обучающихся

1. Работа с лекционным материалом, предусматривающая проработку конспекта лекций и учебной литературы, по всем темам из п. 6 настоящей рабочей программы.
2. Выполнение домашнего задания, предусматривающего решение задач, выполнение упражнений, выдаваемых на практических занятиях, по всем темам из п. 6 настоящей рабочей программы.

Руководствуясь положениями статьи 47 и статьи 48 Федерального закона от 29 декабря 2012 г. N 273-ФЗ «Об образовании в Российской Федерации» научно-педагогические работники и иные лица, привлекаемые университетом к реализации данной образовательной программы, пользуются предоставленными академическими правами и свободами в части свободы преподавания, свободы от вмешательства в профессиональную деятельность; свободы выбора и использования педагогически обоснованных форм, средств, методов обучения и воспитания; права на творческую инициативу, разработку и применение авторских программ и методов обучения и воспитания в пределах реализуемой образовательной программы и отдельной дисциплины.

Исходя из рамок, установленных учебным планом по трудоемкости и видам учебной работы по дисциплине, преподаватель самостоятельно выбирает тематику занятий по формам и количеству часов проведения контактной работы: лекции и иные учебные занятия, предусматривающие преимущественную передачу учебной информации преподавателем и (или) занятия семинарского типа (семинары, практические занятия, практикумы, лабораторные работы, коллоквиумы и иные аналогичные занятия), и (или) групповые консультации, и (или) индивидуальную работу обучающихся с преподавателем, в том числе индивидуальные консультации (по курсовым

работам/проектам – при наличии курсовой работы/проекта по данной дисциплине в учебном плане).

Рекомендуемая тематика занятий максимально полно реализуется в контактной работе с обучающимися очной формы обучения. В случае реализации образовательной программы в заочной / очно-заочной форме трудоемкость дисциплины сохраняется, однако объем учебного материала в значительной части осваивается обучающимися в форме самостоятельной работы. При этом требования к ожидаемым образовательным результатам обучающихся по данной дисциплине не зависят от формы реализации образовательной программы.

7. Методические рекомендации по видам занятий

Лекционные занятия.

В ходе лекционных занятий обучающимся рекомендуется выполнять следующие действия. Вести конспектирование учебного материала. Обращать внимание на категории, формулировки, раскрывающие содержание тех или иных явлений и процессов, научные выводы и практические рекомендации по их применению. Задавать преподавателю уточняющие вопросы с целью уяснения теоретических положений, разрешения спорных ситуаций.

Желательно оставить в рабочих конспектах поля, на которых во внеаудиторное время можно сделать пометки из рекомендованной литературы, дополняющие материал прослушанной лекции, а также подчеркивающие особую важность тех или иных теоретических положений.

Практические и семинарские занятия.

На практических и семинарских занятиях в зависимости от темы занятия выполняется поиск информации по решению проблем, практические упражнения, контрольные работы, выработка индивидуальных или групповых решений, итоговое обсуждение с обменом знаниями, участие в круглых столах, разбор конкретных ситуаций, командная работа, представление портфолио и т.п.

Самостоятельная работа.

Самостоятельная работа осуществляется в виде изучения литературы, эмпирических данных по публикациям и конкретных ситуаций из практики, подготовке индивидуальных работ, работа с лекционным материалом, самостоятельное изучение отдельных тем дисциплины; поиск и обзор литературы и электронных источников; чтение и изучение учебника и учебных пособий.

8. Фонд оценочных средств

8.1. Перечень компетенций с указанием этапов их формирования в процессе освоения образовательной программы в рамках учебной дисциплины

Основными этапами формирования указанных компетенций при изучении обучающимися дисциплины являются последовательное изучение содержательно связанных между собой тем учебных занятий. Изучение каждой темы предполагает овладение обучающимися необходимыми компетенциями. Результат аттестации обучающихся на различных этапах формирования компетенций показывает уровень освоения компетенций.

Контролируемые разделы (темы) дисциплины	Индекс контроли-	Оценочные средства по этапам формирования компетенций

	руемой компетенции (или её части)	текущий контроль по дисциплине
Матрицы и определители	ОПК-3	Опрос, решение задач, самостоятельная работа
Поле комплексных чисел	ОПК-3	Опрос, решение задач, самостоятельная работа
Кольцо многочленов от одной переменной	ОПК-3	Опрос, решение задач, самостоятельная работа
Векторные пространства и системы линейных уравнений	ОПК-3	Опрос, решение задач, самостоятельная работа
Линейные операторы векторных пространств	ОПК-3	Опрос, решение задач, самостоятельная работа
Евклидовы пространства	ОПК-3	Опрос, решение задач, самостоятельная работа
Квадратичные формы	ОПК-3	Опрос, решение задач, самостоятельная работа
Основные алгебраические структуры	ОПК-3	Опрос, решение задач
Элементы общей алгебры	ОПК-3	Опрос, решение задач

8.2. Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений и навыков и (или) опыта деятельности процессе текущего контроля

Примеры вопросов для устного опроса:

Тема 1.

1. Дать определение матрицы.
2. Записать формулу умножения матриц.
3. В каком случае можно перемножить две прямоугольные матрицы?
4. Что называется определителем n-го порядка?
5. Перечислить основные свойства определителя.
6. Записать формулу разложения определителя по элементам строки (столбца).
7. Записать формулы Крамера решения системы линейных уравнений.
8. Дать определение невырожденной матрицы.
9. Какая система уравнений называется совместной?
10. Сколько решений может иметь система линейных уравнений?

Тема 2.

1. Дать определение алгебраической формы комплексного числа.
2. Дать определение тригонометрической формы комплексного числа.
3. Записать формулы, связывающие алгебраическую и тригонометрическую формы комплексного числа.
4. Как умножаются и делятся комплексные числа в алгебраической форме?
5. Как умножаются и делятся комплексные числа в тригонометрической форме?
6. Перечислить способы возведения комплексных чисел в степень.
7. Как извлекается корень из комплексного числа?
8. Чему равен корень степени 3 из единицы?
9. Как используются корни степени n из единицы при извлечении корня n-ой степени из комплексного числа?

10. Дать определение первообразного корня.

Тема 3.

. 1. Сформулировать теорему деления многочленов с остатком.
2. Дать определение наибольшего общего делителя многочленов.
3. Дать определение взаимно простых многочленов.
4. Сформулировать теорему Безу.
5. Как найти значения от многочлена в точке при помощи схемы Горнера?
6. Дать определение корня многочлена.
7. Дать определение кратности корня многочлена.
8. Записать формулы Виета.
9. Какие многочлены называются приводимыми над данным полем?
10. Как разложить рациональную дробь в сумму простейших дробей?

Тема 4.

1. Дать определение векторного пространства.
2. Какие векторы называются линейно зависимыми (независимыми)?
3. Дать определение базиса.
4. Записать формулу преобразования базиса.
5. Как находятся координаты вектора в новом базисе?
6. Сформулировать теорему о размерности суммы подпространств.
7. Дать определение ранга матрицы.
8. Сформулировать основную теорему о ранге матрицы.
9. Сформулировать критерий совместности системы линейных уравнений.
10. Дать определение фундаментальной системы решений.

Тема 5.

1. Дать определение линейного оператора.
2. Привести примеры линейных операторов.
3. Как записывается матрица линейного оператора в данном базисе?
4. Какой формулой связываются матрицы оператора в разных базисах?
5. Дать определение образа линейного оператора.
6. Дать определение ядра линейного оператора.
7. Сформулировать теорему о ранге и дефекте линейного оператора.
8. Дать определение собственного вектора линейного оператора.
9. Дать определение характеристического многочлена линейного оператора.
10. Дать определение инвариантного подпространства линейного оператора.

Тема 6.

1. Дать определение евклидова пространства.
2. Как находится скалярное произведение векторов?
3. Что называется длиной вектора?
4. Как нормировать вектор?
5. Описать процесс ортогонализации векторов.
6. Дать определение ортонормированного базиса.
7. Какая матрица называется ортогональной?
8. Что такое ортогональное дополнение подпространства?
9. Дать определение симметрического оператора.
10. Сформулировать критерий симметричности оператора.

Тема 7.

1. Дать определение квадратичной формы.

2. Что называется рангом квадратичной формы?

3. Какой вид квадратичной формы называется каноническим?

4. Проиллюстрировать метод элементарных преобразований приведения квадратичной формы к каноническому виду.

5. Проиллюстрировать метод Лагранжа приведения квадратичной формы к каноническому виду.

6. Описать метод приведения квадратичной формы в евклидовом пространстве к каноническому виду ортогональным преобразованием переменных.

7. Что называется нормальным видом квадратичной формы над полем вещественных и комплексных чисел?

8. Дать определение положительно определенной квадратичной формы.

9. Сформулировать критерий Сильвестра.

10. Дать определение распадающихся квадратичных форм.

Тема 8.

1. Дать определение внутренней операции на множестве.
2. Дать определение внешней операции на множестве.
3. Что называется алгебраической структурой?
4. Дать определение группы. Привести пример.
5. Дать определение циклической группы.
6. Дать определение подгруппы. Привести пример.
7. Сформулировать признаки подгруппы.
8. Дать определение кольца. Привести пример.
9. Дать определение поля. Привести пример.
10. Как строится кольцо классов вычетов по заданному модулю?

Тема 9.

1. Дать определение отношения эквивалентности на множестве. Привести примеры.
2. Дать определение гомоморфизма и изоморфизма групп. Что называется ядром гомоморфизма. Привести примеры.
3. Сформулировать теорему об изоморфизме циклических групп.
4. Что понимается под разложением группы по подгруппе.
5. Какие группы называются конечными. Сформулировать теорему Лагранжа.
6. Определить нормальный делитель группы. Привести примеры.
7. Что такое фактор группа. Привести примеры.
8. Сформулировать основную теорему о гомоморфизмах групп.
9. Дать определение гомоморфизма и изоморфизма колец и полей. Что называется ядром гомоморфизма.
10. Привести примеры фактор колец.

Типовые контрольные задания

Первый семестр

Контрольная работа № 1

1. Найти *f(A)*, если $f(x) = x^3 + 3x^2 - 2x + 5$, $A = \begin{pmatrix} 1 & -2 & 3 \\ 2 & -4 & 1 \\ 3 & -5 & 2 \end{pmatrix}$.

2. Найти число инверсий в перестановке и указать, для каких n эта перестановка четна $\{1, 4, 7, \ldots, 3n-2, 2, 5, \ldots, 3n-1, 3, 6, \ldots, 3n\}$.

3. Вычислить определитель $\begin{vmatrix} 5 & 2 & 1 & 3 & 2 \\ 4 & 0 & 7 & 2 & 3 \\ 2 & 3 & 7 & 5 & 3 \\ 2 & 3 & 6 & 4 & 5 \\ 3 & 0 & 4 & 1 & -1 \end{vmatrix}$.

4. Решить систему методом Крамера $\begin{cases} 2x_1 + x_2 + 4x_3 + 8x_4 = -1, \\ x_1 + 3x_2 - 6x_3 + 2x_4 = 3, \\ 3x_1 - 2x_2 + 2x_3 + 2x_4 = 10, \\ 2x_1 - x_2 + 2x_3 = 4. \end{cases}$

5. Решить систему методом исключения неизвестных

$$\begin{cases} x_1 + 2x_2 + 5x_3 + 9x_4 = 79, \\ 3x_1 + 13x_2 + 18x_3 + 30x_4 = 263, \\ 2x_1 + 4x_2 + 11x_3 + 16x_4 = 146, \\ x_1 + 9x_2 + 9x_3 + 9x_4 = 92. \end{cases}$$

6. Решить матричное уравнение и сделать проверку

$$\begin{pmatrix} -2 & 3 & 1 \\ 3 & 6 & 2 \\ 1 & 2 & 1 \end{pmatrix} X = \begin{pmatrix} 5 & 1 & 0 \\ 1 & 2 & 4 \\ -9 & 1 & -1 \end{pmatrix}.$$

Контрольная работа № 2

1. Вычислить $(2+i)(3-i) + \dfrac{2+3i}{3+4i}$.
2. Вычислить $\sqrt{24+10i}$.
3. Представить в тригонометрической форме комплексное число $-\sqrt{2} + i\sqrt{2}$.
4. Вычислить $\sqrt[3]{1-i}$.
5. Изобразить графически $|z+3+4i| > 5$.
6. Вычислить, используя тригонометрическую форму, $(1+i\sqrt{3})(1+i)$.

Второй семестр

Контрольная работа № 1

1. Перемножить многочлены и разделить с остатком многочлен *f(x)* на *g(x)*

$f(x) = 2x^4 - 4x^3 + 4x^2 - 6, \quad g(x) = x^2 - 3x - 1.$

2. Найти *НОД* многочленов $f(x) = x^4 + x^3 - 3x^2 - 4x - 1,\ g(x) = x^3 + x^2 - x - 1$.

3. Используя схему Горнера, определить значение многочлена *f(c)* и всех его производных $f(x) = 4x^3 - 2x^2 + 5x - 1, \quad c = 2.$

4. Используя схему Горнера, определить кратность *k* корня *c* многочлена *f(x)* и разложить *f(x)* на соответствующие множители

$f(x) = x^5 + 7x^4 + 16x^3 + 8x^2 - 16x - 16, \quad c = -2.$

5.Найти рациональные корни многочлена $f(x) = 3x^4 + \frac{1}{2}x^3 + x^2 - 2x + \frac{1}{2}$.

Контрольная работа № 2

1. Исследовать векторы на линейную зависимость
$\vec{a}=(1,4,6),\ \vec{b}=(1,-1,1),\ \vec{c}=(1,1,3)$.

2. Разложить вектор $\vec{x}$ по векторам $\vec{a},\vec{b},\vec{c}$, если $\vec{x}=(-2,4,7)$,
$\vec{a}=(0,1,2),\ \vec{b}=(1,0,1),\ \vec{c}=(-1,2,4).$

3. Найти координаты вектора в новом базисе $\begin{aligned} e_1' &= e_1 + e_2 + 3e_3, \\ e_2' &= 2e_1 - e_2, \\ e_3' &= -e_1 + e_2 + e_3. \end{aligned}$ $\vec{x}=(1,2,4)$.

4. Найти ранг матрицы $A=\begin{pmatrix} 1 & -1 & 5 & 7 \\ -1 & -3 & 2 & 4 \\ 3 & 5 & 1 & -1 \\ 7 & 9 & 7 & 1 \end{pmatrix}$.

5. Найти фундаментальный набор решений системы $\begin{cases} 3x_1-5x_2-x_3-2x_4=0, \\ 8x_1-6x_2+3x_3-7x_4=0, \\ 2x_1+4x_2+5x_3-3x_4=0. \end{cases}$

6. Исследовать на совместность в зависимости от параметра
$\begin{cases} 2x_1-x_2+x_3+x_4=1, \\ x_1+2x_2-x_3+4x_4=2, \\ x_1+7x_2-4x_3+11x_4=a. \end{cases}$

Контрольная работа № 3

1. Найти размерность подпространств, размерности суммы и пересечения. Указать базисы.

L_1: $\vec{a}_1=(1,2,0,1),\ \vec{a}_2=(1,1,1,0)$, L_2: $\vec{b}_1=(1,0,1,0),\ \vec{b}_2=(1,3,0,1)$.

2. Найти матрицу оператора в базисе (e_1',e_2',e_3'), где $\begin{aligned} e_1' &= e_1 - e_2 + e_3, \\ e_2' &= -e_1 + e_2 - 2e_3, \\ e_3' &= -e_1 + 2e_2 + e_3, \end{aligned}$ если она задана в базисе (e_1,e_2,e_3) $A=\begin{pmatrix} 1 & 0 & 2 \\ 3 & -1 & 0 \\ 1 & 1 & -2 \end{pmatrix}$.

3. Найти собственные значения и собственные векторы оператора, заданного матрицей $A=\begin{pmatrix} 4 & -2 & -1 \\ -1 & 3 & -1 \\ 1 & -2 & 2 \end{pmatrix}$.

4. Найти базис образа и базис ядра линейного оператора, заданного в некотором базисе $\vec{e_1}$, $\vec{e_2}$, $\vec{e_3}$, $\vec{e_4}$ матрицей $A=\begin{pmatrix} 2 & -1 & 1 & 1 \\ -1 & 1 & -2 & 2 \\ 2 & 1 & -5 & 11 \\ 1 & 0 & -1 & 3 \end{pmatrix}$.

Контрольная работа № 4

1. Привести квадратичную форму к нормальному виду методом элементарных преобразований, указать преобразование и сделать проверку

$x_1^2 + 4x_1x_2 + 4x_1x_3 + 8x_2^2 + 16x_2x_3 + 7x_3^2$.

2. Преобразовать к каноническому виду ортогональным преобразованием квадратичную форму

$x_1^2 - 5x_2^2 + x_3^2 + 4x_1x_2 + 2x_1x_3 + 4x_2x_3$.

8.3. Перечень вопросов и заданий для промежуточной аттестации по дисциплине

Вопросы для промежуточного контроля (экзамена)

Первый семестр

1. Сложение матриц. Умножение матрицы на число.
2. Умножение матриц. Свойства.
3. Перестановки из n элементов.
4. Подстановки n элементов.
5. Четность подстановки.
6. Понятие определителя порядка n. Определители второго и третьего порядка.
7. Свойства определителей.
8. Теорема о разложении определителя по элементам строки.
9. Формулы Крамера решения систем линейных уравнений.
10. Теорема об определителе произведения матриц.
11. Обратная матрица. Критерий обратимости матрицы.
12. Матричные уравнения.
13. Метод Гаусса решения систем линейных уравнений.
14. Построение поля комплексных чисел.
15. Комплексные числа и действия с ними.
16. Комплексно сопряженные числа.
17. Тригонометрическая форма комплексного числа. Умножение и деление комплексных чисел в тригонометрической форме.
18. Возведение в степень и извлечение корня в области комплексных чисел.
19. Корни степени n из единицы. Первообразные корни.
20. Многочлены от одной переменной и действия с ними.
21. Теорема деления многочленов с остатком.
22. Делимость многочленов.
23. Наибольший общий делитель многочленов. Алгоритм Эвклида.
24. Взаимно простые многочлены. Их свойства.
25. Теорема Безу. Схема Горнера.
26. Корни многочленов. Кратные корни.
27. Основная теорема алгебры многочленов и следствия из нее.
28. Формулы Виета.
29. Многочлены с действительными коэффициентами.
30. Приводимость многочленов над полем.
31. Корни многочленов с рациональными коэффициентами.
32. Рациональные дроби. Понятие простейшей дроби.
33. Теоремы о разложении рациональной дроби в сумму простейших дробей.

Второй семестр

Вопросы для промежуточного контроля (зачета)

1. Внутренние и внешние операции на множестве. Понятие алгебраической структуры.
2. Понятия полугруппы и группы. Примеры. Свойства элементов группы.
3. Группа подстановок.
4. Группа невырожденных матриц.
5. Циклические группы.
6. Подгруппы. Признаки подгрупп.
7. Группы ортогональных и унимодулярных матриц.
8. Кольца, тела, поля. Основные свойства элементов кольца. Примеры.
9. Кольцо матриц.
10. Кольцо классов вычетов.
11. Подкольца. Идеалы. Подполя.
12. Отношение эквивалентности на множестве. Фактор множество.
13. Разложение группы на смежные классы по подгруппе.
14. Нормальный делитель группы.
15. Конечные группы. Теорема Лагранжа.
16. Фактор-группа.
17. Гомоморфизм и изоморфизм групп. Ядро гомоморфизма.
18. Изоморфизм циклических групп.
19. Основная теорема о гомоморфизмах групп.
20. Гомоморфизм и изоморфизм колец и полей. Ядро гомоморфизма.
21. Факторкольцо.
22. Теорема о расширении колец и полей.
23. Простое алгебраическое расширение поля. Алгебраически замкнутые поля.

Вопросы для промежуточного контроля (экзамена)

1. Понятие векторного пространства. Простейшие свойства. Примеры.
2. Линейная зависимость векторов.
3. Базис векторного пространства. Координаты вектора.
4. Теоремы о базисах. Размерность векторного пространства.
5. Формулы преобразования базиса. Формулы преобразования координат.
6. Подпространства векторного пространства. Признак подпространства. Примеры.
7. Сумма и пересечение подпространств. Прямая сумма подпространств.
8. Теорема о размерности суммы подпространств.
9. Линейная оболочка векторов. Ранг системы векторов.
10. Ранг матрицы. Основная теорема о ранге матрицы.
11. Теоремы о ранге матрицы.
12. Критерий совместности системы линейных уравнений.
13. Подпространство решений системы линейных однородных уравнений.
14. Теорема о фундаментальных решениях системы линейных однородных уравнений.
15. Понятие линейного оператора. Простейшие свойства операторов. Примеры.
16. Матрица линейного оператора. Примеры.
17. Операции над линейными операторами. Свойства.
18. Образ и ядро линейного оператора. Свойства. Примеры.
19. Теоремы о ранге и дефекте линейного оператора.
20. Собственные векторы и собственные значения линейного оператора. Примеры.
21. Характеристический многочлен и характеристические корни линейного оператора.
22. Теорема о характеристических корнях и собственных значениях линейного оператора.

23. Подпространства, инвариантные относительно оператора.
24. Разложение векторного пространства в прямую сумму инвариантных подпространств.
25. Понятие евклидова пространства. Скалярное произведение векторов.
26. Процесс ортогонализации векторов.
27. Ортонормированные базисы.
28. Ортогональные матрицы.
29. Ортогональное дополнение подпространства.
30. Симметрические операторы. Примеры. Свойства.
31. Критерий симметричности оператора.
32. Ортогональные операторы. Примеры. Свойства.
33. Понятие квадратичной формы. Ранг квадратичной формы.
34. Канонический вид квадратичной формы.
35. Приведение квадратичной формы к каноническому виду с помощью элементарных преобразований.
36. Приведение квадратичной формы к каноническому виду ортогональным преобразованием переменных.
37. Нормальный вид квадратичной формы.
38. Закон инерции квадратичных форм с действительными коэффициентами.
39. Положительно определенные квадратичные функции и формы.
40. Критерий Сильвестра положительной определенности квадратичной формы.
41. Распадающиеся квадратичные формы.

8.4. Планируемые уровни сформированности компетенций обучающихся и критерии оценивания

Уровни	Содержательное описание уровня	Основные признаки выделения уровня (этапы формирования компетенции, критерии оценки сформированности)	Пятибалльная шкала (академическая) оценка	Двухбалльная шакала, зачет	БРС, % освоения (рейтинговая оценка)
Повышенный	Творческая деятельность	*Включает нижестоящий уровень.* Умение самостоятельно принимать решение, решать проблему/задачу теоретического и прикладного характера на основе изученных методов, приемов, технологий	отлично	зачтено	86-100
Базовый	Применение знаний и умений в более широких контекстах учебной и профессионал	*Включает нижестоящий уровень.* Способность собирать, систематизировать, анализировать и грамотно использовать информацию из самостоятельно	хорошо		71-85

	ьной деятельности, нежели по образцу с большей степени самостоятельности и инициативы	найденных теоретических источников и иллюстрировать ими теоретические положения или обосновывать практику применения			
Удовлетворительный (достаточный)	Репродуктивная деятельность	Изложение в пределах задач курса теоретически и практически контролируемого материала	удовлетворительно		55-70
Недостаточный	Отсутствие признаков удовлетворительного уровня		неудовлетворительно	не зачтено	Менее 55

9. Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины.

Основная литература

1. Скрыдлова, Е. В. Линейная алгебра: учеб. пособие/ Е. В. Скрыдлова, О. О. Белова. - Калининград: РГУ им. И. Канта, 2010. - 149, [1] с. - Библиогр.: с. 146-147 (15 назв.). - ISBN 978-5-9971-0062-9: 44.68, 45.00, р. Имеются экземпляры в отделах /There are copies in departments: всего /all 145: УБ(141), ИБО(2), ч.з.N3(2)
2. Скрыдлова Е. В. Алгебра [Текст] : учеб. пособие / Е. В. Скрыдлова, О. О. Белова, 2013. - 238 с.

Дополнительная литература

1. Курош, А. Г. Курс высшей алгебры: учебник для студ. вузов, обуч. по спец. "Математика", "Прикладная математика"/ А. Г. Курош. - 13-е изд., стер.. - СПб.; М.; Краснодар: Лань, 2004. - 431 с. - Библиогр.: с. 425-426. - ISBN 5-8114-0521-9: 150.04 р. Имеются экземпляры в отделах /There are copies in departments: всего /all 45: УБ(43), НА(2)
2. Проскуряков, И. В. Сборник задач по линейной алгебре: учеб. пособие/ И. В. Проскуряков. - 12-е изд., стер.Изд. 13-е, стер.. - СПб.; М.; Краснодар: Лань, 2008; СПб.; М.; Краснодар: Лань, 2010. - 475 с. - (Классические задачники и практикумы). - (Знание. Уверенность. Успех!). - ISBN 978-5-8114-0707-1: 334.00, р. Имеются экземпляры в отделах /There are copies in departments: всего /all 101: УБ(99), ч.з.N3(2)

10. Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины (модуля).

- НЭБ Национальная электронная библиотека, диссертации и прочие издания
- eLIBRARY.RU Научная электронная библиотека, книги, статьи, тезисы докладов конференций
- Гребенников Электронная библиотека ИД журналы
- ЭБС Лань книги, журналы

- ЭБС Консультант студента
- ПРОСПЕКТ ЭБС
- ЭБС ZNANIUM.COM
- РГБ Информационное обслуживание по МБА
- БЕН РАН
- Электронно-библиотечная система (ЭБС) Кантитана (https://elib.kantiana.ru/)

11. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине.

Программное обеспечение обучения включает в себя:

- система электронного образовательного контента БФУ им. И. Канта – www.lms-3.kantiana.ru, обеспечивающую разработку и комплексное использование электронных образовательных ресурсов;
- серверное программное обеспечение, необходимое для функционирования сервера и связи с системой электронного обучения через Интернет;
- корпоративная платформа Microsoft Teams;
- установленное на рабочих местах обучающихся ПО: Microsoft Windows 7, Microsoft Office Standart 2010, антивирусное программное обеспечение Kaspersky Endpoint Security.
- специализированное ПО не требуется.

12. Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине.

Для проведения занятий лекционного типа, практических и семинарских занятий используются специальные помещения (учебные аудитории), оборудованные техническими средствами обучения – мультимедийной проекционной техникой. Для проведения занятий лекционного типа используются наборы демонстрационного оборудования.

Для проведения лабораторных работ, (практических занятий – при необходимости) используются специальные помещения (учебные аудитории), оснащенные специализированным лабораторным оборудованием: персональными компьютерами с возможностью выхода в интернет и с установленным программным обеспечением, заявленным в п.11.

Для проведения групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации используются специальные помещения (учебные аудитории), оборудованные специализированной мебелью (для обучающихся), меловой / маркерной доской.

Для организации самостоятельной работы обучающимся предоставляются помещения, оснащенные компьютерной техникой с возможностью подключения к сети «Интернет» и обеспечением доступа в электронную информационно-образовательную среду университета.

Для обучения инвалидов и лиц с ограниченными возможностями здоровья университетом могут быть представлены специализированные средства обучения, в том числе технические средства коллективного и индивидуального пользования.

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
федеральное государственное автономное образовательное учреждение высшего образования «Балтийский федеральный университет имени Иммануила Канта»
Институт физико-математических наук и информационных технологий

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

«Геометрия»

Шифр: 10.05.01
Специальность: «Компьютерная безопасность»
Специализация: «Математические методы защиты информации»
Квалификация (степень) выпускника: специалист по защите информации

Калининград
2022

Лист согласования

Составитель: Полякова Катерина Валентиновна, к.ф.-м.н., доцент

Рабочая программа утверждена на заседании учебно-методического совета института физико-математических наук и информационных технологий

Протокол № 01/22 от «01» февраля 2022 г.

Председатель учебно-методического
совета института физико-
математических наук и информационных
технологий

Первый заместитель директора Шпилевой А. А
ИФМНиИТ, к. ф.-м. н., доцент

Ведущий менеджер Е.П.Ставицкая

Содержание

1.Наименование дисциплины: «Геометрия».

Цель дисциплины: целью освоения дисциплины «Геометрия» является фундаментальная подготовка обучающихся в области геометрии, обучение студентов векторно-координатному методу аналитической геометрии и теории линий и поверхностей 1-го и 2-го порядков, расширение и углубление специализированной алгебраической подготовки студентов, обеспечивающей возможность овладения самыми современными математическими методами исследования в области защиты информации и смежных областях; изучение геометрической интерпретации алгебраических структур и овладение методикой перевода геометрических свойств в алгебраические и обратно; расширение математического кругозора и математической эрудиции; усиление методологической подготовки студентов в направлении работы над междисциплинарными и инновационными проектами.

2.Перечень планируемых результатов обучения по дисциплине, соотнесенных с планируемыми результатами освоения образовательной программы

Код компетенции	Результаты освоения образовательной программы (ИДК)	Результаты обучения по дисциплине
ОПК-3. Способен на основании совокупности математических методов разрабатывать, обосновывать и реализовывать процедуры решения задач профессиональной деятельности	ОПК-3.1. Знает необходимые математические методы для решения задач обеспечения защиты информации. ОПК-3.2. Применяет совокупность необходимых математических методов для решения задач обеспечения защиты информации. ОПК-3.3. Разрабатывает, обосновывает и реализует на практике процедуры решения задач обеспечения защиты информации.	- **знать** основные понятия геометрии и основные типы задач, возникающие в геометрии; - **уметь** понять поставленную задачу и использовать аппарат геометрии в процессе ее решения; на основе анализа увидеть и корректно сформулировать результат; использовать полученные знания в профессиональной деятельности; - **владеть** практическими навыками применения стандартных алгоритмов решения типовых геометрических задач.

3. Место дисциплины в структуре образовательной программы

Дисциплина «Геометрия» представляет собой дисциплину обязательной части блока дисциплин подготовки обучающихся.

4. Виды учебной работы по дисциплине.

Виды учебной работы по дисциплине зафиксированы учебным планом основной профессиональной образовательной программы по указанному направлению и профилю, выражаются в академических часах. Часы контактной работы и самостоятельной работы обчающегося и часы, отводимые на процедуры контроля, могут различаться в учебных планах ОПОП по формам обучения. Объем контактной работы включает часы контактной аудиторной работы (лекции/практические занятия/ лабораторные работы), контактной

внеаудиторной работы (контроль самостоятельной работы), часы контактной работы в период аттестации. Контактная работа, в том числе может проводиться посредством электронной информационно-образовательной среды университета с использованием ресурсов сети Интернет и дистанционных технологий

5. Содержание дисциплины, структурированное по темам (разделам)

Исходя из рамок, установленных учебным планом по трудоемкости и видам учебной работы по дисциплине, преподаватель самостоятельно выбирает тематику занятий по формам и количеству часов проведения контактной работы: лекции и иные учебные занятия, предусматривающие преимущественную передачу учебной информации преподавателем и (или) занятия семинарского типа (семинары, практические занятия, практикумы, лабораторные работы, коллоквиумы и иные аналогичные занятия), и (или) групповые консультации, и (или) индивидуальную работу обучающихся с преподавателем, в том числе индивидуальные консультации (по курсовым работам/проектам – при наличии курсовой работы/проекта по данной дисциплине в учебном плане). Рекомендуемая тематика занятий максимально полно реализуется в контактной работе собучающимися очной формы обучения. В случае реализации образовательной программы в заочной / очно-заочной форме трудоемкость дисциплины сохраняется, однако объем учебного материала в значительной части осваивается обучающимися в форме самостоятельной работы. При этом требования к ожидаемым образовательным результатам обучающихся по данной дисциплине не зависят от формы реализации образовательной программы.

№	Наименование раздела	Содержание раздела
1	1. Векторы и операции над ними.	1. Линейные операции над векторами. 2. Признаки коллинеарности и компланарности векторов. 3. Линейная зависимость векторов. 4. Аффинная и прямоугольная декартовы системы координат. 5. Проекция вектора на ось. 6. Скалярное произведение векторов. 7. Векторное произведение векторов. 8. Смешанное произведение векторов..
2	2. Линии 1-го и 2-го порядка на плоскости.	9. Формулы преобразования системы координат. 10. Алгебраические линии. Окружность. 11. Полярная система координат. 12. Прямая на плоскости. 13. Эллипс. 14. Гипербола. 15. Парабола.
3	3. Плоскость и прямая в пространстве.	16. Способы задания плоскости в пространстве. 17. Способы задания прямой в пространстве. 18. Формулы для вычисления расстояний в пространстве. 19. Формулы для вычисления углов. 20. Взаимное расположение прямых и плоскостей

		в пространстве.
4	4. Изучение поверхностей 2-го порядка по их каноническим уравнениям.	21. Поверхности 2-го порядка. (уравнения и рисунки) 22. Поверхности вращения. 23. Цилиндрические поверхности. 24. Конические поверхности второго порядка. Конические сечения. 25. Эллипсоид. 26. Гиперболоиды. 27. Параболоиды. 28. Прямолинейные образующие поверхностей второго порядка. 29. Задачи по теме «Поверхности 2-го порядка».

6. Рекомендуемая тематика учебных занятий в форме контактной работы

Рекомендуемая тематика учебных занятий *лекционного* типа (предусматривающих преимущественную передачу учебной информации преподавателями):

№	Наименование раздела	Темы лекций
1	1. Векторы и операции над ними.	1. Линейные операции над векторами. Признаки коллинеарности и компланарности векторов. 2. Линейная зависимость векторов. Аффинная и прямоугольная декартовы системы координат. 3. Проекция вектора на ось. Скалярное произведение векторов. 4. Векторное произведение векторов. Смешанное произведение векторов..
2	2. Линии 1-го и 2-го порядка на плоскости.	5. Формулы преобразования системы координат. 6. Алгебраические линии. Окружность. Полярная система координат. 7. Прямая на плоскости. 8. Эллипс. Гипербола. Парабола.
3	3. Плоскость и прямая в пространстве.	9. Способы задания плоскости в пространстве. 10. Способы задания прямой в пространстве. 11. Формулы для вычисления расстояний в пространстве. Формулы для вычисления углов. 12. Взаимное расположение прямых и плоскостей в пространстве.
4	4. Изучение поверхностей 2-го порядка по их каноническим	13. Поверхности 2-го порядка. (уравнения и рисунки). Поверхности вращения. Цилиндрические поверхности.

	уравнениям.	14. Конические поверхности второго порядка. Конические сечения. Эллипсоид. Гиперболоиды. Параболоиды. 15. Прямолинейные образующие поверхностей второго порядка. Задачи по теме «Поверхности 2-го порядка».

Рекомендуемая тематика *практических* занятий:

1. Линейные операции над векторами. Признаки коллинеарности и компланарности векторов. Аффинная и прямоугольная декартовы системы координат.
2. Проекция вектора на ось. Скалярное произведение векторов.
3. Векторное произведение векторов.
4. Смешанное произведение векторов. Формулы преобразования системы координат.
5. Алгебраические линии. Окружность. Полярная система координат.
6. Прямая на плоскости.
7. Эллипс.
8. Гипербола.
9. Способы задания плоскости в пространстве.
10. Способы задания прямой в пространстве.
11. Формулы для вычисления расстояний в пространстве. Формулы для вычисления углов.
12. Взаимное расположение прямых и плоскостей в пространстве.
13. Способ Лагранжа приведения уравнения поверхности 2-го порядка к каноническому виду.
14. Поверхности вращения. Цилиндрические поверхности. Конические поверхности второго порядка. Конические сечения.
15. Прямолинейные образующие поверхностей второго порядка. Задачи по теме «Поверхности 2-го порядка».

На практических занятиях решаются задачи по теме занятия.

Требования к самостоятельной работе обучающихся

1. Работа с лекционным материалом, предусматривающая проработку конспекта лекций и учебной литературы, по всем темам из п. 6 настоящей рабочей программы.
2. Выполнение домашнего задания, предусматривающего решение задач, выполнение упражнений, выдаваемых на практических занятиях, по всем темам из п. 6 настоящей рабочей программы.

Руководствуясь положениями статьи 47 и статьи 48 Федерального закона от 29 декабря 2012 г. N 273-ФЗ «Об образовании в Российской Федерации» научно-педагогические работники и иные лица, привлекаемые университетом к реализации данной образовательной программы, пользуются предоставленными академическими правами и свободами в части свободы преподавания, свободы от вмешательства в профессиональную деятельность; свободы выбора и использования педагогически обоснованных форм, средств, методов обучения и воспитания; права на творческую инициативу, разработку и применение авторских программ и методов обучения и воспитания в пределах реализуемой образовательной программы и отдельной дисциплины.

Исходя из рамок, установленных учебным планом по трудоемкости и видам учебной работы по дисциплине, преподаватель самостоятельно выбирает тематику занятий по формам и количеству часов проведения контактной работы: лекции и иные учебные

занятия, предусматривающие преимущественную передачу учебной информации преподавателем и (или) занятия семинарского типа (семинары, практические занятия, практикумы, лабораторные работы, коллоквиумы и иные аналогичные занятия), и (или) групповые консультации, и (или) индивидуальную работу обучающихся с преподавателем, в том числе индивидуальные консультации (по курсовым работам/проектам – при наличии курсовой работы/проекта по данной дисциплине в учебном плане).

Рекомендуемая тематика занятий максимально полно реализуется в контактной работе собучающимися очной формы обучения. В случае реализации образовательной программы в заочной / очно-заочной форме трудоемкость дисциплины сохраняется, однако объем учебного материала в значительной части осваивается обучающимися в форме самостоятельной работы. При этом требования к ожидаемым образовательным результатам обучающихся по данной дисциплине не зависят от формы реализации образовательной программы.

7. Методические рекомендации по видам занятий

Лекционные занятия.

В ходе лекционных занятий обучающимся рекомендуется выполнять следующие действия. Вести конспектирование учебного материала. Обращать внимание на категории, формулировки, раскрывающие содержание тех или иных явлений и процессов, научные выводы и практические рекомендации по их применению. Задавать преподавателю уточняющие вопросы с целью уяснения теоретических положений, разрешения спорных ситуаций.

Желательно оставить в рабочих конспектах поля, на которых во внеаудиторное время можно сделать пометки из рекомендованной литературы, дополняющие материал прослушанной лекции, а также подчеркивающие особую важность тех или иных теоретических положений.

Практические и семинарские занятия.

На практических и семинарских занятиях в зависимости от темы занятия выполняется поиск информации по решению проблем, практические упражнения, контрольные работы, выработка индивидуальных или групповых решений, итоговое обсуждение с обменом знаниями, участие в круглых столах, разбор конкретных ситуаций, командная работа, представление портфолио и т.п.

Самостоятельная работа.

Самостоятельная работа осуществляется в виде изучения литературы, эмпирических данных по публикациям и конкретных ситуаций из практики, подготовке индивидуальных работ, работа с лекционным материалом, самостоятельное изучение отдельных тем дисциплины; поиск и обзор литературы и электронных источников; чтение и изучение учебника и учебных пособий.

8.Фонд оценочных средств

8.1. Перечень компетенций с указанием этапов их формирования в процессе освоения образовательной программы в рамках учебной дисциплины

Основными этапами формирования указанных компетенций при изучении обучающимися дисциплины являются последовательное изучение содержательно связанных между собой тем учебных занятий. Изучение каждой темы предполагает овладение обучающимися необходимыми компетенциями. Результат аттестации обучающихся на различных этапах формирования компетенций показывает уровень освоения компетенций.

Контролируемые разделы (темы) дисциплины	Индекс контроли-руемой компетенции (или её части)	Оценочные средства по этапам формирования компетенций
		текущий контроль по дисциплине
1. Векторы и операции над ними.	ОПК-3	Решение задач.
2. Линии 1-го и 2-го порядка на плоскости.	ОПК-3	Решение задач,
3. Плоскость и прямая в пространстве.	ОПК-3	Решение задач, контрольная работа
4. Изучение поверхностей 2-го порядка по их каноническим уравнениям.	ОПК-3	Опрос, решение задач

8.2. Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений и навыков и (или) опыта деятельности процессе текущего контроля

Примеры вопросов для устного опроса:

По Теме 4.

1. Что называется обыкновенным дифференциальным уравнением?
2. Что такое порядок дифференциального уравнения?
3. Что называется решением дифференциального уравнения?
4. Что такое интеграл дифференциального уравнения?
5. Как формулируется теорема о существовании и единственности дифференциального уравнения?
6. Что называется общим решением дифференциального уравнения первого порядка?
7. Что такое общий интеграл дифференциального уравнения первого порядка?
8. Как задаются начальные условия, для чего они нужны?
9. Что такое изоклины?
10. Что представляет собой особое решение дифференциального уравнения?
11. В каких случаях уравнения 2-го порядка приводятся к уравнениям 1-го порядка?
12. Какое уравнение n-го порядка называется линейным?
13. Каковы свойства решений линейного однородного уравнения?
14. Как выражается определитель Вронского?
15. Какой вид имеют решения линейного однородного уравнения 2-го порядка с постоянными коэффициентами?
16. Как формулируется теорема об общем решении неоднородного уравнения?

Типовые контрольные задания:

Тема 3

1. Найти угол между прямой $\begin{cases} x+4y-2z+7=0 \\ 3x+7y-2z=0 \end{cases}$ и плоскостью $3x+y-z+1=0$.
2. Найти точку, симметричную точке M(-2, -3, 0) относительно плоскости x+ 5y + 4 = 0.

3. Записать уравнение прямой перпендикулярной плоскости 2x – y -- 4z – 2 = 0 и проходящей через точку A(1, -1, -1).
4. Найти проекцию точки $A(4,1,-2)$ на прямую, проходящую через точки B(2, 0, 0), C(-2, 3, -5).
5. Найти уравнение плоскости параллельной плоскости x -- 2y + 2z – 4 = 0 и отстоящей от нее на расстояние d = 3.
6. Записать канонические уравнение прямой 2x - 3y + z + 6 = 0, x - 3y -2z + 3 = 0.

8.3. Перечень вопросов и заданий для промежуточной аттестации по дисциплине

Вопросы для промежуточного контроля (экзамена)

1. Линейные операции над векторами.
2. Признаки коллинеарности и компланарности векторов.
3. Линейная зависимость векторов.
4. Аффинная и прямоугольная декартовы системы координат.
5. Проекция вектора на ось.
6. Скалярное произведение векторов.
7. Векторное произведение векторов.
8. Смешанное произведение векторов.
9. Формулы преобразования системы координат.
10. Алгебраические линии. Окружность.
11. Полярная система координат.
12. Прямая на плоскости.
13. Эллипс.
14. Гипербола.
15. Парабола.
16. Способы задания плоскости в пространстве.
17. Способы задания прямой в пространстве.
18. Формулы для вычисления расстояний в пространстве.
19. Формулы для вычисления углов.
20. Взаимное расположение прямых и плоскостей в пространстве.
21. Поверхности 2-го порядка.
22. Поверхности вращения.
23. Цилиндрические поверхности.
24. Конические поверхности второго порядка. Конические сечения.
25. Эллипсоид.
26. Гиперболоиды.
27. Параболоиды.
28. Прямолинейные образующие поверхностей второго порядка.

8.4. Планируемые уровни сформированности компетенций обучающихся и критерии оценивания

Уровни	Содержательное описание уровня	Основные признаки выделения уровня (этапы формирования компетенции, критерии оценки сформированности)	Пятибалльная шкала (академическая) оценка	Двубалльная шакала, зачет	БРС, % освоения (рейтинговая оценка)
Повышенный	Творческая деятельность	*Включает нижестоящий уровень.* Умение самостоятельно	отлично	зачтено	86-100

		принимать решение, решать проблему/задачу теоретического и прикладного характера на основе изученных методов, приемов, технологий			
Базовый	Применение знаний и умений в более широких контекстах учебной и профессиональной деятельности, нежели по образцу с большей степени самостоятельности и инициативы	*Включает нижестоящий уровень.* Способность собирать, систематизировать, анализировать и грамотно использовать информацию из самостоятельно найденных теоретических источников и иллюстрировать ими теоретические положения или обосновывать практику применения	хорошо		71-85
Удовлетворительный (достаточный)	Репродуктивная деятельность	Изложение в пределах задач курса теоретически и практически контролируемого материала	удовлетворительно		55-70
Недостаточный	Отсутствие признаков удовлетворительного уровня		неудовлетворительно	не зачтено	Менее 55

9. Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины.

Основная литература

1. Попов, Ю.И. Лекции по аналитической геометрии: лекции : учеб. пособие для студентов по направлениям бакалавриата «Прикладная математика и информатика», «Математическое обеспечение и администрирование информационных систем», «Бизнес-информатика» и специальности «Компьютерная безопасность»./ Ю. И. Попов; Балт. федер. ун-т им. И. Канта. - Б.м., 2016 on-line, 250 с.. - Бессрочная лицензия. - Б.ц. Имеются экземпляры в отделах: ЭБСКантиана(1)
2. Попов, Ю.И. Практикум по аналитической геометрии: лекции : учеб. пособие для студентов специальности "Компьютер. безопасность" и бакалавриата «Прикладная математика и информатика», "Мат. обеспечение и администрирование информ. систем"/ Ю. И. Попов ; Балт. федер. ун-т им. И. Канта. - Калининград: БФУ им. И.

Канта, 2012. - 1 on-line. - Бессрочная лицензия. - Б.ц. Имеются экземпляры в отделах: ЭБСКантиана(1)

Дополнительная литература

1. Попов, Ю. И. Приложение аналитической геометрии [Электронный ресурс]: учеб. пособие/ Ю. И. Попов; Балт. федер. ун-т им. И. Канта. - Калининград: БФУ им. И. Канта, 2015. - 1 on-line, 207 с.. - Библиогр. в конце гл.. - Бессрочная лицензия. - Б.ц. Имеются экземпляры в отделах /There are copies in departments: ЭБС Кантиана(1).
2. Попов, Ю. И. Практикум по решению планиметрических задач: учеб. пособие/ Ю. И. Попов; Балт. федер. ун-т им. И. Канта. - Калининград: БФУ им. И. Канта, 2015. - 1 on-line, 105 с.. - Библиогр. в конце гл.. - Бессрочная лицензия. - Б.ц. Имеются экземпляры в отделах: ЭБСКантиана(1)
3. Цубербиллер, О. Н. Задачи и упражнения по аналитической геометрии: сборник/ Цубербиллер О.Н.. - 31-е изд.,стереотип.. - СПб.; М.; Краснодар: Лань, 2003. - 336 с.: черт.. - ISBN 5-8114-0475-1: 97.00;69.85, 122.22, р.Имеются экземпляры в отделах /There are copies in departments: всего /all 84: УБ(82), НА(1), ч.з.N3(1)

10. Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины (модуля).

- НЭБ Национальная электронная библиотека, диссертации и прочие издания
- eLIBRARY.RU Научная электронная библиотека, книги, статьи, тезисы докладов конференций
- Гребенников Электронная библиотека ИД журналы
- ЭБС Лань книги, журналы
- ЭБС Консультант студента
- ПРОСПЕКТ ЭБС
- ЭБС ZNANIUM.COM
- РГБ Информационное обслуживание по МБА
- БЕН РАН
- Электронно-библиотечная система (ЭБС) Кантитана (https://elib.kantiana.ru/)

11. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине.

Программное обеспечение обучения включает в себя:

- система электронного образовательного контента БФУ им. И. Канта – www.lms-3.kantiana.ru, обеспечивающую разработку и комплексное использование электронных образовательных ресурсов;
- серверное программное обеспечение, необходимое для функционирования сервера и связи с системой электронного обучения через Интернет;
- корпоративная платформа Microsoft Teams;
- установленное на рабочих местахобучающихся ПО: Microsoft Windows 7, Microsoft Office Standart 2010, антивирусное программное обеспечение Kaspersky Endpoint Security.
- специализированное ПО не требуется.

12. Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине.

Для проведения занятий лекционного типа, практических и семинарских занятий используются специальные помещения (учебные аудитории), оборудованные техническими средствами обучения – мультимедийной проекционной техникой. Для проведения занятий лекционного типа используются наборы демонстрационного оборудования.

Для проведения лабораторных работ, (практических занятий – при необходимости) используются специальные помещения (учебные аудитории), оснащенные специализированным лабораторным оборудованием: персональными компьютерами с возможностью выхода в интернет и с установленным программным обеспечением, заявленным в п.11.

Для проведения групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации используются специальные помещения (учебные аудитории), оборудованные специализированной мебелью (для обучающихся), меловой / маркерной доской.

Для организации самостоятельной работы обучающимся предоставляются помещения, оснащенные компьютерной техникой с возможностью подключения к сети «Интернет» и обеспечением доступа в электронную информационно-образовательную среду университета.

Для обучения инвалидов и лиц с ограниченными возможностями здоровья университетом могут быть представлены специализированные средства обучения, в том числе технические средства коллективного и индивидуального пользования.

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
федеральное государственное автономное образовательное учреждение высшего образования «Балтийский федеральный университет имени Иммануила Канта»
Институт физико-математических наук и информационных технологий

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

«Информатика»

Шифр: 10.05.01
Специальность: «Компьютерная безопасность»
Специализация: «Математические методы защиты информации»
Квалификация (степень) выпускника: специалист по защите информации

Калининград
2022

Лист согласования

Составитель: Дёмин С.А., старший преподаватель

Рабочая программа утверждена на заседании учебно-методического совета института физико-математических наук и информационных технологий

Протокол № 01/22 от «01» февраля 2022 г.

Председатель учебно-методического совета института физико-математических наук и информационных технологий

Первый заместитель директора ИФМНиИТ, к. ф.-м. н., доцент — Шпилевой А. А

Ведущий менеджер — Е.П.Ставицкая

Содержание

1.Наименование дисциплины: «Информатика».

Цель дисциплины: целью освоения дисциплины «Информатика» является формирование общей информационной культуры студентов, подготовка их к изучению других дисциплин, связанных с использованием современных информационных технологий в практической деятельности и обеспечения их информационной безопасности.

2. Перечень планируемых результатов обучения по дисциплине, соотнесенных с планируемыми результатами освоения образовательной программы

Код компетенции	Результаты освоения образовательной программы (ИДК)	Результаты обучения по дисциплине
ОПК-2. Способен применять программные средства системного и прикладного назначений, в том числе отечественного производства, для решения задач профессиональной деятельности;	ОПК-2.1. Понимает современные информационные технологии и программные средства, в том числе отечественного производства, для решения задач профессиональной деятельности. ОПК-2.2. Выбирает современные информационные технологии и программные средства, в том числе отечественного производства, для решения задач профессиональной деятельности. ОПК-2.3. Обладает навыками применения современных информационных технологий и программных средств, в том числе отечественного производства, для решения задач профессиональной деятельности.	***Знать:*** • формы и способы представления данных в компьютере; • логико-математические основы построение электронных цифровых устройств; • состав, назначение функциональных компонентов и программного обеспечения персонального компьютера; ***Уметь:*** • применять типовые программные средства сервисного назначения; • пользоваться сетевыми средствами обмена данными, в том числе с использованием глобальной информационной сети интернет; • пользоваться возможностями интерфейса командной строки современных операционных систем; ***Владеть*:** • навыками работы с офисными приложениями. • навыками алгоритмизации и структурного программирования на языке высокого уровня.

3. Место дисциплины в структуре образовательной программы

Дисциплин «Информатика» входит в базовую часть (Б1.О.06.01) обязательной части блока дисциплин (модулей) подготовки специалистов по специальности 10.05.01«Компьютерная безопасность», специализация N 2 "Математические методы защиты информации"

4. Виды учебной работы по дисциплине.

Виды учебной работы по дисциплине зафиксированы учебным планом основной профессиональной образовательной программы по указанному направлению и профилю, выражаются в академических часах. Часы контактной работы и самостоятельной работы обчающегося и часы, отводимые на процедуры контроля, могут различаться в учебных планах ОПОП по формам обучения. Объем контактной работы включает часы контактной аудиторной работы (лекции/практические занятия/ лабораторные работы), контактной внеаудиторной работы (контроль самостоятельной работы), часы контактной работы в период аттестации. Контактная работа, в том числе может проводиться посредством электронной информационно-образовательной среды университета с использованием ресурсов сети Интернет и дистанционных технологий

5. Содержание дисциплины, структурированное по темам (разделам)

Исходя из рамок, установленных учебным планом по трудоемкости и видам учебной работы по дисциплине, преподаватель самостоятельно выбирает тематику занятий по формам и количеству часов проведения контактной работы: лекции и иные учебные занятия, предусматривающие преимущественную передачу учебной информации преподавателем и (или) занятия семинарского типа (семинары, практические занятия, практикумы, лабораторные работы, коллоквиумы и иные аналогичные занятия), и (или) групповые консультации, и (или) индивидуальную работу обучающихся с преподавателем, в том числе индивидуальные консультации (по курсовым работам/проектам – при наличии курсовой работы/проекта по данной дисциплине в учебном плане). Рекомендуемая тематика занятий максимально полно реализуется в контактной работе с обучающимися очной формы обучения. В случае реализации образовательной программы в заочной / очно-заочной форме трудоемкость дисциплины сохраняется, однако объем учебного материала в значительной части осваивается обучающимися в форме самостоятельной работы. При этом требования к ожидаемым образовательным результатам обучающихся по данной дисциплине не зависят от формы реализации образовательной программы.

№ п/п	**Наименование темы**	**Содержание темы**
Раздел 1 «Алгоритмизация и программирования».		
1	Введение.	История развития языков высокого уровня. Общая схема решения задачи на компьютере. Алгоритм. Свойства алгоритма. Текст программы. Компиляция, отладка и тестирование. Структура С++-программы. Средства разработки программ. Комментарии.
2	Начальные сведения о языке программировани я.	Идентификаторы. Типы данных. Константы. Оператор присваивания. Метки и безусловный переход. Консольный ввод и вывод. Форматированный вывод числовых данных в языке С и С++.
3	Типы данных.	Арифметические типы данных: целый и вещественный тип. Арифметические операции. Стандартные арифметические функции. Арифметические выражения. Логический тип данных и операции над переменными данного типа. Эквивалентность и

		совместимость типов данных. Математическая библиотека. Унарные операции.
4	Операторы ветвления и выбора. Циклы.	Операторы ветвления if и case. Цикл с параметром. Цикл с предусловием. Цикл с постусловием. Вложенные циклы.
5	Массивы.	Одномерные массивы. Указатели и их связь с массивами. Косвенная адресация в массивах. Динамическое выделение памяти в языке С. Динамическое выделение памяти в языке С++. Двумерные динамические массивы. Массивы указателей.
6	Символьный и строковый тип данных.	Символьный и строковый тип данных в языке С. Символьный и строковый тип данных в языке С++. Примеры. Библиотека string. Ввод и вывод символов и строк.
7	Подпрограммы.	Назначение и виды функций. Типы функций. Обращение к функции. Формальные и фактические параметры функции. Описание и объявление функции. Прототип функции. Передача параметров. Изменяемые значения параметров. Перегруженные функции.
8	Файлы.	Типы файлов. Объявление файловой переменной в языке С. Открытие и закрытие файлов. Чтение и запись для текстовых файлов. Потоки ввода вывода в языке С++. Подпрограммы работы с файлами.
9	Алгоритмы сортировки и поиска данных.	Алгоритм сортировка пузырьком. Алгоритм сортировки вставками. Алгоритм сортировки слиянием. Алгоритм быстрой сортировки. Алгоритм линейного поиска. Алгоритм двоичного поиска
10	Структуры.	Определение и описание структуры. Доступ к элементам структур. Операции над структурами.
11	Рекурсия.	Понятие рекурсии. Формы рекурсивных процедур. Задача о ханойских башнях. Быстрая сортировка. Понятие динамического программирования.
12	Динамические структуры данных	Динамическое распределение памяти. Структура односвязного линейного списка и двухсвязного циклического списка с фиктивным элементом. Работа со списками. Стек.
13	Компьютерный практикум	Решение прикладных задач. Разработка алгоритма решения задачи. Написание программы. Отладка программ.
Раздел 2 «Основы теории информации».		
14	Основные понятия теории информации.	Подходы к определению «информации» и «информатики». Виды и свойства информации. Информационные процессы, технологии, ресурсы. Информатизация общества.

15	Кодирование и измерение информации.	Подходы к измерению информации. Формулы Хартли и Шеннона. Понятие кодирование информации. Колы Хаффмана и Шеннона - Фано.
Раздел 3 «Представление информации в компьютере».		
16	Арифметические основы компьютера.	Позиционные системы счисления, алгоритмы перевода из одной системы счисления в другую. Представление в памяти компьютера числовой информации.
17	Представление текстовой и графической информации.	Таблицы кодировок. Дискретизация и квантование. Векторное и растровое представление информации. Цветовые модели.
18	Представление звуковой информации.	Звукозапись. Виды модуляции. Принципы компьютерного воспроизведения звука. Формат MIDI. Методы сжатия цифровой информации: обратимые методы, методы с регулируемой потерей информации.
Раздел 4 «Элементы теории алгоритмов».		
19	Уточнение понятия алгоритма.	Понятие алгоритмов. Свойства алгоритмов. Машина Тьюринга.
20	Машина Поста как уточнение понятия алгоритма.	Машина Поста. Алгоритмически неразрешимые задачи.
21	Понятие сложности алгоритма.	Сложность алгоритма. Анализ сложности алгоритмов поиска и сортировки.
Раздел 5 «Основы построения компьютера».		
22	Логические основы компьютера и элементы схемотехники.	Основы алгебры логики. Логические функции. Логические элементы электронных схем. Основные логические устройства компьютера.
23	Архитектура организации ЭВМ.	Обобщенная схема персонального компьютера. Состав и назначение функциональных узлов компьютера. Организация памяти ПК.
Раздел 6 «Программное обеспечение компьютера».		
24	Программное обеспечение информационных систем.	Классификация программного обеспечения. Свободное программное обеспечение. Общественная лицензия GNU. Понятие операционной системы (ОС). Структура, основные компоненты, ядро ОС. Понятие файловой системы. Организация файловых систем. Именование файлов и каталогов. Права доступа к файлам и каталогам. Физическая реализация файловой системы.

25	Командные оболочки.	Понятие командной оболочки. Обзор командных оболочек. Команды для работы с файлами и каталогами.
Раздел 7 «Компьютерные сети и проблемы безопасности компьютерных сетей».		
26	Введение в компьютерные сети.	Назначение и классификация компьютерных сетей. Сетевые архитектуры Сеть Интернет. Настройка компьютера.
27	Основные понятия информационной безопасности компьютерных систем.	Основные понятия информационной безопасности. Направления обеспечения информационной безопасности. Нормативны документы по обеспечению информационной безопасности. Основные методы защиты информации. Математические методы защиты информации.

6. Рекомендуемая тематика учебных занятий в форме контактной работы

Рекомендуемая тематика учебных занятий *лекционного* типа (предусматривающих преимущественную передачу учебной информации преподавателями):

№	Наименование раздела	Темы лекций
1	Раздел 1. «Алгоритмизация и программирование»	Лекция 1. Введение.
		Лекция 2. Начальные сведения о языке программирования.
		Лекция 3. Типы данных.
		Лекция 4. Операторы ветвления и выбора. Циклы.
		Лекции 5-6. Массивы.
		Лекция 7. Символьный и строковый тип данных.
		Лекции 8-9. Подпрограммы.
		Лекции 10-11. Файлы.
		Лекция 12. Алгоритмы сортировки и поиска данных.
		Лекция 13. Структуры.
		Лекция 14. Рекурсия.
		Лекции 15-16. Динамические структуры данных
2	Раздел 2. «Основы теории информации»	Лекции 17-18. Основные понятия теории информации.
		Лекции 19-20. Кодирование и измерение информации.
3	Раздел 3 «Представление информации в компьютере».	Лекции 21-22. Арифметические основы компьютера.
		Лекция 23. Представление текстовой и графической информации.
		Лекция 24. Представление звуковой информации.
4	Раздел 4. «Элементы теории алгоритмов»	Лекция 25. Уточнение понятия алгоритма.
		Лекция 26. Машина Поста как уточнение понятия алгоритма.
		Лекция 27. Понятие сложности алгоритма.

5	Раздел 5. «Основы построения компьютера».	Лекция 28. Логические основы компьютера и элементы схемотехники.
		Лекция 29.Архитектура организации ЭВМ.
6	Раздел 6. «Программное обеспечение компьютера».	Лекция 30. Программное обеспечение информационных систем.
		Лекция 30. Командные оболочки.
7	Раздел 7. Компьютерные сети и проблемы информационной безопасности.	Лекция 31. Введение в компьютерные сети.
		Лекция 32. Основные понятия информационной безопасности компьютерных систем.

Тематика лабораторных работ:

№ п/п	Наименование темы	Тематика лабораторных работ.
Раздел 1 «Алгоритмизация и программирования».		
1	Введение.	1. Инструментальные программные оболочки сред программирования на языках С/С++. 2-3. Разработка блок-схем алгоритмов.
2	Начальные сведения о языке программировани я.	По данной теме лабораторные работы не предусмотрены.
3	Типы данных.	4. Стандартные типы данных и операторы языка С/С++: условный оператор, составной оператор, оператор выбора
4	Операторы ветвления и выбора. Циклы.	5. Стандартные типы данных и операторы языка С/С++: циклы с предусловием, циклы с постусловием, циклы с заданным числом итераций
5	Массивы.	6-7. Работа с элементами одномерными массива. 8. Работа с элементами двумерного массива.
6	Символьный и строковый тип данных.	9-10. Распаковка текста
7	Подпрограммы.	11. Подпрограммы
8	Файлы.	12. Разработка программ обработки числовых и текстовых данных, хранящихся в файле 16. Разработка программы обработки данных бинарного файла.
9	Алгоритмы сортировки и поиска данных.	13. Алгоритмы сортировки
10	Структуры.	По данной теме лабораторные работы не предусмотрены.
11	Рекурсия.	По данной теме лабораторные работы не предусмотрены.
12	Динамические структуры данных	14-15. Односвязные и двухсвязные линейные списки
13	Компьютерный практикум	17-20. Отработка практических навыков структурного программирования. 21-26. Освоение методики тестирования и отладки программ.
Раздел 2 «Основы теории информации».		
14	Основные понятия теории информации.	27. Измерение информации.

15	Кодирование и измерение информации.	28. Кодирование информации.
Раздел 3 «Представление информации в компьютере».		
16	Арифметические основы компьютера.	29. Системы счисления. 30. Представление чисел в компьютере.
17	Представление текстовой и графической информации.	Лабораторные работы по данной теме не предусмотрены.
18	Представление звуковой информации.	Лабораторные работы по данной теме не предусмотрены.
Раздел 4 «Элементы теории алгоритмов».		
19	Уточнение понятия алгоритма.	31. Машина Тьюринга.
20	Машина Поста как уточнение понятия алгоритма.	32. Машина Поста.
21	Понятие сложности алгоритма.	Лабораторные работы по данной теме не предусмотрены.
Раздел 5 «Основы построения компьютера».		
22	Логические основы компьютера и элементы схемотехники.	33. Логические основы компьютера.
23	Архитектура организации ЭВМ.	Лабораторные работы по данной теме не предусмотрены.
Раздел 6 «Программное обеспечение компьютера».		
24	Программное обеспечение информационных систем.	34. Программное обеспечение персонального компьютера.
25	Командные оболочки.	Лабораторные работы по данной теме не предусмотрены.
Раздел 7 «Компьютерные сети и проблемы безопасности компьютерных сетей».		
26	Введение в компьютерные сети.	35. Компьютерные сети.
27	Основные понятия информационной безопасности компьютерных систем.	36. Математические алгоритмы, обеспечивающие конфиденциальность информации.

Требования к самостоятельной работе обучающихся

1. Работа с лекционным материалом, предусматривающая проработку конспекта лекций и учебной литературы, по всем темам из п. 6 настоящей рабочей программы.

2. Выполнение домашнего задания, предусматривающего решение задач, выполнение упражнений, выдаваемых на практических занятиях, по всем темам из п. 6 настоящей рабочей программы.

Руководствуясь положениями статьи 47 и статьи 48 Федерального закона от 29 декабря 2012 г. N 273-ФЗ «Об образовании в Российской Федерации» научно-педагогические работники и иные лица, привлекаемые университетом к реализации данной образовательной программы, пользуются предоставленными академическими правами и свободами в части свободы преподавания, свободы от вмешательства в профессиональную деятельность; свободы выбора и использования педагогически обоснованных форм, средств, методов обучения и воспитания; права на творческую инициативу, разработку и применение авторских программ и методов обучения и воспитания в пределах реализуемой образовательной программы и отдельной дисциплины.

Исходя из рамок, установленных учебным планом по трудоемкости и видам учебной работы по дисциплине, преподаватель самостоятельно выбирает тематику занятий по формам и количеству часов проведения контактной работы: лекции и иные учебные занятия, предусматривающие преимущественную передачу учебной информации преподавателем и (или) занятия семинарского типа (семинары, практические занятия, практикумы, лабораторные работы, коллоквиумы и иные аналогичные занятия), и (или) групповые консультации, и (или) индивидуальную работу обучающихся с преподавателем, в том числе индивидуальные консультации (по курсовым работам/проектам – при наличии курсовой работы/проекта по данной дисциплине в учебном плане).

Рекомендуемая тематика занятий максимально полно реализуется в контактной работе с обучающимися очной формы обучения. В случае реализации образовательной программы в заочной / очно-заочной форме трудоемкость дисциплины сохраняется, однако объем учебного материала в значительной части осваивается обучающимися в форме самостоятельной работы. При этом требования к ожидаемым образовательным результатам обучающихся по данной дисциплине не зависят от формы реализации образовательной программы.

№ п/п	**Наименование темы**	**Тематика самостоятельных работ.**
Раздел 1 «Алгоритмизация и программирования».		
1	Введение.	Повторение теоретического материала к лабораторным работам. Ознакомление с литературой по курсу. Подготовка к контрольной работе.
2	Начальные сведения о языке программировани я.	Повторение теоретического материала к лабораторным работам. Ознакомление с литературой по курсу. Подготовка к контрольной работе.
3	Типы данных.	Повторение теоретического материала к лабораторным работам. Ознакомление с литературой по курсу. Подготовка к контрольной работе.
4	Операторы ветвления и выбора. Циклы.	Повторение теоретического материала к лабораторным работам. Ознакомление с литературой по курсу. Подготовка к контрольной работе.

5	Массивы.	Повторение теоретического материала к лабораторным работам. Ознакомление с литературой по курсу. Подготовка к контрольной работе.
6	Символьный и строковый тип данных.	Повторение теоретического материала к лабораторным работам. Ознакомление с литературой по курсу. Подготовка к контрольной работе.
7	Подпрограммы.	Повторение теоретического материала к лабораторным работам. Ознакомление с литературой по курсу. Подготовка к контрольной работе.
8	Файлы.	Повторение теоретического материала к лабораторным работам. Ознакомление с литературой по курсу. Подготовка к контрольной работе.
9	Алгоритмы сортировки и поиска данных	Повторение теоретического материала к лабораторным работам. Ознакомление с литературой по курсу. Подготовка к контрольной работе.
10	Структуры	Повторение теоретического материала к лабораторным работам. Ознакомление с литературой по курсу. Подготовка к контрольной работе.
11	Рекурсия.	Повторение теоретического материала к лабораторным работам. Ознакомление с литературой по курсу. Подготовка к контрольной работе.
12	Динамические структуры данных	Повторение теоретического материала к лабораторным работам. Ознакомление с литературой по курсу. Подготовка к контрольной работе.
13	Компьютерный практикум	Повторение теоретического материала к лабораторным работам. Ознакомление с литературой по курсу. Подготовка к контрольной работе.
Раздел 2 «Основы теории информации».		
14	Основные понятия теории информации.	Повторение теоретического материала к лабораторным работам. Ознакомление с литературой по курсу. Подготовка к контрольной работе.
15	Кодирование и измерение информации.	Повторение теоретического материала к лабораторным работам. Ознакомление с литературой по курсу. Подготовка к контрольной работе.
Раздел 3 «Представление информации в компьютере».		
16	Арифметические основы компьютера.	Повторение теоретического материала к лабораторным работам. Ознакомление с литературой по курсу. Подготовка к контрольной работе.
17	Представление текстовой и графической информации.	Повторение теоретического материала к лабораторным работам. Ознакомление с литературой по курсу. Подготовка к контрольной работе.
18	Представление звуковой информации.	Повторение теоретического материала к лабораторным работам. Ознакомление с литературой по курсу. Подготовка к контрольной работе.
Раздел 4 «Элементы теории алгоритмов».		
19	Уточнение понятия алгоритма.	Повторение теоретического материала к лабораторным работам. Ознакомление с литературой по курсу. Подготовка к контрольной работе.
20	Машина Поста как уточнение	Повторение теоретического материала к лабораторным работам. Ознакомление с литературой по курсу. Подготовка к контрольной работе.

	понятия алгоритма.	
21	Понятие сложности алгоритма.	Повторение теоретического материала к лабораторным работам. Ознакомление с литературой по курсу. Подготовка к контрольной работе.
Раздел 5 «Основы построения компьютера».		
22	Логические основы компьютера и элементы схемотехники.	Повторение теоретического материала к лабораторным работам. Ознакомление с литературой по курсу. Подготовка к контрольной работе.
23	Архитектура организации ЭВМ.	Повторение теоретического материала к лабораторным работам. Ознакомление с литературой по курсу. Подготовка к контрольной работе.
Раздел 6 «Программное обеспечение компьютера».		
24	Программное обеспечение информационных систем.	Повторение теоретического материала к лабораторным работам. Ознакомление с литературой по курсу. Подготовка к контрольной работе.
25	Командные оболочки.	Повторение теоретического материала к лабораторным работам. Ознакомление с литературой по курсу. Подготовка к контрольной работе.
Раздел 7 «Компьютерные сети и проблемы безопасности компьютерных сетей».		
26	Введение в компьютерные сети.	Повторение теоретического материала к лабораторным работам. Ознакомление с литературой по курсу. Подготовка к контрольной работе.
27	Основные понятия информационной безопасности компьютерных систем.	Повторение теоретического материала к лабораторным работам. Ознакомление с литературой по курсу. Подготовка к контрольной работе.

7. Методические рекомендации по видам занятий

Лекционные занятия.

В ходе лекционных занятий обучающимся рекомендуется выполнять следующие действия. Вести конспектирование учебного материала. Обращать внимание на категории, формулировки, раскрывающие содержание тех или иных явлений и процессов, научные выводы и практические рекомендации по их применению. Задавать преподавателю уточняющие вопросы с целью уяснения теоретических положений, разрешения спорных ситуаций.

Желательно оставить в рабочих конспектах поля, на которых во внеаудиторное время можно сделать пометки из рекомендованной литературы, дополняющие материал прослушанной лекции, а также подчеркивающие особую важность тех или иных теоретических положений.

Практические и семинарские занятия.

На практических и семинарских занятиях в зависимости от темы занятия выполняется поиск информации по решению проблем, практические упражнения, контрольные работы, выработка индивидуальных или групповых решений, итоговое обсуждение с обменом знаниями, участие в круглых столах, разбор конкретных ситуаций, командная работа, представление портфолио и т.п.

Самостоятельная работа.

Самостоятельная работа осуществляется в виде изучения литературы, эмпирических данных по публикациям и конкретных ситуаций из практики, подготовке индивидуальных работ, работа с лекционным материалом, самостоятельное изучение отдельных тем дисциплины; поиск и обзор литературы и электронных источников; чтение и изучение учебника и учебных пособий.

8. Фонд оценочных средств

8.1. Перечень компетенций с указанием этапов их формирования в процессе освоения образовательной программы в рамках учебной дисциплины

Основными этапами формирования указанных компетенций при изучении обучающимися дисциплины являются последовательное изучение содержательно связанных между собой тем учебных занятий. Изучение каждой темы предполагает овладение обучающимися необходимыми компетенциями. Результат аттестации обучающихся на различных этапах формирования компетенций показывает уровень освоения компетенций.

Контролируемые модули, разделы (темы) дисциплины	Индекс контролируемой компетенции (или её части)	Оценочные средства по этапам формирования компетенций
		текущий контроль по дисциплине
Тема 1. Введение.	ОПК-2	Защита лабораторных работ № 2-3.
Тема 2. Начальные сведения о языке программирования.	ОПК-2	Устный опрос.
Тема 3. Типы данных.	ОПК-2	Защита лабораторной работы № 4.
Тема 4. Операторы ветвления и выбора. Циклы.	ОПК-2	Защита лабораторной работы № 5.
Тема 5. Массивы.	ОПК-2	Защита лабораторных работ № 6-8.
Тема 6. Символьный и строковый тип данных.	ОПК-2	Защита лабораторной работы № 9-10.
Тема 7. Подпрограммы.	ОПК-2	Защита лабораторной работы № 11.
Тема 8. Файлы.	ОПК-2	Защита лабораторных работ № 12,16.
Тема 9. Алгоритмы сортировки и поиска данных	ОПК-2	Защита лабораторной работы № 13.
Тема 10. Структуры.	ОПК-2	Устный опрос.
Тема 11. Рекурсия.	ОПК-2	Устный опрос.
Тема 12. Динамические структуры данных	ОПК-2	Защита лабораторных работ № 14 - 15.

Тема 13. Компьютерный практикум.	ОПК-2	Защита лабораторных работ № 17 - 26.
Тема 14. Основные понятия теории информации.	ОПК-2	Защита лабораторной работы № 27.
Тема 15. Кодирование и измерение информации.	ОПК-2	Защита лабораторной работы № 28.
Тема 16. Арифметические основы компьютера.	ОПК-2	Защита лабораторных работ № 29 - 30.
Тема 17. Представление текстовой и графической информации.	ОПК-2	Устный опрос
Тема 18. Представление звуковой информации.	ОПК-2	Устный опрос
Тема 19. Уточнение понятия алгоритма.	ОПК-2	Защита лабораторной работы № 31.
Тема 20. Машина Поста как уточнение понятия алгоритма.	ОПК-2	Защита лабораторной работы № 32.
Тема 21. Понятие сложности алгоритма.	ОПК-2	Устный опрос
Тема 22. Логические основы компьютера и элементы схемотехники.	ОПК-2	Защита лабораторной работы № 33.
Тема 23.Архитектура организации ЭВМ.	ОПК-2	Устный опрос.
Тема 24. Программное обеспечение информационных систем.	ОПК-2	Защита лабораторной работы № 34.
Тема 25. Командные оболочки.	ОПК-2	Устный опрос.
Тема 26. Введение в компьютерные сети.	ОПК-2	Защита лабораторной работы № 35.
Тема 27. Основные понятия информационной безопасности компьютерных систем.	ОПК-2	Защита лабораторной работы № 36.

8.2. Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений и навыков и (или) опыта деятельности процессе текущего контроля

Лабораторные работы. Задания:

Тема 1. «Введение».

Лабораторная работа № 1: «Инструментальные программные оболочки сред программирования для я зыка С/С++».

План:

1. Команды редактора.

2. Работа с окнами в интегрированной среде.

3. Разработка первой программы.

Лабораторная работа выполняется под руководством преподавателя для каждой среды программирования.

Лабораторная работа № 2-3: «Разработка блок-схем алгоритмов».

План:

1. Постановка задачи для выполнения лабораторной работы.

2. Самостоятельное выполнение каждым студентом своего индивидуального задания.

3. Консультирование по вопросам теоретической части задания.

4. Защита работы.

Типовой образец задания для одного варианта:

1. Начертить блок-схему алгоритма. Ввести последовательность целых чисел {Aj},j=1,...,n. Найти сумму чисел, делящихся на 3 или на 7, наименьшее из таких чисел, и номер этого числа в последовательности.

2. Начертить блок-схему алгоритма. Ввести числовую матрицу {Aij}i=1,...,n;j=1,...,m. Найти сумму произведений элементов строк.

3. Начертить блок-схему алгоритма. Ввести последовательность натуральных чисел {Aj}j=1...n. Упорядочить последовательность по неубыванию первой цифры числа, числа с одинаковыми первыми цифрами дополнительно упорядочить по неубыванию суммы цифр числа, числа с одинаковыми первыми цифрами и одинаковыми суммами цифр дополнительно упорядочить по неубыванию самого числа.

4. Начертить блок-схему алгоритма. Ввести целочисленную матрицу {Aij}i=1..n,j=1..m. Найти столбец с наименьшей суммой элементов и увеличить все элементы этого столбца на 3.

5. Начертить блок-схему алгоритма. Дано множество чисел X(i,j,k), i=I1,...,I2, j=J1,...,J2, k=K1,...K2. Вычислить величину $\min_{i=I1...I2} \max_{j=J1...J2} \left(\sum_{k=K1}^{K2} X(i,j,k) + \prod_{k=K1}^{K2} X(i,j,k) \right)$.

Использовать не менее одного цикла с предусловием и не менее одного цикла с постусловием.

Тема 3. «Типы данных».

Лабораторная работа 4: «Стандартные типы данных и операторы языка».

План:

1. Постановка задачи для выполнения лабораторной работы.

2. Самостоятельное выполнение каждым студентом своего индивидуального задания.

3. Консультирование по вопросам теоретической части задания.

4. Защита работы.

Типовой образец задания одного варианта:

1. Ввести натуральные числа A, B и C. Если A кратно B и B больше C, то вывести A/B+C, если A кратно B и B меньше C, то вывести A/B-C, в остальных случаях вывести (A+B)*C.

2. Дана последовательность натуральных чисел {Aj} (длина последовательности заранее не известна). Найти произведение чисел, заканчивающихся цифрой 2 или 4, наименьшее из таких чисел и номер этого числа в последовательности.

Тема 4. «Операторы ветвления и выбора. Циклы».

Лабораторная работа 5: «Циклы с предусловием, циклы с постусловием, циклы с заданным числом итераций; условный оператор, составной оператор, оператор выбора».
План:

1. Постановка задачи для выполнения лабораторной работы.

2. Самостоятельное выполнение каждым студентом своего индивидуального задания.

3. Консультирование по вопросам теоретической части задания.

4. Защита работы.

Типовой образец задания одного варианта:

1. Ввести натуральные числа A, B и C. Если A кратно B и B больше C, то вывести A/B+C, если A кратно B и B меньше C, то вывести A/B-C, в остальных случаях вывести (A+B)*C.

2. Дана последовательность натуральных чисел {Aj} (длина последовательности заранее не известна). Найти произведение чисел, заканчивающихся цифрой 2 или 4, наименьшее из таких чисел и номер этого числа в последовательности.

Тема 5 «Массивы».

Лабораторная работа № 6-8: «Работа с элементами одномерного и двумерного массивов».

План:

1. Постановка задачи для выполнения лабораторной работы.

2. Самостоятельное выполнение каждым студентом своего индивидуального задания.

3. Консультирование по вопросам теоретической части задания.

4. Защита работы.

Типовой образец задания:

1. Дана последовательность натуральных чисел {aj}j=1...n (n<=10000). Если в последовательности есть хотя бы одно число, начинающееся цифрой 1, упорядочить последовательность по неубыванию.

2.Ввести последовательность натуральных чисел {Aj}j=1...n (n<=1000). Упорядочить последовательность по неубыванию суммы цифр числа, числа с одинаковыми суммами цифр дополнительно упорядочить по неубыванию первой цифры числа, числа с одинаковыми суммами цифр и одинаковыми первыми цифрами дополнительно упорядочить по неубыванию самого числа.

3. Дана последовательность натуральных чисел {Aj}j=1...n (n<=10000). Удалить из последовательности числа, сумма цифр которых кратна шести. Среди оставшихся продублировать числа, начинающиеся цифрой 1.

Лабораторная работа № 9-10: «Работа с элементами двумерного массива».

План:

1. Постановка задачи для выполнения лабораторной работы.

2. Самостоятельное выполнение каждым студентом своего индивидуального задания.

3. Консультирование по вопросам теоретической части задания.

4. Защита работы.

Типовой образец задания:

1. Дана целочисленная матрица {Aij}i=1,...,n;j=1,...,m (n,m<=20). Найти сумму произведений элементов строк.

2. Дана целочисленная матрица {Aij}i=1..n,j=1..m (n,m<=100). Найти строку с наименьшей суммой элементов и заменнить все элементы этой строки этой суммой.

Тема 6 «Символьный и строковый тип данных».

Лабораторная работа № 9-10: «Распаковка текста».

План:

1. Постановка задачи для выполнения лабораторной работы.

2. Самостоятельное выполнение каждым студентом своего индивидуального задания.

3. Консультирование по вопросам теоретической части задания.

4. Защита работы.

Типовой образец задания:

1. Дана строка, содержащая русский текст. Если в тексте нет слов-палиндромов длиной более 1-й буквы, то вывести слова текста в соответствии с убыванием количества согласных, в противном случае продублировать в словах текста гласные буквы и вывести полученные слова в порядке, обратном к алфавитному.

Тема 7 «Подпрограммы».

Лабораторная работа № 11: «Работа с двумерными массивами с использованием подпрограмм функций и процедур».

План:

1. Постановка задачи для выполнения лабораторной работы.

2. Самостоятельное выполнение каждым студентом своего индивидуального задания.

3. Консультирование по вопросам теоретической части задания.

4. Защита работы.

Типовой образец задания:

1. Дана целочисленная матрица {Aij}i=1...n;j=1..n , n<=100. Если в матрице есть два одинаковых столбца и есть хотя бы один элемент, абсолютная величина которого - простое число, упорядочить строки матрицы по неубыванию суммы модулей элементов. Использовать процедуры и функции!

2. В текстовом файле input.txt записан русский текст. Найти в тексте слова, содержащие не менее четырех из пяти наиболее часто встречающихся букв текста, записать их заглавными буквами и указать после каждого такого слова в скобках найденные буквы. Полученный текст записать в файл output.txt. Весь текст, кроме найденных слов, должен остаться неизменным, включая и знаки препинания

Тема 8 «Файлы».

Лабораторная работа № 12, 16: «Разработка программ обработки числовых данных, хранящихся в файле».

План:

1. Постановка задачи для выполнения лабораторной работы.

2. Самостоятельное выполнение каждым студентом своего индивидуального задания.

3. Консультирование по вопросам теоретической части задания.

4. Защита работы.

Типовой образец задания:

1. Дана целочисленная матрица {Aij}i=1...n;j=1..n , n<=100. Если в матрице есть еще один элемент, равный ее минимальному элементу, и не менее 2-х элементов, абсолютные величины которых - простые числа, упорядочить строки матрицы по невозрастанию произведений элементов.

2..Работа с числовыми данными в бинарном файле.

Тема 9 «Алгоритмы сортировки и поиска данных».

Лабораторная работа № 13: «Алгоритмы сортировки».

План:

1. Постановка задачи для выполнения лабораторной работы.

2. Самостоятельное выполнение каждым студентом своего индивидуального задания.

3. Консультирование по вопросам теоретической части задания.

4. Защита работы.

Типовой образец задания:

1. Дан файл, содержащий русский текст. Найти в тексте N<=2000 самых длинных слов, оканчивающихся заданной буквой. Записать найденные слова в текстовый файл в порядке невозрастания длины. Все найденные слова должны быть разными! Входные данные находятся в текстовом файле input.txt, а результат работы программы записать в файл output.txt.

Тема 12 «Динамические структуры данных».

Лабораторная работа № 14-15: «Линейные списки».

План:

1. Постановка задачи для выполнения лабораторной работы.

2. Самостоятельное выполнение каждым студентом своего индивидуального задания.

3. Консультирование по вопросам теоретической части задания.

4. Защита работы.

Типовой образец задания:

1. Ввести последовательность натуральных чисел. Если в последовательности есть простые числа, упорядочить последовательность по неубыванию суммы цифр. В противном случае удалить из последовательности числа с нечетным количеством цифр и продублировать 4-хзначные числа. Последовательность хранить в односвязном списке. Перед завершением программы очистить динамическую память с помощью процедуры Dispose.

2. Ввести последовательность натуральных чисел. Если в последовательности нет чисел - палиндромов, упорядочить последовательность по невозрастанию. В противном

случае удалить из последовательности простые числа и продублировать числа, заканчивающиеся нулем. Последовательность хранить в двусвязном циклическом списке с фиктивным элементом. Перед завершением программы очистить динамическую память с помощью процедуры Dispose.

Фактические лабораторные работы №№ 1-16 содержат варианты индивидуальных заданий для каждого студента (количество вариантов лабораторной работы соответствует количеству обучающихся студентов, т.е. от 30 до 60 вариантов).

Тема 14: «Компьютерный практикум программирования на языке C/C++».

Цели:

- проверка остаточных знаний раздела «Алгоритмизация и программирование»;
- приобретение практических навыков структурного программирования;
- освоение методики тестирования и отладки программ.

План:

1. Постановка задачи для выполнения лабораторной работы.

2. Самостоятельное выполнение каждым студентом трех заданий своего варианта.

3. Проверка работ в автоматизированном режиме с использованием проверяющей системы «Executor».

4. Разбор ошибок.

Типовой образец задания:

Задача А. «Последовательность»

Входной файл: input.txt ***Выходной файл:output.txt***

Дана последовательность натуральных чисел. Если в последовательности нет простых чисел, то упорядочить последовательность по не возрастанию. В противном случае найти самое большое простое число в последовательности.

Вход: Во входном файле записано не более 1000 натуральных чисел. Каждое число не превосходит 2^{31}-1.

Выход: Запишите в выходной файл упорядоченную последовательность или найденное простое число.

Пример входных и выходных данных

input.txt	***output.txt***
1 10 100	100 10 1
3 2 11 99	11

Задача В. «Текст»

Входной файл: input.txt ***Выходной файл:output.txt***

Дан русский текст. Найдите первое и последнее слово текста.

Вход: Во входном файле записан не пустой русский текст. Размер файла не превосходит 1 М байт.

Выход: Запишите в первой строке выходного файла первое слово текста, а во второй строке – последнее слово текста.

Пример входных и выходных данных

input.txt	***output.txt***
Дан русский	Дан текст

текст.	

<u>Задача С</u>. «Матрица»
Входной файл: input.txt ***Выходной файл:output.txt***

Дано целочисленная матрица. Найдите наименьшую сумму элементов столбца.
Вход: В первой строке входного файла записано натуральное число $2 \le \boldsymbol{n}, \boldsymbol{m} \le 100$. В остальных строках записана целочисленная матрица $\{A_{ij}\}$ $i = 1 \ldots n$, $j = 1 \ldots m$, ($|A_{ij}| \le 10^7$).
Выход: Запишите в выходной файл найденную сумму.

Пример входных и выходных данных

input.txt	***output.txt***
2 3 1 -1 3 -2 2 -1	-1

Количество разрабатываемых вариантов на подгруппу – 5 (всего 15 задач на каждое занятие практикума).

Раздел 2 «Основы теории информации».

Тема 14 «Основные понятия теории информации».

Лабораторная работа № 27: «Измерение информации».

План:

1. Постановка задачи для выполнения лабораторной работы.

2. Самостоятельное выполнение каждым студентом своего индивидуального задания.

3. Консультирование по вопросам теоретической части задания.

3. Защита работы.

Типовой образец задания:

1. В корзине лежат 32 шара одного цвета. Сколько бит информации несет сообщение о том, что из корзины вытащили красный шар?
2. В корзине лежат шары (белые и черные). Среди них – 4 белых. Сообщение о том, что достали белый шар, несет 3 бита информации. Сколько всего шаров было в корзине?
3. На остановке останавливаются автобусы с разными номерами. Сообщение о том, что к остановке подошел автобус с номером №1 несет 4 бита информации. Вероятность появления на остановке автобуса с номером №2 в два раза меньше, чем вероятность появления автобуса с номером №1. Сколько бит информации несет сообщение о появлении автобуса с номером №2 на остановке?
4. Вычислить энтропию опыта, состоящего в определении цвета наугад вынутого шарика, если в непрозрачном мешочке хранятся 35 белых, 25 красных, 15 синих и 45 зеленых шариков.
5. Имеется следующий текст: "Современное общество характеризуется постоянным увеличением информационных потоков. Наибольший рост объема информации наблюдается в промышленности, торговле и финансово-банковской сфере. Существенно меняется роль информации в общественной жизни, в частности экономической информации, представляющей собой различные сведения экономического характера, полученные в процессе производственно-хозяйственной деятельности, и отражающие социально-экономические процессы. Экономическая информация характеризуется через систему натуральных, стоимостных и относительных показателей и подвергается таким

процедурам преобразования как сбор и регистрация, передача, хранение, поиск, обработка, защита."

Найдите количество информации, которую переносят следующие буквы Ф и А

Тема 15 «Кодирование и измерение информации».

Лабораторная работа 28: «Кодирование информации».

План:

1. Постановка задачи для выполнения лабораторной работы.

2. Самостоятельное выполнение каждым студентом своего индивидуального задания.

3. Консультирование по вопросам теоретической части задания.

3. Защита работы.

Типовой образец задания:

1. Найдите сколько чисел можно закодировать при использовании кода, длиной 8 знаков и алфавита {!, @, #, $}
2. Определите длину кода, если алфавит состоит из знаков {q, j, s, u}. Число закодированных слов 72.
3. Построить код Хаффмана для алфавита, состоящего из 6-ти символов a, b, c, d, e. f с частотами (вероятностями появления в тексте) 0,3 (a); 0,15 (b); 0,16 (c); 0,09 (d); 0,15 (e); 0,11 (f).
4. Построить код Шеннона-Фано для алфавита, указанного в предыдущем задании.
5. Задано сообщение **aaabbbbccdddeeeeeeeeeffffgghhi**, состоящее из букв алфавита {a, b, c, d, e, f, g, h, i}.
   1) Построить для данного алфавита равномерный код. Определить размер сообщения при равномерном кодировании.
   2) Построить код Хаффмана. Определить размер сообщения при кодировании кодом Хаффмана.

Раздел 3 «Представление информации на компьютере».

Тема 16 «Компьютерная арифметика».

Лабораторная работа № 29: «Системы счисления».

План:

1. Постановка задачи для выполнения лабораторной работы.

2. Самостоятельное выполнение каждым студентом своего индивидуального задания.

3. Консультирование по вопросам теоретической части задания.

3. Защита работы.

Типовой образец задания:

1. а) $666_{(10)}$; б) $305_{(10)}$; в) $153{,}25_{(10)}$; г) $162{,}25_{(10)}$; д) $248{,}46_{(10)}$
2. а) $1100111011_{(2)}$; б) $10000000111_{(2)}$; в) $10110101{,}1_{(2)}$; г) $100000110{,}10101_{(2)}$; д) $671{,}24_{(8)}$; е) $41A{,}6_{(16)}$.
3. а) $10000011_{(2)}+1000011_{(2)}$; б) $1010010000_{(2)}+1101111011_{(2)}$; в) $110010{,}101_{(2)}+1011010011{,}01_{(2)}$; г) $356{,}5_{(8)}+1757{,}04_{(8)}$; д) $293{,}8_{(16)}+3CC{,}98_{(16)}$.
4. а) $100111001_{(2)}-110110_{(2)}$; б) $1111001110_{(2)}-111011010_{(2)}$;

в) $1101111011,01_{(2)}$-$101000010,0111_{(2)}$; г) $2025,2_{(8)}$-$131,2_{(8)}$;
д) $2D8,4_{(16)}$-$A3,B_{(16)}$.

5. а) $1100110_{(2)}$´ $1011010_{(2)}$; б) $2001,6_{(8)}$´ $125,2_{(8)}$;
в) $2C,4_{(16)}$´ $12,98_{(16)}$.

6. а) $110011000_{(2)}$: $10001_{(2)}$; б) $2410_{(8)}$: $27_{(8)}$;
в) $D4A_{(16)}$: $1B_{(16)}$;

Лабораторная работа № 30: «Представление чисел в компьютере».

План:

1. Постановка задачи для выполнения лабораторной работы.

2. Самостоятельное выполнение каждым студентом своего индивидуального задания.

3. Консультирование по вопросам теоретической части задания.

3. Защита работы.

Типовой образец задания:

Задание 1. Выполнить арифметические действия за компьютер над двумя числами при заданном представлении (однобайтовое или двухбайтовое) чисел.

При выполнении данного задания необходимо придерживаться последовательного выполнения следующих действий:

1. Перевод первого числа в двоичную систему счисления, прямой, обратный и дополнительный коды.

2. Перевод второго числа в двоичную систему счисления, прямой, обратный и дополнительный коды.

3. Выполнение действия с помощью обратного кода.

4. Выполнение действия с помощью дополнительного кода.

5. Прямой, обратный и дополнительный код результата.

Задание 2. Привести в формат с фиксированной точкой следующие целые числа, используя шестнадцатиразрядную регистровую сетку.

Задание 3. Перевести во внутреннее представление формата с плавающей точкой в 32-х разрядной сетке, заданные числа без использования вычислительной техники.

Задание 4. Дано десятичное число. Записать нормализованную форму данного числа в системе счисления с основанием p=2, 8, 16.

Раздел 4 «Элементы теории алгоритмов».

Тема 19 «Уточнение понятия алгоритма».

Лабораторная работа № 31: «Машина Тьюринга».

План:

1. Постановка задачи для выполнения лабораторной работы.

2. Самостоятельное выполнение каждым студентом своего индивидуального задания.

3. Консультирование по вопросам теоретической части задания.

3. Защита работы.

Типовой образец задания:

1. Написать программу для машины Тьюринга, которая к числу в семеричной системе счисления прибавляет цифру 1. В исходном состоянии каретка стоит на некотором расстоянии справа от числа.

2. Опишите, какой алгоритм выполняет данная машина Тьюринга.

	a_0	0	1
q_1	a_0 Н !	a_0 П q_1	a_0 П q_1

К каким словам, составленным из символов данного алфавита, применима машина?

Тема 20 «Машина Поста как уточнение понятия алгоритма».

Лабораторная работа № 32: «Машина Поста».

План:

1. Постановка задачи для выполнения лабораторной работы.

2. Самостоятельное выполнение каждым студентом своего индивидуального задания.

3. Консультирование по вопросам теоретической части задания.

3. Защита работы.

Типовой образец задания:

1. Написать программу для машины Поста, которая к массиву, содержащему *n* единиц, прибавляет справа и слева по одной единице. В исходном состоянии каретка стоит на некотором расстоянии справа от массива.
2. По заданной программе для машины Поста определить, какую задачу она решает.

Раздел 5 «Основы построения компьютера».

Тема 22 «Логические основы компьютера».

Лабораторная работа № 33: «Логические основы компьютера».

План:

1. Постановка задачи для выполнения лабораторной работы.

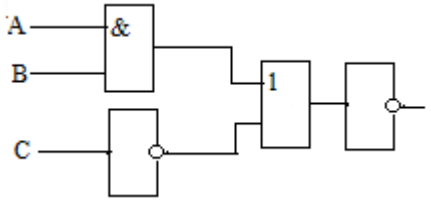
2. Самостоятельное выполнение каждым студентом своего индивидуального задания.

3. Консультирование по вопросам теоретической части задания.

3. Защита работы.

Типовой образец задания:

1. Построить таблицу истинности для формулы $X \wedge ((X \vee Y) \to (X \to Y))$.
2. Построить логическую схему по формуле $A \wedge B \wedge C \vee \overline{A}$.
3. Определить логическую функцию, реализуемую логической схемой



4. Построить логическое выражение по таблице истинности

A	B	C	X
0	0	0	0
0	0	1	0
0	1	0	0
0	1	1	1
1	0	0	0
1	0	1	0

1	1	0	1
1	1	1	1

Раздел 6 «Программное обеспечение компьютера».

Тема 24 «Программное обеспечение персонального компьютера».

Лабораторная работа № 34: «Программное обеспечение персонального компьютера».

План:

1. Постановка задачи для выполнения лабораторной работы.

2. Самостоятельное выполнение каждым студентом своего индивидуального задания.

3. Консультирование по вопросам теоретической части задания.

3. Защита работы.

Типовой образец задания:

Задание №1. Изучение основных команд и служебных утилит при работе с файлами в ОС Windows 10.

Задание №2. Исследовать основные способы применения команды копирования Copy на конкретных примерах.

Задание №3. Исследовать основные способы применения команды копирования Xcopy на конкретных примерах.

Задание №4. Исследовать основные способы применения команды перемещения Move на конкретных примерах.

Задание №5. Исследовать основные способы применения команды замены Replace на конкретных примерах.

Задание №6. Исследовать основные способы применения команды переименования Ren (Rename) на конкретных примерах.

Задание №7. Исследовать основные способы применения команды форматирования Format на конкретных примерах

Раздел 7 «Компьютерные сети и проблемы безопасности компьютерный сетей».

Тема 26 «Компьютерные сети».

Лабораторная работа № 35: «Компьютерные сети».

План:

1. Постановка задачи для выполнения лабораторной работы.

2. Самостоятельное выполнение каждым студентом своего индивидуального задания.

3. Консультирование по вопросам теоретической части задания.

3. Защита работы.

Типовой образец задания:

Используя сетевые утилиты PING, TRACEROUTE и NSLOOKUP исследовать свойства сетевых соединений компьютера.

Тема 27 «Основные понятия информационной безопасности компьютерных систем».

Лабораторная работа № 36: «Математические алгоритмы, обеспечивающие конфиденциальность сообщения».

План:

1. Постановка задачи для выполнения лабораторной работы.

2. Самостоятельное выполнение каждым студентом своего индивидуального задания.

3. Консультирование по вопросам теоретической части задания.

3. Защита работы.

Типовой образец задания:

1. Дана матрица A над кольцом вычетов Z_8. Определите, существует ли у данной матрицы обратная матрица над кольцом вычетов Z_8.

$$A = \begin{pmatrix} 7 & 6 & 1 \\ 0 & 4 & 5 \\ 2 & 2 & 5 \end{pmatrix}$$

2. Для шифрования сообщений при переписке с друзьями Коля использует шифр Хилла. Ключом для шифрования является матрица A над кольцом вычетов Z_{31}:

$$A = \begin{pmatrix} 19 & 4 & 16 \\ 21 & 14 & 16 \\ 0 & 2 & 25 \end{pmatrix}$$

При расшифровании зашифрованных текстов используется A^{-1} (обратная матрица над кольцом вычетов Z_{31}). Помогите Коле её вычислить.

Типовые контрольные задания

Контрольная работа № 1 «Алгоритмы сортировки и поиска данных»

Вариант 1

Задача А. Дана матрица $\mathbf{A_{n\times m}}$, $0<=\mathbf{a_{i,j}}<=10^9$ (n,m<=100). Вычислить количество столбцов содержащих не менее двух простых числа. Если в матрице нет простых чисел, то вывести 0.

Входные данные: В файле **Input.txt** в первой строке записаны числа **n** и **m** задающие размер матрицы. В следующих **n** строках построчно записаны элементы матрицы **A**.

Выходные данные: В файл **Output.txt** записать количество столбцов содержащих не менее двух простых чисел, если в матрице нет простых чисел, то вывести 0.

Пример входных и выходных данных

Input.txt	*Output.txt*
3 3 1 2 3 4 5 6 7 8 9	1

1 5 1 0 4 8 6	0

Задача B. Дана последовательность целых чисел $\{A_j\}$. Количество чисел заранее неизвестно, но известно, что оно не превосходит 10^4. $|A_j|<=10^9$. Если в последовательности есть число палиндром с суммой цифр большей 10, то упорядочить данную последовательность по невозрастанию. В противном случае, найти номер наибольшего элемента в последовательности, а если таковых элементов несколько, то определить номер последнего.

Входные данные: в файле Input.txt записаны элементы последовательности $\{A_j\}$.

Выходные данные: в файле Output.txt упорядоченная последовательность $\{A_j\}$. по невозрастанию или номер последнего максимального элемента.

Пример входных и выходных данных

Input.txt	***Output.txt***
1 2 -909 27 5	27 5 2 1 -909
1 2 505 27 5 121	3
-121 35 55 121 45 121 33	6

Задача C. Задано слово, записанное с помощью букв английского алфавита. Под словом будем понимать последовательность подряд идущих букв английского алфавита, а иные символы считаются разделителями слов. В тексте подсчитать количество слов, которые в результате перестановки букв в них дают заданное слово. Если таких слов нет, то вывести 0. Заглавные буквы и незаглавные считать неразличимыми.

Входные данные: В файле **Input.txt** в первой строке находится заданное слово, а в последующих строках записан текст содержащий слова.

Выходные данные: В файл **Output.txt** записать количество слов, которые в результате перестановки букв в них дают заданное слово. Если таких слов нет, то вывести 0.

Пример входных и выходных данных

Input.txt	***Output.txt***
okt Kit Kot tik, kto.Tok	3
Ledok Ledokol Dok Led	0

Задача D. Дана последовательность натуральных чисел. Если в последовательности нет простых чисел, то упорядочить последовательность по не возрастанию. В противном случае найти самое большое простое число в последовательности.

Вход: Во входном файле Input.txt записано не более 1000 натуральных чисел. Каждое число не превосходит 2^{31}-1.

Выход: Запишите в выходной файл Output.txt упорядоченную последовательность или найденное простое число.

Пример входных и выходных данных

input.txt	***output.txt***
1 10 100	100 10 1
3 2 11 99	11

Задача E. Дан русский текст. Найдите первое и последнее слово текста.

Вход: Во входном файле Input.txt записан не пустой русский текст. Размер файла не превосходит 1 М байт.

Выход: Запишите в первой строке выходного файла Output.txt первое слово текста, а во второй строке – последнее слово текста.

Пример входных и выходных данных

input.txt	***output.txt***
Дан русский текст.	Дан текст

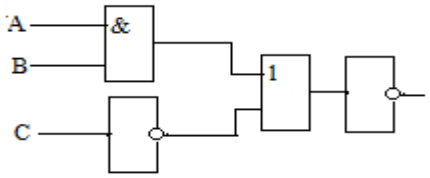
Время, отводимое на решение задач составляет 1 час 30 минут.

Количество вариантов соответствует количеству студентов в подгруппе.

Контрольная работа № 2 «Логические основы компьютера»

Вариант 1

1. Построить таблицу истинности для формулы $X \wedge ((X \vee Y) \rightarrow (X \rightarrow Y))$.
2. Построить логическую схему по формуле $A \wedge B \wedge C \vee \overline{A}$.
3. Определить логическую функцию, реализуемую логической схемой



4. Построить логическое выражение по заданной таблице истинности**.**

A	B	C	X
0	0	0	0
0	0	1	0
0	1	0	0
0	1	1	1
1	0	0	1
1	0	1	1
1	1	0	0
1	1	1	1

4. Изобразите с использованием элементов схемотехники полусумматор, сумматор и многоразрядный сумматор. Приведите аналитические выражения для соответствующих схем.

Количество вариантов соответствует количеству студентов в группе.

Устные опросы

Тема 2 «Начальные сведения о языке программирования».

1. Общая характеристика языка программирования: место в классификации языков программирования, основные объекты и правила записи алгоритмов, структура программы.
2. Арифметические типы данных.
3. Ввод и вывод данных. Параметры процедур ввода и вывода. Форматирование вывода.

4. Классификация типов данных.
5. Линейный алгоритм и его запись на языке программирования.
6. Алгоритмическая конструкция выбора.
7. Циклические алгоритмы.
8. Символьный и логический типы данных.

Тема 17 «Представление текстовой и графической информации».

1. Понятие информации и виды информационных процессов.
2. Дискретное представление информации.
3. Понятие кодирование информации. Выбор способа представления информации.
4. Кодирование текстовой информации. Основные приемы преобразования текcов.
5. Гипертекстовое представление информации.
6. Кодирование графической информации. Растровая и векторная графика.
7. Средства и технологии работы с графикой.
8. Аппаратные средства ввода и вывода графических изображений.
9. Графические редакторы.

Тема 18 «Представление звуковой информации».

1. Кодирование звуковой информации.
2. Форматы звуковых файлов.
3. Ввод и обработка звуковых файлов.
4. Вычисление информационных характеристик звукового файла: объема и времени звучания.

Тема 21 «Понятие сложности алгоритма».

1. Неформальное понятие алгоритма. Необходимость формализации.
2. Формализация понятия алгоритма на примере машин Тьюринга и Поста.
3. Устройство машины Тьюринга. Программа для машины Тьюринга.
4. Система команд и устройство машины поста.
5. Примеры программ для машин Тьюринга и Поста.
6. Алгоритмические неразрешимые проблемы.
7. Тезис Чёрча.
8. Расчет сложности алгоритма поиска.
9. Расчет сложности алгоритмов «пузырьковой сортировки» и «сортировки вставками».

Тема 23 «Архитектура организации ЭВМ».

1. Архитектура компьютера.
2. Внутренняя память.
3. Характеристики процессора.
4. Внешняя память (носители информации).
5. Структура клавиатуры.
6. Классификация программного обеспечения.
7. Операционная система.
8. Организация и хранение информации.
9. Представление данных в компьютере.
10. Средства поиска информации.

11. Взаимосвязь программного и аппаратного обеспечения компьютера.

Тема 26 «Командные оболочки».

1. Назначение и классификация прикладного программного обеспечения.
2. Работа с командной строкой.
3. Назначение программ-оболочек.
4. Характеристики программы Total Comander.
5. Характеристики программы Far Manager.
6. Характеристики программы Norton Comander.

8.3 <u>Вопросы для промежуточного контроля (экзамена)</u>

Теоретическая часть.

1. Типы данных языка программирования.
2. Операторы языка программирования.
3. Массивы.
4. Подпрограммы.
5. Файлы.
6. Списки.
7. Алгоритмы поиска данных.
8. Алгоритмы сортировки.
9. Информация. Информационные объекты различных видов. Основные информационные процессы: хранение, передача и обработка информации. Роль информации в жизни людей.
10. Понятие количества информации: различные подходы. Формула Хартли и количество информации. Формула Шеннона. Единицы измерения количества информации. Информационный объем.
11. Кодирование информации. Равнозначные и разнозначные коды. Префиксные коды. Условия однозначного декодирования. Коды Хаффмана и Шеннона – Фанно. Алгоритм сжатия информации RLE.
12. Системы счисления. Позиционные и непозиционные системы счисления. Запись чисел в различных системах счисления. Алгоритмы перевода из одной системы счисления в другую. Представление числа в виде разложения по степеням основания системы счисления и доказательство единственности такого представления.
13. Представление целых чисел в компьютере: положительные числа, отрицательные числа, алгоритмы получения дополнительного кода.
14. Представление вещественных чисел в компьютере: мантисса, порядок, нормализованная запись вещественного числа. Выполнение арифметических операций над вещественными числами.
15. Представление текстовой информации в компьютере.
16. Логические основы компьютера: логические операции, законы алгебры логики, таблицы истинности, синтез логических выражений, логические элементы компьютера, сумматор, многоразрядный сумматор.
17. Информационная безопасность. Правовая защита программ и данных.
18. Прикладное программное обеспечение.
19. Системное программное обеспечение.
20. Системы программирования.
21. Компьютерные сети: топология, локальная сеть, сети с выделенным сервером, терминальный доступ, беспроводные сети, сетевое оборудование.

Практическая часть.

1. Задачи по программированию (обработка числовых данных, числовых массивов, линейных списков, обработка символьных данных, чтение данных из файла и вывод данных в файл).
2. Вычисление объема сообщения, количества информации сообщения.
3. Представление числовой информации в компьютере.
4. Перевод чисел из одной позиционной системы счисления в другую.
5. Кодирование информации (методы Хаффмана, Шеннона – Фанно, RLE).
6. Разработка логических схем и синтез логических выражений.
7. Разработка программ для машин Тьюринга и Поста.

Типовые практические задания для промежуточного контроля (экзамена)

1. Дана целочисленная матрица {Aij}i=1..n,j=1..m (n,m<=100). Найти строку, сумма элементов которой наиболее близка к 0, и заменить все элементы этой строки числом 0.
2. Дана целочисленная матрица {Aij}i=1..n,j=1..m (n,m<=100). Найти столбец с наименьшей суммой элементов и увеличить все элементы этого столбца на 3.
3. Дана целочисленная матрица {Aij}i=1..n,j=1..m (n,m<=100). Найти столбец содержащий наименьший элемент матрицы и заменить все отрицательные элементы этого столбца числом 0.
4. Дана целочисленная матрица {Aij}i=1..n,j=1..m (n,m<=100). Найти строку с наименьшей суммой элементов и заменнить все элементы этой строки этой суммой.
5. Дана целочисленная матрица {Aij}i=1..n,j=1..m (n,m<=100). Найти строку с наибольшей по абсолютной величине суммой элементов и заменить все элементы этой строки числом 9999.
6. Дана целочисленная матрица {Aij}i=1..n,j=1..m (n,m<=100). Найти строку с наибольшим произведением элементов и заменить все элементы этой строки этим произведением.
7. Дана целочисленная матрица {Aij}i=1..n,j=1..m (n,m<=100). Найти строку с наибольшей суммой элементов и увеличить все элементы этой строки на 1.
8. Дана последовательность натуральных чисел {Aj}j=1...n (n<=10000). Удалить из последовательности простые числа и продублировать составные числа, сумма цифр которых равна 15.
9. Дана последовательность натуральных чисел {Aj}j=1...n (n<=10000). Удалить из последовательности числа, сумма цифр которых равна 18, а среди оставшихся продублировать числа, произведение цифр которых кратно 35.
10. Дана последовательность натуральных чисел {Aj}j=1...n (n<=10000). Удалить из последовательности числа, сумма цифр которых кратна шести. Среди оставшихся продублировать числа, начинающиеся цифрой 1.
11. Дана последовательность натуральных чисел {Aj}j=1...n (n<=10000). Удалить из последовательности числа, произведение цифр которых равно 144, а среди оставшихся продублировать числа, содержащие цифру 8.
12. Дана последовательность натуральных чисел {Aj}j=1...n (n<=10000). Удалить из последовательности числа, произведение цифр которых кратно 18, а среди оставшихся продублировать числа, содержащие цифру 7, но не содержащие цифру 0.
13. Дана последовательность натуральных чисел {Aj}j=1...n (n<=10000). Удалить из последовательности числа, начинающиеся цифрой 2, а среди оставшихся продублировать числа, все цифры которых различны.
14. Дана строка, содержащая русский текст. Если в тексте нет слов-палиндромов длиной более 1-й буквы, то вывести слова текста в соответствии с убыванием количества согласных, в противном случае продублировать в словах текста гласные буквы и вывести полученные слова в порядке, обратном к алфавитному.
15. Дана строка, содержащая русский текст. Если в тексте есть слово-палиндром длиной более 1-й буквы, то вывести слова текста в соответствии с убыванием количества гласных, в противном случае продублировать в словах текста гласные буквы и вывести полученные слова в алфавитном порядке.

16. Дана строка, содержащая русский текст. Вывести в порядке, обратном к алфавитному, слова текста, содержащие не менее 3-х гласных, в остальных словах удалить гласные и продублировать согласные буквы.
17. Дана строка, содержащая русский текст. Вывести в алфавитном порядке слова текста, содержащие не более 3-х согласных, в остальных словах удалить гласные и продублировать согласные буквы.
18. Дана строка, содержащая русский текст. Вывести в алфавитном порядке слова текста, содержащие повторяющиеся гласные буквы, остальные слова инвертировать.

8.4. Планируемые уровни сформированности компетенций обучающихся и критерии оценивания

Уровни	Содержательное описание уровня	Основные признаки выделения уровня (этапы формирования компетенции, критерии оценки сформированности)	Пятибалльная шкала (академическая) оценка	Двухбалльная шакала, зачет	БРС, % освоения (рейтинговая оценка)
Повышенный	Творческая деятельность	*Включает нижестоящий уровень.* Умение самостоятельно принимать решение, решать проблему/задачу теоретического и прикладного характера на основе изученных методов, приемов, технологий	отлично	зачтено	86-100
Базовый	Применение знаний и умений в более широких контекстах учебной и профессиональной деятельности, нежели по образцу с большей степени самостоятельности и инициативы	*Включает нижестоящий уровень.* Способность собирать, систематизировать, анализировать и грамотно использовать информацию из самостоятельно найденных теоретических источников и иллюстрировать ими теоретические положения или обосновывать практику применения	хорошо		71-85
Удовлетворительный (достаточный)	Репродуктивная деятельность	Изложение в пределах задач курса теоретически и практически контролируемого материала	удовлетворительно		55-70

Недостаточный	Отсутствие признаков удовлетворительного уровня	неудовлетворительно	не зачтено	Менее 55

9. Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины.

Основная литература

1. Яшин, В. Н. Информатика : учебник / В.Н. Яшин, А.Е. Колоденкова. — Москва : ИНФРА-М, 2022. — 522 с. — (Высшее образование: Бакалавриат). — DOI 10.12737/1069776. - ISBN 978-5-16-015924-9. - Текст : электронный. - URL: https://znanium.com/catalog/product/1853592 (дата обращения: 27.04.2022). – Режим доступа: по подписке.
2. Федотова, Е. Л. Информатика : учебное пособие / Е.Л. Федотова. — 2-е изд., перераб. и доп. — Москва : ИНФРА-М, 2022. — 453 с. — (Высшее образование: Бакалавриат). — DOI 10.12737/1200564. - ISBN 978-5-16-016625-4. - Текст : электронный. - URL: https://znanium.com/catalog/product/1200564 (дата обращения: 27.04.2022). – Режим доступа: по подписке.

Дополнительная литература

1. Литвиненко, В. А. Программирование на С++ задач на графах: Учебное пособие / Литвиненко В.А. - Таганрог:Южный федеральный университет, 2016. - 83 с.: ISBN 978-5-9275-2311-5. - Текст : электронный. - URL: https://znanium.com/catalog/product/997083 (дата обращения: 30.03.2022). – Режим доступа: по подписке.
2. Кузин, А. В. Программирование на языке Си : учебное пособие / А.В. Кузин, Е.В. Чумакова. — Москва : ФОРУМ : ИНФРА-М, 2021. — 144 с. — (Высшее образование). - ISBN 978-5-00091-066-5. - Текст : электронный. - URL: https://znanium.com/catalog/product/1222078 (дата обращения: 30.03.2022). – Режим доступа: по подписке.

10. Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины (модуля).

- НЭБ Национальная электронная библиотека, диссертации и прочие издания
- eLIBRARY.RU Научная электронная библиотека, книги, статьи, тезисы докладов конференций
- Гребенников Электронная библиотека ИД журналы
- ЭБС Лань книги, журналы
- ЭБС Консультант студента
- ПРОСПЕКТ ЭБС
- ЭБС ZNANIUM.COM
- РГБ Информационное обслуживание по МБА
- БЕН РАН
- Электронно-библиотечная система (ЭБС) Кантитана (https://elib.kantiana.ru/)

11. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине.

Программное обеспечение обучения включает в себя:

- система электронного образовательного контента БФУ им. И. Канта – www.lms-3.kantiana.ru, обеспечивающую разработку и комплексное использование электронных образовательных ресурсов;
- серверное программное обеспечение, необходимое для функционирования сервера и связи с системой электронного обучения через Интернет;
- корпоративная платформа Microsoft Teams;
- установленное на рабочих местах обучающихся ПО: Microsoft Windows 7, Microsoft Office Standart 2010, антивирусное программное обеспечение Kaspersky Endpoint Security.
- Среда программирования Microsoft Visual Studio (любая версия);
- Qt версии 5.0 и выше

12. Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине.

Для проведения занятий лекционного типа, практических и семинарских занятий используются специальные помещения (учебные аудитории), оборудованные техническими средствами обучения – мультимедийной проекционной техникой. Для проведения занятий лекционного типа используются наборы демонстрационного оборудования.

Для проведения лабораторных работ, (практических занятий – при необходимости) используются специальные помещения (учебные аудитории), оснащенные специализированным лабораторным оборудованием: персональными компьютерами с возможностью выхода в интернет и с установленным программным обеспечением, заявленным в п.11.

Для проведения групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации используются специальные помещения (учебные аудитории), оборудованные специализированной мебелью (для обучающихся), меловой / маркерной доской.

Для организации самостоятельной работы обучающимся предоставляются помещения, оснащенные компьютерной техникой с возможностью подключения к сети «Интернет» и обеспечением доступа в электронную информационно-образовательную среду университета.

Для обучения инвалидов и лиц с ограниченными возможностями здоровья университетом могут быть представлены специализированные средства обучения, в том числе технические средства коллективного и индивидуального пользования.

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
федеральное государственное автономное образовательное учреждение высшего образования «Балтийский федеральный университет имени Иммануила Канта»
Институт физико-математических наук и информационных технологий

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

«Дифференциальные уравнения»

Шифр: 10.05.01
Специальность: «Компьютерная безопасность»
Специализация: «Математические методы защиты информации»
Квалификация (степень) выпускника: специалист по защите информации

Калининград
2022

Лист согласования

Составитель: Шевченко Юрий Иванович, к.ф.-м.н., профессор

Рабочая программа утверждена на заседании учебно-методического совета института физико-математических наук и информационных технологий

Протокол № 01/22 от «01» февраля 2022 г.

Председатель учебно-методического
совета института физико-
математических наук и информационных
технологий

Первый заместитель директора Шпилевой А. А
ИФМНиИТ, к. ф.-м. н., доцент

Ведущий менеджер Е.П.Ставицкая

Содержание

1.Наименование дисциплины: «Дифференциальные уравнения».

Цель дисциплины: целью освоения дисциплины «Дифференциальные уравнения» является фундаментальная подготовка обучающихся в области дифференциальных уравнений.

2. Перечень планируемых результатов обучения по дисциплине, соотнесенных с планируемыми результатами освоения образовательной программы

Код компетенции	Результаты освоения образовательной программы (ИДК)	Результаты обучения по дисциплине
ОПК-3. Способен на основании совокупности математических методов разрабатывать, обосновывать и реализовывать процедуры решения задач профессиональной деятельности.	ОПК-3.1. Знает необходимые математические методы для решения задач обеспечения защиты информации. ОПК-3.2. Применяет совокупность необходимых математических методов для решения задач обеспечения защиты информации. ОПК-3.3. Разрабатывает, обосновывает и реализует на практике процедуры решения задач обеспечения защиты информации.	- **знать** основные понятия теории дифференциальных уравнений и основные типы задач, возникающих в теории дифференциальных уравнений; - **уметь** ориентироваться в постановках задач; на основе анализа увидеть и корректно сформулировать результат; применять совокупность необходимых математических методов для решения задач обеспечения защиты информации; - **владеть** практическими навыками решения обыкновенных дифференциальных уравнений, систем дифференциальных уравнений, исследования решений на устойчивость.

3. Место дисциплины в структуре образовательной программы

Дисциплина «Дифференциальные уравнения» представляет собой дисциплину обязательной части блока дисциплин подготовки обучающихся.

4. Виды учебной работы по дисциплине.

Виды учебной работы по дисциплине зафиксированы учебным планом основной профессиональной образовательной программы по указанному направлению и профилю, выражаются в академических часах. Часы контактной работы и самостоятельной работы обчающегося и часы, отводимые на процедуры контроля, могут различаться в учебных планах ОПОП по формам обучения. Объем контактной работы включает часы контактной аудиторной работы (лекции/практические занятия/ лабораторные работы), контактной внеаудиторной работы (контроль самостоятельной работы), часы контактной работы в период аттестации. Контактная работа, в том числе может проводиться посредством электронной информационно-образовательной среды университета с использованием ресурсов сети Интернет и дистанционных технологий

5. Содержание дисциплины, структурированное по темам (разделам)

Исходя из рамок, установленных учебным планом по трудоемкости и видам учебной работы по дисциплине, преподаватель самостоятельно выбирает тематику занятий по формам и количеству часов проведения контактной работы: лекции и иные учебные занятия, предусматривающие преимущественную передачу учебной информации преподавателем и (или) занятия семинарского типа (семинары, практические занятия, практикумы, лабораторные работы, коллоквиумы и иные аналогичные занятия), и (или) групповые консультации, и (или) индивидуальную работу обучающихся с преподавателем, в том числе индивидуальные консультации (по курсовым работам/проектам – при наличии курсовой работы/проекта по данной дисциплине в учебном плане). Рекомендуемая тематика занятий максимально полно реализуется в контактной работе с обучающимися очной формы обучения. В случае реализации образовательной программы в заочной / очно-заочной форме трудоемкость дисциплины сохраняется, однако объем учебного материала в значительной части осваивается обучающимися в форме самостоятельной работы. При этом требования к ожидаемым образовательным результатам обучающихся по данной дисциплине не зависят от формы реализации образовательной программы.

№	Наименование раздела	Содержание раздела
1	Общие понятия теории дифференциальных уравнений	Понятие дифференциального уравнения и его решения. Уравнение скорости падания тела. Уравнение цепной линии. Общие определения в теории дифференциальных уравнений. Теорема существования и единственности решения. Общее и частное решения. Интегралы дифференциального уравнения. Пример с общим, частным и вырожденным решением. Интерпретация решений дифференциальных уравнений с помощью изоклин.
2	Дифференциальные уравнения первого порядка	Элементарные приемы интегрирования. Уравнения с разделяющимися переменными. Однородные уравнения и приводящиеся к ним линейные уравнения. Уравнения в полных дифференциалах и интегрирующий множитель. Уравнение Бернулли. Метод введения параметра. Уравнения Лагранжа и Клеро.
3	Приложения дифференциальных уравнений к геометрии и физике	Огибающая семейства кривых. Дискриминантная кривая. Кривая особых точек. Особое решение дифференциального уравнения первого порядка. Ортогональные и изогональные траектории. Дифференциальное уравнение скорости падения тел. Дифференциальное уравнение массы радия при распаде. Огибающая траекторий полета снарядов. Линии тока как ортогональные траектории эквипотенциальных поверхностей. Дифференциальное уравнение цепной линии. Закон постоянства суммы кинетической и потенциальной энергии. Задача о второй космической скорости. Движение материальной точки с переменной скоростью под действием непостоянной силы.
4	Дифференциальные уравнения высших порядков	Общие понятия для дифференциальных уравнений высших порядков. Простейшие уравнения высших порядков. Дифференциального уравнения второго

		порядка, приводимые к уравнениям первого порядка: без искомой функции, без аргумента.
5	Линейные однородные уравнения	Свойства линейных однородных уравнений второго порядка. Определитель Вронского, формула Лиувилля–Остроградского. Однородные линейные уравнения второго и высшего порядков с постоянными коэффициентами. Фундаментальные системы решений и общее решение линейного однородного уравнения высшего порядка.
6	Линейные неоднородные уравнения второго порядка	Теорема об общем решении неоднородного дифференциального уравнения. Метод вариации произвольных постоянных. Нахождение частного решения в случае. Когда правая часть уравнения есть сумма двух функций. Неоднородные линейные дифференциальные уравнения с постоянными коэффициентами. Неоднородные линейные дифференциальные уравнения высших порядков.
7	Системы обыкновенных дифференциальных уравнений. Устойчивость.	Сведение системы дифференциальных уравнений к одному дифференциальному уравнению высшего порядка. Системы линейных однородных дифференциальных уравнений с постоянными коэффициентами. Фундаментальные системы и общее решение линейной однородной системы уравнений. Неоднородные линейные системы дифференциальных уравнений. Неоднородные системы линейных уравнений с постоянными коэффициентами и неоднородностями специального вида. Устойчивость по Ляпунову и асимптотическая устойчивость. Критерий устойчивости линейной системы с постоянными коэффициентами. Теорема Ляпунова об устойчивости по первому приближению. Функция Ляпунова.
8	Решения дифференциальных уравнений в окрестностях особых точек. Фазовая плоскость.	Однородное дифференциальное уравнение второго порядка, присоединенное к системе, его характеристическое уравнение. Различные случаи для корней характеристического уравнения. Фазовая плоскость. Топология фазовых кривых. Классификация особых точек на плоскости: узел, седло, фокус, центр. Предельный цикл. Критерий устойчивости и его применение.

6. Рекомендуемая тематика учебных занятий в форме контактной работы

Рекомендуемая тематика учебных занятий *лекционного* типа (предусматривающих преимущественную передачу учебной информации преподавателями):

№	Наименование раздела	Темы лекций
1	Общие понятия теории дифференциальных	Лекция 1. Понятие дифференциального уравнения и его решения. Общие понятия теории

	уравнений	дифференциальных уравнений. Теорема существования и единственности решения. Общее и частное решения.
2	Дифференциальные уравнения первого порядка	Лекция 2. Элементарные приемы интегрирования. Уравнения с разделяющимися переменными. Лекция 3. Однородные уравнения и приводящиеся к ним линейные уравнения. Уравнения в полных дифференциалах и интегрирующий множитель. Лекция 4. Уравнение Бернулли. Метод введения параметра. Уравнения Лагранжа и Клеро.
3	Приложения дифференциальных уравнений к геометрии и физике	Лекция 5. Приложения дифференциальных уравнений к геометрии. Приложения дифференциальных уравнений к физике.
4	Дифференциальные уравнения высших порядков	Лекция 6. Общие понятия для дифференциальных уравнений высших порядков. Простейшие уравнения высших порядков. Лекция 7. Дифференциального уравнения второго порядка, приводимые к уравнениям первого порядка: без искомой функции, без аргумента.
5	Линейные однородные уравнения	Лекция 8. Свойства линейных однородных уравнений второго порядка. Определитель Вронского, формула Лиувилля–Остроградского. Лекция9. Однородные линейные уравнения второго и высшего порядков с постоянными коэффициентами. Лекция 10. Фундаментальные системы решений и общее решение линейного однородного уравнения высшего порядка.
6	Линейные неоднородные уравнения второго порядка	Лекция 11. Теорема об общем решении неоднородного дифференциального уравнения. Линейные дифференциальные уравнения с постоянными коэффициентами. Лекция 12. Неоднородные линейные дифференциальные уравнения высших порядков.
7	Системы обыкновенных дифференциальных уравнений. Устойчивость.	Лекция 13. Системы линейных однородных дифференциальных уравнений с постоянными коэффициентами. Фундаментальные системы и общее решение линейной однородной системы уравнений. Лекция 14. Неоднородные линейные системы дифференциальных уравнений. Неоднородные системы линейных уравнений с постоянными коэффициентами и неоднородностями специального вида.
8	Решения дифференциальных уравнений в окрестностях особых точек. Фазовая плоскость.	Лекция 15. Однородное дифференциальное уравнение второго порядка, присоединенное к системе, его характеристическое уравнение. Различные случаи для корней характеристического уравнения. Классификация особых точек на плоскости: узел, седло, фокус, центр.

Рекомендуемая тематика *практических* занятий:

1. Понятие дифференциального уравнения и его решения. Интегральные кривые, поле направлений, изоклины. Уравнения с разделяющимися переменными. Задачи, приводящие к уравнениям с разделяющимися переменными
2. Однородные уравнения. Линейные уравнения.
3. Уравнение Бернулли.
4. Уравнения в полных дифференциалах. Интегрирующий множитель.
5. Метод введения параметра, уравнения Лагранжа и Клеро.
6. Линейная зависимость и независимость функций. Определитель Вронского. Формула Лиувилля–Остроградского.
7. Фундаментальные системы и общее решение линейного однородного уравнения. Однородные линейные уравнения с постоянными коэффициентами.
8. Неоднородные линейные уравнения. Метод вариации постоянных.
9. Неоднородные линейные уравнения с постоянными коэффициентами и неоднородностями специального вида.
10. Фундаментальные системы и общее решение линейной однородной системы. Однородные линейные системы с постоянными коэффициентами.
11. Неоднородные линейные системы. Метод вариации постоянных.
12. Неоднородные линейные и системы с постоянными коэффициентами и неоднородностями специального вида.
13. Устойчивость. Критерий устойчивости линейной системы с постоянными коэффициентами. Теорема Ляпунова об устойчивости по первому приближению.
14. Особые точки на плоскости: узел, седло, фокус, центр. Предельный цикл.
15. Уравнения в вариациях.

На практических занятиях решаются задачи по теме занятия.

Требования к самостоятельной работе обучающихся

1. Работа с лекционным материалом, предусматривающая проработку конспекта лекций и учебной литературы, по всем темам из п. 6 настоящей рабочей программы.

2. Выполнение домашнего задания, предусматривающего решение задач, выполнение упражнений, выдаваемых на практических занятиях, по всем темам из п. 6 настоящей рабочей программы.

Руководствуясь положениями статьи 47 и статьи 48 Федерального закона от 29 декабря 2012 г. N 273-ФЗ «Об образовании в Российской Федерации» научно-педагогические работники и иные лица, привлекаемые университетом к реализации данной образовательной программы, пользуются предоставленными академическими правами и свободами в части свободы преподавания, свободы от вмешательства в профессиональную деятельность; свободы выбора и использования педагогически обоснованных форм, средств, методов обучения и воспитания; права на творческую инициативу, разработку и применение авторских программ и методов обучения и воспитания в пределах реализуемой образовательной программы и отдельной дисциплины.

Исходя из рамок, установленных учебным планом по трудоемкости и видам учебной работы по дисциплине, преподаватель самостоятельно выбирает тематику занятий по формам и количеству часов проведения контактной работы: лекции и иные учебные занятия, предусматривающие преимущественную передачу учебной информации преподавателем и (или) занятия семинарского типа (семинары, практические занятия, практикумы, лабораторные работы, коллоквиумы и иные аналогичные занятия), и (или) групповые консультации, и (или) индивидуальную работу обучающихся с преподавателем, в том числе индивидуальные консультации (по курсовым работам/проектам – при наличии курсовой работы/проекта по данной дисциплине в учебном плане).

Рекомендуемая тематика занятий максимально полно реализуется в контактной работе с обучающимися очной формы обучения. В случае реализации образовательной программы в заочной / очно-заочной форме трудоемкость дисциплины сохраняется, однако объем учебного материала в значительной части осваивается обучающимися в форме самостоятельной работы. При этом требования к ожидаемым образовательным результатам обучающихся по данной дисциплине не зависят от формы реализации образовательной программы.

7. Методические рекомендации по видам занятий

Лекционные занятия.

В ходе лекционных занятий обучающимся рекомендуется выполнять следующие действия. Вести конспектирование учебного материала. Обращать внимание на категории, формулировки, раскрывающие содержание тех или иных явлений и процессов, научные выводы и практические рекомендации по их применению. Задавать преподавателю уточняющие вопросы с целью уяснения теоретических положений, разрешения спорных ситуаций.

Желательно оставить в рабочих конспектах поля, на которых во внеаудиторное время можно сделать пометки из рекомендованной литературы, дополняющие материал прослушанной лекции, а также подчеркивающие особую важность тех или иных теоретических положений.

Практические и семинарские занятия.

На практических и семинарских занятиях в зависимости от темы занятия выполняется поиск информации по решению проблем, практические упражнения, контрольные работы, выработка индивидуальных или групповых решений, итоговое обсуждение с обменом знаниями, участие в круглых столах, разбор конкретных ситуаций, командная работа, представление портфолио и т.п.

Самостоятельная работа.

Самостоятельная работа осуществляется в виде изучения литературы, эмпирических данных по публикациям и конкретных ситуаций из практики, подготовке индивидуальных работ, работа с лекционным материалом, самостоятельное изучение отдельных тем дисциплины; поиск и обзор литературы и электронных источников; чтение и изучение учебника и учебных пособий.

8. Фонд оценочных средств

8.1. Перечень компетенций с указанием этапов их формирования в процессе освоения образовательной программы в рамках учебной дисциплины

Основными этапами формирования указанных компетенций при изучении обучающимися дисциплины являются последовательное изучение содержательно связанных между собой тем учебных занятий. Изучение каждой темы предполагает

овладение обучающимися необходимыми компетенциями. Результат аттестации обучающихся на различных этапах формирования компетенций показывает уровень освоения компетенций.

Контролируемые разделы (темы) дисциплины	Индекс контроли-руемой компетенции (или её части)	Оценочные средства по этапам формирования компетенций
		текущий контроль по дисциплине
1. Общие понятия теории дифференциальных уравнений	ОПК-3	Опрос, решение задач.
2. Дифференциальные уравнения первого порядка	ОПК-3	Опрос, решение задач, контрольная работа
3. Приложения дифференциальных уравнений к геометрии и физике	ОПК-3	Опрос, решение задач
4. Дифференциальные уравнения высших порядков	ОПК-3	Опрос, решение задач
5. Линейные однородные уравнения	ОПК-3	Опрос, решение задач
6. Линейные неоднородные уравнения второго порядка	ОПК-3	Опрос, решение задач
7. Системы обыкновенных дифференциальных уравнений. Устойчивость.	ОПК-3	Опрос, решение задач, контрольная работа
8. Решения дифференциальных уравнений в окрестностях особых точек. Фазовая плоскость.	ОПК-3	Опрос, решение задач

8.2. Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений и навыков и (или) опыта деятельности процессе текущего контроля

Примеры вопросов для устного опроса:

По Теме 2. Дифференциальные уравнения первого порядка

1. Что называется обыкновенным дифференциальным уравнением?
2. Что такое порядок дифференциального уравнения?
3. Что называется решением дифференциального уравнения?
4. Что такое интеграл дифференциального уравнения?
5. Как формулируется теорема о существовании и единственности дифференциального уравнения?
6. Что называется общим решением дифференциального уравнения первого порядка?
7. Что такое общий интеграл дифференциального уравнения первого порядка?
8. Как задаются начальные условия, для чего они нужны?
9. Что такое изоклины?
10. Что представляет собой особое решение дифференциального уравнения?

По Теме 4. Дифференциальные уравнения высших порядков

1. В каких случаях уравнения 2-го порядка приводятся к уравнениям 1-го порядка?
2. Какое уравнение n-го порядка называется линейным?
3. Каковы свойства решений линейного однородного уравнения?

4. Как выражается определитель Вронского?
5. Какой вид имеют решения линейного однородного уравнения 2-го порядка с постоянными коэффициентами?
6. Как формулируется теорема об общем решении неоднородного уравнения?
7. Какова идея метода вариации произвольных постоянных?
8. Как искать частное решение линейного уравнения 2-го порядка с постоянными коэффициентами?
9. Какой вид имеет нормальная система обыкновенных дифференциальных уравнений?
10. Какова идея решения системы линейных однородных дифференциальных уравнений с постоянными коэффициентами?

Типовые контрольные задания:

Тема: Дифференциальные уравнения первого порядка

1. Решить уравнение $(y^2 - 2xy)dx + x^2dy = 0$.

2. Решить уравнение $y' = 2\left(\frac{y+2}{x+y-1}\right)^2$.

3. Решить уравнение $y' + ytgx = \sec x$.

4. Решить уравнение $(x^2 + y^2 + x)dx + ydy = 0$.

5. Решить уравнение $y^2(ydx - 2xdy) = x^3(xdy - 2ydx)$.

6. Решить уравнение $y = xy' - y'^2$.

Тема: Исследование на устойчивость уравнений и систем

1. Исследовать на устойчивость решение задачи Коши $\dot{x} = 4 - t^2x$, $x(0) = 0$.

2. Исследовать на устойчивость с помощью теоремы Ляпунова об устойчивости по первому приближению нулевое решение системы:

$$\begin{cases} \dot{x} = e^{x+2y} - \cos 3x, \\ \dot{y} = \sqrt{4+8x} - 2e^{y}. \end{cases}$$

3. Найти все положения равновесия системы и исследовать их на устойчивость:

$$\begin{cases} \dot{x} = (x-1)(y-1), \\ \dot{y} = xy - 2. \end{cases}$$

8.3. Перечень вопросов и заданий для промежуточной аттестации по дисциплине

Вопросы для промежуточного контроля (зачета)

1. Понятие дифференциального уравнения и его решения. Задачи, приводящие к дифференциальным уравнениям.
2. Дифференциальные уравнения 1-го порядка. Теорема существования и единственности (формулировка). Геометрическая интерпретация уравнения 1-го порядка, разрешённого относительно производной и его решения.
3. Уравнения с разделёнными и разделяющимися переменными.
4. Однородные уравнения и приводимые к ним.
5. Линейные уравнения.
6. Уравнение Бернулли.
7. Уравнения в полных дифференциалах.
8. Интегрирующий множитель.
9. Дифференциальные уравнения 1-го порядка, не разрешенные относительно производной.
10. Уравнения Лагранжа и Клеро.
11. Особые решения.
12. Дифференциальные уравнения высших порядков. Теоремы существования и единственности (формулировка). Методы понижения порядка уравнения.
13. Доказательство теоремы существования и единственности решения для дифференциального уравнения первого порядка. Метод последовательных приближений. Пример.
14. Системы дифференциальных уравнений. Нормальная система дифференциальных уравнений. Сведение дифференциального уравнения порядка n к нормальной системе n-го порядка и обратная задача.
15. Теорема существования и единственности для нормальной системы уравнений.
16. Линейные дифференциальные уравнения высших порядков и линейные системы с переменными коэффициентами. Область существования решения.
17. Линейные однородные уравнения. Векторное пространство решений.
18. Линейная зависимость функций и определитель Вронского.
19. Формула Лиувилля–Остроградского.
20. Фундаментальная система и общее решение линейного однородного дифференциального уравнения.
21. Линейные однородные дифференциальные уравнения с постоянными коэффициентами.
22. Линейные неоднородные уравнения. Метод вариации постоянных.
23. Неоднородные линейные дифференциальные уравнения с постоянными коэффициентами и неоднородностями специального вида.
24. Системы линейных однородных дифференциальных уравнений с постоянными коэффициентами. Метод Эйлера.
25. Неоднородные системы линейных дифференциальных уравнений. Метод вариации.
26. Неоднородные системы линейных дифференциальных уравнений с неоднородностями специального вида.
27. Устойчивость по Ляпунову. Теорема Ляпунова об устойчивости по первому приближению.
28. Фазовые траектории двумерной линейной системы с постоянными коэффициентами.
29. Особые точки: седло, узел, фокус, центр.
30. Первые интегралы системы дифференциальных уравнений.

8.4. Планируемые уровни сформированности компетенций обучающихся и критерии оценивания

Уровни	Содержательное описание уровня	Основные признаки выделения уровня (этапы формирования компетенции, критерии оценки сформированности)	Пятибалльная шкала (академическая) оценка	Двухбалльная шакала, зачет	БРС, % освоения (рейтинговая оценка)
Повышенный	Творческая деятельность	*Включает нижестоящий уровень.* Умение самостоятельно принимать решение, решать проблему/задачу теоретического и прикладного характера на основе изученных методов, приемов, технологий	отлично	зачтено	86-100
Базовый	Применение знаний и умений в более широких контекстах учебной и профессиональной деятельности, нежели по образцу с большей степени самостоятельности и инициативы	*Включает нижестоящий уровень.* Способность собирать, систематизировать, анализировать и грамотно использовать информацию из самостоятельно найденных теоретических источников и иллюстрировать ими теоретические положения или обосновывать практику применения	хорошо		71-85
Удовлетворительный (достаточный)	Репродуктивная деятельность	Изложение в пределах задач курса теоретически и практически контролируемого материала	удовлетворительно		55-70
Недостаточный	Отсутствие признаков удовлетворительного уровня		неудовлетворительно	не зачтено	Менее 55

9. Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины.

Основная литература

1. Осадчий, Ю. М. Дифференциальные уравнения : учеб. пособие / Ю.М. Осадчий. — Москва : ИНФРА-М, 2019. — 157 с. - ISBN 978-5-16-107965-2. - Текст : электронный. - URL: https://znanium.com/catalog/product/1039633 (дата обращения: 01.03.2022). – Режим доступа: по подписке.

Дополнительная литература

1. Коган, Е. А. Обыкновенные дифференциальные уравнения и вариационное исчисление : учебное пособие / Е. А. Коган. — Москва : ИНФРА-М, 2020. — 293 с. — (Высшее образование: Бакалавриат). - ISBN 978-5-16-015817-4. - Текст : электронный. - URL: https://znanium.com/catalog/product/1058922 (дата обращения: 01.03.2022). – Режим доступа: по подписке.

10. Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины (модуля).

- НЭБ Национальная электронная библиотека, диссертации и прочие издания
- eLIBRARY.RU Научная электронная библиотека, книги, статьи, тезисы докладов конференций
- Гребенников Электронная библиотека ИД журналы
- ЭБС Лань книги, журналы
- ЭБС Консультант студента
- ПРОСПЕКТ ЭБС
- ЭБС ZNANIUM.COM
- РГБ Информационное обслуживание по МБА
- БЕН РАН
- Электронно-библиотечная система (ЭБС) Кантитана (https://elib.kantiana.ru/)

11. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине.

Программное обеспечение обучения включает в себя:

- система электронного образовательного контента БФУ им. И. Канта – www.lms-3.kantiana.ru, обеспечивающую разработку и комплексное использование электронных образовательных ресурсов;
- серверное программное обеспечение, необходимое для функционирования сервера и связи с системой электронного обучения через Интернет;
- корпоративная платформа Microsoft Teams;
- установленное на рабочих местах обучающихся ПО: Microsoft Windows 7, Microsoft Office Standart 2010, антивирусное программное обеспечение Kaspersky Endpoint Security.
- специализированное ПО не требуется.

12. Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине.

Для проведения занятий лекционного типа, практических и семинарских занятий используются специальные помещения (учебные аудитории), оборудованные техническими средствами обучения – мультимедийной проекционной техникой. Для проведения занятий лекционного типа используются наборы демонстрационного оборудования.

Для проведения лабораторных работ, (практических занятий – при необходимости) используются специальные помещения (учебные аудитории), оснащенные специализированным лабораторным оборудованием: персональными компьютерами с

возможностью выхода в интернет и с установленным программным обеспечением, заявленным в п.11.

Для проведения групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации используются специальные помещения (учебные аудитории), оборудованные специализированной мебелью (для обучающихся), меловой / маркерной доской.

Для организации самостоятельной работы обучающимся предоставляются помещения, оснащенные компьютерной техникой с возможностью подключения к сети «Интернет» и обеспечением доступа в электронную информационно-образовательную среду университета.

Для обучения инвалидов и лиц с ограниченными возможностями здоровья университетом могут быть представлены специализированные средства обучения, в том числе технические средства коллективного и индивидуального пользования.

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
федеральное государственное автономное образовательное учреждение высшего образования «Балтийский федеральный университет имени Иммануила Канта»
Институт физико-математических наук и информационных технологий

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

«Комплексный анализ»

Шифр: 10.05.01
Специальность: «Компьютерная безопасность»
Специализация: «Математические методы защиты информации»
Квалификация (степень) выпускника: специалист по защите информации

Калининград
2022

Лист согласования

Составитель: Шевченко Юрий Иванович, к.ф.-м.н., профессор

Рабочая программа утверждена на заседании учебно-методического совета института физико-математических наук и информационных технологий

Протокол № 01/22 от «01» февраля 2022 г.

Председатель учебно-методического
совета института физико-
математических наук и информационных
технологий

Первый заместитель директора Шпилевой А. А
ИФМНиИТ, к. ф.-м. н., доцент

Ведущий менеджер Е.П.Ставицкая

Содержание

1.Наименование дисциплины: «Комплексный анализ».

Цель дисциплины: целью освоения дисциплины «Комплексный анализ» является фундаментальная подготовка обучающихся в области комплексного анализа.

2. Перечень планируемых результатов обучения по дисциплине, соотнесенных с планируемыми результатами освоения образовательной программы

Код компетенции	Результаты освоения образовательной программы (ИДК)	Результаты обучения по дисциплине
ОПК-3. Способен на основании совокупности математических методов разрабатывать, обосновывать и реализовывать процедуры решения задач профессиональной деятельности.	ОПК-3.1. Знает необходимые математические методы для решения задач обеспечения защиты информации. ОПК-3.2. Применяет совокупность необходимых математических методов для решения задач обеспечения защиты информации. ОПК-3.3. Разрабатывает, обосновывает и реализует на практике процедуры решения задач обеспечения защиты информации.	**- знать:** основные понятия комплексного анализа; возможные сферы приложения методов комплексного анализа для решения практических задач; **- уметь:** использовать полученные теоретические знания для решения конкретных прикладных задач, производить математические расчеты в стандартных постановках, производить содержательный анализ результатов вычислений; применять совокупность необходимых математических методов для решения задач обеспечения защиты информации; **- владеть:** профессиональным языком предметной области; навыками применения теоретических основ комплексного анализа для составления алгоритмов решения задач практической деятельности.

3. Место дисциплины в структуре образовательной программы

Дисциплина « Комплексный анализ» представляет собой дисциплину обязательной части блока дисциплин подготовки обучающихся.

4. Виды учебной работы по дисциплине.

Виды учебной работы по дисциплине зафиксированы учебным планом основной профессиональной образовательной программы по указанному направлению и профилю, выражаются в академических часах. Часы контактной работы и самостоятельной работы обчающегося и часы, отводимые на процедуры контроля, могут различаться в учебных планах ОПОП по формам обучения. Объем контактной работы включает часы контактной аудиторной работы (лекции/практические занятия/ лабораторные работы), контактной внеаудиторной работы (контроль самостоятельной работы), часы контактной работы в

период аттестации. Контактная работа, в том числе может проводиться посредством электронной информационно-образовательной среды университета с использованием ресурсов сети Интернет и дистанционных технологий

5. Содержание дисциплины, структурированное по темам (разделам)

Исходя из рамок, установленных учебным планом по трудоемкости и видам учебной работы по дисциплине, преподаватель самостоятельно выбирает тематику занятий по формам и количеству часов проведения контактной работы: лекции и иные учебные занятия, предусматривающие преимущественную передачу учебной информации преподавателем и (или) занятия семинарского типа (семинары, практические занятия, практикумы, лабораторные работы, коллоквиумы и иные аналогичные занятия), и (или) групповые консультации, и (или) индивидуальную работу обучающихся с преподавателем, в том числе индивидуальные консультации (по курсовым работам/проектам – при наличии курсовой работы/проекта по данной дисциплине в учебном плане). Рекомендуемая тематика занятий максимально полно реализуется в контактной работе с обучающимися очной формы обучения. В случае реализации образовательной программы в заочной / очно-заочной форме трудоемкость дисциплины сохраняется, однако объем учебного материала в значительной части осваивается обучающимися в форме самостоятельной работы. При этом требования к ожидаемым образовательным результатам обучающихся по данной дисциплине не зависят от формы реализации образовательной программы.

№	Наименование раздела	Содержание раздела
1	Введение в комплексный анализ	Понятие о дисциплине. Основные определения и факты, связанные с комплексными числами. Топология комплексной плоскости. Расширенная комплексная плоскость. Сфера Римана, стереографическая проекция, сферическое расстояние. Топология (расширенной) комплексной плоскости. Предел, непрерывность.
2	Дифференцируемость функций комплексного переменного	Дифференцируемые функции комплексного переменного. Правила дифференцирования (производная и арифметические операции, производная сложной функции, производная обратной функции). Условия Коши-Римана. Аналитические функции. Геометрический смысл аргумента и модуля производной. Понятие о конформных отображениях. Однолистность. Принцип сохранения области. Критерий локальной однолистности.
3	Элементарные аналитические функции	Степенная функция с натуральным показателем, полиномы. Линейная и дробно-линейная функции. Конформность и групповое свойство. Круговое свойство. Неподвижные точки. Сохранение симметрии. Функция Жуковского. Профили Жуковского. Автоморфизмы единичного круга. Понятие о теореме Римана о конформной эквивалентности односвязных областей и о соответствии границ при конформном отображении. Понятие о многозначных аналитических функциях, их точках ветвления.

		Показательная функция и ее свойства (групповое свойство, формула Эйлера, экспоненциальная форма записи комплексных чисел, множество значений, периодичность). Тригонометрические функциии их свойства (четность, периодичность, формулы сложения, множества значений). Гиперболические функции и их свойства (связь с тригонометрическими функциями, формулы сложения, множества значений). Обратные тригонометрические и гиперболические функции. (свойства, выделение однозначной ветви). Логарифмическая функция и ее главное значение, свойства (связь с экспоненциальной функцией, групповое свойство, выделение однозначной ветви). Степенная функция и степень ее многозначности в зависимости от показателя (случаи целого, рационального и иррационального действительного показателя).
4	Интегрирование функций комплексного переменного	Пути и кривые на плоскости. Комплексные криволинейные интегралы. Первообразная, формула Ньютона – Лейбница. Интегральная теорема Коши для простого и составного контуров. Интегральная формула Коши. Интеграл типа Коши. Бесконечная дифференцируемость аналитических функций, формулы Коши для производных аналитических функций. Теорема Морера. Гармонические функции, их связь с аналитическими. Принцип максимума, теорема единственности, теорема о среднем. Интегралы Пуассона и Шварца.
5	Последовательности и ряды аналитических функций	Функциональные последовательности и ряды. Виды сходимости. Сходимость, равномерная внутри области. Теорема Вейерштрасса о последовательностях и рядах аналитических функций. Теорема Рунге. Степенной ряд, теорема Абеля. Радиус сходимости. Формула Коши – Адамара. Аналитичность суммы степенного ряда. Разложение аналитической функции в степенной ряд, единственность разложения, ряд Тейлора. Действия со степенными рядами. Нули аналитической функции, порядок нуля. Теорема единственности для аналитических функций.
6	Ряд Лорана и особые точки однозначного характера	Ряд Лорана, область его сходимости. Разложение аналитической функции в ряд Лорана, единственность разложения. Формулы для коэффициентов разложения, неравенства Коши.Теорема об устранимой особой точке, теорема Лиувилля. Классификация изолированных особых точек однозначного характера. Полюс и существенно особая точка. Случай бесконечно удаленной точки. Теорема Сохоцкого, понятие о теореме Пикара.
7	Теория вычетов и ее	Определение вычета, теорема о вычетах. Формулы

	приложения	для вычисления вычетов. Применение к вычислению интегралов. Логарифмический вычет, принцип аргумента. Теорема Руше, теорема Гурвица. Принцип сохранения области.

6. Рекомендуемая тематика учебных занятий в форме контактной работы

Рекомендуемая тематика учебных занятий *лекционного* типа (предусматривающих преимущественную передачу учебной информации преподавателями):

№	Наименование раздела	Темы лекций
1	Введение в комплексный анализ	Лекция 1. Понятие о дисциплине. Основные определения и факты, связанные с комплексными числами. Лекция 2. Топология комплексной плоскости. Расширенная комплексная плоскость. Сфера Римана, стереографическая проекция, сферическое расстояние. Предел, непрерывность.
2	Дифференцируемость функций комплексного переменного	Лекция 3. Дифференцируемые функции комплексного переменного. Правила дифференцирования (производная и арифметические операции, производная сложной функции, производная обратной функции). Условия Коши-Римана. Лекция 4. Аналитические функции. Геометрический смысл аргумента и модуля производной. Понятие о конформных отображениях. Однолистность. Принцип сохранения области. Критерий локальной однолистности.
3	Элементарные аналитические функции	Лекция 5. Степенная функция с натуральным показателем, полиномы. Линейная и дробно-линейная функции. Конформность и групповое свойство. Круговое свойство. Неподвижные точки. Сохранение симметрии. Лекция 6. Функция Жуковского. Профили Жуковского. Автоморфизмы единичного круга. Понятие о теореме Римана о конформной эквивалентности односвязных областей и о соответствии границ при конформном отображении. Понятие о многозначных аналитических функциях, их точках ветвления. Лекция 7. Показательная функция и ее свойства (групповое свойство, формула Эйлера, экспоненциальная форма записи комплексных чисел, множество значений, периодичность). Лекция 8. Тригонометрические функциии их свойства (четность, периодичность, формулы сложения, множества значений). Гиперболические функции и их свойства (связь с

		тригонометрическими функциями, формулы сложения, множества значений). Обратные тригонометрические и гиперболические функции. (свойства, выделение однозначной ветви). Лекция 9. Логарифмическая функция и ее главное значение, свойства (связь с экспоненциальной функцией, групповое свойство, выделение однозначной ветви). Степенная функция и степень ее многозначности в зависимости от показателя (случаи целого, рационального и иррационального действительного показателя).
4	Интегрирование функций комплексного переменного	Лекция 10. Пути и кривые на плоскости. Комплексные криволинейные интегралы. Первообразная, формула Ньютона – Лейбница. Интегральная теорема Коши для простого и составного контуров. Интегральная формула Коши. Интеграл типа Коши. Лекция 11. Бесконечная дифференцируемость аналитических функций, формулы Коши для производных аналитических функций. Теорема Морера. Лекция 12. Гармонические функции, их связь с аналитическими. Принцип максимума, теорема единственности, теорема о среднем. Интегралы Пуассона и Шварца.
5	Последовательности и ряды аналитических функций	Лекция 13. Функциональные последовательности и ряды. Виды сходимости. Сходимость, равномерная внутри области. Теорема Вейерштрасса о последовательностях и рядах аналитических функций. Теорема Рунге. Лекция 14. Степенной ряд, теорема Абеля. Радиус сходимости. Формула Коши – Адамара. Аналитичность суммы степенного ряда. Разложение аналитической функции в степенной ряд, единственность разложения, ряд Тейлора. Действия со степенными рядами. Нули аналитической функции, порядок нуля. Теорема единственности для аналитических функций.
6	Ряд Лорана и особые точки однозначного характера	Лекция 15. Ряд Лорана, область его сходимости. Разложение аналитической функции в ряд Лорана, единственность разложения. Формулы для коэффициентов разложения, неравенства Коши. Лекция 16. Теорема об устранимой особой точке, теорема Лиувилля. Классификация изолированных особых точек однозначного характера. Полюс и существенно особая точка. Случай бесконечно удаленной точки. Теорема Сохоцкого, понятие о теореме Пикара.
7	Теория вычетов и ее приложения	Лекция 17. Определение вычета, теорема о вычетах. Формулы для вычисления вычетов. Применение к вычислению интегралов. Лекция 18. Логарифмический вычет, принцип

		аргумента. Теорема Руше, теорема Гурвица. Принцип сохранения области.

Рекомендуемая тематика *практических* занятий:

1. Комплексные числа и операции над ними. Алгебраическая и тригонометрическая формы комплексных чисел.
2. Расширенная комплексная плоскость. Сфера Римана, стереографическая проекция.
3. Функция комплексной переменной, ее предел и непрерывность.
4. Пределы и непрерывность функции комплексной переменной.
5. Условия Коши-Римана. Гармонические функции.
6. Аналитические функции.
7. Элементарные аналитические функции.
8. Показательная функция и ее свойства. Логарифмическая функция.
9. Комплексные криволинейные интегралы.
10. Интегральная теорема Коши.
11. Функциональные последовательности и ряды.
12. Степенные ряды.
13. Ряды Лорана.
14. Классификация изолированных особых точек однозначного характера.
15. Определение вычета, теорема о вычетах. Формулы для вычисления вычетов.
16. Приложения теории вычетов.

На практических занятиях решаются задачи по теме занятия.

Требования к самостоятельной работе обучающихся

1. Работа с лекционным материалом, предусматривающая проработку конспекта лекций и учебной литературы, по всем темам из п. 6 настоящей рабочей программы.

2. Выполнение домашнего задания, предусматривающего решение задач, выполнение упражнений, выдаваемых на практических занятиях, по всем темам из п. 6 настоящей рабочей программы.

Руководствуясь положениями статьи 47 и статьи 48 Федерального закона от 29 декабря 2012 г. N 273-ФЗ «Об образовании в Российской Федерации» научно-педагогические работники и иные лица, привлекаемые университетом к реализации данной образовательной программы, пользуются предоставленными академическими правами и свободами в части свободы преподавания, свободы от вмешательства в профессиональную деятельность; свободы выбора и использования педагогически обоснованных форм, средств, методов обучения и воспитания; права на творческую инициативу, разработку и применение авторских программ и методов обучения и воспитания в пределах реализуемой образовательной программы и отдельной дисциплины.

Исходя из рамок, установленных учебным планом по трудоемкости и видам учебной работы по дисциплине, преподаватель самостоятельно выбирает тематику занятий по формам и количеству часов проведения контактной работы: лекции и иные учебные занятия, предусматривающие преимущественную передачу учебной информации преподавателем и (или) занятия семинарского типа (семинары, практические занятия, практикумы, лабораторные работы, коллоквиумы и иные аналогичные занятия), и (или) групповые консультации, и (или) индивидуальную работу обучающихся с преподавателем, в том числе индивидуальные консультации (по курсовым

работам/проектам – при наличии курсовой работы/проекта по данной дисциплине в учебном плане).

Рекомендуемая тематика занятий максимально полно реализуется в контактной работе с обучающимися очной формы обучения. В случае реализации образовательной программы в заочной / очно-заочной форме трудоемкость дисциплины сохраняется, однако объем учебного материала в значительной части осваивается обучающимися в форме самостоятельной работы. При этом требования к ожидаемым образовательным результатам обучающихся по данной дисциплине не зависят от формы реализации образовательной программы.

7. Методические рекомендации по видам занятий

Лекционные занятия.

В ходе лекционных занятий обучающимся рекомендуется выполнять следующие действия. Вести конспектирование учебного материала. Обращать внимание на категории, формулировки, раскрывающие содержание тех или иных явлений и процессов, научные выводы и практические рекомендации по их применению. Задавать преподавателю уточняющие вопросы с целью уяснения теоретических положений, разрешения спорных ситуаций.

Желательно оставить в рабочих конспектах поля, на которых во внеаудиторное время можно сделать пометки из рекомендованной литературы, дополняющие материал прослушанной лекции, а также подчеркивающие особую важность тех или иных теоретических положений.

Практические и семинарские занятия.

На практических и семинарских занятиях в зависимости от темы занятия выполняется поиск информации по решению проблем, практические упражнения, контрольные работы, выработка индивидуальных или групповых решений, итоговое обсуждение с обменом знаниями, участие в круглых столах, разбор конкретных ситуаций, командная работа, представление портфолио и т.п.

Самостоятельная работа.

Самостоятельная работа осуществляется в виде изучения литературы, эмпирических данных по публикациям и конкретных ситуаций из практики, подготовке индивидуальных работ, работа с лекционным материалом, самостоятельное изучение отдельных тем дисциплины; поиск и обзор литературы и электронных источников; чтение и изучение учебника и учебных пособий.

8. Фонд оценочных средств

8.1. Перечень компетенций с указанием этапов их формирования в процессе освоения образовательной программы в рамках учебной дисциплины

Основными этапами формирования указанных компетенций при изучении обучающимися дисциплины являются последовательное изучение содержательно связанных между собой тем учебных занятий. Изучение каждой темы предполагает овладение обучающимися необходимыми компетенциями. Результат аттестации обучающихся на различных этапах формирования компетенций показывает уровень освоения компетенций.

Контролируемые разделы (темы) дисциплины	Индекс контроли-	Оценочные средства по этапам формирования компетенций

	руемой компетенции (или её части)	текущий контроль по дисциплине
1. Введение в комплексный анализ	ОПК-3	Опрос, решение задач, контрольная работа
2. Дифференцируемость функций комплексного переменного	ОПК-3	Опрос, решение задач,
3. Элементарные аналитические функции	ОПК-3	Опрос, решение задач
4. Интегрирование функций комплексного переменного	ОПК-3	Опрос, решение задач
5. Последовательности и ряды аналитических функций	ОПК-3	Опрос, решение задач, контрольная работа
6. Ряд Лорана и особые точки однозначного характера	ОПК-3	Опрос, решение задач
7. Теория вычетов и ее приложения	ОПК-3	Опрос, решение задач,

8.2. Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений и навыков и (или) опыта деятельности процессе текущего контроля

Примеры вопросов для устного опроса:

1. Комплексные числа.
2. Комплексная плоскость.
3. Расширенная комплексная плоскость.
4. Пути и кривые.
5. Области.
6. Понятие функции комплексного переменного.
7. Предел и непрерывность функции.
8. Дифференцируемость и производная.
9. Голоморфная функция.
10. Геометрическая и гидродинамическая интерпретация.
11. Понятие о конформном отображении.
12. Дробно-линейные функции и их свойства.
13. Дробно-линейные изоморфизмы и автоморфизмы.
14. Степенная функция.
15. Показательная функция.
16. Тригонометрические функции.
17. Понятие интеграла по комплексному переменному.
18. Первообразная.
19. Гомотопия. Теорема Коши.
20. Обобщения теоремы Коши.
21. Интегральная формула Коши.

22. Ряд Тейлора и его свойства.
23. Свойства голоморфных функций.
24. Теорема единственности и нули функции.
25. Теорема Вейерштрасса.
26. Ряд Лорана и его свойства.
27. Изолированные особые точки.
28. Целые и мероморфные функции.
29. Вычеты.
30. Применение вычетов.
31. Аналитическое продолжение.
32. Элементарные многозначные аналитические функции (корень, логарифм, обратные тригонометрические функции, степенная функция, показательная функция).
33. Элементарный подход к понятию римановой поверхности.
34. Принцип аргумента и теорема Руше.
35. Принцип максимума модуля и лемма Шварца.
36. Теорема Римана.
37. Соответствие границ при конформном отображении.
38. Гармонические функции.
39. Задача Дирихле.

Типовые контрольные задания:

Контрольная работа по теме:

Операции над комплексными числами.

Геометрическая интерпретация комплексных чисел.

Вариант 1.	***Вариант 2.***
Вычислить: а) $\left(\frac{1-i\sqrt{3}}{1+i}\right)^{45}$; б) $(1+i)^{2-2i}$; 2. Изобразить графически: а) $\lvert z\rvert > 1-\operatorname{Re} z$; б) $\frac{\pi}{4} < \arg \pi z < \frac{\pi}{2}$. 3. Решить уравнение: $e^{ix} = \cos \pi x (x \in R)$.	1. Вычислить а) $\left(\frac{1-i^5}{\sqrt{3}+i}\right)^{70}$ б) $(1-i)^{4i}$; в) $th(1+\pi i)$. 2. Изобразить графически: а) $\lvert z\rvert < 1+\operatorname{Im} z$ б) $\operatorname{Re}(z(1-i)) < \sqrt{2}$ 3. Решить уравнение:

.	$\cos z = \frac{3i}{4}$

Контрольная работа по теме:

Интегрирование функций и ряды.

B-1	B-2
Вычислить интегралы:	Вычислить интегралы:
1.. $\int_L z\bar{z}dz, L:\{\|z\| = 1, Re z \geq 0\}.$	1. $\int_L z\bar{z}dz, L:\{\|z\| = 1, Im z \geq 0\}.$
2. $\int_{\|z\|=5} \frac{dz}{z^2+16}.$	2. $\int_{\|z-i\|=5} \frac{dz}{z^2+16}.$
3. $\int_{\|z\|=\frac{1}{2}} \frac{1-\sin z}{z^2}dz.$	3. $\int_{\|z\|=1} \frac{1-\sin z}{z^3}dz.$
4. Найти радиус и область сходимости ряда: $\sum_{n=1}^{\infty} \frac{3^n+1}{(z+2i)^n}.$	4. Найти радиус и область сходимости ряда: $\sum_{n=1}^{\infty} \frac{3^n}{(z-2i)^n}.$
5. Найти все лорановские разложения f(z) по степеням z: $f(z) = \frac{1}{z^2+1}$	5. Найти все лорановские разложения f(z) по степеням z: $f(z) = \frac{1}{z^2-1}$

8.3. Перечень вопросов и заданий для промежуточной аттестации по дисциплине

Вопросы для промежуточного контроля (зачета)

1. Конечный предел последовательности комплексных чисел.
2. Бесконечный предел последовательности комплексных чисел.
3. Сфера Римана.
4. Ряд комплексных чисел.
5. Функция комплексной переменной.
6. Пределы функции комплексной переменной.
7. Непрерывность функции комплексной переменной.

8. Дифференцируемость функции комплексной переменной. Условия Коши-Римана.
9. Регулярные функции.
10. Экспонента.
11. Тригонометрические функции.
12. Неограниченность синуса.
13. Гармонические функции.
14. Однолистность функции комплексной переменной.
15. Главная ветвь натурального корня.
16. Главная ветвь логарифмической функции.
17. Интеграл функции комплексной переменной по контуру.
18. Свойства интеграла функции комплексной переменной.
19. Интегральная теорема Коши.
20. Расширенная теорема Коши.
21. Обобщенная теорема Коши.
22. Интегральное представление регулярной функции.
23. Бесконечная дифференцируемость интеграла типа Коши и регулярной функции.
24. Теорема Абеля о сходимости степенного ряда.
25. Ряды Тейлора и Маклорена, представление регулярной функции.
26. Две теоремы Вейерштрасса о локально равномерно сходящихся рядах регулярной функции.
27. Свойство единственности регулярной функции.
28. Условие существования регулярной первообразной.
29. Формула Ньютона-Лейбница.
30. Ряд Лорана.
31. Изолированные особые точки.
32. Порядок полюса.
33. Вычет в конечной точке.
34. Два правила вычисления вычетов в полюсах.
35. Вычет в бесконечной точке.
36. Теорема Коши о вычетах и следствие.

8.4. Планируемые уровни сформированности компетенций обучающихся и критерии оценивания

Уровни	Содержательное описание уровня	Основные признаки выделения уровня (этапы формирования компетенции, критерии оценки сформированности)	Пятибалльная шкала (академическая) оценка	Двухбалльная шакала, зачет	БРС, % освоения (рейтинговая оценка)
Повышенный	Творческая деятельность	*Включает нижестоящий уровень.* Умение самостоятельно принимать решение, решать проблему/задачу теоретического и прикладного характера на основе изученных методов, приемов, технологий	отлично	зачтено	86-100

Базовый	Применение знаний и умений в более широких контекстах учебной и профессиональной деятельности, нежели по образцу с большей степени самостоятельности и инициативы	*Включает нижестоящий уровень.* Способность собирать, систематизировать, анализировать и грамотно использовать информацию из самостоятельно найденных теоретических источников и иллюстрировать ими теоретические положения или обосновывать практику применения	хорошо		71-85
Удовлетворительный (достаточный)	Репродуктивная деятельность	Изложение в пределах задач курса теоретически и практически контролируемого материала	удовлетворительно		55-70
Недостаточный	Отсутствие признаков удовлетворительного уровня		неудовлетворительно	не зачтено	Менее 55

9. Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины.

Основная литература

1. Шабунин М. И. Теория функций комплексного переменного [Текст] : учеб. для вузов / М. И. Шабунин, Ю. В. Сидоров, 2013. - 246, [1] с. (Наличие: УА 50 экз., ч.з. №3(1))

Дополнительная литература

1. Шабунин М. И. Сборник задач по теории функций комплексного переменного [Текст] : учеб. пособие для вузов / М. И. Шабунин, Е. С. Половинкин, М. И. Карлов, 2014. - 362 с. (Наличие: УА 50 экз., ч.з. №3(1))
2. Леонтьева Т. А. Задачи по теории функций комплексного переменного [Текст] : [Учеб. пособие для ун-тов и высш. техн. учеб. заведений] / Т. А. Леонтьева, В. С. Панферов, В. С. Серов, 1992. - 253 с. (Наличие: УА 37 экз., ч.з. №3(1))

10. Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины (модуля).

- НЭБ Национальная электронная библиотека, диссертации и прочие издания
- eLIBRARY.RU Научная электронная библиотека, книги, статьи, тезисы докладов конференций
- Гребенников Электронная библиотека ИД журналы

- ЭБС Лань книги, журналы
- ЭБС Консультант студента
- ПРОСПЕКТ ЭБС
- ЭБС ZNANIUM.COM
- РГБ Информационное обслуживание по МБА
- БЕН РАН
- Электронно-библиотечная система (ЭБС) Кантитана (https://elib.kantiana.ru/)

11. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине.

Программное обеспечение обучения включает в себя:

- система электронного образовательного контента БФУ им. И. Канта – www.lms-3.kantiana.ru, обеспечивающую разработку и комплексное использование электронных образовательных ресурсов;
- серверное программное обеспечение, необходимое для функционирования сервера и связи с системой электронного обучения через Интернет;
- корпоративная платформа Microsoft Teams;
- установленное на рабочих местах обучающихся ПО: Microsoft Windows 7, Microsoft Office Standart 2010, антивирусное программное обеспечение Kaspersky Endpoint Security.
- специализированное ПО не требуется.

12. Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине.

Для проведения занятий лекционного типа, практических и семинарских занятий используются специальные помещения (учебные аудитории), оборудованные техническими средствами обучения – мультимедийной проекционной техникой. Для проведения занятий лекционного типа используются наборы демонстрационного оборудования.

Для проведения лабораторных работ, (практических занятий – при необходимости) используются специальные помещения (учебные аудитории), оснащенные специализированным лабораторным оборудованием: персональными компьютерами с возможностью выхода в интернет и с установленным программным обеспечением, заявленным в п.11.

Для проведения групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации используются специальные помещения (учебные аудитории), оборудованные специализированной мебелью (для обучающихся), меловой / маркерной доской.

Для организации самостоятельной работы обучающимся предоставляются помещения, оснащенные компьютерной техникой с возможностью подключения к сети «Интернет» и обеспечением доступа в электронную информационно-образовательную среду университета.

Для обучения инвалидов и лиц с ограниченными возможностями здоровья университетом могут быть представлены специализированные средства обучения, в том числе технические средства коллективного и индивидуального пользования.

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
федеральное государственное автономное образовательное учреждение высшего образования «Балтийский федеральный университет имени Иммануила Канта»
Институт физико-математических наук и информационных технологий

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

«ТЕОРИЯ ВЕРОЯТНОСТЕЙ И МАТЕМАТИЧЕСКАЯ СТАТИСТИКА»

Шифр: 10.05.01
Специальность: «Компьютерная безопасность»
Специализация: «Математические методы защиты информации»
Квалификация (степень) выпускника: Специалист по защите информации

Калининград
2022

Лист согласования

Составитель: Степанов Алексей Васильевич, д.ф.-м.н., профессор

Рабочая программа утверждена на заседании учебно-методического совета института физико-математических наук и информационных технологий

Протокол № 01/22 от «01» февраля 2022 г.

Председатель учебно-методического
совета института физико-
математических наук и информационных
технологий

Первый заместитель директора Шпилевой А. А
ИФМНиИТ, к. ф.-м. н., доцент

Ведущий менеджер Е.П.Ставицкая

Содержание

1.Наименование дисциплины: «Теория вероятностей и математическая статистика».

Цель дисциплины: целью освоения дисциплины «Теория вероятностей и математическая статистика» является формирование математической культуры, овладение студентами математическим аппаратом теории вероятностей и математической статистики, который используется непосредственно для решения прикладных задач и построения вероятностных моделей в различных областях практической деятельности.

2. Перечень планируемых результатов обучения по дисциплине, соотнесенных с планируемыми результатами освоения образовательной программы

Код компетенции	Результаты освоения образовательной программы (ИДК)	Результаты обучения по дисциплине
ОПК-3 Способен на основании совокупности математических методов разрабатывать, обосновывать и реализовывать процедуры решения задач профессиональной деятельности.	ОПК-3.1. Знает необходимые математические методы для решения задач обеспечения защиты информации. ОПК-3.2. Применяет совокупность необходимых математических методов для решения задач обеспечения защиты информации. ОПК-3.3. Разрабатывает, обосновывает и реализует на практике процедуры решения задач обеспечения защиты информации.	**-знать:** – основные методы и модели теории вероятностей и математической статистики; – о возможностях, предоставляемых точными науками по интерпретации и обобщению научных исследований; – знать о возможностях, предоставляемых теорией вероятностей при решении прикладных задач; **уметь** применять стандартные методы и модели к решению типовых теоретико-вероятностных и статистических задач; **владеть практическими навыками**: – использования математического аппарата теории вероятностей для решения конкретных задач; – навыками по поиску дополнительного материала по каждой теме курса; – навыками формализации задач, составления алгоритмов решения, пригодных для последующего программирования; – владеть профессиональным

		языком предметной области знания

3. Место дисциплины в структуре образовательной программы

Дисциплина «Теория вероятностей и математическая статистика» представляет собой дисциплину обязательной части блока дисциплин подготовки обучающихся.

4. Виды учебной работы по дисциплине.

Виды учебной работы по дисциплине зафиксированы учебным планом основной профессиональной образовательной программы по указанному направлению и профилю, выражаются в академических часах. Часы контактной работы и самостоятельной работы обучающегося и часы, отводимые на процедуры контроля, могут различаться в учебных планах ОПОП по формам обучения. Объем контактной работы включает часы контактной аудиторной работы (лекции/практические занятия/ лабораторные работы), контактной внеаудиторной работы (контроль самостоятельной работы), часы контактной работы в период аттестации. Контактная работа, в том числе может проводиться посредством электронной информационно-образовательной среды университета с использованием ресурсов сети Интернет и дистанционных технологий

5. Содержание дисциплины, структурированное по темам (разделам)

Исходя из рамок, установленных учебным планом по трудоемкости и видам учебной работы по дисциплине, преподаватель самостоятельно выбирает тематику занятий по формам и количеству часов проведения контактной работы: лекции и иные учебные занятия, предусматривающие преимущественную передачу учебной информации преподавателем и (или) занятия семинарского типа (семинары, практические занятия, практикумы, лабораторные работы, коллоквиумы и иные аналогичные занятия), и (или) групповые консультации, и (или) индивидуальную работу обучающихся с преподавателем, в том числе индивидуальные консультации (по курсовым работам/проектам – при наличии курсовой работы/проекта по данной дисциплине в учебном плане). Рекомендуемая тематика занятий максимально полно реализуется в контактной работе с обучающимися очной формы обучения. В случае реализации образовательной программы в заочной / очно-заочной форме трудоемкость дисциплины сохраняется, однако объем учебного материала в значительной части осваивается обучающимися в форме самостоятельной работы. При этом требования к ожидаемым образовательным результатам обучающихся по данной дисциплине не зависят от формы реализации образовательной программы.

№	Наименование раздела	Содержание раздела
1	Пространство элементарных событий	Пространство событий. Операции над событиями. Алгебра событий. Измеримое пространство. Вероятность случайных событий. Комбинаторно-вероятностные схемы. Аксиоматика Колмогорова. Вероятностная мера и вероятностное пространство. Свойства вероятности. Условная вероятность. Независимость событий. Теорема умножения вероятностей. Формула полной вероятности и формула Байеса.
2	Биномиальное распределение	Биномиальная и полиномиальная схемы независимых испытаний. Локальная и интегральная

		предельные теоремы Муавра-Лапласа. Теорема Пуассона.
3	Случайная величина. Функция распределения.	Определение и описание случайной величины: функция распределения и плотность распределения вероятностей, их свойства. Основные дискретные и абсолютно непрерывные распределения: биномиальное, геометрическое, пуассоновское, нормальное, показательное, равномерное, распределение Стьюдента.
4	Многомерные случайные величины.	Многомерные случайные величины: функция распределения вероятностей многомерных случайных величин, их свойства. Ковариация случайных величин. Коэффициент корреляции и его свойства. Корреляционная матрица. Совместная функция распределения случайных величин. Дискретные и абсолютно случайные непрерывные векторы. Независимость случайных величин. Критерии независимости дискретных и абсолютно непрерывных случайных величин. Распределение функции от случайных величин. Свертка распределений.
5	Числовые характеристики случайной величины	Интеграл Лебега от случайной величины по вероятностной мере на пространстве элементарных событий. Математическое ожидание случайной величины и его свойства. Интеграл Лебега–Стилтьеса и его связь с интегралом Лебега. Вычислительные формулы для математических ожиданий дискретных и абсолютно непрерывных случайных величин. Математические ожидания и дисперсии типовых распределений. Моменты случайных величин. Дисперсия случайной величины и ее свойства. Основные неравенства классической теории вероятностей: неравенства Чебышева, неравенства Маркова. Ковариация и коэффициент корреляции, их свойства. Понятие об условном математическом ожидании. Условная плотность.
6	Предельные теоремы	Типы сходимости случайных величин. Теоремы, связывающие различные типы сходимостей. Неравенство Чебышева. Центральная предельная теорема. Теорема непрерывности. Условие Линдберга. Центральная теорема в форме Линдберга. Теорема Ляпунова. Закон больших чисел. Теорема Бернулли. Теорема Хинчина. Усиленный закон больших чисел Колмогорова. Теорема Бореля.
7	Цепи Маркова	Определение марковского процесса. Уравнение Колмогорова-Чепмена. Классификация состояний марковской цепи. Эргодическая теорема. Определение марковского процесса. Уравнение Колмогорова-Чепмена. Матрица интенсивностей и её свойства. Система дифференциальных уравнений Колмогорова, е решение. Предельное распределение

		вероятностей. Простейший поток событий. Пуассоновский процесс. Процессы размножения и гибели.
8	Статистические модели. Вариационный ряд и его характеристики.	Статистические модели и основные задачи статистического анализа, примеры; экспоненциальные семейства. Вариационный ряд. Эмпирическая функция распределения. Теорема Гливенко. Теорема Колмогорова об оценке неизвестной функции распределения. Выборочные распределения. Асимптотические распределения выборочных моментов.
9	Статистическое оценивание неизвестных параметров распределения.	Статистическое оценивание. Состоятельные, несмещённые, эффективные оценки. Неравенство информации. Достаточные статистики. Условное распределение, условное математическое ожидание. Улучшение несмещенной оценки посредством усреднения по достаточной статистике. Полные достаточные статистики. Наилучшие несмещенные оценки. Теорема факторизации.
10	Методы оценивания.	Метод максимального правдоподобия и метод моментов
11	Оценки наибольшего правдоподобия.	Оценки наибольшего правдоподобия, их состоятельность. Понятие асимптотической нормальности случайной последовательности. Асимптотическая нормальность оценок максимального правдоподобия. Примеры преобразований, стабилизирующих экспертные оценки.
12	Метод наименьших квадратов.	Метод наименьших квадратов. Ортогональные планы. Анализ нормальной выборки. Свойства оценок метода наименьших квадратов. Теорема Гаусса - Маркова.
13	Доверительные интервалы.	Интервальные оценки. Нахождение доверительных и асимптотически доверительных интервалов.
14	Проверка статистических гипотез.	Проверка статистических гипотез, основные понятия. Ошибки первого и второго рода. Лемма Неймана-Пирсона. Равномерно наиболее мощные критерии, примеры. Проверка гипотез значимости. Критерии К. Пирсона «хи-квадрат» и Колмогорова.

6. Рекомендуемая тематика учебных занятий в форме контактной работы

Рекомендуемая тематика учебных занятий *лекционного* типа (предусматривающих преимущественную передачу учебной информации преподавателями):

№	Наименование раздела	Темы лекций
1	Пространство элементарных событий	Лекция 1. Дискретное пространство элементарных событий. Лекция 2. Произвольное пространство

		элементарных событий.
2	Биномиальное распределение	Лекция 3. Биномиальное распределение.
3	Случайная величина. Функция распределения.	Лекция 4. Случайная величина. Функция распределения.
4	Многомерные случайные величины.	Лекция 5. Многомерные случайные величины
5	Числовые характеристики случайной величины.	Лекция 6. Числовые характеристики случайной величины.
6	Предельные теоремы.	Лекция 7. Сходимость случайных величин. Лекция 8. Центральная предельная теорема. Лекция 9. Закон больших чисел.
7	Цепи Маркова.	Лекция 10. Дискретные цепи Маркова Лекция 11. Марковские процессы с дискретным множеством состояний и непрерывным временем.
8	Статистические модели. Вариационный ряд и его характеристики.	Лекции 12. Статистические модели. Вариационный ряд и его характеристики.
9	Статистическое оценивание неизвестных параметров распределения.	Лекция 13. Статистическое оценивание неизвестных параметров распределения.
10	Методы оценивания.	Лекции 14. Методы оценивания.
11	Оценки наибольшего правдоподобия.	Лекция 15. Оценки наибольшего правдоподобия
12	Метод наименьших квадратов.	Лекция 16. Метод наименьших квадратов.
13	Доверительные интервалы.	Лекция 17. Доверительные интервалы.
14	Проверка статистических гипотез.	Лекция 18. Проверка статистических гипотез.

Рекомендуемая тематика *практических* занятий:

Тема 1. Дискретное пространство элементарных событий
Тема 2. Произвольное пространство элементарных событий
Тема 3. Биномиальное распределение
Тема 4. Случайная величина. Функция распределения
Тема 5. Многомерные случайные величины
Тема 6. Числовые характеристики случайной величины.
Тема 7. Сходимость случайных величин
Тема 8. Центральная предельная теорема
Тема 9. Закон больших чисел
Тема 10. Дискретные цепи Маркова
Тема 11. Марковские процессы с дискретным множеством состояний и непрерывным временем.
Тема 12. Статистические модели. Вариационный ряд и его характеристики
Тема 13. Статистическое оценивание неизвестных параметров распределения
Тема 14. Методы оценивания.
Тема 15. Оценки наибольшего правдоподобия

Тема 16. Метод наименьших квадратов
Тема 17. Доверительные интервалы
Тема 18. Проверка статистических гипотез

На практических занятиях решаются задачи по теме занятия.

Требования к самостоятельной работе обучающихся

1. Работа с лекционным материалом, предусматривающая проработку конспекта лекций и учебной литературы, по всем темам из п. 6 настоящей рабочей программы.
2. Выполнение домашнего задания, предусматривающего решение задач, выполнение упражнений, выдаваемых на практических занятиях, по всем темам из п. 6 настоящей рабочей программы.

Руководствуясь положениями статьи 47 и статьи 48 Федерального закона от 29 декабря 2012 г. N 273-ФЗ «Об образовании в Российской Федерации» научно-педагогические работники и иные лица, привлекаемые университетом к реализации данной образовательной программы, пользуются предоставленными академическими правами и свободами в части свободы преподавания, свободы от вмешательства в профессиональную деятельность; свободы выбора и использования педагогически обоснованных форм, средств, методов обучения и воспитания; права на творческую инициативу, разработку и применение авторских программ и методов обучения и воспитания в пределах реализуемой образовательной программы и отдельной дисциплины.

Исходя из рамок, установленных учебным планом по трудоемкости и видам учебной работы по дисциплине, преподаватель самостоятельно выбирает тематику занятий по формам и количеству часов проведения контактной работы: лекции и иные учебные занятия, предусматривающие преимущественную передачу учебной информации преподавателем и (или) занятия семинарского типа (семинары, практические занятия, практикумы, лабораторные работы, коллоквиумы и иные аналогичные занятия), и (или) групповые консультации, и (или) индивидуальную работу обучающихся с преподавателем, в том числе индивидуальные консультации (по курсовым работам/проектам – при наличии курсовой работы/проекта по данной дисциплине в учебном плане).

Рекомендуемая тематика занятий максимально полно реализуется в контактной работе с обучающимися очной формы обучения. В случае реализации образовательной программы в заочной / очно-заочной форме трудоемкость дисциплины сохраняется, однако объем учебного материала в значительной части осваивается обучающимися в форме самостоятельной работы. При этом требования к ожидаемым образовательным результатам обучающихся по данной дисциплине не зависят от формы реализации образовательной программы.

7. Методические рекомендации по видам занятий

Лекционные занятия.

В ходе лекционных занятий обучающимся рекомендуется выполнять следующие действия. Вести конспектирование учебного материала. Обращать внимание на категории, формулировки, раскрывающие содержание тех или иных явлений и процессов, научные выводы и практические рекомендации по их применению. Задавать преподавателю

уточняющие вопросы с целью уяснения теоретических положений, разрешения спорных ситуаций.

Желательно оставить в рабочих конспектах поля, на которых во внеаудиторное время можно сделать пометки из рекомендованной литературы, дополняющие материал прослушанной лекции, а также подчеркивающие особую важность тех или иных теоретических положений.

Практические и семинарские занятия.

На практических и семинарских занятиях в зависимости от темы занятия выполняется поиск информации по решению проблем, практические упражнения, контрольные работы, выработка индивидуальных или групповых решений, итоговое обсуждение с обменом знаниями, участие в круглых столах, разбор конкретных ситуаций, командная работа, представление портфолио и т.п.

Самостоятельная работа.

Самостоятельная работа осуществляется в виде изучения литературы, эмпирических данных по публикациям и конкретных ситуаций из практики, подготовке индивидуальных работ, работа с лекционным материалом, самостоятельное изучение отдельных тем дисциплины; поиск и обзор литературы и электронных источников; чтение и изучение учебника и учебных пособий.

8. Фонд оценочных средств

8.1. Перечень компетенций с указанием этапов их формирования в процессе освоения образовательной программы в рамках учебной дисциплины

Основными этапами формирования указанных компетенций при изучении обучающимися дисциплины являются последовательное изучение содержательно связанных между собой тем учебных занятий. Изучение каждой темы предполагает овладение обучающимися необходимыми компетенциями. Результат аттестации обучающихся на различных этапах формирования компетенций показывает уровень освоения компетенций.

Контролируемые разделы (темы) дисциплины	Индекс контроли-руемой компетенции (или её части)	Оценочные средства по этапам формирования компетенций
		текущий контроль по дисциплине
Пространство элементарных событий	ОПК-3	Опрос, решение задач.
Биномиальное распределение	ОПК-3	Опрос, решение задач, контрольная работа
Случайная величина. Функция распределения.	ОПК-3	Опрос, решение задач
Многомерные случайные величины.	ОПК-3	Опрос, решение задач
Числовые характеристики случайной величины.	ОПК-3	Опрос, решение задач
Предельные теоремы.	ОПК-3	Опрос, решение задач
Цепи Маркова.	ОПК-3	Опрос, решение задач,
Статистические модели. Вариационный ряд и его	ОПК-3	Опрос, решение задач, контрольная работа

Контролируемые разделы (темы) дисциплины	Индекс контроли-руемой компетенции (или её части)	Оценочные средства по этапам формирования компетенций
		текущий контроль по дисциплине
характеристики.		
Статистическое оценивание неизвестных параметров распределения.	ОПК-3	Опрос, решение задач
Методы оценивания.	ОПК-3	Опрос, решение задач
Оценки наибольшего правдоподобия.	ОПК-3	Контрольная работа
Метод наименьших квадратов.	ОПК-3	Решение задач
Доверительные интервалы.	ОПК-3	Опрос, решение задач
Проверка статистических гипотез.	ОПК-3	Консультация, опрос, самостоятельная работа

8.2. Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений и навыков и (или) опыта деятельности процессе текущего контроля

Примеры вопросов для устного опроса:

Тема 4. Случайная величина. Функция распределения.

1. Случайная величина.
2. Функция распределения и её свойства.
3. Дискретные случайные величины и их описание.
4. Примеры дискретных случайных величин.
5. Биномиальное распределение.
6. Распределение Пуассона.
7. Абсолютно непрерывные случайные величины их описание.
8. Плотность распределения одномерной случайной величины и ее свойства.
9. Примеры абсолютно непрерывных случайных величин.
10. Равномерное распределение.
11. Показательный закон.
12. Нормальное распределение.

Тема 6. Числовые характеристики случайной величины.

1.Интеграл Лебега-Стилтьеса.
2.Математическое ожидание и его свойства.
3.Дисперсия и её свойства.
4.Моменты случайной величины и их применение.
5. Мода, медиана.

Типовые контрольные задания:

Контрольная работа по темам 4 и 6

1. В урне имеются четыре шара под номерами 1,2,3. Вынули один за другим 2 шара. Найти ряд распределения, функцию распределения, математическое ожидание и дисперсию разности номеров вынутых шаров.
2. Плотность распределения случайной величины ξ имеет вид

$$f(x)=a\, e^{-|x|} \quad (-\infty < x < \infty).$$

Найти параметр a, функцию распределения, математическое ожидание, дисперсию, моду и медиану этой случайной величины.

3. Вероятность поломки каждого из 5 работающих станков равна 0,08. Найдите функцию распределения количества сломанных станков.
4. Многократно измеряют некоторую величину. Вероятность того, что эта величина по модулю не превзойдёт 10, равна 0,99. Найти систематическую ошибку прибора, если среднеквадратическая ошибка измерений равна 1 и ошибки измерения распределены по нормальному закону.

Контрольная работа по темам 3 и 5

1. Рыбак забросил спиннинг 80 раз. Какова вероятность того, что он поймал хотя бы одну рыбу, если одна рыба приходится в среднем на 200 забрасываний?
2. Случайная величина X равномерно распределена на интервале (-a, a). Найти математическое ожидание и дисперсию случайной величины У=5X-2a.
3. Известно распределение случайного вектора (X,Y)

	X = 2	X = 4	X = 6
Y = –2	0,1	0,1	0,3
Y = –4	0,2	0,2	0,1

Выясните, зависимы ли события XY № 0 и X + Y = 0.

Найдите ковариацию X и У, ряд распределения величины Z=X+У.

4.. В здании включено 2000 ламп. Вероятность перегорания каждой равна 0,05. Найти вероятность того, что перегорит не более 50. Оценить вероятность того, что абсолютная величина разности между числом работающих ламп и средним числом исправных ламп, окажется меньше 40.

5.. Производится 12 независимых испытаний с вероятностью успеха 0,1 в каждом испытании. Пусть X – число успехов в испытаниях с номерами 1,2,…,6, Y – число успехов в испытаниях с номерами 4,5,…,12. Найдите дисперсию D[X+2Y].

8.3. Перечень вопросов и заданий для промежуточной аттестации по дисциплине

Вопросы для промежуточного контроля (экзамен)

1.Дискретное вероятностное пространство.
2.Аксиомы теории вероятностей для произвольного вероятностного пространства.
3.Вероятность события (классическое, геометрическое, статистическое определения, вероятностная мера)
4.Свойства вероятности.

5.Условная вероятность. Теорема умножения. Независимость событий.
6.Формула полной вероятности.
7.Формула Байеса.
8.Математическая модель n независимых опытов (схема Бернулли). Биномиальное распределение.
9.Случайная величина. Функция распределения и её свойства.
10.Дискретные случайные величины и их описание.
11.Примеры дискретных случайных величин. Биномиальное распределение. Распределение Пуассона.
12.Абсолютно непрерывные случайные величины их описание. Плотность распределения одномерной случайной величины и ее свойства.
13.Примеры абсолютно непрерывных случайных величин. Равномерное распределение. Показательный закон. Нормальное распределение.
14.Многомерная случайная величина. Функция распределения многомерной случайной величины и её свойства.
15.Независимые случайные величины.
16.Распределение суммы независимых случайных величин.
17.Функции от случайных величин.
18.Интеграл Лебега-Стилтьеса.
19.Математическое ожидание и его свойства.
20.Дисперсия и её свойства.
21.Моменты случайной величины и их применение. Мода, медиана.
22.Условные законы распределения и числовые характеристики случайной величины.
23.Ковариация случайных величин и её свойства.
24.Коэффициент корреляции случайных величин и его свойства.
25.Сходимость случайных величин.
26.Неравенство Чебышева.
27.Теорема Пуассона для одинаково распределенных случайных величин.
28.Локальная теорема Муавра-Лапласа.
29.Интегральная теорема Муавра-Лапласа.
30.Центральная предельная теорема в простейшей форме.
31.Центральная предельная теорема в форме Линдеберга.
32.Сходимость к нормальному распределению в форме Ляпунова.
33.Закон больших чисел. Теорема Бернулли.

Вопросы для промежуточного контроля (зачет с оценкой)

1. Определение, классификация и описание случайного процесса.
2. Определение дискретной цепи Маркова.
3. Однородная дискретная цепь Маркова.
4. Уравнения Колмогорова-Чепмена.
5. Классификация состояний дискретной цепи Маркова.
6. Эргодическая цепь Маркова.
7. Марковские случайные процессы с дискретным множеством состояний и непрерывным временем.
8. Простейший поток событий.
9. Пуассоновский случайный процесс.
10. Предельное распределение вероятностей.
11. Процесс размножения и гибели.
12. Вариационный и статистический ряд, Полигон и гистограмма.

13. Эмпирическая функция распределения и ее свойства Теоремы Гливенко и Колмогорова
14. Распределение Фишера
15. Распределение Стъюдента.
16. χ^2 распределение
17. Выборочное среднее и его свойства.
18. Выборочная дисперсия и ее свойства.
19. Выборочные начальные моменты и их свойства.
20. Выборочные центральные моменты и их свойства.
21. Асимптотические свойства выборочного распределения
22. Статистическая оценка. Несмещенные оценки. Примеры несмещенных оценок.
23. Состоятельные оценки. Примеры.
24. Метод моментов
25. Метод наибольшего правдоподобия
26. Эффективные оценки. Неравенство Рао-Крамера.
27. Асимптотически эффективные оценки.
28. Достаточные статистики. Критерий Неймана-Пирсона.
29. Метод доверительных интервалов.
30. Проверка гипотез. Ошибки 1 и 2 рода.
31. Общая схема проверки гипотез.
32. Критерий проверки. Критическая область.

Критерий согласия

8.4. Планируемые уровни сформированности компетенций обучающихся и критерии оценивания

Уровни	Содержательное описание уровня	Основные признаки выделения уровня (этапы формирования компетенции, критерии оценки сформированности)	Пятибалльная шкала (академическая) оценка	Двухбалльная шакала, зачет	БРС, % освоения (рейтинговая оценка)
Повышенный	Творческая деятельность	*Включает нижестоящий уровень.* Умение самостоятельно принимать решение, решать проблему/задачу теоретического и прикладного характера на основе изученных методов, приемов, технологий	отлично	зачтено	86-100
Базовый	Применение знаний и умений в более широких контекстах учебной и	*Включает нижестоящий уровень.* Способность собирать, систематизировать, анализировать и грамотно использовать информацию из	хорошо		71-85

	профессиональной деятельности, нежели по образцу с большей степени самостоятельности и инициативы	самостоятельно найденных теоретических источников и иллюстрировать ими теоретические положения или обосновывать практику применения			
Удовлетворительный (достаточный)	Репродуктивная деятельность	Изложение в пределах задач курса теоретически и практически контролируемого материала	удовлетворительно		55-70
Недостаточный	Отсутствие признаков удовлетворительного уровня		неудовлетворительно	не зачтено	Менее 55

9. Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины.

Основная литература

1. Коган, Е. А. Теория вероятностей и математическая статистика : учебник / Е.А. Коган, А.А. Юрченко. — Москва : ИНФРА-М, 2021. — 250 с. — (Высшее образование: Бакалавриат). — DOI 10.12737/textbook_5cde54d3671a96.35212605. - ISBN 978-5-16-014235-7. - Текст : электронный. - URL: https://znanium.com/catalog/product/1541962 (дата обращения: 06.04.2022). – Режим доступа: по подписке.
2. Бочаров, П. П. Теория вероятностей. Математическая статистика [Электронный ресурс] / П. П. Бочаров, А. В. Печинкин. - 2-е изд. - Москва : ФИЗМАТЛИТ, 2005. - 296 с. - ISBN 5-9221-0633-3. - Текст : электронный. - URL: https://znanium.com/catalog/product/405754 (дата обращения: 06.04.2022). – Режим доступа: по подписке.

Дополнительная литература

3. Ананьевский, С. М. Теория вероятностей с примерами и задачами: Учебное пособие / Ананьевский С.М., Невзоров В.Б. - СПб:СПбГУ, 2013. - 240 с.: ISBN 978-5-288-05491-4. - Текст : электронный. - URL: https://znanium.com/catalog/product/940734 (дата обращения: 06.04.2022). – Режим доступа: по подписке.
4. Корчагин, В. В. Теория вероятностей и математическая статистика : практикум / В. В. Корчагин, С. В. Белокуров, Р. В. Кузьменко. - Воронеж : Воронежский институт ФСИН России, 2019. - 162 с. - Текст : электронный. - URL: https://znanium.com/catalog/product/1086219 (дата обращения: 06.04.2022). – Режим доступа: по подписке.

5. Двойцова, И. Н. Элементы теории вероятностей и математической статистики : учебное пособие / И. Н. Двойцова. - Железногорск : ФГБОУ ВО Сибирская пожарно-спасательная академия ГПС МЧС России, 2021. - 136 с. - Текст : электронный. - URL: https://znanium.com/catalog/product/1844137 (дата обращения: 06.04.2022). – Режим доступа: по подписке.

10. Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины (модуля).

- НЭБ Национальная электронная библиотека, диссертации и прочие издания
- eLIBRARY.RU Научная электронная библиотека, книги, статьи, тезисы докладов конференций
- Гребенников Электронная библиотека ИД журналы
- ЭБС Лань книги, журналы
- ЭБС Консультант студента
- ПРОСПЕКТ ЭБС
- ЭБС ZNANIUM.COM
- РГБ Информационное обслуживание по МБА
- БЕН РАН
- Электронно-библиотечная система (ЭБС) Кантитана (https://elib.kantiana.ru/)

11. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине.

Программное обеспечение обучения включает в себя:

- система электронного образовательного контента БФУ им. И. Канта – www.lms-3.kantiana.ru, обеспечивающую разработку и комплексное использование электронных образовательных ресурсов;
- серверное программное обеспечение, необходимое для функционирования сервера и связи с системой электронного обучения через Интернет;
- корпоративная платформа Microsoft Teams;
- установленное на рабочих местах обучающихся ПО: Microsoft Windows 7, Microsoft Office Standart 2010, антивирусное программное обеспечение Kaspersky Endpoint Security.
- специализированное ПО не требуется.

12. Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине.

Для проведения занятий лекционного типа, практических и семинарских занятий используются специальные помещения (учебные аудитории), оборудованные техническими средствами обучения – мультимедийной проекционной техникой. Для проведения занятий лекционного типа используются наборы демонстрационного оборудования.

Для проведения лабораторных работ, (практических занятий – при необходимости) используются специальные помещения (учебные аудитории), оснащенные специализированным лабораторным оборудованием: персональными компьютерами с

возможностью выхода в интернет и с установленным программным обеспечением, заявленным в п.11.

Для проведения групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации используются специальные помещения (учебные аудитории), оборудованные специализированной мебелью (для обучающихся), меловой / маркерной доской.

Для организации самостоятельной работы обучающимся предоставляются помещения, оснащенные компьютерной техникой с возможностью подключения к сети «Интернет» и обеспечением доступа в электронную информационно-образовательную среду университета.

Для обучения инвалидов и лиц с ограниченными возможностями здоровья университетом могут быть представлены специализированные средства обучения, в том числе технические средства коллективного и индивидуального пользования.

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
федеральное государственное автономное образовательное учреждение высшего образования «Балтийский федеральный университет имени Иммануила Канта»
Институт физико-математических наук и информационных технологий

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

«Языки программирования»

Шифр: 10.05.01
Специальность: «Компьютерная безопасность»
Специализация: «Математические методы защиты информации»
Квалификация (степень) выпускника: специалист по защите информации

Калининград
2022

Лист согласования

Составитель: Верещагин Сергей Верещагин, к.ф.-м.н., доцент

Рабочая программа утверждена на заседании учебно-методического совета института физико-математических наук и информационных технологий

Протокол № 01/22 от «01» февраля 2022 г.

Председатель учебно-методического
совета института физико-
математических наук и информационных
технологий

Первый заместитель директора Шпилевой А. А
ИФМНиИТ, к. ф.-м. н., доцент

Ведущий менеджер Е.П.Ставицкая

Содержание

1.Наименование дисциплины: «Языки программирования».

Цель дисциплины: целью освоения дисциплины «Языки программирования» является фундаментальная и практическая подготовка обучающихся в области методы программирования.

2. Перечень планируемых результатов обучения по дисциплине, соотнесенных с планируемыми результатами освоения образовательной программы

Код компетенции	Результаты освоения образовательной программы (ИДК)	Результаты обучения по дисциплине
ОПК-7. Способен создавать программы на языках высокого и низкого уровня, применять методы и инструментальные средства программирования для решения профессиональных задач, осуществлять обоснованный выбор инструментария программирования и способов организации программ;	ОПК-7.1. Разрабатывает программы на языках высокого и низкого уровня. ОПК-7.2. Применяет известные методы программирования и возможности базового языка программирования для решения типовых профессиональных задач. ОПК-7.3. Осуществляет обоснованный выбор инструментария программирования и способов организации программ.	**Знать:** - Синтаксис языка С++ - Синтаксис основных библиотек языка С++ - Основные способы организации данных в языке С++ - Синтаксис основных библиотек языка С++, их особенности, достоинства и недостатки - Основные способы организации данных в языке С++, их особенности, достоинства и недостатки **уметь:** - писать программы на языке С++ - подключать дополнительные библиотеки - находить и исправлять ошибки в коде - оптимизировать программный код **владеть:** - навыками практической работы с IDE языка С++ - навыками поиска информации о библиотеках языка С++, чтения их документации
ОПК-13. Способен разрабатывать компоненты	ОПК-13.1. Знает принципы функционирования программных и программно-	- **Знать:** - Принципы написания безопасного кода на языке С++

программных и программно-аппаратных средств защиты информации в компьютерных системах и проводить анализ их безопасности;	аппаратных средств защиты информации в компьютерных системах, принципы и методы разработки их компонент, методики анализа их безопасности. ОПК-13.2. Способен разрабатывать компоненты программных и программно-аппаратных средств защиты информации в компьютерных системах ОПК-13.3. Способен проводить анализ безопасности компонент программных и программно-аппаратных средств защиты информации в компьютерных системах	- Особенности реализации обработки ошибок и работы с памятью на языке Python - Способы обезопашивания ввода на языке C++ - Основы использования криптографических библиотек в языке C++ - **уметь:** - Писать код на языке C++ корректно обрабатывающий пользовательский ввод, возможные ошибочные ситуации - Применять стандартные криптографическое библиотеки - **владеть:** - Навыками идентификации небезопасного кода и исправления его - средствами автоматизированного тестирования кода

3. Место дисциплины в структуре образовательной программы

Дисциплин «Языки программирования» входит в базовую часть (Б1.О.07.01) обязательной части блока дисциплин (модулей) подготовки специалистов по специальности 10.05.01«Компьютерная безопасность», специализация N 2 "Математические методы защиты информации"

4. Виды учебной работы по дисциплине.

Виды учебной работы по дисциплине зафиксированы учебным планом основной профессиональной образовательной программы по указанному направлению и профилю, выражаются в академических часах. Часы контактной работы и самостоятельной работы обучающегося и часы, отводимые на процедуры контроля, могут различаться в учебных планах ОПОП по формам обучения. Объем контактной работы включает часы контактной аудиторной работы (лекции/практические занятия/ лабораторные работы), контактной внеаудиторной работы (контроль самостоятельной работы), часы контактной работы в период аттестации. Контактная работа, в том числе может проводиться посредством электронной информационно-образовательной среды университета с использованием ресурсов сети Интернет и дистанционных технологий

5. Содержание дисциплины, структурированное по темам (разделам)

Исходя из рамок, установленных учебным планом по трудоемкости и видам учебной работы по дисциплине, преподаватель самостоятельно выбирает тематику занятий по формам и количеству часов проведения контактной работы: лекции и иные учебные занятия, предусматривающие преимущественную передачу учебной информации преподавателем и (или) занятия семинарского типа (семинары, практические занятия, практикумы, лабораторные работы, коллоквиумы и иные аналогичные занятия), и (или) групповые консультации, и (или) индивидуальную работу обучающихся с

преподавателем, в том числе индивидуальные консультации (по курсовым работам/проектам – при наличии курсовой работы/проекта по данной дисциплине в учебном плане). Рекомендуемая тематика занятий максимально полно реализуется в контактной работе с обучающимися очной формы обучения. В случае реализации образовательной программы в заочной / очно-заочной форме трудоемкость дисциплины сохраняется, однако объем учебного материала в значительной части осваивается обучающимися в форме самостоятельной работы. При этом требования к ожидаемым образовательным результатам обучающихся по данной дисциплине не зависят от формы реализации образовательной программы.

№	Наименование раздела	Содержание раздела
1	Тема 1. Общее понятие о программировании. Виды языков программирования. Язык C++	Общее понятие о программировании. Виды языков программирования. Компиляция и интерпретация. Языки C, C++, C#
2	Тема 2. Базовые типы данных языка C++	Int,long, long int. float, double long double. Bool. Char. Unsigned, const.
3	Тема 3. Условия и циклы	if..else, условия, while, do..while, for. Break и continue.
4	Тема 4. Функции. Lamda-выпаженния	Функции. Возврат и передача значений. Рекрсия. Анонимные функции.
5	Тема 5. Структуры данных	Массивы и строки в C. Struct, union, enum
6	Тема 6. Ввод/вывод в C и C++. Работа с файлами	Printf и scanf. Cin и cout. Библиотека fstream
7	Тема 7. Ссылки и указатели. Динамическое выделение памяти	Ссылки и указатели.Зачем они нужны, чем отличаются и что у них общего. New и delete. Указатели на функции.
8	Тема 8. Классы, ООП.	Общее понятие класса.Методы. Инкапсуляция, абстракция, полиморфизм. Public, private, protected. Friend
9	Тема 9. Конструкторы и деструкторы	Конструкторы и деструкторы. Конструктор копирования. Преобразование типов.
10	Тема 10. Переопределение операторов	Переопределение стандартных операторов Переопределение операторов ввода вывода. Оператор []. Оператор ().
11	Тема 11. Наследование	Наследование. Virtual, Абстрактные классы. Множественно наследование

12	Тема 12. Шаблоны	Шаблоны templates. Множественность типов данных в шаблонах
13	Тема 13 Классы-контейнеры STL. Итераторы	STL. <string>,<vector>,<list>, <set>,<map>,<deque>. Итераторы. Пользовательские классы-контейнеры
14	Тема 14. Исключения и их обработка	Исключения. Try..throw..catch. Класс Exception
15	Тема 15. Стандартные библиотеки языка С и С++	Стандартные библиотеки языков С и С++. Algorithm.h.

6. Рекомендуемая тематика учебных занятий в форме контактной работы

Рекомендуемая тематика учебных занятий *лекционного* типа (предусматривающих преимущественную передачу учебной информации преподавателями):

№	Наименование раздела	Темы лекций
1	Тема 1. Общее понятие о программировании. Виды языков программирования. Язык Python	Языки программирования. Компиляция и интерпретация. Менеджмент памяти. Процедурное, функциональное, объектно-ориентированное программирование. Основные языки программирования. Особенности языка Python. IDE. Интерактивный и пакетный режим работы языка Python.
2	Тема 2. Базовые типы данных языка Python	Переменные. Int, float, str, list. Арифметические операции. Ввод и вывод
3	Тема 3. Условия и циклы	Базовые понятия условий и циклов. if..else. Условия. True и False. Булева алгебра и логические операции. Цикл while. Цикл for. Range. Break и Continue. Pass. Match.
4	Тема 4. Функции. Lambda-выражения	Определение функции. Передача параметров и возврат значений. Локальные, нелокальные и глобальные переменные. Рекурсия. Функция как переменная и функции высших порядков. Замыкания. Docstring. Lambda-выражения
5	Тема 5. Структуры	Коллективные типы данных. List, Tuple, Set, Dict. Стек и очередь. List и Set comprehension. Вложение

	данных	структур данных. Работа с файлам. JSON.
6	Тема 6. Модули	Стандартные библиотеки. Подключение модулей. Создание своих модулей. Иерархическая стркутуризация модулей.
7	Тема 7. Классы, ООП.	Объектно ориентированное программитрование. Классы. Инстансы. Переопределение операторов. Наследование.
8	Тема 8. Исключения и их обработка	Исключения. Стандартные исключения. Обработка исключений. Пользовательские исключения
9	Тема 9. Стандартные библиотеки языка Python	Стандартные библиотеки языка Python. os. Glob,sys, re, math, random, statistics, urllib, datetime, timeit, doctest, unittest, template, zipfile,array
10	Тема 10. Библиотеки для работы с математикой	Numpy, SciPy, Matplotlib, SymPy
11	Тема 11. Реализация GUI в языке Python	Базовые представления о GUI. Обзор основных библиотек для работы с GUI. TKinter
12	Тема 12. Работа с графическими файлами	Бибилиотека Pillow
13	Тема 13. Работа с компьютерными сетями	Бибилиотека requests. Криптография и https. RPC
14	Тема 14. Параллельное программирование	Базовые идеи. Yield. Async

Тематика лабораторных работ:

№ темы	Наименование работ
1	Первая самостоятельная программа. Ввод-вывод
2	Работа с переменными
3	Условия и циклы
4	Функции.
5	Работа с массивами
6	Работа с файлами
7	Ссылки и указатели.

8	Классы,
9	Конструкторы и деструкторы
10	Переопределение операторов
11	Наследование
12	Шаблоны
13	Классы-контейнеры STL.
14	Исключения и их обработка
15	Стандартные библиотеки языка С и С++

Требования к самостоятельной работе обучающихся

1. Работа с лекционным материалом, предусматривающая проработку конспекта лекций и учебной литературы, по всем темам из п. 6 настоящей рабочей программы.
2. Выполнение домашнего задания, предусматривающего решение задач, выполнение упражнений, выдаваемых на практических занятиях, по всем темам из п. 6 настоящей рабочей программы.

Руководствуясь положениями статьи 47 и статьи 48 Федерального закона от 29 декабря 2012 г. N 273-ФЗ «Об образовании в Российской Федерации» научно-педагогические работники и иные лица, привлекаемые университетом к реализации данной образовательной программы, пользуются предоставленными академическими правами и свободами в части свободы преподавания, свободы от вмешательства в профессиональную деятельность; свободы выбора и использования педагогически обоснованных форм, средств, методов обучения и воспитания; права на творческую инициативу, разработку и применение авторских программ и методов обучения и воспитания в пределах реализуемой образовательной программы и отдельной дисциплины.

Исходя из рамок, установленных учебным планом по трудоемкости и видам учебной работы по дисциплине, преподаватель самостоятельно выбирает тематику занятий по формам и количеству часов проведения контактной работы: лекции и иные учебные занятия, предусматривающие преимущественную передачу учебной информации преподавателем и (или) занятия семинарского типа (семинары, практические занятия, практикумы, лабораторные работы, коллоквиумы и иные аналогичные занятия), и (или) групповые консультации, и (или) индивидуальную работу обучающихся с преподавателем, в том числе индивидуальные консультации (по курсовым работам/проектам – при наличии курсовой работы/проекта по данной дисциплине в учебном плане).

Рекомендуемая тематика занятий максимально полно реализуется в контактной работе с обучающимися очной формы обучения. В случае реализации образовательной программы в заочной / очно-заочной форме трудоемкость дисциплины сохраняется, однако объем учебного материала в значительной части осваивается обучающимися в форме самостоятельной работы. При этом требования к ожидаемым образовательным результатам обучающихся по данной дисциплине не зависят от формы реализации образовательной программы.

7. Методические рекомендации по видам занятий

Лекционные занятия.

В ходе лекционных занятий обучающимся рекомендуется выполнять следующие действия. Вести конспектирование учебного материала. Обращать внимание на категории, формулировки, раскрывающие содержание тех или иных явлений и процессов, научные выводы и практические рекомендации по их применению. Задавать преподавателю уточняющие вопросы с целью уяснения теоретических положений, разрешения спорных ситуаций.

Желательно оставить в рабочих конспектах поля, на которых во внеаудиторное время можно сделать пометки из рекомендованной литературы, дополняющие материал прослушанной лекции, а также подчеркивающие особую важность тех или иных теоретических положений.

Практические и семинарские занятия.

На практических и семинарских занятиях в зависимости от темы занятия выполняется поиск информации по решению проблем, практические упражнения, контрольные работы, выработка индивидуальных или групповых решений, итоговое обсуждение с обменом знаниями, участие в круглых столах, разбор конкретных ситуаций, командная работа, представление портфолио и т.п.

Самостоятельная работа.

Самостоятельная работа осуществляется в виде изучения литературы, эмпирических данных по публикациям и конкретных ситуаций из практики, подготовке индивидуальных работ, работа с лекционным материалом, самостоятельное изучение отдельных тем дисциплины; поиск и обзор литературы и электронных источников; чтение и изучение учебника и учебных пособий.

8. Фонд оценочных средств

8.1. Перечень компетенций с указанием этапов их формирования в процессе освоения образовательной программы в рамках учебной дисциплины

Основными этапами формирования указанных компетенций при изучении обучающимися дисциплины являются последовательное изучение содержательно связанных между собой тем учебных занятий. Изучение каждой темы предполагает овладение обучающимися необходимыми компетенциями. Результат аттестации обучающихся на различных этапах формирования компетенций показывает уровень освоения компетенций.

Контролируемые модули, разделы (темы) дисциплины	Индекс контролируемой компетенции (или её части)	Оценочные средства по этапам формирования компетенций
		текущий контроль по дисциплине
Тема 1. Общее понятие о программировании. Виды языков программирования.	ОПК-7 ОПК-13	Написание и проверка контрольной программы

Язык С++		
Тема 2. Базовые типы данных языка С++	ОПК-7 ОПК-13	Написание и проверка контрольной программы
Тема 3. Условия и циклы	ОПК-7 ОПК-13	Написание и проверка контрольной программы
Тема 4. Функции. Lamda-выпаженния	ОПК-7 ОПК-13	Написание и проверка контрольной программы
Тема 5. Структуры данных	ОПК-7 ОПК-13	Написание и проверка контрольной программы
Тема 6. Ввод/вывод в С и С++. Работа с файлами	ОПК-7 ОПК-13	Написание и проверка контрольной программы
Тема 7. Ссылки и указатели. Динамическое выделение памяти	ОПК-7 ОПК-13	Написание и проверка контрольной программы
Тема 8. Классы, ООП.	ОПК-7 ОПК-13	Написание и проверка контрольной программы
Тема 9. Конструкторы и деструкторы	ОПК-7 ОПК-13	Написание и проверка контрольной программы
Тема 10. Переопределение операторов	ОПК-7 ОПК-13	Написание и проверка контрольной программы
Тема 11. Наследование	ОПК-7 ОПК-13	Написание и проверка контрольной программы
Тема 12. Шаблоны	ОПК-7 ОПК-13	Написание и проверка контрольной программы
Тема 13 Классы-контейнеры STL. Итераторы	ОПК-7 ОПК-13	Написание и проверка контрольной программы
Тема 14. Исключения и их обработка	ОПК-7 ОПК-13	Написание и проверка контрольной программы

Тема 15. Стандартные библиотеки языка С и С++	ОПК-7 ОПК-13	Написание и проверка контрольной программы

8.2. Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений и навыков и (или) опыта деятельности процессе текущего контроля

Тема 1. Общее понятие о программировании. Виды языков программирования. Язык С++

Написать программу выводящую на экран пирамидку из 5 звёздочек

Тема 2. Базовые типы данных языка С++

Написать программу выводящую на экран площадь круга, радиус которого вводится с клавиатуры.

Тема 3. Условия и циклы

Написать программу выводящую на экран решение квадратного уравнения, коэффициенты которого вводятся с клавиатуры.

Тема 4. Функции. Lamda-выпаженния

Написать функцию, проверяющую числа на простоту

Тема 5. Структуры данных

Написать программу сортировки массива методом пузырька

Тема 6. Ввод/вывод в С и С++. Работа с файлами

Написать программу сортировки массива методом пузырька. Массив прочитать их файла

Тема 7. Ссылки и указатели. Динамическое выделение памяти

Выделитьдинамически память для матрицы 5 на 5. Прочитать её из файла. Посчитать её определитель

Тема 8. Классы, ООП.

Создать класс для хранения 3-х мерного вектора

Тема 9. Конструкторы и деструкторы

Создать класс считывающий в конструкторе строку из файла, и записывающий её в деструкторе обратно в файл

Тема 10. Переопределение операторов

Создать класс для хранения 3-х мерного вектора с поддержкой всей арифметики векторов

Тема 11. Наследование

Создать класс для хранения 4-х мерного вектора наследованием от класса для 3-ч мерного вектора

Тема 12. Шаблоны

Создать шаблонный класс для работы с парой элементов одинакового типа.

Тема 13 Классы-контейнеры STL. Итераторы

Написать программу сортировки массива . Массив прочитать их файла. Использовать <array> и стандартную функцию сортировки

Тема 14. Исключения и их обработка

Написать программу сортировки массива . Массив прочитать их файла. Использовать <array> и стандартную функцию сортировки. Корректно обработать любые проблемы чтения из файла.

Тема 15. Стандартные библиотеки языка C и C++

Вывести на экран все простые числа до 1000. Нельзя использовать циклы, можно только примитивы из algorithm.h

8.3 Вопросы для промежуточного контроля (экзамена)

1. Общее представление о программировании. Компиляторы и интерпретаторы.
2. Процедурное, функциональное, объектно-ориентированное
3. программирование.C,C++,C#.
4. Типы данных и переменные в C и C++. Модификаторы типов данных.
5. Составные типы данных в C/C++.
6. Ввод/вывод в C и C++. Работа с файлами
7. Операторы условия и цикла
8. Функции, рекурсия, области видимости.
9. Ссылки и указатели. Динамическое выделение памяти
10. ООП. Классы, методы. Инкапсуляция, абстракция, полиморфизм. Public,
11. private, protected. Friend
12. Конструкторы и деструкторы. Конструктор копирования. Преобразование
13. типов.

14. Переопределение операторов. Включая операторы ввода-вывода

15. Наследование. Virtual, Абстрактные классы

16. Шаблоны

17. Классы-контейнеры STL. Итераторы

18. Стандартные библиотеки C и C++. Algorithm.h. sting.h

19. Обработка исключений

8.4. Планируемые уровни сформированности компетенций обучающихся и критерии оценивания

Уровни	Содержательное описание уровня	Основные признаки выделения уровня (этапы формирования компетенции, критерии оценки сформированности)	Пятибалльная шкала (академическая) оценка	Двухбалльная шакала, зачет	БРС, % освоения (рейтинговая оценка)
Повышенный	Творческая деятельность	*Включает нижестоящий уровень.* Умение самостоятельно принимать решение, решать проблему/задачу теоретического и прикладного характера на основе изученных методов, приемов, технологий	отлично	зачтено	86-100
Базовый	Применение знаний и умений в более широких контекстах учебной и профессиональной деятельности, нежели по образцу с большей степени самостоятельности и инициативы	*Включает нижестоящий уровень.* Способность собирать, систематизировать, анализировать и грамотно использовать информацию из самостоятельно найденных теоретических источников и иллюстрировать ими теоретические положения или обосновывать практику применения	хорошо		71-85
Удовлетворительный	Репродуктивная	Изложение в пределах задач курса	удовлетворительно		55-70

(достаточный)	деятельность	теоретически и практически контролируемого материала			
Недостаточный	Отсутствие признаков удовлетворительного уровня		неудовлетворительно	не зачтено	Менее 55

9. Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины.

Основная литература

1.Кузин, А. В. Программирование на языке Си : учебное пособие / А.В. Кузин, Е.В. Чумакова. — Москва : ФОРУМ : ИНФРА-М, 2021. — 144 с. — (Высшее образование). - ISBN 978-5-00091-066-5. - Текст : электронный. - URL: https://znanium.com/catalog/product/1222078 (дата обращения: 30.03.2022). – Режим доступа: по подписке.

Дополнительная литература

1.Литвиненко, В. А. Программирование на С++ задач на графах: Учебное пособие / Литвиненко В.А. - Таганрог:Южный федеральный университет, 2016. - 83 с.: ISBN 978-5-9275-2311-5. - Текст : электронный. - URL: https://znanium.com/catalog/product/997083 (дата обращения: 30.03.2022). – Режим доступа: по подписке.

10. Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины (модуля).

- НЭБ Национальная электронная библиотека, диссертации и прочие издания
- eLIBRARY.RU Научная электронная библиотека, книги, статьи, тезисы докладов конференций
- Гребенников Электронная библиотека ИД журналы
- ЭБС Лань книги, журналы
- ЭБС Консультант студента
- ПРОСПЕКТ ЭБС
- ЭБС ZNANIUM.COM
- РГБ Информационное обслуживание по МБА
- БЕН РАН
- Электронно-библиотечная система (ЭБС) Кантитана (https://elib.kantiana.ru/)

11. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине.

Программное обеспечение обучения включает в себя:

- система электронного образовательного контента БФУ им. И. Канта – www.lms-3.kantiana.ru, обеспечивающую разработку и комплексное использование электронных образовательных ресурсов;
- серверное программное обеспечение, необходимое для функционирования сервера и связи с системой электронного обучения через Интернет;
- корпоративная платформа Microsoft Teams;

- установленное на рабочих местах обучающихся ПО: Microsoft Windows 7, Microsoft Office Standart 2010, антивирусное программное обеспечение Kaspersky Endpoint Security.
- Среда программирования Microsoft Visual Studio (любая версия);
- Qt версии 5.0 и выше

12. Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине.

Для проведения занятий лекционного типа, практических и семинарских занятий используются специальные помещения (учебные аудитории), оборудованные техническими средствами обучения – мультимедийной проекционной техникой. Для проведения занятий лекционного типа используются наборы демонстрационного оборудования.

Для проведения лабораторных работ, (практических занятий – при необходимости) используются специальные помещения (учебные аудитории), оснащенные специализированным лабораторным оборудованием: персональными компьютерами с возможностью выхода в интернет и с установленным программным обеспечением, заявленным в п.11.

Для проведения групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации используются специальные помещения (учебные аудитории), оборудованные специализированной мебелью (для обучающихся), меловой / маркерной доской.

Для организации самостоятельной работы обучающимся предоставляются помещения, оснащенные компьютерной техникой с возможностью подключения к сети «Интернет» и обеспечением доступа в электронную информационно-образовательную среду университета.

Для обучения инвалидов и лиц с ограниченными возможностями здоровья университетом могут быть представлены специализированные средства обучения, в том числе технические средства коллективного и индивидуального пользования.

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
федеральное государственное автономное образовательное учреждение высшего образования «Балтийский федеральный университет имени Иммануила Канта»
Институт физико-математических наук и информационных технологий

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

«Дискретная математика»

Шифр: 10.05.01
Специальность: «Компьютерная безопасность»
Специализация: «Математические методы защиты информации»
Квалификация (степень) выпускника: специалист по защите информации

Калининград
2022

Лист согласования

Составитель: Белова Ольга Олеговна, к.ф.-м.н., доцент

Рабочая программа утверждена на заседании учебно-методического совета института физико-математических наук и информационных технологий

Протокол № 01/22 от «01» февраля 2022 г.

Председатель учебно-методического совета института физико-математических наук и информационных технологий

Первый заместитель директора ИФМНиИТ, к. ф.-м. н., доцент — Шпилевой А. А

Ведущий менеджер — Е.П.Ставицкая

Содержание

1.Наименование дисциплины: «Дискретная математика».

Цель дисциплины: целью освоения дисциплины «Дискретная математика» является ознакомление студентов с основными разделами дискретной математики и ее применением для решения практических задач, а также обеспечение фундаментальной подготовки в одной из важнейших областей современной математики.

2. Перечень планируемых результатов обучения по дисциплине, соотнесенных с планируемыми результатами освоения образовательной программы

Код компетенции	Результаты освоения образовательной программы (ИДК)	Результаты обучения по дисциплине
ОПК-3. Способен на основании совокупности математических методов разрабатывать, обосновывать и реализовывать процедуры решения задач профессиональной деятельности.	ОПК-3.1. Знает необходимые математические методы для решения задач обеспечения защиты информации. ОПК-3.2. Применяет совокупность необходимых математических методов для решения задач обеспечения защиты информации. ОПК-3.3. Разрабатывает, обосновывает и реализует на практике процедуры решения задач обеспечения защиты информации.	● ***Знать*:** − основные дискретные структуры: конечные автоматы, грамматики, графы, комбинаторные структуры; − методы перечисления для основных дискретных структур; – основы комбинаторного анализа; – основные понятия и алгоритмы теории графов. ● ***Уметь*:** – решать задачи периодичности и эквивалентности для конечных автоматов; − применять аппарат производящих функций и рекуррентных соотношений для решения перечислительных задач; − решать оптимизационные задачи на графах; − применять стандартные методы дискретной математики для решения профессиональных задач; − грамотно применять изученные математические методы. ● ***Владеть*:** − навыками применения языка и средств дискретной математики; − навыками решения комбинаторных и теоретико-графовых задач; − навыками построения дискретных моделей при решении профессиональных задач; − навыками обращения с дискретными конструкциями и методами математического и

		алгоритмического моделирования при решении прикладных задач.

3. Место дисциплины в структуре образовательной программы

Дисциплина «Дискретная математика» представляет собой дисциплину обязательной части блока дисциплин подготовки обучающихся.

4. Виды учебной работы по дисциплине.

Виды учебной работы по дисциплине зафиксированы учебным планом основной профессиональной образовательной программы по указанному направлению и профилю, выражаются в академических часах. Часы контактной работы и самостоятельной работы обчающегося и часы, отводимые на процедуры контроля, могут различаться в учебных планах ОПОП по формам обучения. Объем контактной работы включает часы контактной аудиторной работы (лекции/практические занятия/ лабораторные работы), контактной внеаудиторной работы (контроль самостоятельной работы), часы контактной работы в период аттестации. Контактная работа, в том числе может проводиться посредством электронной информационно-образовательной среды университета с использованием ресурсов сети Интернет и дистанционных технологий

5. Содержание дисциплины, структурированное по темам (разделам)

Исходя из рамок, установленных учебным планом по трудоемкости и видам учебной работы по дисциплине, преподаватель самостоятельно выбирает тематику занятий по формам и количеству часов проведения контактной работы: лекции и иные учебные занятия, предусматривающие преимущественную передачу учебной информации преподавателем и (или) занятия семинарского типа (семинары, практические занятия, практикумы, лабораторные работы, коллоквиумы и иные аналогичные занятия), и (или) групповые консультации, и (или) индивидуальную работу обучающихся с преподавателем, в том числе индивидуальные консультации (по курсовым работам/проектам – при наличии курсовой работы/проекта по данной дисциплине в учебном плане). Рекомендуемая тематика занятий максимально полно реализуется в контактной работе с обучающимися очной формы обучения. В случае реализации образовательной программы в заочной / очно-заочной форме трудоемкость дисциплины сохраняется, однако объем учебного материала в значительной части осваивается обучающимися в форме самостоятельной работы. При этом требования к ожидаемым образовательным результатам обучающихся по данной дисциплине не зависят от формы реализации образовательной программы.

№	Наименование раздела	Содержание раздела
1	Элементы теории множеств.	Операции над множествами. Отношение эквивалентности. Отображения. Типы отображений. Эквивалентность множеств. Равносильные формулы.
2	Теория графов.	Элементы графа, способы задания графов. Графы ориентированные и неориентированные. Матрицы инцидентности, смежности, расстояний и достижимости. Операции над графами. Метрические характеристики графа. Степени вершин графа. Теорема Эйлера о сумме степеней. Изоморфизмы. Пути. Маршруты. Разложение графа на компоненты связности. Двудольные графы. Деревья. Теорема о характеризации деревьев. Остовы графа. Остовное

		дерево графа. Алгоритм построения наименьшего остовного дерева. Реберная и вершинная связность. Неравенство Уитни-Харари. Необходимые и достаточные условия эйлеровости. Построение эйлерового цикла и эйлеровой цепи. Гамильтоновы графы. Достаточные условия гамильтоновости графа и орграфа. Планарные графы. Теорема о том, что К5 и К3,3 не планарны. Критерий планарности Понтрягина-Куратовского (без доказательства). Покрытия и независимые множества. Задача о наименьшем покрытии (без доказательства). Сильная связность в орграфах. Компоненты сильной связности. Анализ графа цепи Маркова. Алгоритмы поиска кратчайших путей в графах. Задача поиска гамильтонова цикла в графе. Задача о коммивояжере. Паросочетания. Максимальное паросочетание. Задача о назначениях.
3	Основные комбинаторные методы.	Рекуррентные соотношения. Производящие функции. Главная теорема комбинаторики (теорема о включениях и исключениях). Метод ветвей и границ. Ортогональные латинские квадраты. Матрицы Адамара. Перечисление графов отображений. Экстремальные задачи и перебор. Универсальные задачи. Метод ветвей и границ.

6. Рекомендуемая тематика учебных занятий в форме контактной работы

Рекомендуемая тематика учебных занятий *лекционного* типа (предусматривающих преимущественную передачу учебной информации преподавателем):

№	Наименование раздела	Темы лекций
1	Элементы теории множеств.	1. Множества. Операции над ними 2. Свойства операций над множествами. 3. Отношения. 4. Отношение эквивалентности. 5. Матрицы бинарных отношений.
2	Теория графов.	1. Задание графов с помощью матриц. 2. Задание орграфов с помощью матриц. Операции над графами. 3. Операции над графами. 4. Маршруты и цепи. Компоненты связности. 5. Орграфы. Матрица достижимости. 6. Матрица Кирхгофа. Алгоритмы Краскала и Прима. 7. Деревья, кодировка. 8. Метрические характеристики графов. 9. Алгоритм Форда --- Беллмана нахождения кратчайшего маршрута. 10. Алгоритм Дейкстры. 11. Фундаментальные циклы и разрезы. 12. Поток в сети.

		13. Раскраска графа. 14. Паросочетания. Задача о назначениях. Венгерский алгоритм, основанный на теории чередующихся цепей Петерсена. 15. Эйлеровы графы. Эйлеров цикл. 16. Двойственные графы. 17. Гамильтоновы графы. Гамильтонов цикл.
4	Основные комбинаторные методы.	1. Рекуррентные соотношения. 2. Производящие функции. 3. Главная теорема комбинаторики (теорема о включениях и исключениях) 4. Метод ветвей и границ.

Рекомендуемая тематика *практических* занятий:

5. Множества. Операции над ними
6. Свойства операций над множествами.
7. Отношения.
8. Отношение эквивалентности.
9. Матрицы бинарных отношений.
10. Задание графов с помощью матриц.
11. Задание орграфов с помощью матриц. Операции над графами.
12. Операции над графами.
13. Маршруты и цепи. Компоненты связности.
14. Орграфы. Матрица достижимости.
15. Матрица Кирхгофа. Алгоритмы Краскала и Прима.
16. Деревья, кодировка.
17. Метрические характеристики графов.
18. Алгоритм Форда --- Беллмана нахождения кратчайшего маршрута.
19. Алгоритм Дейкстры.
20. Фундаментальные циклы и разрезы.
21. Поток в сети.
22. Раскраска графа.
23. Паросочетания. Задача о назначениях. Венгерский алгоритм, основанный на теории чередующихся цепей Петерсена.
24. Эйлеровы графы. Эйлеров цикл.
25. Двойственные графы.
26. Гамильтоновы графы. Гамильтонов цикл.
27. Рекуррентные соотношения.
28. Производящие функции.
29. Главная теорема комбинаторики (теорема о включениях и исключениях)
30. Метод ветвей и границ.

На практических занятиях решаются задачи по теме занятия.

Требования к самостоятельной работе обучающихся

1. Работа с лекционным материалом, предусматривающая проработку конспекта лекций и учебной литературы, по всем темам из п. 6 настоящей рабочей программы.

2. Выполнение домашнего задания, предусматривающего решение задач, выполнение упражнений, выдаваемых на практических занятиях, по всем темам из п. 6 настоящей рабочей программы.

Руководствуясь положениями статьи 47 и статьи 48 Федерального закона от 29 декабря 2012 г. N 273-ФЗ «Об образовании в Российской Федерации» научно-педагогические работники и иные лица, привлекаемые университетом к реализации данной образовательной программы, пользуются предоставленными академическими правами и свободами в части свободы преподавания, свободы от вмешательства в профессиональную деятельность; свободы выбора и использования педагогически обоснованных форм, средств, методов обучения и воспитания; права на творческую инициативу, разработку и применение авторских программ и методов обучения и воспитания в пределах реализуемой образовательной программы и отдельной дисциплины.

Исходя из рамок, установленных учебным планом по трудоемкости и видам учебной работы по дисциплине, преподаватель самостоятельно выбирает тематику занятий по формам и количеству часов проведения контактной работы: лекции и иные учебные занятия, предусматривающие преимущественную передачу учебной информации преподавателем и (или) занятия семинарского типа (семинары, практические занятия, практикумы, лабораторные работы, коллоквиумы и иные аналогичные занятия), и (или) групповые консультации, и (или) индивидуальную работу обучающихся с преподавателем, в том числе индивидуальные консультации (по курсовым работам/проектам – при наличии курсовой работы/проекта по данной дисциплине в учебном плане).

Рекомендуемая тематика занятий максимально полно реализуется в контактной работе с обучающимися очной формы обучения. В случае реализации образовательной программы в заочной / очно-заочной форме трудоемкость дисциплины сохраняется, однако объем учебного материала в значительной части осваивается обучающимися в форме самостоятельной работы. При этом требования к ожидаемым образовательным результатам обучающихся по данной дисциплине не зависят от формы реализации образовательной программы.

7. Методические рекомендации по видам занятий

Лекционные занятия.

В ходе лекционных занятий обучающимся рекомендуется выполнять следующие действия. Вести конспектирование учебного материала. Обращать внимание на категории, формулировки, раскрывающие содержание тех или иных явлений и процессов, научные выводы и практические рекомендации по их применению. Задавать преподавателю уточняющие вопросы с целью уяснения теоретических положений, разрешения спорных ситуаций.

Желательно оставить в рабочих конспектах поля, на которых во внеаудиторное время можно сделать пометки из рекомендованной литературы, дополняющие материал прослушанной лекции, а также подчеркивающие особую важность тех или иных теоретических положений.

Практические и семинарские занятия.

На практических и семинарских занятиях в зависимости от темы занятия выполняется поиск информации по решению проблем, практические упражнения, контрольные работы, выработка индивидуальных или групповых решений, итоговое обсуждение с обменом знаниями, участие в круглых столах, разбор конкретных ситуаций, командная работа, представление портфолио и т.п.

Самостоятельная работа.

Самостоятельная работа осуществляется в виде изучения литературы, эмпирических данных по публикациям и конкретных ситуаций из практики, подготовке индивидуальных

работ, работа с лекционным материалом, самостоятельное изучение отдельных тем дисциплины; поиск и обзор литературы и электронных источников; чтение и изучение учебника и учебных пособий.

8. Фонд оценочных средств

8.1. Перечень компетенций с указанием этапов их формирования в процессе освоения образовательной программы в рамках учебной дисциплины

Основными этапами формирования указанных компетенций при изучении обучающимися дисциплины являются последовательное изучение содержательно связанных между собой тем учебных занятий. Изучение каждой темы предполагает овладение обучающимися необходимыми компетенциями. Результат аттестации обучающихся на различных этапах формирования компетенций показывает уровень освоения компетенций.

Контролируемые разделы (темы) дисциплины	Индекс контроли-руемой компетенции (или её части)	Оценочные средства по этапам формирования компетенций
		текущий контроль по дисциплине
1. Элементы теории множеств.	ОПК-3	Опрос, решение задач, контрольная работа
2. Теория графов.	ОПК-3	Опрос, решение задач, контрольная работа
3. Основные комбинаторные методы.	ОПК-3	Опрос, решение задач, контрольная работа

8.2. Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений и навыков и (или) опыта деятельности процессе текущего контроля

Примеры вопросов для устного опроса:

Тема 1.

1. Что такое прямое произведение множеств?
2. Как определяется бинарное отношение? Сформулировать свойства симметричности, рефлексивности и транзитивности.
3. Что такое отношение эквивалентности? Как определяются классы эквивалентности.
4. Какие бывают типы отображений?

Тема 2.

1. Что такое неориентированный граф?
2. Как определяются степени вершин в неориентированном графе?
3. Какие существуют способы задания неориентированного графа?
4. Что такое простой граф?
5. Что такое мультиграф?

6. Что такое псевдограф?
7. Какой граф называется полным?
8. Какие существуют операции над графами?
9. Чем отличается матрица инцидентности неориентированного графа от матрицы инцидентности ориентированного графа ?
10. Чем отличается путь от простого пути?
11. Что такое простая цепь?
12. Чем отличается матрица смежности простого графа от матрицы смежности графа с петлями?
13. Какими свойствами обладают матрицы инциденций?
14. Какими свойствами обладают матрицы смежности?
15. Что такое деревья? Перечислить свойства деревьев.
16. Как находится минимальное частичное дерево?
17. Что такое корневое дерево?
18. Как производится подсчет числа деревьев с занумерованными вершинами?
19. Что такое эйлеров цикл? Эйлеров граф?
20. Необходимое условие эйлеровости графа.
21. Что такое реберный граф?
22. Какой граф называется гамильтоновым?
23. Будет ли полный граф гамильтоновым?
24. Что такое плоские и планарные графы?
25. Что означает укладка графа в пространство?
26. Как определяются грани плоского графа?
27. Какие свойства у плоских укладок?
28. Формула Эйлера о числе вершин, ребер и граней плоского графа.
29. Задача о трех домах и трех колодцах.
30. Алгоритмы поиска кратчайших путей в графах.
31. Задача поиска гамильтонова цикла в графе.
32. Задача о коммивояжере.
33. Алгоритм нахождения максимального потока.
34. Что такое максимальное паросочетание?
35. Теорема Холла о паросочетаниях в двудольном графе.
36. Критерий планарности.
37. Раскраска графов.
38. Что такое хроматический многочлен?
39. Задача о назначениях.

Тема 3. Основные комбинаторные методы.

1. В чем состоит принцип включения и исключения?
2. Что такое производящая функция?
3. Рекуррентные уравнения. Методы решений.

Типовые контрольные задания:

Контрольная работа по теме 1.

1. Доказать равенство множеств

$$(A \cup B) \setminus C = (A \setminus C) \cup (B \setminus C).$$

2. Доказать равенство множеств

$$A(B \setminus C) = (AB) \setminus (AC)$$

Контрольная работа по теме 2.

1. Постройте граф для приведенного ниже отношения R на множестве A:

A={a, b, c, d, e}, R={ (a,b), (b,a), (b,c), (c,b), (c,a), (a,c), (d,e), (e,d)}.

2. Постройте орграф со следующими свойствами: множество вершин {a, b, c, d, e, f} и отношение R для ребер имеет вид: R={ (a,b), (b,c), (d,c), (d,e), (f,e), (f,a), (b,e)}.

3. Изобразите граф со следующим набором степеней вершин: {2; 2; 2; 1; 1}.

4. Постройте дерево по последовательности степеней его вершин: {1;1;1:3;1;2;4;2;1;1}.

5. Граф на *n* вершинах имеет *m* ребер. Сколько ребер имеет его дополнение?

6. Сколько граней у плоского графа?

Контрольная работа по теме 4 «Основные комбинаторные методы»

1. В группе 27 студентов. Сколькими способами можно выделить четырех человек для участия в конференции?

2. Сколькими способами можно выбрать 5 одинаковых или разных пирожных в кондитерской, где есть 8 разных сортов пирожных?

8.3. Перечень вопросов и заданий для промежуточной аттестации по дисциплине

Вопросы для промежуточного контроля (экзамена)

1. Кортежи и прямое произведение множеств.
2. Бинарное отношение. Свойства симметричности, рефлексивности и транзитивности.
3. Отношение эквивалентности. Классы эквивалентности.
4. Отображения и функциональные отношения.
5. Типы отображений.
6. Логические операции и правила вывода.
7. Равносильность логических формул.
8. Принцип сложения и умножения.
9. Подмножества. Примеры использования принципа сложения и умножения.
10. Принцип включения и исключения.
11. Выборки.
12. Размещениями с повторениями.
13. Размещения без повторений.

14. Сочетания без повторений.
15. Формула бинома Ньютона. Свойства биномиальных коэффициентов.
16. Полиномиальная формула.
17. Сочетания с повторениями.
18. Перестановки без повторений. Свойства перестановок.
19. Перестановки без повторений.
20. Перестановки с повторениями.
21. Задача о размещениях.
22. Разбиения. Числа Стирлинга второго рода.
23. Числа Стирлинга первого рода.
24. Разбиение числа на слагаемые.
25. Простые примеры рекуррентных последовательностей.
26. Числа Фибоначчи. Свойства чисел Фибоначчи.
27. Нерекуррентная формула для чисел Фибоначчи.
28. Вывод нерекуррентной формулы для чисел Фибоначчи с помощью производящей функции.
29. Однородное линейное рекуррентное уравнение. Случай простых корней характеристического многочлена.
30. Однородное линейное рекуррентное уравнение. Случай кратных корней характеристического многочлена P(x).
31. Неоднородное линейное рекуррентное уравнение.
32. Рекуррентные соотношения и передача информации.
33. Однородное линейное рекуррентное уравнение.
34. Производящие функции. Операции над рядами.
35. Производящие функции. Примеры.
36. Основные определения теории графов.
37. Задание графа. Матрицы инциденций, смежности и их свойства.
38. Деревья. Свойства деревьев.
39. Нахождение минимального частичного дерева.
40. Корневое дерево. Подсчет числа деревьев с занумерованными вершинами.
41. Транспортные сети. Теорема Форда-Фалкерсона.
42. Плоские и планарные графы. Укладка графа в пространство.
43. Грани плоского графа. Свойства плоских укладок. Формула Эйлера о числе вершин, ребер и граней плоского графа. Следствия. Критерий планарности (Понтрягина-Куратовского).
44. Степени вершин графа, теорема о сумме степеней и следствие из неё.
45. Пути, маршруты, разложение графа на компоненты связности.
46. Соотношения между числами независимых циклов, вершин, ребер и компонент графа.
47. Теорема о характеризации деревьев.
48. Алгоритм нахождения наименьшего остова.
49. Реберная и вершинная связность.
50. Необходимое и достаточное условия существования эйлерова цикла.
51. Необходимое и достаточное условия существования эйлеровой цепи.
52. Доказательство непланарности K5 и K3,3.
53. Сильная связность, компоненты сильной связности орграфа.
54. Алгоритм поиска кратчайших путей в графах.
55. Поиск гамильтонова цикла в графе.
56. Задача коммивояжера.
57. Алгоритмы нахождения наибольшего паросочетания.
58. Задача о назначениях и способы ее решения.
59. Теорема Холла о системе различных представителей.

60. Латинские прямоугольники и квадраты. Примеры.
61. Экстремальные задачи и перебор.
62. Метод ветвей и границ.

8.4. Планируемые уровни сформированности компетенций обучающихся и критерии оценивания

Уровни	Содержательное описание уровня	Основные признаки выделения уровня (этапы формирования компетенции, критерии оценки сформированности)	Пятибалльная шкала (академическая) оценка	Двухбалльная шакала, зачет	БРС, % освоения (рейтинговая оценка)
Повышенный	Творческая деятельность	*Включает нижестоящий уровень.* Умение самостоятельно принимать решение, решать проблему/задачу теоретического и прикладного характера на основе изученных методов, приемов, технологий	отлично	зачтено	86-100
Базовый	Применение знаний и умений в более широких контекстах учебной и профессиональной деятельности, нежели по образцу с большей степени самостоятельности и инициативы	*Включает нижестоящий уровень.* Способность собирать, систематизировать, анализировать и грамотно использовать информацию из самостоятельно найденных теоретических источников и иллюстрировать ими теоретические положения или обосновывать практику применения	хорошо		71-85
Удовлетворительный (достаточный)	Репродуктивная деятельность	Изложение в пределах задач курса теоретически и практически контролируемого материала	удовлетворительно		55-70
Недостаточный	Отсутствие признаков удовлетворительного уровня		неудовлетворительно	не зачтено	Менее 55

9. Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины.

Основная литература*

1. Белова О.О. Дискретная математика: Учебное пособие. Изд-во БФУ им. И. Канта, 2021.

Дополнительная литература:

2. Алексеев, В. Б. Дискретная математика: учебник / В.Б. Алексеев. — Москва: ИНФРА-М, 2022. — 133 с. — (Высшее образование: Бакалавриат). — DOI 10.12737/1172256. - ISBN 978-5-16-016520-2. - Текст: электронный. - URL: https://znanium.com/catalog/product/1840955 (дата обращения: 10.01.2022). – Режим доступа: по подписке.
3. Соболева, Т. С. Дискретная математика. Углубленный курс: учебник / под ред. А. В. Чечкина. - Москва: КУРС: ИНФРА-М, 2020. - 278 с. - ISBN 978-5-906818-11-9. - Текст: электронный. - URL: https://znanium.com/catalog/product/1015049 (дата обращения: 10.01.2022). – Режим доступа: по подписке.

Электронные издания:

1. Ерош И.Л. Дискретная математика. Комбинаторика (http://mat.net.ua/mat/biblioteka/Erosh-Discretnaya-matematika.pdf)

2. Ю.Ю. Громов, О.Г. Иванова, Ю.В. Кулаков, В.А. Гриднев, В.Г. Однолько Дискретная математика (http://window.edu.ru/resource/070/80070/files/gromov.pdf)

10. Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины (модуля).

- НЭБ Национальная электронная библиотека, диссертации и прочие издания
- eLIBRARY.RU Научная электронная библиотека, книги, статьи, тезисы докладов конференций
- Гребенников Электронная библиотека ИД журналы
- ЭБС Лань книги, журналы
- ЭБС Консультант студента
- ПРОСПЕКТ ЭБС
- ЭБС ZNANIUM.COM
- РГБ Информационное обслуживание по МБА
- БЕН РАН
- Электронно-библиотечная система (ЭБС) Кантитана (https://elib.kantiana.ru/)

11. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине.

Программное обеспечение обучения включает в себя:

- система электронного образовательного контента БФУ им. И. Канта – www.lms-3.kantiana.ru, обеспечивающую разработку и комплексное использование электронных образовательных ресурсов;

- серверное программное обеспечение, необходимое для функционирования сервера и связи с системой электронного обучения через Интернет;
- корпоративная платформа Microsoft Teams;
- специализированное ПО не требуется.

12. Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине.

Для проведения занятий лекционного типа, практических и семинарских занятий используются специальные помещения (учебные аудитории), оборудованные техническими средствами обучения – мультимедийной проекционной техникой. Для проведения занятий лекционного типа используются наборы демонстрационного оборудования.

Для проведения лабораторных работ, (практических занятий – при необходимости) используются специальные помещения (учебные аудитории), оснащенные специализированным лабораторным оборудованием: персональными компьютерами с возможностью выхода в интернет и с установленным программным обеспечением, заявленным в п.11.

Для проведения групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации используются специальные помещения (учебные аудитории), оборудованные специализированной мебелью (для обучающихся), меловой / маркерной доской.

Для организации самостоятельной работы обучающимся предоставляются помещения, оснащенные компьютерной техникой с возможностью подключения к сети «Интернет» и обеспечением доступа в электронную информационно-образовательную среду университета.

Для обучения инвалидов и лиц с ограниченными возможностями здоровья университетом могут быть представлены специализированные средства обучения, в том числе технические средства коллективного и индивидуального пользования.

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
федеральное государственное автономное образовательное учреждение высшего образования «Балтийский федеральный университет имени Иммануила Канта»
Институт физико-математических наук и информационных технологий

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

«Математическая логика и теория алгоритмов»

Шифр: 10.05.01
Специальность: «Компьютерная безопасность»
Специализация: «Математические методы защиты информации»
Квалификация (степень) выпускника: специалист по защите информации

Калининград
2022

Лист согласования

Составитель: Кулешов Артур Владимирович, к.ф.-м.н., доцент

Рабочая программа утверждена на заседании учебно-методического совета института физико-математических наук и информационных технологий
Протокол № 01/22 от «01» февраля 2022 г.
Председатель учебно-методического
совета института физико-
математических наук и информационных
технологий
Первый заместитель директора Шпилевой А. А
ИФМНиИТ, к. ф.-м. н., доцент

Ведущий менеджер Е.П.Ставицкая

Содержание

1.Наименование дисциплины: «Математическая логика и теория алгоритмов».

Цель дисциплины: целью освоения дисциплины «**Математическая логика и теория алгоритмов**» является фундаментальная подготовка обучающихся в области математической логики и теории алгоритмов.

2. Перечень планируемых результатов обучения по дисциплине, соотнесенных с планируемыми результатами освоения образовательной программы

Код компетенции	Результаты освоения образовательной программы (ИДК)	Результаты обучения по дисциплине
ОПК-3 Способен на основании совокупности математических методов разрабатывать, обосновывать и реализовывать процедуры решения задач профессиональной деятельности.	ОПК-3.1. Знает необходимые математические методы для решения задач обеспечения защиты информации. ОПК-3.2. Применяет совокупность необходимых математических методов для решения задач обеспечения защиты информации. ОПК-3.3. Разрабатывает, обосновывает и реализует на практике процедуры решения задач обеспечения защиты информации.	- **знать** систему основных понятий и теорем алгебры (логики) высказываний и предикатов, теории булевых функций, аксиоматического исчисления высказываний; - **уметь** применять формулы алгебры высказываний и булевы функции в решении прикладных задач, а также строить формальные доказательства в рамках исчисления высказываний; - **владеть практическими навыками** составления алгоритмов решения типовых задач математической логики, анализа логической структуры математических утверждений

3. Место дисциплины в структуре образовательной программы

Дисциплина «**Математическая логика и теория алгоритмов**» относится к обязательной части Блока 1 Дисциплины (модули), входит в Модуль 3. Дискретная математика.

4. Виды учебной работы по дисциплине.

Виды учебной работы по дисциплине зафиксированы учебным планом основной профессиональной образовательной программы по указанному направлению и профилю, выражаются в академических часах. Часы контактной работы и самостоятельной работы обчающегося и часы, отводимые на процедуры контроля, могут различаться в учебных планах ОПОП по формам обучения. Объем контактной работы включает часы контактной аудиторной работы (лекции/практические занятия/ лабораторные работы), контактной внеаудиторной работы (контроль самостоятельной работы), часы контактной работы в период аттестации. Контактная работа, в том числе может проводиться посредством электронной информационно-образовательной среды университета с использованием ресурсов сети Интернет и дистанционных технологий

5. Содержание дисциплины, структурированное по темам (разделам)

Исходя из рамок, установленных учебным планом по трудоемкости и видам учебной работы по дисциплине, преподаватель самостоятельно выбирает тематику занятий по формам и количеству часов проведения контактной работы: лекции и иные учебные занятия, предусматривающие преимущественную передачу учебной информации преподавателем и (или) занятия семинарского типа (семинары, практические занятия, практикумы, лабораторные работы, коллоквиумы и иные аналогичные занятия), и (или) групповые консультации, и (или) индивидуальную работу обучающихся с преподавателем, в том числе индивидуальные консультации (по курсовым работам/проектам – при наличии курсовой работы/проекта по данной дисциплине в учебном плане). Рекомендуемая тематика занятий максимально полно реализуется в контактной работе с обучающимися очной формы обучения. В случае реализации образовательной программы в заочной / очно-заочной форме трудоемкость дисциплины сохраняется, однако объем учебного материала в значительной части осваивается обучающимися в форме самостоятельной работы. При этом требования к ожидаемым образовательным результатам обучающихся по данной дисциплине не зависят от формы реализации образовательной программы.

№	Наименование раздела	Содержание раздела
1	Тема 1. Введение в математическую логику.	История развития математической логики. Математическая логика и основания математики. Значение математической логики и её место в ряду других математических дисциплин.
2	Тема 2. Булевы функции	Понятие булевых функций; табличный способ задания; существенные и несущественные переменные; формулы; эквивалентность формул; элементарные функции и их свойства; разложение функций по переменной; совершенная дизъюнктивная нормальная форма; полные системы функций; полиномы Жегалкина; представление булевых функций полиномами. Замыкание; свойства операции замыкания; замкнутые классы; Классы $\mathbf{T_0}$ и $\mathbf{T_1}$; линейные функции; лемма о нелинейной функции; самодвойственные функции; принцип двойственности; лемма о несамодвойственной функции; монотонные функции; лемма о немонотонной функции; теорема о неполноте систем функций алгебры логики; предполные классы; базисы; примеры базисов.
3	Тема 3. Алгебра высказываний. Исчисление высказываний.	Понятие высказывания. Операции над высказываниями. Свойства этих операций. Тавтологии. Нормальные формы. Контактные схемы. Общее понятие о логическом исчислении. Язык, аксиомы и правила вывода исчисления высказываний. Тождественная истинность выводимых формул. Выводимость и доказуемость формул в исчислении высказываний. Теорема дедукции. Непротиворечивость и полнота исчисления высказываний.
4	Тема 4. Алгебра предикатов. Исчисление предикатов.	Предикаты на множестве и их связь с отношениями. Местность предиката. Логические операции над предикатами. Операции квантификации. Свойства

		операций. Свободные и связанные переменные. Определение формулы алгебры предикатов. Выполнимые, тождественно истинные и тождественно ложные формулы. Равносильность формул, основные соотношения равносильности и их использование для упрощения формул. Приведение формул к нормальным формам. Понятие об интерпретации исчисления предикатов. Язык, аксиомы и правила вывода исчисления предикатов. Выводимость и доказуемость формул в исчислении предикатов. Эквивалентность формул. Непротиворечивость исчисления предикатов. Непротиворечивые, полные и выполнимые системы формул. Теорема Геделя о полноте исчисления предикатов. Применение исчисления предикатов для записи математических утверждений и для автоматического доказательства теорем.
5	Тема 5. Вычислимые функции. Машины Тьюринга.	Вычислимые функции: машины Тьюринга; вычислимые функции; тезис Черча; примеры вычислимых функций; рекурсивные, рекурсивно перечислимые множества и их алгоритмическая характеристика; теорема Поста; примеры алгоритмически неразрешимых проблем; неразрешимость проблем самоприменимости, применимости; теорема Поста-Маркова о существовании ассоциативного исчисления с алгоритмически неразрешимой проблемой равенства.
6	Тема 6. Сложность вычислений.	Вычислительные проблемы. Сложность алгоритмов и сложность задач. Классы сложности. Класс P. Класс E. Класс NP. Проблема равенства классов P и NP.

6. Рекомендуемая тематика учебных занятий в форме контактной работы

Рекомендуемая тематика учебных занятий *лекционного* типа (предусматривающих преимущественную передачу учебной информации преподавателями):

№	Наименование раздела	Темы лекций
1.	Введение в математическую логику	Лекция 1. История развития математической логики.
2	Булевы функции.	Лекция 2. Понятие булевых функций. Способы задания булевых функций Лекция 3. совершенная дизъюнктивная нормальная форма. Полином Жегалкина. Лекция 4. Замыкание. Классы T_0 и T_1.
3	Алгебра высказываний. Исчисление высказываний.	Лекция 5. Понятие высказывания. Операции над высказываниями. Лекция 6. Нормальные формы. Контактные схемы.

		Лекция 7. Выводимость и доказуемость формул в исчислении высказываний Лекция 8. Теорема дедукции. Непротиворечивость и полнота исчисления высказываний.
4	Алгебра предикатов. Исчисление предикатов.	Лекция 9. Предикаты на множестве и их связь с отношениями. Лекция 10. Приведение формул к нормальным формам. Лекция 11. Язык, аксиомы и правила вывода исчисления предикатов. Лекция 12. Теорема Геделя о полноте исчисления предикатов.
5	Вычислимые функции. Машины Тьюринга.	Лекция 13. Вычислимые функции Лекция 14. Теорема Поста Лекция 15. Неразрешимость проблем самоприменимости, применимости Лекция 16. Теорема Поста-Маркова о существовании ассоциативного исчисления с алгоритмически неразрешимой проблемой равенства.
6	Сложность вычислений.	Лекция 17. Вычислительные проблемы Лекция 18. Классы сложности

Рекомендуемая тематика *практических* занятий:

№ п/п	**Наименование Темы**	**Содержание темы**
1	Булевы функции. Совершенные дизъюнктивные и конъюнктивные нормальные формы. Эквивалентные формулы.	Построение таблиц истинности для функций; проверка эквивалентности формул; построение совершенных дизъюнктивных и конъюнктивных нормальных форм для конкретных функций; разложение функции по переменным.
2	Двойственные функции. Самодвойственные, монотонные функции.	Нахождение двойственной функции, проверка функции на самодвойственность, исследование функций на монотонность.
3	Полином Жегалкина. Линейные функции.	Нахождение полинома Жегалкина конкретных функций, проверка функции на линейность.
4	Полные системы функций.	Исследование конкретных систем функций на полноту.
5	Высказывания и операции над ними.	Построение сложных высказываний из простых. Перевод рассуждений в формулы алгебры высказываний. Исследование рассуждений на логичность.
6	Применение законов логики высказываний.	Упрощение формул алгебры высказываний с помощью законов; упрощение систем высказываний; применение законов математической логики при доказательстве различных утверждений.
7	Нормальные формы.	Построение функции проводимости конкретных

	Применение к контактным схемам.	контактных схем; упрощение контактных схем; проверка контактных схем на равносильность; построение контактных схем, удовлетворяющих определённым условиям с применением нормальных форм.
8	Исчисление высказываний. Примеры выводимых формул.	Построение выводов для конкретных формул алгебры высказываний.
9	Предикаты. Логические операции над ними. Операции квантификации.	Нахождение области истинности конкретных предикатов. Перевод рассуждений с формулы логики предикатов. Проверка формул логики предикатов на выполнимость. Построение высказываний из конкретных предикатов с помощью кванторов.
10	Предикаты. Эквивалентные формулы. Нормальные формы.	Проверка формул на эквивалентность. Построение ПНФ (предварённой нормальной формы) для конкретных формул логики предикатов.
11	Предикаты. Использование интерпретаций в доказательстве нелогичности рассуждений.	Доказательство неравносильности конкретных формул с помощью построения интерпретаций. Построение интерпретаций для доказательства нелогичности конкретных рассуждений.
12	Исчисление предикатов. Вывод и вывод из гипотез.	Построение вывода для конкретных формул логики предикатов.
13	Машина Тьюринга. Примеры вычислимых функций.	Исследование работы конкретных машин Тьюринга. Построение машин Тьюринга, вычисляющие заданные функции.
14	Оценка сложности алгоритмов.	Оценка сложности конкретных алгоритмов.

Требования к самостоятельной работе обучающихся

1. Работа с лекционным материалом, предусматривающая проработку конспекта лекций и учебной литературы, по всем темам из п. 6 настоящей рабочей программы.
2. Выполнение домашнего задания, предусматривающего решение задач, выполнение упражнений, выдаваемых на практических занятиях, по всем темам из п. 6 настоящей рабочей программы.

Руководствуясь положениями статьи 47 и статьи 48 Федерального закона от 29 декабря 2012 г. N 273-ФЗ «Об образовании в Российской Федерации» научно-педагогические работники и иные лица, привлекаемые университетом к реализации данной образовательной программы, пользуются предоставленными академическими правами и свободами в части свободы преподавания, свободы от вмешательства в профессиональную деятельность; свободы выбора и использования педагогически обоснованных форм, средств, методов обучения и воспитания; права на творческую инициативу, разработку и применение авторских программ и методов обучения и воспитания в пределах реализуемой образовательной программы и отдельной дисциплины.

Исходя из рамок, установленных учебным планом по трудоемкости и видам учебной работы по дисциплине, преподаватель самостоятельно выбирает тематику занятий по формам и количеству часов проведения контактной работы: лекции и иные учебные занятия, предусматривающие преимущественную передачу учебной информации преподавателем и (или) занятия семинарского типа (семинары, практические занятия, практикумы, лабораторные работы, коллоквиумы и иные аналогичные занятия), и (или) групповые консультации, и (или) индивидуальную работу обучающихся с преподавателем, в том числе индивидуальные консультации (по курсовым работам/проектам – при наличии курсовой работы/проекта по данной дисциплине в учебном плане).

Рекомендуемая тематика занятий максимально полно реализуется в контактной работе с обучающимися очной формы обучения. В случае реализации образовательной программы в заочной / очно-заочной форме трудоемкость дисциплины сохраняется, однако объем учебного материала в значительной части осваивается обучающимися в форме самостоятельной работы. При этом требования к ожидаемым образовательным результатам обучающихся по данной дисциплине не зависят от формы реализации образовательной программы.

7. Методические рекомендации по видам занятий

Лекционные занятия.

В ходе лекционных занятий обучающимся рекомендуется выполнять следующие действия. Вести конспектирование учебного материала. Обращать внимание на категории, формулировки, раскрывающие содержание тех или иных явлений и процессов, научные выводы и практические рекомендации по их применению. Задавать преподавателю уточняющие вопросы с целью уяснения теоретических положений, разрешения спорных ситуаций.

Желательно оставить в рабочих конспектах поля, на которых во внеаудиторное время можно сделать пометки из рекомендованной литературы, дополняющие материал прослушанной лекции, а также подчеркивающие особую важность тех или иных теоретических положений.

Практические и семинарские занятия.

На практических и семинарских занятиях в зависимости от темы занятия выполняется поиск информации по решению проблем, практические упражнения, контрольные работы, выработка индивидуальных или групповых решений, итоговое обсуждение с обменом знаниями, участие в круглых столах, разбор конкретных ситуаций, командная работа, представление портфолио и т.п.

Самостоятельная работа.

Самостоятельная работа осуществляется в виде изучения литературы, эмпирических данных по публикациям и конкретных ситуаций из практики, подготовке индивидуальных работ, работа с лекционным материалом, самостоятельное изучение отдельных тем дисциплины; поиск и обзор литературы и электронных источников; чтение и изучение учебника и учебных пособий.

8. Фонд оценочных средств

8.1. Перечень компетенций с указанием этапов их формирования в процессе освоения образовательной программы в рамках учебной дисциплины

Основными этапами формирования указанных компетенций при изучении обучающимися дисциплины являются последовательное изучение содержательно связанных между собой тем учебных занятий. Изучение каждой темы предполагает

овладение обучающимися необходимыми компетенциями. Результат аттестации обучающихся на различных этапах формирования компетенций показывает уровень освоения компетенций.

Контролируемые разделы (темы) дисциплины	Индекс контроли-руемой компетенции (или её части)	Оценочные средства по этапам формирования компетенций
		текущий контроль по дисциплине
Тема 1. Введение в математическую логику.	ОПК-3.1 ОПК-3.2 ОПК-3.3	Устный опрос
Тема 2. Булевы функции	ОПК-3.1 ОПК-3.2 ОПК-3.3	Устный опрос, тестирование, реферат
Тема 3. Алгебра высказываний. Исчисление высказываний.	ОПК-3.1 ОПК-3.2 ОПК-3.3	Устный опрос, тестирование, реферат, контрольная работа
Тема 4. Алгебра предикатов. Исчисление предикатов.	ОПК-3.1 ОПК-3.2 ОПК-3.3	Устный опрос, тестирование, реферат, контрольная работа
Тема 5. Вычислимые функции. Машины Тьюринга.	ОПК-3.1 ОПК-3.2 ОПК-3.3	Устный опрос, тестирование, реферат
Тема 6. Сложность вычислений.	ОПК-3.1 ОПК-3.2 ОПК-3.3	Устный опрос, тестирование, реферат

8.2. Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений и навыков и (или) опыта деятельности процессе текущего контроля

Примеры вопросов для устного опроса:

Тема 1.

1. Когда и кем были заложены основы математической логики?
2. Когда и в связи с чем возникали кризисы в основаниях математики?
3. Как развитие математической логики помогло в разрешении кризиса?

Тема 2.

1. Что такое булева функция?
2. Перечислите способы задания булевых функций.
3. Сколько существует булевых функций, зависящих от n переменных?
4. Какая булева функция называется самодвойственной?
5. Какая булева функция называется монотонной?
6. Какая булева функция называется линейной?
7. Какая система функций называется замкнутой?
8. Какие замкнутые классы функций вы знаете?
9. Какие системы функций называются полными?

Тема 3.

1. Что такое высказывание?
2. Какие операции можно совершать над высказываниями?
3. Какие нормальные формы для формул логики высказываний вам известны?
4. Каковы аксиомы исчисления высказываний?
5. Какое высказывание является выводимым в рамках данной теории?
6. Сформулируйте теорему о дедукции.
7. В чём заключается непротиворечивость исчисления высказываний?
8. В чём заключается полнота исчисления высказываний?

Тема 4.

1. Что такое предикат?
2. Дайте определение формулы алгебры предикатов.
3. Какие переменные называются свободными, а какие связанными?
4. Как изменится местность предиката, если применить к нему операцию квантификации?
5. Что такое интерпритация в исчислении предикатов?
6. Сформулируйте аксиомы исчисления предикатов.
7. Какие правила вывода используются в исчислении предикатов?
8. Какая формула называется выводимой в исчислении предикатов?

Тема 5.

1. Как работает машина Тьюринга?
2. Какая функция называется частично-рекурсивной?
3. Какая функция является универсальной вычислимой?
4. Сформулируйте тезис Черча.
5. Сформулируйте теорему Поста.
6. Приведите примеры алгоритмически неразрешимых проблем.

Тема 6.

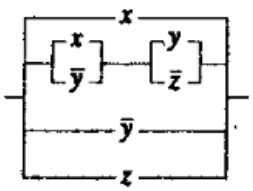
1. Что такое временная сложность алгоритма?
2. Какие алгоритмы называют линейными? Приведите примеры.
3. Какие алгоритмы называют полиномиальными? Приведите примеры.
4. Какие алгоритмы называют экспоненциальными? Приведите примеры.
5. Какие алгоритмы являются наиболее быстрыми?
6. В чём суть проблемы P = NP?

Типовые контрольные задания:

Контрольная работа № 1 «Высказывания»

Вариант 1

1. Найти функцию проводимости схемы; упростить схему



2. Применяя равносильные преобразования, привести формулу к наиболее простому виду

$$\neg((P \to Q) \wedge P) \wedge (\neg P \vee \neg Q)$$

3. Для данной функции $f = (0,0,1,0,1,0,1,1)$, заданной значениями на стандартных наборах:

- Построить СДНФ
- Представить функцию наиболее простой формулой
- Разложить функцию по переменной x
- Построить СКНФ

4. Выяснить, является ли первая формула последовательности формул логическим следствием остальных

$$z \to x;\ x \to y,\ \bar{y} \to \bar{z}$$

5. Проверить с помощью теоремы Поста на полноту следующую систему функций

$$z \vee xz',\ x + y,\ x \leftrightarrow y,\ 1.$$

Контрольная работа № 2 «Предикаты»

Вариант 1

Задание 1. Задана формула исчисления предикатов и множество $M = \{a, b\}$.

1.Привести формулу к предваренной нормальной форме.

2. Вычислить значение истинности формулы на множестве M с заданной интерпретацией предикатов.

3. Определить, является ли формула на множестве M (а) выполнимой; (б) опровержимой?

$P(a)$ = «и», $P(b)$ = «л», $R(a)$ = «л», $R(b)$ = «л», $Q(a, a)$ = «и», $Q(a, b)$ = «и», $Q(b, a)$ = «л», $Q(b,b)$=«и».

$$\Phi = \forall x\left(P(x) \Rightarrow \left(R(x) \Rightarrow \forall y Q(x, y)\right)\right)$$

Задание 2. Проанализировать рассуждение на предмет его правильности:

Все ромбы – параллелограммы. Все прямоугольники - параллелограммы. Следовательно, все ромбы – прямоугольники.

Задание 3. Доказать тождественную истинность следующей формулы:

$$\overline{(\exists x)P(x)} \Rightarrow \overline{(\forall x)P(x)}$$

Типовые тестовые задания

Тема 2. Булевы функции

	Вопрос теста	Варианты ответов

Оценка «удовлетворительно» или низкой уровень освоения компетенции	Сколько существует всего булевых функций, зависящих от n переменных?	2^n 2^{2^n} $2^n - 1$
Оценка «хорошо» или повышенный уровень освоения компетенции	Какая из данных функций не является монотонной?	$x_1 \wedge x_2$ $x_1 \vee x_2$ $x_1 \to x_2$
Оценка «отлично» или высокий уровень освоения компетенции	Полином Жегалкина для функции $f(x_1, x_2)$, заданной двоичным набором (0111) имеет вид …	$x_1 \oplus x_2 \oplus x_1 \cdot x_2$ $1 \oplus x_2 \oplus x_1 \cdot x_2$ $x_2 \oplus x_1 \cdot x_2$

Тема 3. Алгебра высказываний. Исчисление высказываний

	Вопрос теста	Варианты ответов
Оценка «удовлетворительно» или низкой уровень освоения компетенции	Укажите тавтологию	$(p \to q) \wedge p$ $(\overline{p} \to \overline{q}) \leftrightarrow (q \to p)$ $((r \vee q) \to (q \wedge r))$
Оценка «хорошо» или повышенный уровень освоения компетенции	Формулой равносильной к $\overline{(p \to q) \wedge (q \to \overline{p})}$ является …	$q \vee \overline{p}$ p 1
Оценка «отлично» или высокий уровень освоения компетенции	СДНФ формулы алгебры логики $p \to q$:	$(\overline{p} \vee q)$ $(p \wedge q) \vee (\overline{p} \wedge q) \vee (\overline{p} \wedge \overline{q})$ $(\overline{p} \wedge q) \vee (\overline{p} \wedge \overline{q})$

Тема 4. Алгебра предикатов. Исчисление предикатов

	Вопрос теста	Варианты ответов
Оценка «удовлетворительно» или низкой уровень освоения компетенции	Пусть $p(x) = (x \div 12)$, $r(x) = (x \div 3)$, $x \in N$. Укажите выражение на языке алгебры предикатов высказывания: «Некоторые натуральные числа кратные 12 не являются кратными 3».	$\exists x(p(x) \to \overline{r(x)})$ $\exists x\, \overline{p(x) \wedge r(x)}$ $\exists x(p(x) \wedge \overline{r(x)})$
Оценка «хорошо» или повышенный уровень освоения компетенции	Переведите на русский язык следующую символьную запись: $\forall n[\exists m(n=2m) \wedge (n>2) \to \exists x \exists y(R(x) \wedge R(y) \wedge (n=x+y))]$, где $n, m \in N$, $R(x), R(y)$ - простые числа.	Каждое, четное число >2, есть сумма двух чисел, из которых одно простое. Всякое натуральное число, >2 является суммой двух простых. Всякое натуральное четное число, >2 является

		суммой двух простых.
Оценка «отлично» или высокий уровень освоения компетенции	Предваренной формой к формуле $\forall xR(x) \to \exists yQ(y)$ является …	$\exists x\exists y\left(\overline{R(x)} \vee Q(y)\right)$ $\forall x\exists y(R(x) \to Q(y))$ $\exists x\exists y(R(x) \vee Q(y))$

Тема 5. Вычислимые функции. Машины Тьюринга

	Вопрос теста	Варианты ответов
Оценка «удовлетворительно» или низкой уровень освоения компетенции	Машина Тьюринга - это …	транспортное средство реально существующее вычислительное устройство воображаемое вычислительное устройство
Оценка «хорошо» или повышенный уровень освоения компетенции	Команда машины Тьюринга состоит из элементарных действий	двух трёх любого числа
Оценка «отлично» или высокий уровень освоения компетенции	Символы, которые машина Тьюринга читает и пишет на ленте, образуют	алфавит конфигурацию выражения

Тема 6. Сложность вычислений

	Вопрос теста	Варианты ответов
Оценка «удовлетворительно» или низкой уровень освоения компетенции	Понятие, характеризующее время работы, используемое алгоритмом, как функции от длины строки, представляющей входные данные – это …	Средняя сложность алгоритма Асимптотическая временная сложность алгоритма Временная сложность наихудшего случая алгоритма
Оценка «хорошо» или повышенный уровень освоения компетенции	Полиномиальный алгоритм- это алгоритм, временная сложность которого …	$O(n)$ $O(n^2)$ $O(n^k)$, $k \in N$
Оценка «отлично» или высокий уровень освоения компетенции	Умножение матриц имеет порядок сложности	$O(n^2)$ $O(n^3)$ $O(n\log n)$

Темы рефератов

Темы рефератов

Тема 1. Применение булевых функций к диагностике заболеваний. Распознавание образов.

Тема 2. Базисные системы булевых функций.

Тема 3.

Темы рефератов

Тема 1. Метаматематика (свойства формальных аксиоматических теорий).
Тема 2. Формализация теории аристотелевских силлогизмов.
Тема 3. Возникновении и развитие идеи формальной математической теории.

Тема 4.

Темы рефератов

Тема 1. Математическая логика и системы искусственного интеллекта.
Тема 2. Применение компьютеров для доказательства теорем математической логики.
Тема 3. Формальная арифметика и её свойства.

Тема 5.

Темы рефератов

Тема 1. Теория алгоритмов и математическая логика – фундаментальная основа программирования.
Тема 2. Описание программирования и анализ его концепций с помощью математической логики.
Тема 3. Описание компьютерных программ с помощью математической логики.
Тема 4. Верификация компьютерных программ с помощью математической логики.

Тема 6.

Темы рефератов

Тема 1. Неразрешимые алгоритмически проблемы.
Тема 2. Алгоритмы быстрых вычислений.
Тема 3. Приближённые алгоритмы.
Тема 4. NP-полные задачи.

Тема реферата также может быть индивидуально предложена студентом. Все темы рефератов согласуются с преподавателем.

8.3. Перечень вопросов и заданий для промежуточной аттестации по дисциплине

Вопросы для промежуточного контроля (зачета)

1. Понятие булевых функций. Табличный способ задания. Существенные и несущественные переменные
2. Формулы; эквивалентность формул; элементарные функции и их свойства.
3. Теорема о разложении функции по m-переменным и следствия. Совершенная дизъюнктивная нормальная форма
4. Полные системы функций. Примеры.
5. Замыкание систем функций, свойства.
6. Двойственные функции. Самодвйственные функции. Принцип двойственности.
7. Совершенная конъюнктивная нормальная форма.
8. Лемма о несамодвойственной функции.
9. Монотонные функции. Лемма о немонотонной функции.
10. Полиномы Жегалкина. Линейные функции.

11. Классы T_0, T_1.
12. Теорема о полноте (Поста). Следствия.
13. Предполный класс и его замкнутость.
14. Определение высказывания. Логические операции над высказываниями.
15. Определение формулы. Истинностные значения формул. Равносильность. Равносильные преобразования формул. Определения тавтологии и противоречия.
16. Законы логики высказываний.
17. Определения ДН-формы и КН-формы, приводимость всякой формулы к нормальной форме, примеры.
18. Логическое следствие.
19. Контактные схемы.
20. Аксиомы исчисления высказываний и правила вывода. Доказуемость формул.
21. Выводимость из гипотез, правила выводимости.
22. Теоремы дедукции
23. Непротиворечивость исчисления высказываний.
24. Полнота и разрешимость исчисления высказываний.
25. Назависимость аксиом.
26. Теорема о выводимости любой тавтологии в рамках данной теории.
27. Предикаты. Определение и операции над ними.
28. Свойства операций квантификации.
29. Предикатные формулы, равносильные формулы. Выполнимые, тождественно истинные и тождественно ложные формулы.
30. Интерпритации в логике предикатов.
31. Приведение формул к нормальным формам. Предварённая номальная форма.
32. Исчисление предикатов, язык, аксиомы, правила вывода.
33. Проблема разрешимости в логике предикатов. Непротиворечивость исчисления предикатов.
34. Непротиворечивые, полные и выполнимые системы формул. Теорема Геделя о полноте исчисления предикатов.
35. Машина Тьюринга, примеры.
36. Примитивно- рекурсивные функции. Примеры.
37. Вычислимые функции.
38. Нормальный алгоритм Маркова.
39. Асимптотические обозначения. Сложность алгоритмов и задач.
40. Классификация задач по сложности. Проблема P = NP.

8.4. Планируемые уровни сформированности компетенций обучающихся и критерии оценивания

Уровни	Содержательное описание уровня	Основные признаки выделения уровня (этапы формирования компетенции, критерии оценки сформированности)	Пятибалльная шкала (академическая) оценка	Двухбалльная шакала, зачет	БРС, % освоения (рейтинговая оценка)
Повышенный	Творческая деятельность	*Включает нижестоящий уровень.* Умение самостоятельно принимать решение, решать проблему/задачу	отлично	зачтено	86-100

		теоретического и прикладного характера на основе изученных методов, приемов, технологий			
Базовый	Применение знаний и умений в более широких контекстах учебной и профессиональной деятельности, нежели по образцу с большей степени самостоятельности и инициативы	*Включает нижестоящий уровень.* Способность собирать, систематизировать, анализировать и грамотно использовать информацию из самостоятельно найденных теоретических источников и иллюстрировать ими теоретические положения или обосновывать практику применения	хорошо		71-85
Удовлетворительный (достаточный)	Репродуктивная деятельность	Изложение в пределах задач курса теоретически и практически контролируемого материала	удовлетворительно		55-70
Недостаточный	Отсутствие признаков удовлетворительного уровня		неудовлетворительно	не зачтено	Менее 55

9. Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины.

Основная литература

1. Игошин, В. И. Математическая логика : учебное пособие / В. И. Игошин. — Москва : ИНФРА-М, 2019. — 398 с. — (Высшее образование: Бакалавриат). - ISBN 978-5-16-011691-4. - Текст : электронный. - URL: https://znanium.com/catalog/product/987006. – Режим доступа: по подписке.
2. Игошин, В. И. Сборник задач по математической логике и теории алгоритмов : учебное пособие / В. И. Игошин. - Москва : КУРС : ИНФРА-М, 2019. - 392 с. - ISBN 978-5-906818-08-9. - Текст : электронный. - URL: https://znanium.com/catalog/product/986940.
3. Гринченков, Д. В. Математическая логика и теория алгоритмов для программистов [Электронный ресурс]: учеб. пособие для вузов/ Д. В. Гринченков, С. И. Потоцкий. - Москва: КноРус, 2014. - 1 эл. опт. диск (CD-ROM), 206 с.. - (Бакалавриат). - Библиогр.: с. 205-206 (24 назв.). - Лицензия до 2021 г.. - ISBN 978-5-406-04041-6: 15.000 р. Имеются экземпляры в отделах /There are copies in departments: всего /all 2: ЭБС Кантиана(1), ч.з.N1(1) Свободны / free: ЭБС Кантиана(1), ч.з.N1(1)

Дополнительная литература

1. Перемитина, Т. О. Математическая логика и теория алгоритмов : учебное пособие / Т. О. Перемитина. - Томск : ФДО, ТУСУР, 2016. - 132 с. - Текст : электронный. - URL: https://znanium.com/catalog/product/1845832 (дата обращения: 16.01.2022). – Режим доступа: по подписке.
2. 5. Гуров, С. И. Логика высказываний : учебное пособие / С.И. Гуров. - Москва : Издательство Московского университета, 2015. - 268 с. - (Бакалавриат. Учебные пособия). - ISBN 978-5-19-011105-7. - Текст : электронный. - URL: https://znanium.com/catalog/product/1022892. – Режим доступа: по подписке.
3. Попов, Ю.И. Практикум. Элементы математической логики [Электронный ресурс]: учеб.-метод. пособие/ Ю. И. Попов. - Калининград: Калинингр. гор. тип., 2001. - 80 с.. - Библиогр.:с.79. - Бессрочная лицензия. - ISBN 5-87869-093-4: 25.00 р. Имеются экземпляры в отделах /There are copies in departments: всего /all 2: ЭБС Кантиана(1), ИБО(1) Свободны / free: ЭБС Кантиана(1), ИБО(1)
4. Башашина, К. В. Элементы математической логики [Электронный ресурс]: учеб. пособие/ К. В. Башашина, Ю. И. Попов; Балт. федер. ун-т им. И. Канта. - Калининград: БФУ им. И. Канта, 2015 on-line, 147 с.. - Бессрочная лицензия. - ISBN 978-5-9971-0342-2: Б.ц. Имеются экземпляры в отделах /There are copies in departments: ЭБС Кантиана(1) Свободны / free: ЭБС Кантиана(1)

10. Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины (модуля).

- НЭБ Национальная электронная библиотека, диссертации и прочие издания
- eLIBRARY.RU Научная электронная библиотека, книги, статьи, тезисы докладов конференций
- Гребенников Электронная библиотека ИД журналы
- ЭБС Лань книги, журналы
- ЭБС Консультант студента
- ПРОСПЕКТ ЭБС
- ЭБС ZNANIUM.COM
- РГБ Информационное обслуживание по МБА
- БЕН РАН
- Электронно-библиотечная система (ЭБС) Кантитана (https://elib.kantiana.ru/)

11. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине.

Программное обеспечение обучения включает в себя:

- система электронного образовательного контента БФУ им. И. Канта – www.lms-3.kantiana.ru, обеспечивающую разработку и комплексное использование электронных образовательных ресурсов;
- серверное программное обеспечение, необходимое для функционирования сервера и связи с системой электронного обучения через Интернет;
- корпоративная платформа Microsoft Teams;
- установленное на рабочих местах обучающихся ПО: Microsoft Windows 7, Microsoft Office Standart 2010, антивирусное программное обеспечение Kaspersky Endpoint Security.
- специализированное ПО не требуется.

12. Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине.

Для проведения занятий лекционного типа, практических и семинарских занятий используются специальные помещения (учебные аудитории), оборудованные техническими средствами обучения – мультимедийной проекционной техникой. Для проведения занятий лекционного типа используются наборы демонстрационного оборудования.

Для проведения лабораторных работ, (практических занятий – при необходимости) используются специальные помещения (учебные аудитории), оснащенные специализированным лабораторным оборудованием: персональными компьютерами с возможностью выхода в интернет и с установленным программным обеспечением, заявленным в п.11.

Для проведения групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации используются специальные помещения (учебные аудитории), оборудованные специализированной мебелью (для обучающихся), меловой / маркерной доской.

Для организации самостоятельной работы обучающимся предоставляются помещения, оснащенные компьютерной техникой с возможностью подключения к сети «Интернет» и обеспечением доступа в электронную информационно-образовательную среду университета.

Для обучения инвалидов и лиц с ограниченными возможностями здоровья университетом могут быть представлены специализированные средства обучения, в том числе технические средства коллективного и индивидуального пользования.

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
федеральное государственное автономное образовательное учреждение высшего образования «Балтийский федеральный университет имени Иммануила Канта»
Институт физико-математических наук и информационных технологий

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

«Методы программирования»

Шифр: 10.05.01
Специальность: «Компьютерная безопасность»
Специализация: «Математические методы защиты информации»
Квалификация (степень) выпускника: специалист по защите информации

Калининград
2022

Лист согласования

Составитель: Верещагин Сергей Верещагин, к.ф.-м.н., доцент

Рабочая программа утверждена на заседании учебно-методического совета института физико-математических наук и информационных технологий

Протокол № 01/22 от «01» февраля 2022 г.

Председатель учебно-методического совета института физико-математических наук и информационных технологий

Первый заместитель директора ИФМНиИТ, к. ф.-м. н., доцент — Шпилевой А. А

Ведущий менеджер — Е.П.Ставицкая

Содержание

1.Наименование дисциплины: «Методы программирования».

Цель дисциплины: целью освоения дисциплины «Методы программирования» является фундаментальная и практическая подготовка обучающихся в области методы программирования.

2. Перечень планируемых результатов обучения по дисциплине, соотнесенных с планируемыми результатами освоения образовательной программы

Код компетенции	Результаты освоения образовательной программы (ИДК)	Результаты обучения по дисциплине
ОПК-7. Способен создавать программы на языках высокого и низкого уровня, применять методы и инструментальные средства программирования для решения профессиональных задач, осуществлять обоснованный выбор инструментария программирования и способов организации программ;	ОПК-7.1. Разрабатывает программы на языках высокого и низкого уровня. ОПК-7.2. Применяет известные методы программирования и возможности базового языка программирования для решения типовых профессиональных задач. ОПК-7.3. Осуществляет обоснованный выбор инструментария программирования и способов организации программ.	**Знать:** - Синтаксис языка Python - Синтаксис основных библиотек языка Python - Основные способы организации данных в языке Python - Синтаксис основных библиотек языка Python,их особенности, достоинства и недостатки - Основные способы организации данных в языке Python, их особенности, достоинства и недостатки **уметь:** - писать программы на языке Python - подключать дополнительные библиотеки - находить и исправлять ошибки в коде - оптимизировать программный код **владеть:** - навыками практической работы с IDE языка Python - навыками поиска информации о библиотеках языка Python, чтения их документации
ОПК-13. Способен разрабатывать компоненты программных и программно-аппаратных средств защиты информации в компьютерных системах и проводить анализ их безопасности;	ОПК-13.1. Знает принципы функционирования программных и программно-аппаратных средств защиты информации в компьютерных системах, принципы и методы разработки их компонент, методики анализа их безопасности. ОПК-13.2. Способен разрабатывать компоненты программных и программно-	- **Знать:** Принципы написания безопасного кода на языке Python Особенности реализации обработки ошибок и работы с паямятью на языке Python Способы обезопашивания ввода на языке Python Основы использования криптографических библиотек в языке Python - **уметь:**

	аппаратных средств защиты информации в компьютерных системах ОПК-13.3. Способен проводить анализ безопасности компонент программных и программно-аппаратных средств защиты информации в компьютерных системах	Писать код на языке Python корректно обрабатывающий пользовательский ввод, возможные ошибочные ситуации Применять стандартные криптографическое библиотеки - **владеть:** Навыками идентификации небезопасного кода и исправления его средствами автоматизированного тестирования кода

3. Место дисциплины в структуре образовательной программы

Дисциплин «Методы программирования» относится к обязательной части Блока 1 Дисциплины (Модули) подготовки специалиста по специальности 10.05.01«Компьютерная безопасность», специализация N 2 "Математические методы защиты информации".

4. Виды учебной работы по дисциплине.

Виды учебной работы по дисциплине зафиксированы учебным планом основной профессиональной образовательной программы по указанному направлению и профилю, выражаются в академических часах. Часы контактной работы и самостоятельной работы обчающегося и часы, отводимые на процедуры контроля, могут различаться в учебных планах ОПОП по формам обучения. Объем контактной работы включает часы контактной аудиторной работы (лекции/практические занятия/ лабораторные работы), контактной внеаудиторной работы (контроль самостоятельной работы), часы контактной работы в период аттестации. Контактная работа, в том числе может проводиться посредством электронной информационно-образовательной среды университета с использованием ресурсов сети Интернет и дистанционных технологий

5. Содержание дисциплины, структурированное по темам (разделам)

Исходя из рамок, установленных учебным планом по трудоемкости и видам учебной работы по дисциплине, преподаватель самостоятельно выбирает тематику занятий по формам и количеству часов проведения контактной работы: лекции и иные учебные занятия, предусматривающие преимущественную передачу учебной информации преподавателем и (или) занятия семинарского типа (семинары, практические занятия, практикумы, лабораторные работы, коллоквиумы и иные аналогичные занятия), и (или) групповые консультации, и (или) индивидуальную работу обучающихся с преподавателем, в том числе индивидуальные консультации (по курсовым работам/проектам – при наличии курсовой работы/проекта по данной дисциплине в учебном плане). Рекомендуемая тематика занятий максимально полно реализуется в контактной работе с обучающимися очной формы обучения. В случае реализации образовательной программы в заочной / очно-заочной форме трудоемкость дисциплины сохраняется, однако объем учебного материала в значительной части осваивается обучающимися в форме самостоятельной работы. При этом требования к ожидаемым образовательным результатам обучающихся по данной дисциплине не зависят от формы реализации образовательной программы.

№	Наименование раздела	Содержание раздела
1	Тема 1. Общее понятие о программировании.	Языки программирования. Компиляция и интерпретация. Менеджмент памяти. Процедурное,

	Виды языков программирования. Язык Python	функциональное, объектно-ориентированное программирование. Основные языки программирования. Особенности языка Python. IDE. Интерактивный и пакетный режим работы языка Python.
2	Тема 2. Базовые типы данных языка Python	Переменные. Int, float, str, list. Арифметические операции. Ввод и вывод
3	Тема 3. Условия и циклы	Базовые понятия условий и циклов. if..else. Условия. True и False. Булева алгебра и логические операции. Цикл while. Цикл for. Range. Break и Continue. Pass. Match.
4	Тема 4. Функции. Lambda-выражения	Определение функции. Передача параметров и возврат значений. Локальные, нелокальные и глобальные переменные. Рекурсия. Функция как переменная и функции высших порядков. Замыкания. Docstring. Lambda-выражения
5	Тема 5. Структуры данных	Коллективные типы данных. List, Tuple, Set, Dict. Стек и очередь. List и Set comprehension. Вложение структур данных. Работа с файлам. JSON.
6	Тема 6. Модули	Стандартные библиотеки. Подключение модулей. Создание своих модулей. Иерархическая стркутуризация модулей.
7	Тема 7. Классы, ООП.	Объектно ориентированное программитрование. Классы. Инстансы. Переопределение операторов. Наследование.
8	Тема 8. Исключения и их обработка	Исключения. Стандартные исключения. Обработка исключений. Пользовательские исключения
9	Тема 9. Стандартные библиотеки языка Python	Стандартные библиотеки языка Python. os. Glob,sys, re, math, random, statistics, urllib, datetime, timeit, doctest, unittest, template, zipfile,array
10	Тема 10. Библиотеки для работы с математикой	Numpy, SciPy, Matplotlib, SymPy
11	Тема 11. Реализация GUI в языке Python	Базовые представления о GUI. Обзор основных библиотек для работы с GUI. TKinter
12	Тема 12. Работа с графическими файлами	Бибилиотека Pillow

13	Тема 13. Работа с компьютерными сетями	Бибилиотека requests. Криптография и https. RPC
14	Тема 14. Параллельное программирование	Базовые идеи. Yield. Async

6. Рекомендуемая тематика учебных занятий в форме контактной работы

Рекомендуемая тематика учебных занятий *лекционного* типа (предусматривающих преимущественную передачу учебной информации преподавателями):

№	Наименование раздела	Темы лекций
1	Тема 1. Общее понятие о программировании. Виды языков программирования. Язык Python	Языки программирования. Компиляция и интерпретация. Менеджмент памяти. Процедурное, функциональное, объектно-ориентированное программирование. Основные языки программирования. Особенности языка Python. IDE. Интерактивный и пакетный режим работы языка Python.
2	Тема 2. Базовые типы данных языка Python	Переменные. Int, float, str, list. Арифметические операции. Ввод и вывод
3	Тема 3. Условия и циклы	Базовые понятия условий и циклов. if..else. Условия. True и False. Булева алгебра и логические операции. Цикл while. Цикл for. Range. Break и Continue. Pass. Match.
4	Тема 4. Функции. Lambda-выражения	Определение функции. Передача параметров и возврат значений. Локальные, нелокальные и глобальные переменные. Рекурсия. Функция как переменная и функции высших порядков. Замыкания. Docstring. Lambda-выражения
5	Тема 5. Структуры данных	Коллективные типы данных. List, Tuple, Set, Dict. Стек и очередь. List и Set comprehension. Вложение структур данных. Работа с файлам. JSON.
6	Тема 6. Модули	Стандартные библиотеки. Подключение модулей. Создание своих модулей. Иерархическая стркутуризация модулей.
7	Тема 7. Классы, ООП.	Объектно ориентированное программитрование. Классы. Инстансы. Переопределение операторов. Наследование.

8	Тема 8. Исключения и их обработка	Исключения. Стандартные исключения. Обработка исключений. Пользовательские исключения
9	Тема 9. Стандартные библиотеки языка Python	Стандартные библиотеки языка Python. os. Glob,sys, re, math, random, statistics, urllib, datetime, timeit, doctest, unittest, template, zipfile,array
10	Тема 10. Библиотеки для работы с математикой	Numpy, SciPy, Matplotlib, SymPy
11	Тема 11. Реализация GUI в языке Python	Базовые представления о GUI. Обзор основных библиотек для работы с GUI. TKinter
12	Тема 12. Работа с графическими файлами	Бибилиотека Pillow
13	Тема 13. Работа с компьютерными сетями	Бибилиотека requests. Криптография и https. RPC
14	Тема 14. Параллельное программирование	Базовые идеи. Yield. Async

Тематика лабораторных работ

№ темы	Наименование работ
1	Освоение IDE. Работа в интерактивном и пакетном режиме. Использование отладчика.
2	Написание программы демонстрирующей работу с базовыми типами данных
3	Написание программы демонстрирующей работу с циклами и условиями
4	Написание программы демонстрирующей работу с функциями
5	Написание программы демонстрирующей работу со сложными структурами данных
6	Написание программы демонстрирующей работу с модулями
7	Написание программы демонстрирующей работу с классами
8	Написание программы демонстрирующей работу с исключениями
9	Написание программы демонстрирующей работу со стандартными библиотеками языка Python

10	Написание программы демонстрирующей работу с библиотеками для работы с математикой
11	Написание программы демонстрирующей работу с Tkinter
12	Написание программы демонстрирующей работу с графическими файлами
13	Написание программы демонстрирующей работу с компьютерными сетями
14	Написание программы демонстрирующей параллельное программирование

Требования к самостоятельной работе обучающихся

1. Работа с лекционным материалом, предусматривающая проработку конспекта лекций и учебной литературы, по всем темам из п. 6 настоящей рабочей программы.
2. Выполнение домашнего задания, предусматривающего решение задач, выполнение упражнений, выдаваемых на практических занятиях, по всем темам из п. 6 настоящей рабочей программы.

Руководствуясь положениями статьи 47 и статьи 48 Федерального закона от 29 декабря 2012 г. N 273-ФЗ «Об образовании в Российской Федерации» научно-педагогические работники и иные лица, привлекаемые университетом к реализации данной образовательной программы, пользуются предоставленными академическими правами и свободами в части свободы преподавания, свободы от вмешательства в профессиональную деятельность; свободы выбора и использования педагогически обоснованных форм, средств, методов обучения и воспитания; права на творческую инициативу, разработку и применение авторских программ и методов обучения и воспитания в пределах реализуемой образовательной программы и отдельной дисциплины.

Исходя из рамок, установленных учебным планом по трудоемкости и видам учебной работы по дисциплине, преподаватель самостоятельно выбирает тематику занятий по формам и количеству часов проведения контактной работы: лекции и иные учебные занятия, предусматривающие преимущественную передачу учебной информации преподавателем и (или) занятия семинарского типа (семинары, практические занятия, практикумы, лабораторные работы, коллоквиумы и иные аналогичные занятия), и (или) групповые консультации, и (или) индивидуальную работу обучающихся с преподавателем, в том числе индивидуальные консультации (по курсовым работам/проектам – при наличии курсовой работы/проекта по данной дисциплине в учебном плане).

Рекомендуемая тематика занятий максимально полно реализуется в контактной работе с обучающимися очной формы обучения. В случае реализации образовательной программы в заочной / очно-заочной форме трудоемкость дисциплины сохраняется, однако объем учебного материала в значительной части осваивается обучающимися в форме самостоятельной работы. При этом требования к ожидаемым образовательным результатам обучающихся по данной дисциплине не зависят от формы реализации образовательной программы.

7. Методические рекомендации по видам занятий

Лекционные занятия.

В ходе лекционных занятий обучающимся рекомендуется выполнять следующие действия. Вести конспектирование учебного материала. Обращать внимание на категории, формулировки, раскрывающие содержание тех или иных явлений и процессов, научные выводы и практические рекомендации по их применению. Задавать преподавателю уточняющие вопросы с целью уяснения теоретических положений, разрешения спорных ситуаций.

Желательно оставить в рабочих конспектах поля, на которых во внеаудиторное время можно сделать пометки из рекомендованной литературы, дополняющие материал прослушанной лекции, а также подчеркивающие особую важность тех или иных теоретических положений.

Практические и семинарские занятия.

На практических и семинарских занятиях в зависимости от темы занятия выполняется поиск информации по решению проблем, практические упражнения, контрольные работы, выработка индивидуальных или групповых решений, итоговое обсуждение с обменом знаниями, участие в круглых столах, разбор конкретных ситуаций, командная работа, представление портфолио и т.п.

Самостоятельная работа.

Самостоятельная работа осуществляется в виде изучения литературы, эмпирических данных по публикациям и конкретных ситуаций из практики, подготовке индивидуальных работ, работа с лекционным материалом, самостоятельное изучение отдельных тем дисциплины; поиск и обзор литературы и электронных источников; чтение и изучение учебника и учебных пособий.

8. Фонд оценочных средств

8.1. Перечень компетенций с указанием этапов их формирования в процессе освоения образовательной программы в рамках учебной дисциплины

Основными этапами формирования указанных компетенций при изучении обучающимися дисциплины являются последовательное изучение содержательно связанных между собой тем учебных занятий. Изучение каждой темы предполагает овладение обучающимися необходимыми компетенциями. Результат аттестации обучающихся на различных этапах формирования компетенций показывает уровень освоения компетенций.

образовательной программы в рамках учебной дисциплины

Контролируемые модули, разделы (темы) дисциплины	Индекс контролируемой компетенции (или её части)	Оценочные средства по этапам формирования компетенций
		текущий контроль по дисциплине
Тема 1. Общее понятие о программировании. Виды языков программирования. Язык Python	ОПК-7 ОПК-13	Написание и проверка контрольной программы
Тема 2. Базовые типы данных языка Python	ОПК-7	Написание и проверка контрольной программы

	ОПК-13	
Тема 3. Условия и циклы	ОПК-7 ОПК-13	Написание и проверка контрольной программы
Тема 4. Функции. Lambda-выражения	ОПК-7 ОПК-13	Написание и проверка контрольной программы
Тема 5. Структуры данных	ОПК-7 ОПК-13	Написание и проверка контрольной программы
Тема 6. Модули	ОПК-7 ОПК-13	Написание и проверка контрольной программы
Тема 7. Классы, ООП.	ОПК-7 ОПК-13	Написание и проверка контрольной программы
Тема 8. Исключения и их обработка	ОПК-7 ОПК-13	Написание и проверка контрольной программы
Тема 9. Стандартные библиотеки языка Python	ОПК-7 ОПК-13	Написание и проверка контрольной программы
Тема 10. Библиотеки для работы с математикой	ОПК-7 ОПК-13	Написание и проверка контрольной программы
Тема 10. Библиотеки для работы с математикой	ОПК-7 ОПК-13	Написание и проверка контрольной программы
Тема 11. Реализация GUI в языке Python	ОПК-7 ОПК-13	Написание и проверка контрольной программы
Тема 12. Работа с графическими файлами	ОПК-7 ОПК-13	Написание и проверка контрольной программы
Тема 13. Работа с компьютерными сетями	ОПК-7 ОПК-13	Написание и проверка контрольной программы
Тема 14. Параллельное программирование	ОПК-7 ОПК-13	Написание и проверка контрольной программы

8.2. Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений и навыков и (или) опыта деятельности процессе текущего контроля

Тема 1. Общее понятие о программировании. Виды языков программирования. Язык Python

Рассчитать в консоли (2+5)**3/3.3

Тема 2. Базовые типы данных языка Python

Вывести пирамиду квадрат 3 на 3 из символов *

Тема 3. Условия и циклы

Вывести на экран все простые числа меньше 1000

Тема 4. Функции. Lambda-выражения

Вывести на экран все простые числа меньше 1000. Оформить проверку на простоту в виде отдельной функции.

Тема 5. Структуры данных

Вывести на экран список содержащий все простые числа меньше 1000. Использовать list comprehension для формирования этого списка.

Тема 6. Модули

Вывести на экран все простые числа меньше 1000. Оформить проверку на простоту в виде отдельной функции, которая должна быть вынесена в отдельный модуль и подключаться из него.

Тема 7. Классы, ООП.

Создать класс для работы с 3-х мерными векторами, поддерживающий все необходимые арифметические операции.

Тема 8. Исключения и их обработка

Создать программу которая ищет в файле самое большое число. Программа должна корректно обрабатывать все возможные проблемы чтения из файла при помощи исключений.

Тема 9. Стандартные библиотеки языка Python

Создать программу которая выводит на экран текущее время.

Тема 10. Библиотеки для работы с математикой

Создать программу которая рисует график $y=x^2$

Тема 11. Реализация GUI в языке Python

Написать графический калькулятор, который складывает 2 числа

Тема 12. Работа с графическими файлами

Создать программу которая считывает jpeg файл, подписывает его ткущим числом и сохраняет обратно то что получилось.

Тема 13. Работа с компьютерными сетями

Создать программу которая ищет в файле самое большое число. Файл должен быть считан с web-сервера в интернете.

Тема 14. Параллельное программирование

Вывести на экран все простые числа меньше 1000. Проверка на простоту должна осущевствляться в несколько потоков.

8.3 Вопросы для промежуточного контроля (зачёта)

1. Общее понятие о программировании. Виды языков программирования. Язык Python
2. Базовые типы данных языка Python
3. Условия и циклы
4. Функции. Lamda-выпаженния

5. Структуры данных
6. Модули
7. Классы, ООП.
8. Исключения и их обработка
9. Стандартные библиотеки языка Python
10. Библиотеки для работы с математикой
11. Реализация GUI в языке Python
12. Работа с графическими файлами
13. Работа с компьютерными сетями
14. Параллельное программирование

8.4. Планируемые уровни сформированности компетенций обучающихся и критерии оценивания

Уровни	Содержательное описание уровня	Основные признаки выделения уровня (этапы формирования компетенции, критерии оценки сформированности)	Пятибалльная шкала (академическая) оценка	Двухбалльная шакала, зачет	БРС, % освоения (рейтинговая оценка)
Повышенный	Творческая деятельность	*Включает нижестоящий уровень.* Умение самостоятельно принимать решение, решать проблему/задачу теоретического и прикладного характера на основе изученных методов, приемов, технологий	отлично	зачтено	86-100
Базовый	Применение знаний и умений в более широких контекстах учебной и профессиональной деятельности, нежели по образцу с	*Включает нижестоящий уровень.* Способность собирать, систематизировать, анализировать и грамотно использовать информацию из самостоятельно найденных теоретических источников и иллюстрировать ими	хорошо		71-85

	большей степени самостоятельности и инициативы	теоретические положения или обосновывать практику применения			
Удовлетворительный (достаточный)	Репродуктивная деятельность	Изложение в пределах задач курса теоретически и практически контролируемого материала	удовлетворительно		55-70
Недостаточный	Отсутствие признаков удовлетворительного уровня		неудовлетворительно	не зачтено	Менее 55

9. ПЕРЕЧЕНЬ ОСНОВНОЙ И ДОПОЛНИТЕЛЬНОЙ ЛИТЕРАТУРЫ, НЕОБХОДИМОЙ ДЛЯ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Основная литература

1. Гуриков Сергей Ростиславович «Основы алгоритмизации и программирования на Python» [Электронный ресурс]: учеб. ISBN 978-5-16-102278-8 : Б.ц. Имеются экземпляры в отделах: ЭБС Знаниум(3)
https://znanium.com/catalog/document?id=379975

Дополнительная литература

2. Жуков Роман Александрович «Язык программирования Python: практикум » [Электронный ресурс]: учеб. ISBN 978-5-16-107207-3 Б.ц. Имеются экземпляры в отделах: ЭБС Знаниум(3)
https://znanium.com/catalog/document?id=378601

10. Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины (модуля).

- НЭБ Национальная электронная библиотека, диссертации и прочие издания
- eLIBRARY.RU Научная электронная библиотека, книги, статьи, тезисы докладов конференций
- Гребенников Электронная библиотека ИД журналы
- ЭБС Лань книги, журналы
- ЭБС Консультант студента
- ПРОСПЕКТ ЭБС
- ЭБС ZNANIUM.COM
- РГБ Информационное обслуживание по МБА
- БЕН РАН
- Электронно-библиотечная система (ЭБС) Кантитана (https://elib.kantiana.ru/)

11. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине.

Программное обеспечение обучения включает в себя:

- система электронного образовательного контента БФУ им. И. Канта – www.lms-3.kantiana.ru, обеспечивающую разработку и комплексное использование электронных образовательных ресурсов;

- серверное программное обеспечение, необходимое для функционирования сервера и связи с системой электронного обучения через Интернет;
- корпоративная платформа Microsoft Teams;
- установленное на рабочих местах обучающихся ПО: Microsoft Windows 7, Microsoft Office Standart 2010, антивирусное программное обеспечение Kaspersky Endpoint Security.
- Среда программирования Microsoft Visual Studio (любая версия);
- Qt версии 5.0 и выше

12. Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине.

Для проведения занятий лекционного типа, практических и семинарских занятий используются специальные помещения (учебные аудитории), оборудованные техническими средствами обучения – мультимедийной проекционной техникой. Для проведения занятий лекционного типа используются наборы демонстрационного оборудования.

Для проведения лабораторных работ, (практических занятий – при необходимости) используются специальные помещения (учебные аудитории), оснащенные специализированным лабораторным оборудованием: персональными компьютерами с возможностью выхода в интернет и с установленным программным обеспечением, заявленным в п.11.

Для проведения групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации используются специальные помещения (учебные аудитории), оборудованные специализированной мебелью (для обучающихся), меловой / маркерной доской.

Для организации самостоятельной работы обучающимся предоставляются помещения, оснащенные компьютерной техникой с возможностью подключения к сети «Интернет» и обеспечением доступа в электронную информационно-образовательную среду университета.

Для обучения инвалидов и лиц с ограниченными возможностями здоровья университетом могут быть представлены специализированные средства обучения, в том числе технические средства коллективного и индивидуального пользования.

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
федеральное государственное автономное образовательное учреждение высшего образования «Балтийский федеральный университет имени Иммануила Канта»
Институт физико-математических наук и информационных технологий

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

«ТЕОРИЯ ПСЕВДОСЛУЧАЙНЫХ ГЕНЕРАТОРОВ»

Шифр: 10.05.01
Специальность: «Компьютерная безопасность»
Специализация: «Математические методы защиты информации»
Квалификация (степень) выпускника: специалист по защите информации

Калининград
2022

Лист согласования

Составитель: БОЛТНЕВ ЮРИЙ ФЕДОРОВИЧ. старший преподаватель

Рабочая программа утверждена на заседании учебно-методического совета института физико-математических наук и информационных технологий
Протокол № 01/22 от «01» февраля 2022 г.

Председатель учебно-методического совета института физико-математических наук и информационных технологий
Первый заместитель директора ИФМНиИТ, к. ф.-м. н., доцент — Шпилевой А. А

Ведущий менеджер — Е.П.Ставицкая

СОДЕРЖАНИЕ

1. Наименование дисциплины: «ТЕОРИЯ ПСЕВДОСЛУЧАЙНЫХ ГЕНЕРАТОРОВ»

Целями освоения дисциплины «***Теория псевдослучайных генераторов***» являются:

- углубление общей математической подготовки студентов в областях прикладной алгебры, теории вероятностей и математической статистики, непосредственно используемых в криптографии и теории кодирования;
- изучение методов построения и исследования свойств потоковых шифров, способов их применения в компьютерных системах.

2. <u>Перечень планируемых результатов обучения по дисциплине, соотнесенных с планируемыми результатами освоения образовательной программы</u>

Код компетенции	**Результаты освоения образовательной программы (ИДК)**	**Результаты обучения по дисциплине**
ОПК-2.2. Способен разрабатывать и анализировать математические модели механизмов защиты информации	ОПК-2.2.1. Знает принципы построения средств криптографической защиты информации ОПК-2.2.2. Умеет выявлять наиболее целесообразные подходы к обеспечению защиты информации компьютерной системы ОПК-2.2.3. Владеет методами разработки математических моделей, реализуемых в средствах защиты информации	***знать***: - классификацию методов и принципы построения потоковых шифров; - классификацию и методы анализа стойкости потоковых шифров; - структуру и принципы работы регистров сдвига; - принципы и методы проектирования потоковых шифров; - общие принципы экспериментального и теоретического исследования потоковых шифров; оценки сложности алгоритмов. - общие принципы экспериментального и теоретического исследования задачи построения псевдослучайных последовательностей, подходящих для криптографических приложений. ***уметь***: - строить схемы и математические модели регистров сдвига; - проектировать потоковые шифры; - осуществлять тестирование статистических свойств псевдослучайных последовательностей; - строить математическую модель генератора, соответствующую схеме его работы; - проводить анализ безопасности компьютерных систем на соответствие стандартам в области компьютерной безопасности. - формулировать задачу по оцениванию безопасности криптографического алгоритма применительно к конкретным условиям; применять математические методы исследования криптографических алгоритмов. ***владеть***: - методикой проектирования потоковых шифров;

		− математическими методами оценки статистического качества потоковых шифров; − методикой проектирования потоковых шифров на основе комбинирования различных ГПСЧ; − методикой предварительной оценки стойкости различных типов потоковых шифров; − методами оценки корректности и стойкости соответствующих алгоритмов; навыками математического моделирования в криптографии.

3. Место дисциплины в структуре ООП ВО

Дисциплина «*Теория псевдослучайных генераторов»* представляет собой дисциплину базовой части блока дисциплин подготовки обучающихся.

4. Виды учебной работы по дисциплине.

Виды учебной работы по дисциплине зафиксированы учебным планом основной профессиональной образовательной программы по указанному направлению и профилю, выражаются в академических часах. Часы контактной работы и самостоятельной работы студента и часы, отводимые на процедуры контроля, могут различаться в учебных планах ОПОП по формам обучения. Объем контактной работы включает часы контактной аудиторной работы (лекции/практические занятия/ лабораторные работы), контактной внеаудиторной работы (контроль самостоятельной работы), часы контактной работы в период аттестации. Контактная работа, в том числе может проводиться посредством электронной информационно-образовательной среды университета с использованием ресурсов сети Интернет и дистанционных технологий

5. Содержание дисциплины, структурированное по темам (разделам)

Исходя из рамок, установленных учебным планом по трудоемкости и видам учебной работы по дисциплине, преподаватель самостоятельно выбирает тематику занятий по формам и количеству часов проведения контактной работы: лекции и иные учебные занятия, предусматривающие преимущественную передачу учебной информации преподавателем и (или) занятия семинарского типа (семинары, практические занятия, практикумы, лабораторные работы, коллоквиумы и иные аналогичные занятия), и (или) групповые консультации, и (или) индивидуальную работу обучающихся с преподавателем, в том числе индивидуальные консультации (по курсовым работам/проектам – при наличии курсовой работы/проекта по данной дисциплине в учебном плане). Рекомендуемая тематика занятий максимально полно реализуется в контактной работе со студентами очной формы обучения. В случае реализации образовательной программы в заочной / очно-заочной форме трудоемкость дисциплины сохраняется, однако объем учебного материала в значительной части осваивается студентами в форме самостоятельной работы. При этом требования к ожидаемым образовательным результатам студентов по данной дисциплине не зависят от формы реализации образовательной программы.

Тема 1. ЛРП, регистры сдвига и потоковые шифры. Методы статистического анализа случайных и псевдослучайных последовательностей

Задачи и программа курса. Место теории ЛРП в ряду других математических дисциплин. Источники её развития и области приложения. Формы самостоятельной работы студентов по изучению курса. Основная литература к курсу.

Равномерно распределённая случайная последовательность. Потоковые шифры. Связь потоковых шифров с ПСГ и ЛРП. Реальные случайные последовательности.

Линейная сложность. Постулаты Голомба. Статистические тесты. Универсальный алгоритм статистического тестирования. Тест на частоту. Последовательный тест. Тест серий. Покерный тест. Тест пробегов. Тест автокорреляции. Обзор других тестов.

Тема 2. Общие свойства ЛРП. ЛРП над конечными полями

Умножение последовательности на многочлен. Генератор ЛРП. Минимальный многочлен и аннулятор ЛРП. Вычисление многочлена по заданной ЛРП. Соотношения между свойствами ЛРП с различными характеристическими многочленами. Биномиальный базис пространства ЛРП над полем.

Представление ЛРП над конечным полем с помощью функции следа. Периодические последовательности. Периодические многочлены. Периодичность ЛРП над конечным кольцом. Линейные рекуррентные последовательности в конечных полях: вычисление периода и длины подхода ЛРП над конечным полем.

Тема 3 m-последовательности. Корреляционные свойства ЛРП

ЛРП максимального периода над конечным полем. Связь бинарных m-последовательностей с регистрами сдвига. Свойства минимального многочлена m-последовательности.

Автокорреляционная функция, её свойства и вычисление. Функция кросс-корреляции и экспоненциальные суммы над конечными полями. Суммы Клостермана. Квадратичные формы над конечными полями. Их свойства и связи с m-последовательностями.

Тема 4. Регистры сдвига. Методы построения потоковых шифров

Регистры сдвига с линейной обратной связью (LFSR). Математическая модель. Примеры. Аддитивные генераторы. Примеры. Генератор Таусворта. Регистры сдвига с обратной связью по переносу (FCSR). Регистры сдвига с нелинейной обратной связью. Примеры.

Системно-теоретический подход к проектированию. Сложностно-теоретический подход. Примеры. Полиномиальное комбинирование генераторов. Комбинирование генераторов с помощью псевдослучайного прореживания. Примеры.

6. Рекомендуемая тематика учебных занятий в форме контактной работы

Рекомендуемая тематика учебных занятий лекционного типа (предусматривающих преимущественную передачу учебной информации преподавателями):

№	Наименование раздела	Темы лекций
1	ЛРП, регистры сдвига и потоковые шифры. Методы	Задачи и программа курса. Место теории ЛРП в ряду других

	статистического анализа случайных и псевдослучайных последовательностей	математических дисциплин. Источники её развития и области приложения. Формы самостоятельной работы студентов по изучению курса. Основная литература к курсу. Равномерно распределённая случайная последовательность. Потоковые шифры. Связь потоковых шифров с ПСГ и ЛРП. Реальные случайные последовательности. Линейная сложность. Постулаты Голомба. Статистические тесты. Универсальный алгоритм статистического тестирования. Тест на частоту. Последовательный тест. Тест серий. Покерный тест. Тест пробегов. Тест автокорреляции. Обзор других тестов.
2	Общие свойства ЛРП. ЛРП над конечными полями	Умножение последовательности на многочлен. Генератор ЛРП. Минимальный многочлен и аннулятор ЛРП. Вычисление многочлена по заданной ЛРП. Соотношения между свойствами ЛРП с различными характеристическими многочленами. Биномиальный базис пространства ЛРП над полем. Представление ЛРП над конечным полем с помощью функции следа. Периодические последовательности. Периодические многочлены. Периодичность ЛРП над конечным кольцом. Линейные рекуррентные последовательности в конечных полях: вычисление периода и длины подхода ЛРП над конечным полем
3	m-последовательности. Корреляционные свойства ЛРП	ЛРП максимального периода над конечным полем. Связь бинарных m-последовательностей с регистрами сдвига. Свойства минимального многочлена m-последовательности. Автокорреляционная функция, её свойства и вычисление. Функция кросс-корреляции и экспоненциальные суммы над конечными полями. Суммы Клостермана. Квадратичные формы над конечными полями. Их свойства и связи с m-последовательностями
4	Регистры сдвига. Методы построения потоковых шифров	Регистры сдвига с линейной обратной связью (LFSR). Математическая модель. Примеры. Аддитивные генераторы. Примеры. Генератор Таусворта. Регистры сдвига с обратной связью по переносу (FCSR). Регистры сдвига с нелинейной обратной связью. Примеры. Системно-теоретический подход к проектированию. Сложностно-теоретический подход. Примеры. Полиномиальное комбинирование генераторов. Комбинирование генераторов с помощью псевдослучайного прореживания. Примеры.

Тематика практических занятий

Тема 1. Равномерно распределённая случайная последовательность. Потоковые шифры. Связь потоковых шифров с ПСГ и ЛРП. Реальные случайные последовательности.

Статистическое тестирование конкретных последовательностей с использованием различных тестов.

Тема 2. Алгоритм умножения ЛРП на многочлен. Вычисление генератора, минимального многочлена и аннулятора ЛРП. Вычисление характеристик пространств ЛРП. Построение примеров биномиальных базисов пространства ЛРП.

Построение ЛРП над конечным полем с помощью функции следа. Вычисление их характеристик. Вычисление периода и длины подхода периодических многочленов и периодических ЛРП.

Тема 3. Реализация, анализ быстродействия и стойкости m-последовательностей, генерируемых различными LFSR.

Вычисление автокорреляционной функции ЛРП над конечным полем. Вычисление кросс-корреляционной функции ЛРП над конечным полем.

Тема 4. Реализация, анализ быстродействия и стойкости регистров сдвига различных типов. Проектирование конкретных примеров потоковых шифров.

Темы практических заданий

1. Разработать программу для построения линейной рекуррентной последовательности заданного периода. Рассчитать примеры. Дать краткое описание методики.
2. Разработать программу, вычисляющую характеристический многочлен линейной рекуррентной последовательности (ЛРП), полученной из *m*-последовательности путем децимации. Рассчитать примеры. Дать краткое описание методики.
3. Разработать программу, вычисляющую функцию кросс-корреляции между *m*-последовательностью и ее децимацией. Дать краткое описание методики.
4. Разработать программу для построения ЛРП на основе линейного регистра сдвига с обратной связью (LFSR). Определить период построенной ЛРП. Дать краткое описание методики.
5. Разработать программу для построения линейного конгруэнтного генератора. Исследовать зависимость периода ЛРП от параметров генератора. Дать краткое описание методики.
6. Разработать программу для статистического тестирования псевдослучайных последовательностей. Дать краткое описание методики.
7. Разработать программу, для построения BBS-генератора. Исследовать свойства построенной генератором последовательности. Дать краткое описание методики.

Требования к самостоятельной работе обучающихся

1. Работа с лекционным материалом, предусматривающая проработку конспекта лекций и учебной литературы, по всем темам из п. 6 настоящей рабочей программы.
2. Выполнение домашнего задания, предусматривающего решение задач, выполнение упражнений, выдаваемых на практических занятиях, по всем темам из п. 6 настоящей рабочей программы.

Руководствуясь положениями статьи 47 и статьи 48 Федерального закона от 29 декабря 2012 г. N 273-ФЗ «Об образовании в Российской Федерации» научно-педагогические работники и иные лица, привлекаемые университетом к реализации данной образовательной программы, пользуются

предоставленными академическими правами и свободами в части свободы преподавания, свободы от вмешательства в профессиональную деятельность; свободы выбора и использования педагогически обоснованных форм, средств, методов обучения и воспитания; права на творческую инициативу, разработку и применение авторских программ и методов обучения и воспитания в пределах реализуемой образовательной программы и отдельной дисциплины.

Исходя из рамок, установленных учебным планом по трудоемкости и видам учебной работы по дисциплине, преподаватель самостоятельно выбирает тематику занятий по формам и количеству часов проведения контактной работы: лекции и иные учебные занятия, предусматривающие преимущественную передачу учебной информации преподавателем и (или) занятия семинарского типа (семинары, практические занятия, практикумы, лабораторные работы, коллоквиумы и иные аналогичные занятия), и (или) групповые консультации, и (или) индивидуальную работу обучающихся с преподавателем, в том числе индивидуальные консультации (по курсовым работам/проектам – при наличии курсовой работы/проекта по данной дисциплине в учебном плане).

Рекомендуемая тематика занятий максимально полно реализуется в контактной работе с обучающимися очной формы обучения. В случае реализации образовательной программы в заочной / очно-заочной форме трудоемкость дисциплины сохраняется, однако объем учебного материала в значительной части осваивается обучающимися в форме самостоятельной работы. При этом требования к ожидаемым образовательным результатам обучающихся по данной дисциплине не зависят от формы реализации образовательной программы.

7. Методические рекомендации по видам занятий

Лекционные занятия.

В ходе лекционных занятий обучающимся рекомендуется выполнять следующие действия. Вести конспектирование учебного материала. Обращать внимание на категории, формулировки, раскрывающие содержание тех или иных явлений и процессов, научные выводы и практические рекомендации по их применению. Задавать преподавателю уточняющие вопросы с целью уяснения теоретических положений, разрешения спорных ситуаций.

Желательно оставить в рабочих конспектах поля, на которых во внеаудиторное время можно сделать пометки из рекомендованной литературы, дополняющие материал прослушанной лекции, а также подчеркивающие особую важность тех или иных теоретических положений.

Практические и семинарские занятия.

На практических и семинарских занятиях в зависимости от темы занятия выполняется поиск информации по решению проблем, практические упражнения, контрольные работы, выработка индивидуальных или групповых решений, итоговое обсуждение с обменом знаниями, участие в круглых столах, разбор конкретных ситуаций, командная работа, представление портфолио и т.п.

Самостоятельная работа.

Самостоятельная работа осуществляется в виде изучения литературы, эмпирических данных по публикациям и конкретных ситуаций из практики, подготовке индивидуальных работ, работа с лекционным материалом, самостоятельное изучение отдельных тем дисциплины; поиск и обзор литературы и электронных источников; чтение и изучение учебника и учебных пособий.

8. Фонд оценочных средств

8.1 Перечень компетенций с указанием этапов их формирования в процессе освоения образовательной программы

Основными этапами формирования указанных компетенций при изучении студентами дисциплины являются последовательное изучение содержательно связанных между собой *разделов*

(*тем*) учебных занятий. Изучение каждого раздела (темы) предполагает овладение студентами необходимыми компетенциями. Результат аттестации студентов на различных этапах формирования компетенций показывает уровень освоения компетенций студентами.

Контролируемые модули, разделы (темы) дисциплины	Индекс контролируемой компетенции (или её части)	Оценочные средства по этапам формирования компетенций
Тема 1. ЛРП, регистры сдвига и потоковые шифры. Методы статистического анализа случайных и псевдослучайных последовательностей	ОПК-2.2	Решение задач
Тема 2. Общие свойства ЛРП. ЛРП над конечными полями	ОПК-2.2	Решение задач Контр. работа
Тема 3. m-последовательности. Корреляционные свойства ЛРП	ОПК-2.2	Решение задач. Контр. работа
Тема 4. Регистры сдвига. Методы построения потоковых шифров	ОПК-2.2	Решение задач

8.2. Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений и навыков и (или) опыта деятельности процессе текущего контроля

Типовые контрольные задания

Контрольная работа №1

«Вычисление характеристик ЛРП над конечными полями»

1. Найти минимальный многочлен ЛРП u над полем Φ_2, если $(X+1)^3(X^2+X)u = (01111011\ldots)$
2. Вычислить период многочлена

$$f(X) = X^5 + X^2 + X + 1$$

над полем Φ_2. Имеет ли этот многочлен максимальный период?
3. Построить регистр сдвига для m-последовательности с характеристическим многочленом

$$X^3 + X + 1.$$

4. Пусть $f = X^2 + X + 2 \in \Phi_3[X]$. Задать ЛРП максимального периода с характеристическим многочленом f над Φ_3 с помощью функции следа.

Контрольные вопросы для самоконтроля

Тема 1. ЛРП, регистры сдвига и потоковые шифры. Методы статистического анализа случайных и псевдослучайных последовательностей.

	Вопрос

Оценка «удовлетворительно» - низкой уровень освоения компетенции	Перечислить постулаты Голомба
Оценка «хорошо» - повышенный уровень освоения компетенции	Дать описание последовательного теста
Оценка «отлично» - высокий уровень освоения компетенции	Дать описание теста пробегов

Примеры задач для решения

Тема 2. Общие свойства ЛРП. ЛРП над конечными полями

	Задача
Оценка «удовлетворительно» или низкой уровень освоения компетенции	Вычислить период многочлена $f(X) = X^4 + 2X^2 + X + 2$ над полем Φ_3. Имеет ли этот многочлен максимальный период?
Оценка «хорошо» или повышенный уровень освоения компетенции	Найти генератор и минимальный многочлен ЛРП u над полем $k = \Phi_5$ с характеристическим многочленом $F(X) = X^5 + X^3 + 3X^2 + 4X + 1$, если $u(0, 1,\ldots, m-1) = (01234)$
Оценка «отлично» или высокий уровень освоения компетенции	Пусть $f = X^2 + X + 2 \in \Phi_3[X]$. Задать ЛРП максимального периода с характеристическим многочленом f над Φ_3 с помощью функции следа.

Тема 3. m-последовательности. Корреляционные свойства ЛРП.

	Задача
Оценка «удовлетворительно» или низкой уровень освоения компетенции	Вычислить значение кросскорреляционной функции для последовательности (+1,–1,+1,–1,–1,–1,–1,+1,+1) и её циклического сдвига на $\tau = 3$.
Оценка «хорошо» или повышенный уровень освоения компетенции	Пусть $x = (-1,+1,-1,-1)$, $y = (-1,-1,-1,+1,+1,-1,+1)$ есть m-последовательности длины 4 и 7 соответственно. Вычислить значение кросскорреляционной функции $C(\tau)$ для $0 \le \tau \le 10$.
Оценка «отлично» или высокий уровень освоения компетенции	Пусть $x = (+1,+1,-1,-1,+1)$, $y = (+1,-1,-1,+1,-1,-1,+1)$ есть m-последовательности длины 5 и 7 соответственно. Вычислить значение кросскорреляционной функции $C(\tau)$ для $0 \le \tau \le 10$.

Тема 4. Регистры сдвига. Методы построения потоковых шифров.

	Задача
Оценка «удовлетворительно» или низкой уровень освоения компетенции	Построить регистр сдвига для m-последовательности с характеристическим многочленом $X^3 + X + 1$.
Оценка «хорошо» или повышенный уровень освоения компетенции	Построить два ГПСЧ с характеристическими многочленами $X^{17} + X^5 + 1$ и $X^{11} + X^2 + 1$.
Оценка «отлично» или высокий уровень освоения компетенции	Построить два ГПСЧ с характеристическими многочленами $X^{18} + X^6 + 1$ и $X^9 + X^4 + 1$. Используя псевдослучайное прореживание, построить комбинированный генератор.

8.3. Перечень вопросов и заданий для промежуточной аттестации по дисциплине

Вопросы для промежуточного контроля (экзамена)

1. Равномерно распределённая случайная последовательность и её свойства. Связь с потоковыми шифрами.
2. Методы генерации реальных случайных последовательностей.
3. Линейная сложность. Постулаты Голомба. Статистические тесты.
4. Универсальный алгоритм статистического тестирования.
5. Тест на частоту. Последовательный тест.
6. Тест серий. Покерный тест.
7. Тест пробегов. Тест автокорреляции.
8. Линейные рекуррентные последовательности. Определение и простейшие свойства.
9. Умножение последовательности на многочлен. Пространство последовательностей.
10. Операции над последовательностями: умножение на элемент кольца. Сдвиг, полиномиальный оператор.
11. Характеристический многочлен ЛРП, начальный вектор.
12. Образующие элементы модуля ЛРП. Генератор ЛРП.
13. Аннулирующий идеал. Аннулирующий многочлен, его свойства.
14. Минимальный многочлен и аннулятор ЛРП. Основное свойство минимального многочлена.
15. Соотношения между свойствами ЛРП с различными характеристическими многочленами.
16. Биномиальный базис пространства ЛРП над полем.
17. Представление ЛРП над конечным полем с помощью функции следа.
18. Периодические последовательности. Периодические многочлены. Периодичность ЛРП над конечным кольцом.
19. Вычисление периода неприводимого многочлена.
20. Вычисление периода произвольного многочлена по его каноническому разложению.

21. Вычисление периода ЛРП над конечным полем по её минимальному многочлену.
22. ЛРП максимального периода над конечным полем, их простейшие свойства. Генерирование бинарной последовательности с помощью регистра сдвига.
23. Биномиальная последовательность и её минимальный многочлен.
24. Примитивность характеристического многочлена.
25. Циклическая эквивалентность последовательностей.
26. Проективная циклическая эквивалентность последовательностей.
27. Автокорреляционная функция, её свойства и вычисление.
28. Функция кросс-корреляции и экспоненциальные суммы над конечными полями.
29. Регистры сдвига с линейной обратной связью (LFSR). Математическая модель. Примеры.
30. Аддитивные генераторы. Примеры.
31. Регистры сдвига с обратной связью по переносу (FCSR). Примеры.
32. Регистры сдвига с нелинейной обратной связью. Примеры.
33. Различные подходы к проектированию потоковых шифров. Примеры.
34. Полиномиальное комбинирование генераторов. Примеры.
35. Комбинирование генераторов с помощью псевдослучайного прореживания. Примеры.

8.4. Планируемые уровни сформированности компетенций обучающихся и критерии оценивания

Уровни	Содержательное описание уровня	Основные признаки выделения уровня (этапы формирования компетенции, критерии оценки сформированности)	Пятибалльная шкала (академическая) оценка	Двухбалльная шакала, зачет	БРС, % освоения (рейтинговая оценка)
Повышенный	Творческая деятельность	*Включает нижестоящий уровень.* Умение самостоятельно принимать решение, решать проблему/задачу теоретического и прикладного характера на основе изученных методов, приемов, технологий	отлично	зачтено	86-100
Базовый	Применение знаний и умений в более широких контекстах учебной и профессиональной	*Включает нижестоящий уровень.* Способность собирать, систематизировать, анализировать и грамотно использовать информацию из самостоятельно найденных	хорошо		71-85

	деятельности, нежели по образцу с большей степени самостоятельности и инициативы	теоретических источников и иллюстрировать ими теоретические положения или обосновывать практику применения			
Удовлетворительный (достаточный)	Репродуктивная деятельность	Изложение в пределах задач курса теоретически и практически контролируемого материала	удовлетворительно		55-70
Недостаточный	Отсутствие признаков удовлетворительного уровня		неудовлетворительно	не зачтено	Менее 55

9. Перечень основной и дополнительной литературы, необходимой для освоения дисциплины

Основная литература.

1. *Алешников С.И., Болтнев Ю.Ф.* Математические методы защиты информации. Часть 1. Алгебраические методы: Учебное пособие / Калинингр. ун-т. – Калининград, 2000. Переиздано: электронное издание, Изд-во БФУ, 2015 г Математические методы защиты информации. Ч. 1 (полный текст). ЭБС Кантиана.

Дополнительная литература

2. *Романьков, В. А.* Введение в криптографию : курс лекций / В.А. Романьков. — 2-е изд., испр. и доп. — Москва : ФОРУМ : ИНФРА-М, 2021. https://znanium.com/catalog/product/1514566

10. Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины

- НЭБ Национальная электронная библиотека, диссертации и прочие издания https://rusneb.ru/
- eLIBRARY.RU Научная электронная библиотека, книги, статьи, тезисы докладов конференций http://elibrary.ru/defaultx.asp
- Гребенников Электронная библиотека ИД журналы
- ЭБС Лань книги, журналы http://e.lanbook.com/
- ЭБС Консультант студента
- ПРОСПЕКТ ЭБС
- ЭБС ZNANIUM.COM https://znanium.com
- РГБ Информационное обслуживание по МБА

- БЕН РАН
- Электронно-библиотечная система (ЭБС) Кантиана (https://lib.kantiana.ru/jirbis2/)

Дополнительные ресурсы

1. http://csrc.nist.gov/groups/ST/toolkit/rng/index.html - центр генерирования и тестирования псевдослучайных чисел.
2. http://www.billthelizard.com/2009/05/how-do-you-test-random-number-generator.html - тест для генератора псевдослучайных чисел..
3. http://www.math.utah.edu/~pa/Random/Random.html - генератор псевдослучайных чисел.
4. http://www.math.unb.ca/~knight/random1.htm - ссылки по генераторам псевдослучайных чисел.
5. http://www.cs.fsu.edu/~mascagni/rng_bib.html - сборник работ по генераторам псевдослучайных чисел.
6. Библиотека научной литературы. Раздел «Криптография» http://lib.org.by/_djvu/Cs_Computer%20science/CsCr_Cryptography/
7. Сайт Семьянова «Криптографический ликбез» http://www.ssl.stu.neva.ru/psw/crypto.html
8. Электронная библиотека механико-математического факультета Московского государственного университета. Раздел Криптография http://lib.mexmat.ru/catalogue.php?dir=02_06
9. *Шнайер Б.* Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си http://www.ssl.stu.neva.ru/psw/crypto/appl_rus/appl_cryp.htm
10. *A. Menezes, P. van Oorschot, S. Vanstone.* Handbook of Applied Cryptography. — http://www.cacr.math.uwaterloo.ca/hac/

Электронные книги

1. *Глухов М.М., Круглов И.А., Пичкур А.Б., Черемушкин А.В.* Введение в теоретико-числовые методы криптографии http://e.lanbook.com/books/element.php?pl1_id=1540

11. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине

Программное обеспечение обучения включает в себя:

- система электронного образовательного контента БФУ им. И. Канта – www.lms-3.kantiana.ru, обеспечивающую разработку и комплексное использование электронных образовательных ресурсов;
- серверное программное обеспечение, необходимое для функционирования сервера и связи с системой электронного обучения через Интернет;
- корпоративная платформа Microsoft Teams;
- установленное на рабочих местах обучающихся ПО: Microsoft Windows 7, Microsoft Office Standart 2010, антивирусное программное обеспечение Kaspersky Endpoint Security.
- специализированное ПО - Система компьютерной алгебры SAGE версии 9.0 и выше. (с открытым кодом) http://www.sagemath.org/

Программное обеспечение для электронного обучения в области криптографии

- CRYPTOOL (в свободном доступе) https://www.cryptool.org/en/

12. Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине

Для проведения занятий лекционного типа, практических и семинарских занятий используются специальные помещения (учебные аудитории), оборудованные техническими средствами обучения – мультимедийной проекционной техникой. Для проведения занятий лекционного типа используются наборы демонстрационного оборудования.

Для проведения лабораторных работ, (практических занятий – при необходимости) используются специальные помещения (учебные аудитории), оснащенные специализированным лабораторным оборудованием: персональными компьютерами с возможностью выхода в интернет и с установленным программным обеспечением, заявленным в п.11.

Для проведения групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации используются специальные помещения (учебные аудитории), оборудованные специализированной мебелью (для обучающихся), меловой / маркерной доской.

Для организации самостоятельной работы обучающимся предоставляются помещения, оснащенные компьютерной техникой с возможностью подключения к сети «Интернет» и обеспечением доступа в электронную информационно-образовательную среду университета.

Для обучения инвалидов и лиц с ограниченными возможностями здоровья университетом могут быть представлены специализированные средства обучения, в том числе технические средства коллективного и индивидуального пользования.

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
федеральное государственное автономное образовательное учреждение высшего образования «Балтийский федеральный университет имени Иммануила Канта»
Институт физико-математических наук и информационных технологий

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

«Сети и системы передачи информации»

Шифр: 10.05.01
Специальность: «Компьютерная безопасность»
Специализация: «Математические методы защиты информации»
Квалификация (степень) выпускника: специалист по защите информации

Калининград
2022

Лист согласования

Составитель: Ставицкая Е.П., ведущий менеджер ООП, старший преподаватель

Рабочая программа утверждена на заседании учебно-методического совета института физико-математических наук и информационных технологий
Протокол № 01/22 от «01» февраля 2022 г.
Председатель учебно-методического
совета института физико-
математических наук и информационных
технологий
Первый заместитель директора Шпилевой А. А
ИФМНиИТ, к. ф.-м. н., доцент

Ведущий менеджер Е.П.Ставицкая

Содержание

1.Наименование дисциплины: «Сети и системы передачи информации».

Целью курса «Сети и системы передачи информации» является изучение общих принципов передачи информации.

Задачами дисциплины являются изучение методов и технических средств, обеспечивающих передачу информации по проводным и беспроводным каналам связи, изучения основных технических параметров и характеристик оборудования, обеспечивающего такую передачу, изучения методов и средств кодирования и декодирования информации при её передаче.

2. Перечень планируемых результатов обучения по дисциплине, соотнесенных с планируемыми результатами освоения образовательной программы

Код компетенции	Результаты освоения образовательной программы (ИДК)	Результаты обучения по дисциплине
ОПК-9. Способен решать задачи профессиональной деятельности с учетом текущего состояния и тенденций развития методов защиты информации в операционных системах, компьютерных сетях и системах управления базами данных, а также методов и средств защиты информации от утечки по техническим каналам, сетей и систем передачи информации;	ОПК-9.1. Знает методы защиты информации в операционных системах, компьютерных сетях и системах управления базами данных, а также методы и средства защиты информации от утечки по техническим каналам, сетей и систем передачи информации. ОПК-9.2. Умеет решать задачи профессиональной деятельности с учетом текущего состояния и тенденций развития методов защиты информации в операционных системах, компьютерных сетях и системах управления базами данных, а также методов и средств защиты информации от утечки по техническим каналам, сетей и систем передачи информации. ОПК-9.3. Владеет навыками решения задач профессиональной деятельности с учетом текущего состояния и тенденций развития методов защиты информации в операционных системах, компьютерных сетях и системах управления базами данных, а также методов и	**Знать** основные понятия построения систем и сетей электросвязи и особенности их эксплуатации; тактико-технические характеристики основных телекоммуникационных систем, сигналов и протоколов, применяемых для передачи различных видов сообщений; перспективы развития систем и сетей связи; способы передачи информации по проводным и беспроводным каналам, основные классы систем передачи информации, отличия систем вещания спутниковых группировок на различных типах орбит, разницу в механизмах передачи радиоволн различных диапазонов, возможности использования различных проводных и кабельных линий связи. **Уметь** творчески применять знания о системах электрической связи для решения задач по созданию защищенных телекоммуникационных систем; отслеживать тенденции развития систем и сетей электросвязи, внедрения новых служб и услуг связи; разрабатывать структурные схемы систем связи с заданными характеристиками; читать структурные и функциональные

	средств защиты информации от утечки по техническим каналам, сетей и систем передачи информации.	схемы систем и сетей связи; работать с программными средствами прикладного, системного и специального назначения; проводить сбор и анализ исходных данных для проектирования систем защиты информации; разрабатывать комплексные системы структурированных систем передачи данных с детальной прорисовкой трассировки компьютерных кабелей и необходимых кабельных каналов, определения необходимых элементов сетевой инфраструктуры – коммутаторов, маршрутизаторов, патч-панелей, кроссировочных элементов, необходимых серверов и их систем бесперебойного питания, моделировать компьютерную сеть на специальных программных комплексах. **Владеть:** основными приёмами кодирования информации, основными определениями передачи информации. Владеть навыками анализа основных электрических характеристик и возможностей телекоммуникационных систем по передаче оперативных и специальных сообщений; анализа сетевых протоколов; эксплуатации программного обеспечения и программно-аппаратных средств обеспечения информационной безопасности компьютерных систем; участия в приеме, настройке, регулировке, освоении и восстановлении работоспособности оборудования защиты информации; использования языков и систем программирования, инструментальных средств для решения профессиональных, исследовательских и прикладных задач.

3. Место дисциплины в структуре образовательной программы

«Сети и системы передачи информации» представляет собой дисциплину обязательной части Блока 1 Дисциплины (модули) подготовки обучающихся, входит в Модуль 4. Компьютерные технологии (Б1.О.08.01).

4. Виды учебной работы по дисциплине.

Виды учебной работы по дисциплине зафиксированы учебным планом основной профессиональной образовательной программы по указанному направлению и профилю, выражаются в академических часах. Часы контактной работы и самостоятельной работы обучающегося и часы, отводимые на процедуры контроля, могут различаться в учебных планах ОПОП по формам обучения. Объем контактной работы включает часы контактной аудиторной работы (лекции/практические занятия/ лабораторные работы), контактной внеаудиторной работы (контроль самостоятельной работы), часы контактной работы в период аттестации. Контактная работа, в том числе может проводиться посредством электронной информационно-образовательной среды университета с использованием ресурсов сети Интернет и дистанционных технологий

5. Содержание дисциплины, структурированное по темам (разделам)

Исходя из рамок, установленных учебным планом по трудоемкости и видам учебной работы по дисциплине, преподаватель самостоятельно выбирает тематику занятий по формам и количеству часов проведения контактной работы: лекции и иные учебные занятия, предусматривающие преимущественную передачу учебной информации преподавателем и (или) занятия семинарского типа (семинары, практические занятия, практикумы, лабораторные работы, коллоквиумы и иные аналогичные занятия), и (или) групповые консультации, и (или) индивидуальную работу обучающихся с преподавателем, в том числе индивидуальные консультации (по курсовым работам/проектам – при наличии курсовой работы/проекта по данной дисциплине в учебном плане). Рекомендуемая тематика занятий максимально полно реализуется в контактной работе с обучающимися очной формы обучения. В случае реализации образовательной программы в заочной / очно-заочной форме трудоемкость дисциплины сохраняется, однако объем учебного материала в значительной части осваивается обучающимися в форме самостоятельной работы. При этом требования к ожидаемым образовательным результатам обучающихся по данной дисциплине не зависят от формы реализации образовательной программы.

1	Тема 1. Введение. История развития систем связи.	Краткие исторические сведения о развитии систем электрической связи. Системы электросвязи: первые системы проводной связи, системы радиосвязи, системы передачи данных. Сети электросвязи: сеть ЭВМ «ARPA», гибридные сети, сети сотовой связи, сети следующего поколения. История развития телеграфа. История развития телефона. История открытия радиосвязи, радиолокации (изобретение А. С. Попова, работы его учеников). Развитие систем связи в 20 веке. Коротковолновая связь. Автоматические телефонные станции. Телексы (телетайпы). Телевидение. Спутниковая связь на высокоэллептических орбитах. Спутниковая связь на геостационарной орбите. Мобильные телефоны. Интернет. Смартфоны. Системы

		GPS, Глонас. Понятие спутниковых группировок LEO. Современные технологии – роботы телеприсутствия, интернет вещей (IoT). Архитектура сети связи. Обобщенная структура сети связи. Сеть доступа. Магистральная сеть. Методы коммутации информации в сетях связи. Коммутация каналов. Коммутация пакетов. Эталонная модель взаимодействия открытых систем и протоколы семиуровневой модели Эталонная модель OSI. Уровни модели OSI: физический, канальный, сетевой, транспортный, сеансовый, представления, прикладной. Назначение уровней модели OSI.
2	Тема 2. Определения. Кодирование. Модуляция. Цифровые системы передачи информации	Основные понятия и определения. Информация, сообщение, сигнал, канал связи. Архитектура связи: телекоммуникации, инфокоммуникационная система, система электросвязи, телекоммуникационная сеть, служба связи. Классификация систем электросвязи. Виды систем связи. Системы электросвязи. Вторичные сети электросвязи. Службы связи. Интеграция услуг документальной электросвязи. Перспективы развития систем электросвязи. Тенденции развития телекоммуникационных систем. Пути развития связи в Российской Федерации. Стандартизация систем электросвязи. Принципы построения систем и сетей передачи информации. Общие сведения о преобразованиях сообщений и сигналов в системах и сетях передачи информации. Способы представления сообщений и сигналов. Структура систем передачи информации: состав системы передачи информации, назначение элементов системы передачи информации. Источники информации: виды источников, виды сообщений, характеристики источника дискретных сообщений. Первичные сигналы: виды сигналов, цифровые сигналы данных, основные характеристики сигналов. Каналы связи: виды каналов, виды искажений цифровых сигналов данных, методы регистрации цифровых сигналов данных (метод стробирования, интегральный метод). Характеристики систем передачи информации. Кодирование информации в системах связи. Основные понятия и классификация методов кодирования. Методы кодирования формы сигнала: импульсно-кодовая модуляция, дифференциальная импульсно-кодовая модуляция, дельта-модуляция. Полувокодеры. Методы кодирования параметров сигнала: полосные и формантные вокодеры, вокодеры с линейным предсказанием. Кодирование источников дискретных сообщений: равномерные коды, неравномерные коды. Методы эффективного кодирования источников: кодирование по методу Шеннона-Фано, кодирование по методу Хаффмана. Помехоустойчивое кодирование в системах связи.

		Классификация помехоустойчивых кодов. Обнаружение и исправление ошибок. Простейшие помехоустойчивые коды. Циклические коды. Кодеры и декодеры циклических кодов. Методы модуляции сигналов в системах связи. Амплитудная модуляция (аналоговая) (АМ). Фазовая и частотная аналоговая модуляции (ФМ, ЧМ). Амплитудная импульсная модуляция (АИМ). Амплитудная манипуляция (АМн). Цифровые системы передачи информации. Особенности цифровых систем многоканальной передачи сообщений: необходимость обеспечения синхронизации в ЦСП, общие принципы работы систем тактовой синхронизации, принципы действия систем цикловой синхронизации, технологии иерархических цифровых сетей (плезиохронная цифровая иерархия, синхронная цифровая иерархия). Способы объединения цифровых потоков: цифровой ввод сигналов электросвязи, виды цифровых последовательностей, синхронный способ объединения, асинхронный способ объединения. Особенности передачи дискретных сообщений по цифровым каналам.
3	Тема 3 Кабельные системы. Антены и фидеры. Радиосвязь.	Кабельные и волоконно-оптические системы связи. Краткий исторический обзор использования оптического диапазона. Обобщенные структурные схемы кабельных и ВОЛС. Прохождение оптического излучения в среде распространения: прохождение светового потока через атмосферу, прохождение светового потока в оптическом волокне. Формирование сигнальных потоков в ОЛС: частотное уплотнение, временное уплотнение. Антены и фидеры для различных диапазонов длин волн. Коротковолновые и ультракоротковолновые системы связи. Особенности распространения радиоволн: диапазоны радиочастот и радиоволн, структура атмосферы, земные и ионосферные радиоволны, распространение радиоволн в ионосфере, особенности распространения радиоволн различных диапазонов, многолучевое распространение радиоволн. Структура средств радиосвязи: структура радиопередающих устройств, структура радиоприемных устройств. Системы радиорелейной связи. Принцип радиорелейной связи. Структура радиорелейной станции. Цифровые радиорелейные станции. Системы тропосферной и спутниковой связи. Принцип тропосферной связи. Сущность тропосферной связи. Принцип разнесенного приема. Принцип спутниковой связи. Радиолиния спутниковой связи. Особенности спутниковой связи.
4	Тема 4 Телефония, телеграфия, телевидение.	Системы телефонной связи. Особенности систем передачи речи. Теорема Котельникова. Кодирование формы волны. Параметрическое компандирование на

		основе линейного предсказания. Гибридное кодирование. Кодирование речи с разделением спектра на полосы. Принципы передачи речи с переменной скоростью. Кодирование элементов речи. Системы телеграфной связи. Телеграфные коды. Краевые искажения, дробления сигналов и способы борьбы с ними. Синхронизация и фазирование. Структура и принципы функционирования системы телеграфной связи. Оконечные устройства систем передачи телеграфных сообщений. Оконечный телеграфный аппарат, кодовый метод. Равномерное и неравномерное кодирование. Последовательный и параллельный способ передачи двоичных кодов. Синхронизация. Фазирование. Стартстопы системы телеграфной связи. Структура и принципы функционирования системы телеграфной связи. Телевизионные системы. Передающая трубка видеосигнала (видикон). Трехкомпонентная цветная передающая трубка (ЦПТ). Устройство приемной телевизионной трубки (кинескопа). Кадр, телевизионный растр, линейно-строчная развертка, трехкомпонентная теория. Система NTSC. Система PAL. Система SECAM. Цифровое телевидение.
5	Тема 5 Модемы. Мобильная связь.	Применение телефонных сетей для передачи данных. Модем. Элементарная посылка информационного сигнала. Бодовый интервал, бод, бодовая скорость. Проблема организации одновременной двусторонней связи. Метод частотного разделения канала, ассиметричная дуплексная связь, технология эхоподавления, полудуплескная связь. Рекомендация V.34. Сети подвижной радиосвязи. Рынок систем подвижной радиосвязи. Профессиональные системы подвижной радиосвязи. Транкинговые системы. Принцип повторного использования частот. Эволюция стандартов ССПС. Буферные ячейки. Кластер ячеек в зоне обслуживания. Смежные базовые станции. Коэффициент повторения частот.
6	Тема 6 Компьютерные сети.	Активное сетевое оборудование. Сетевые карты. (адаптеры). Точки доступа - модели, стандарты, скорость передачи, данных, радиус действия, диапазон частот. Основные термины и понятия. Определение коммутаторов, классификация. Общие характеристики, сравнение некоторых моделей D-Link. Интеллектуальные функции коммутаторов. Маршрутизаторы – виды, характеристики, особенности. NAT. ADSL модемы. Принт-серверы и межсетевые экраны. Пассивное сетевое оборудование. Сетевой кабель – виды, категории, особенности конструкции и обжима, полосы пропускания. Кабель-каналы (короба). Сетевые шкафы и стойки. Их элементы. Порядок размещения оборудования в них.

		Дополнительная информация. Особенности структуры и устройств глобальной сети крупной организации на примере БФУ им. И.Канта. Сервера, «зеркалирование», RAID, виртуализация. Линии связи: состав, типы, характеристики. Способы передачи данных на физическом уровне – основные определения и понятия. Стэк протоколов TCP/IP. Адресация в сетях TCP/IP: типы адресов стека TCP/IP, формат IP-адреса, классы IP-адресов. Адресация в сетях TCP/IP: использование масок при IP-адресации. Порядок назначения IP-адресов и технология CIDR. Протокол ARP. Доменные имена. Система DNS.

6. Рекомендуемая тематика учебных занятий в форме контактной работы

Рекомендуемая тематика учебных занятий *лекционного* типа (предусматривающих преимущественную передачу учебной информации преподавателями):

Тема 1 Введение. История развития систем связи.
Тема 2 Определения. Модуляция. Кодирование.
Тема 3 Кабельные системы. Радиосвязь. Антены и фидеры.
Тема 4 Телефония, телеграфия, телевидение.
Тема 5 Модемы. Мобильная связь.
Тема 6 Компьютерные сети

Рекомендуемая тематика *лабораторных* занятий:

№ п/п	Название раздела	Темы лабораторных работ
1.	Тема 3. Кабельные системы. Радиосвязь. Антены и фидеры.	1. Волоконно-оптические системы связи. 2. КВ, УКВ связь. Фидеры, антенны. 3. Радиорелейные и тропосферные системы связи. 4. Спутниковые системы связи.
2.	Тема 4. Телефония, телеграфия, телевидение.	1. Кодирование информации в системах связи. 2. Системы телефонной связи. 3. Системы телеграфной связи. 4. Телевизионные системы.
3.	Тема 5. Модемы. Мобильная связь.	1. Изучение принципов и параметров работы модема. Протоколы передачи данных. 2. Транкинговые системы радиосвязи. 3. Устройство базовых станций связи GPS. 4. Устройство телефонных трубок мобилных телефонов.

4.	Тема 6. Компьютерные сети	1. Обжим и кроссировка кабелей в коммутационных шкафах. 2. Практическое изучение различных моделей коммутаторов 3. Практическое моделирование работы устройств компьютерной сети. 4. Выполнение практической части проектной работы разработки сети масштаба предприятия

Требования к самостоятельной работе обучающихся

1. Работа с лекционным материалом, предусматривающая проработку конспекта лекций и учебной литературы, по всем темам из п. 6 настоящей рабочей программы.

2. Выполнение домашнего задания, предусматривающего решение задач, выполнение упражнений, выдаваемых на практических занятиях, по всем темам из п. 6 настоящей рабочей программы.

Руководствуясь положениями статьи 47 и статьи 48 Федерального закона от 29 декабря 2012 г. N 273-ФЗ «Об образовании в Российской Федерации» научно-педагогические работники и иные лица, привлекаемые университетом к реализации данной образовательной программы, пользуются предоставленными академическими правами и свободами в части свободы преподавания, свободы от вмешательства в профессиональную деятельность; свободы выбора и использования педагогически обоснованных форм, средств, методов обучения и воспитания; права на творческую инициативу, разработку и применение авторских программ и методов обучения и воспитания в пределах реализуемой образовательной программы и отдельной дисциплины.

Исходя из рамок, установленных учебным планом по трудоемкости и видам учебной работы по дисциплине, преподаватель самостоятельно выбирает тематику занятий по формам и количеству часов проведения контактной работы: лекции и иные учебные занятия, предусматривающие преимущественную передачу учебной информации преподавателем и (или) занятия семинарского типа (семинары, практические занятия, практикумы, лабораторные работы, коллоквиумы и иные аналогичные занятия), и (или) групповые консультации, и (или) индивидуальную работу обучающихся с преподавателем, в том числе индивидуальные консультации (по курсовым работам/проектам – при наличии курсовой работы/проекта по данной дисциплине в учебном плане).

Рекомендуемая тематика занятий максимально полно реализуется в контактной работе с обучающимися очной формы обучения. В случае реализации образовательной программы в заочной / очно-заочной форме трудоемкость дисциплины сохраняется, однако объем учебного материала в значительной части осваивается обучающимися в форме самостоятельной работы. При этом требования к ожидаемым образовательным результатам обучающихся по данной дисциплине не зависят от формы реализации образовательной программы.

7. Методические рекомендации по видам занятий

Лекционные занятия.

В ходе лекционных занятий обучающимся рекомендуется выполнять следующие действия. Вести конспектирование учебного материала. Обращать внимание на категории, формулировки, раскрывающие содержание тех или иных явлений и процессов, научные выводы и практические рекомендации по их применению. Задавать преподавателю

уточняющие вопросы с целью уяснения теоретических положений, разрешения спорных ситуаций.

Желательно оставить в рабочих конспектах поля, на которых во внеаудиторное время можно сделать пометки из рекомендованной литературы, дополняющие материал прослушанной лекции, а также подчеркивающие особую важность тех или иных теоретических положений.

Практические и семинарские занятия.

На практических и семинарских занятиях в зависимости от темы занятия выполняется поиск информации по решению проблем, практические упражнения, контрольные работы, выработка индивидуальных или групповых решений, итоговое обсуждение с обменом знаниями, участие в круглых столах, разбор конкретных ситуаций, командная работа, представление портфолио и т.п.

Самостоятельная работа.

Самостоятельная работа осуществляется в виде изучения литературы, эмпирических данных по публикациям и конкретных ситуаций из практики, подготовке индивидуальных работ, работа с лекционным материалом, самостоятельное изучение отдельных тем дисциплины; поиск и обзор литературы и электронных источников; чтение и изучение учебника и учебных пособий.

8. Фонд оценочных средств

8.1. Перечень компетенций с указанием этапов их формирования в процессе освоения образовательной программы в рамках учебной дисциплины

Основными этапами формирования указанных компетенций при изучении обучающимися дисциплины являются последовательное изучение содержательно связанных между собой тем учебных занятий. Изучение каждой темы предполагает овладение обучающимися необходимыми компетенциями. Результат аттестации обучающихся на различных этапах формирования компетенций показывает уровень освоения компетенций.

Контролируемые разделы (темы) дисциплины	Индекс контролируемой компетенции (или её части)	Оценочные средства по этапам формирования компетенций
		текущий контроль по дисциплине
Тема 1 Введение. История развития систем связи.	ОПК-9	Письменные опросы по изученному материалу.
Тема 2. Определения. Модуляция. Кодирование.	ОПК-9	Письменные опросы по изученному материалу.
Тема3. Кабельные системы. Радиосвязь. Антенны и фидеры. Методы и средства измерений физических величин	ОПК-9	Письменные опросы по изученному материалу. Задания для подготовки к лабораторным работам. Защита лабораторной работы с использованием презентации
Тема 4. Телефония, телеграфия, телевидение	ОПК-9	Письменные опросы по изученному материалу. Задания для подготовки к лабораторным работам. Защита лабораторной работы с

Контролируемые разделы (темы) дисциплины	Индекс контролируемой компетенции (или её части)	Оценочные средства по этапам формирования компетенций
		текущий контроль по дисциплине
		использованием презентации
Тема 5. Модемы. Мобильная связь.	ОПК-9	Письменные опросы по изученному материалу. Задания для подготовки к лабораторным работам. Защита лабораторной работы с использованием презентации
Тема 6. Компьютерные сети.	ОПК-9	Письменные опросы по изученному материалу. Задания для подготовки к лабораторным работам. Защита лабораторной работы с использованием презентации

8.2. Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений и навыков и (или) опыта деятельности процессе текущего контроля

Письменные опросы

Примеры вопросов

К темам 1-5.

1. История развития телекоммуникационных систем. Перечислить фундаментальные вехи в 18, 19 и 20-ом веках. Коротковолновая связь, телевидение, спутниковая связь, ГСО, точка стояния, пятно видимости, спутник Астра, интернет, мобильный телефон, GPS, ARPA.
2. История развития телеграфа и радиосвязи. Суть изобретения Попова. Вехи на этом пути – промежуточные достижения, люди, которые их совершали, даты.
3. История развития телефонной связи. Вехи на этом пути – промежуточные достижения, люди, которые их совершали, даты. Работы учеников Попова.
4. Эталонная модель взаимодействия открытых систем. Общие положения. Описание уровней эталонной модели OSI.
5. Основные определения передачи информации. Общее определение уровней передачи. Параметры первичных сигналов.
6. Основные определения сетей связи. Сети передачи индивидуальных сообщений. Соединительный тракт, коммутация каналов, сообщений, пакетов. Сети передачи массовых сообщений (сети вещания), вещательная программа. Сеть звукового вещания. Сеть телевизионного вещания. Сеть передачи газет.
7. Кабельные и воздушные линии связи на основе металлических проводников, симметричные и коаксиальные кабели. Конструкция кабеля для магистральной сети. Волоконно-оптические линии связи, их преимущества. Конструкция ОВ, угол полного отражения, классификация ОВ.
8. Радиолинии. Диапазоны радиоволн и способы их распространения в зависимости от диапазона. Радиорелейные системы передачи. Тропосферные радиорелейные системы передачи.
9. Антенны. Проволочные и апертурные антенны. Основные параметры передающих и приёмных антенн: входное сопротивление, КПД, амплитудная характеристика. Особенности передающих и приёмных антенн различных диа-пазонов. Фидеры.

10. Два основных способа физического кодирования. Дискретная модуляция. Сравнение аналоговой модуляции и цифрового кодирования. Канал тональной частоты. Амплитудно-частотная характеристика канала тональной частоты. Модем. Потенциальное кодирование, амплитудная, частотная и фазовая модуляция.
11. Цифровое кодирование. Методы кодирования: потенциальные и импульсные коды. Требования к методам цифрового кодирования. Основные коды: NRZ, NRZ-I, Биполярный Импульсный Код, Манчестерский Код, 2B1Q.
Часть 2.
12. Модуляция при передаче дискретных сигналов, манипуляция. Квадратурная амплитудная модуляция. Дискретизация аналоговых сигналов, АЦП, ЦАП. Теория Найквиста. Амплитудная импульсная, импульсно-кодовая модуляция. Дельта-модуляция.
13. Методы кодирования параметров сигнала. Вокодеры, форматные фильтры. Полосные вокодеры, вокодеры с линейным предсказанием, гомоморфные вокодеры, полувокодеры. Кодирование источников дискретных сообщений, равномерное и неравномерное кодирование, условие однозначной декодируемости, средняя длина кодового слова. Код Шеннона-Фано. Алгоритм Хаффмана. Помехоустойчивое кодирование.
14. Многоканальные системы связи. Цифровые системы передачи информации и их преимущества перед аналоговыми. Технологии иерархических цифровых сетей. Тактовая и цикловая синхронизация. Способы объединения цифровых потоков. Особенности передачи дискретных сообщений по цифровым каналам.
15. Системы телефонной связи. Цифровое кодирование речи. Импульсно-кодовая модуляция. Кодирование формы сигнала. Дельта-модуляция. Алгоритм адаптивной дифференциальной импульсно-кодовой модуляции. Кодеры исходной информации (вокодеры). Гибридные алгоритмы.
16. Единая система нумерации, зоновый принцип нумерации. Междугородная, городская и сельская телефонные связи. Телефон, микрофон. Принцип действия электромагнитного телефона. Принцип действия угольного микрофона. Номеронабиратель, телефонный аппарат.
17. Цифровая обработка аналоговых сигналов. Этапы аналого-цифрового преобразования. Устройство выборки и хранения. Квантование мгновенных значений сигнала. Ошибка и шум квантования. Неравномерное квантование.
18. Применение телефонных сетей для передачи данных. Модем. Элемен-тарная посылка информационного сигнала. Бодовый интервал, бод, бодовая скорость. Проблема организации одновременной двусторонней связи. Метод частотного разделения канала, ассиметричная дуплексная связь, технология эхоподавления, полудуплескная связь. Рекомендация V.34.
19. Системы телеграфной связи. Оконечный телеграфный аппарат, кодовый метод. Равномерное и неравномерное кодирование. Последовательный и параллельный способ передачи двоичных кодов. Синхронизация. Фазирование. Стартстопы системы телеграфной связи. Структура и принципы функциони-рования системы телеграфной связи.
20. Телевизионные системы. Передающая и приемная трубка. Линейно-строчная и чересстрочная развертки. Примеры телевизионных систем. Методы сжатия. Цифровое телевидение.
21. Системы подвижной радиосвязи. Рынок систем подвижной радиосвязи. Профессиональные системы подвижной радиосвязи. Тракинговые системы.
22. Сотовая связь. Принцип повторного использования частот. Факты хронологии.

Лабораторные работы

Примеры.

К теме 3. Кабельные системы. Антены и фидеры. Радиосвязь.

Работа № 1. Конструкция и характеристики металлических и оптоволоконных кабелей связи.

1. Цель работы

Изучение общей информации о типах воздушных и кабельных линий связи на основе металлических проводников и оптоволокна. Приобретение навыков планирования применения тех или иных кабелей для организации различных вариантов каналов связи. Получение опыта по подбору конкретных моделей и марок кабелей, моделированию их характеристик, кроссированию кабелей.

2. Сведения, необходимые для выполнения работы

Перед выполнением работы необходимо ознакомиться со следующими вопросами:

• Структура и классификация воздушных, симметричных и коаксиальных линий связи.
• Модели, марки, характеристики, способы прокладки воздушных линий связи.
• Модели, марки, характерситики, способы прокладки коаксиальных кабелей связи.
• Модели, марки, характерситики, способы прокладки симметричных кабелей связи.
• Принцип действия, устройство и характеристики волоконно-оптических кабелей связи. Структура и назначение и конструктивное исполнение каждого слоя кабеля ВОЛС. Угол полного внутреннего отражения. Окна прозрачности. Ступенчатые и градиентныее оптические волокна. Одномодовые и многомодовые оптические волокна.

Работа № 2. Конструкции антенн различных диапазонов и их характеристики.

1. Цель работы

Изучение общей информации о типах антенн различных диапазонов связи, их конструктивных особенностей, характеристик, диаграмм направленности. Приобретение навыков планирования применения тех или иных антенн связи для организации различных вариантов каналов связи. Получение опыта по подбору частотного диапазона и конструктивных особенностей конкретных элементов конструкции антены и фидера для реальной задачи.

2. Сведения, необходимые для выполнения работы

Перед выполнением работы необходимо ознакомиться со следующими вопросами:

• основные понятия теории антенн и фидеров, в т.ч. - проволочные и аппертурные антенны, принимающие и передающие;
• параметры антенны: входное сопротивление, коэффициент полезного действия, амплитудная характеристика направленности;
• конструктивная реализация антенн УКВ, КВ, СВ и ДВ, проволочные антенны, мачты и башни;
• конструктивная реализация антенн телевизионного диапазона и СВЧ, волноводы;
• конструктивная реализация антенн спутниковой связи.

Работа № 3. Подробное изучение конструкции и характеристик антенны диполь Герца.

1. Цель работы

Ознакомление с конструкцией и принципом работы простейшей проволочной антенны. Экспериментальное получение её диаграммы направленности.

2. Сведения, необходимые для выполнения работы

Используя рекомендованную литературу и видеоролики в Интернете ознакомьтесь со следующими вопросами:

• Конструкция простейшей проволочной антенны диполь Герца, история её появления и применения.
• Полярная система координат. Углы азимута и склонения.
• Диаграммы направленности диполя Герца в азимутальной и меридиональной плоскостях, построенные в полярной системе координат.
• Оборудование, необходимое для проведения исследований. Форма журнала записи результатов измерений.

Работа № 4. Подробное изучение конструкции и характеристик антенны «волновой канал» (антенна Уда-Яги).

1. Цель работы

Ознакомление с конструкцией и принципом работы антенны «волновой канал» (антенна Уда-Яги). Экспериментальное получение её диаграммы направленности.

2. Сведения, необходимые для выполнения работы

Используя рекомендованную литературу и видеоролики в Интернете ознакомьтесь со следующими вопросами:

• Конструкция антенны «волновой канал» (антенна Уда-Яги), история её появления и применения.
• Диаграммы направленности «игольчатой формы». Направление главного излучения, боковые лепестки.
• Оборудование, необходимое для проведения исследований.

Работа № 5. Подробное изучение аппаратуры спутниковой связи.

1. Цель работы

Ознакомление с оборудованием лаборатории спутниковой связи, его назначением и характеристиками. Экспериментальное получение навыков работы с оборудованием систем спутниковой связи.

2. Сведения, необходимые для выполнения работы

Используя рекомендованную литературу, методические указания, имеющиеся в лаборатории и видеоролики в Интернете, ознакомьтесь со следующими вопросами:

• Типы орбит спутников связи, существующие и перспективные группировки спутников связи.
• Состав, структура и характеристики приемо-передающего оборудования связи, расположенного на спутниках различных типов.
• Состав, структура и характеристики наземного приемо-передающего оборудования спутниковой связи.
• Состав и характеристики оборудования, имеющегося в лаборатории спутниковой связи.

Работа №6 Изучение структуры, характерситк и принципов работы базовой станции сотовой связи и оконечного устройства приёма/передачи (мобильного телефона).

1. Цель работы:

Ознакомление с теоретическими основами сотовой связи и оборудованием её реализующим. Получение навыков настройки каналов связи, проведения их сеансов. Изучение схемотехники современных мобильных телефонов, параметров их приемо-передающей подсистемы.

2. Сведения, необходимые для выполнения работы

- История развития систем сотовой связи в конце 20-го и начале 21-го веков. ССПС, соты, кластеры ячеек, эффективный радиус кластера, хэндовер, DAMPS, CDMA, GSM, JDS?
- Развите систем GSM за последние годы – изменение частот приема/ передачи, мощности сигнала.
- Расстояния между портативным устройством и базовой станцией, многолучевое распространение Синхропоследовательность, функция эстафетной передачи.
- Принцип повторного использования частот, защитный интервал, коэффициент повторения частот.
- Структура и состав оборудования базовых станций разных поколений.
- Структура и состав портативного устройства (мобильного телефона), его прёмо-пеередающей и вспомогательных систем.

К теме 6. Компьютерные сети.

Работа №7. Построение макета и модели простейшей компьютерной сети.

1.Цель работы.

Изучить принцип действия и устройство базовых устройств компьютерной сети – сетевых карт, коммутаторов, сетевых кабелей, серверов и сетевого программного обеспечения. Собрать макет простейшей компьютерной сети. Построить её модель в прикладном пакете NetEmul. Изучить особенности измерения уровня сигнала специальными измерительными устройствами. Получить практические навыки работы с измерительными приборами.

2. Сведения, необходимые для выполнения работы.

- Классификация сетевых адаптеров, их общее устройство и варианты конструкции.
- Операции сетевых адаптеров, их характеристики. Сравнительная таблица моделей сетевых адаптеров.
- Сетевой кабель – виды, категории, особенности конструкции и обжима, полосы пропускания.
- Сетевые коммутаторы первого уровня – структура, принцип действия, характеристики, сводная таблица моделей.
- Стэк протоколов TCP/IP: типы адресов стека, формат IP-адреса, классы IP-адресов.

Работа №8. Изучение характеристик коммутаторов и маршрутизаторов.

1.Цель работы

Изучить всю номенклатуру существующих коммутаторов и маршрутизаторов, провести её анализ, сранить модели по устройству и функционалу, составить сравнительную таблицу. Заменить в созданном ранее макете комьютерной сети коммутаторы на интеллектуальные, показать возникшие дополнительные возможности. Получить навыки удалённого администрирования сетей. Получить навыки в измерении физических характеристик сети. Добавить в макет дополнительные устройства – беспроводные камеры, сетевые хранилища. Отразить в модели сети внесённые изменения.

2. Сведения, необходимые для выполнения работы
• Сетевые коммутаторы второго и третьего уровней – структура, принцип действия, характеристики, сводная таблица моделей.
• Маршрутизаторы – виды, характеристики, особенности.
• Механизм NAT, позволяющий преобразовывать в сетях TCP/IP IP адреса транзитных пакетов.
• Беспроводные камеры видеонаблюдения, сетевые хранилища данных, в том числе с функцией видеомониторинга помещений и объектов.

Работа №9. Построение макета и модели компьютерной сети масштаба предприятия.

1.Цель работы

Расширить созданный ранее макет компьютерной сети до уровня масштаба предприятия. Добавить устройства, устанавливаемые в коммутационные и серверные шкафы. Произвести прокладку и кроссирование кабелей, обжим патч-кордов шкафа, установку коммутационных панелей и органайзеров, настройку серверов, подключение устройств бесперебойного питания, медиаконвертеров. Смакетировать во втором шкафу сетевую подсистему отдельной производственной площадки. Подключить контроллеры промышленного оборудования со стендов-макетов предприятия.

2. Сведения, необходимые для выполнения работы.
• Межсетевые экраны. Термины и определения компьютерных сетй. Пассивное сетевое оборудование.
• Состав сетевого оборудования, размещаемого в сетевых шкафах и стойках; серверные и коммутационные стойки.
•Порядок расположения сетевого оборудования в сетевых шкафах, кроссирование, патч-корды, органайзеры. Кабель-каналы.
• Классификация и модели сетевых серверов, особенности организации их дисковых массивов. Горячее резервирование. Лезвия.
• Адресация в сетях TCP/IP: использование масок, порядок назначения, технология CIDR.
• Протокол ARP. Доменные имена. Система DNS.

8.3. Перечень вопросов и заданий для промежуточной аттестации по дисциплине

Вопросы для промежуточного контроля (зачет)

1. История развития телекоммуникационных систем, основные технологии телекоммуникационных систем в 18-20 веках, их современное применение.
2. История развития телеграфа. Перечислить основные вехи на этом пути – достижения, люди, даты.
3. История развития телефонной связи. Перечислить основные вехи на этом пути – достижения, люди, даты.
4. История развития радиосвязи. Перечислить основные вехи на этом пути – достижения, люди, даты.
5. Эталонная модель взаимодействия открытых систем (OSI). Описание её уровней.
6. Основные определения передачи информации, её уровней и параметров первичных сигналов.
7. Основные определения сетей связи.

8. Кабельные и воздушные линии связи на основе металлических проводников, симметричных и коаксиальных кабелей.
9. Волоконно-оптические линии связи: физическая суть, конструкция, преимущества, классификация.
10. Диапазоны радиоволн и способы их распространения в зависимости от диапазона.
11. Радиолинии. Радиорелейные системы передачи. Тропосферные радиорелейные системы передачи.
12. Антенны – виды, параметры, особенности для различных диапазонов.Фидеры.
13. Модуляция, кодирование – основыне определения. Канал тональной частоты, его АЧХ.
14 Модем. Потенциальное кодирование. Сравнение АМ, ЧМ и ФМ.
15. Цифровое кодирование, потенциальные и импульсные коды. NRZ, NRZ-I, Биполярный Импульсный Код, Манчестерский Код, 2B1Q.
16. Манипуляция. Квадратурная амплитудная модуляция. Дискретизация,АЦП, ЦАП. Теорема Котельникова. АИМ, ИКМ, δ-модуляция.
17. Вокодеры: полосные, с линенйым предсказанием, гомоморфные, полувокодеры. Форматные фильтры.
18 Равномерное ое и неравномерное кодирование.длина кодового слова. Код Шеннона-Фано. Алгоритм Хаффмана. Помехоустойчивое кодирование.
19. Способы объединения цифровых потоков и особенности передачи дискретных сообщений по цифровым каналам.
20. Системы телефонной связи. Цифровое кодирование речи.
21. Алгоритм адаптивной дифференциальной импульсно-кодовой модуляции. . Гибридные алгоритмы.
22. Единая система нумерации, зоновый принцип нумерации. Междугородная, городская и сельская телефонные связи.
23.Телефон, микрофон, номеронабиратель, телефонный аппарат. Принцип действия электромагнитного телефона, угольного микрофона.
24. ЦОС. Этапы АЦП. Выборка и хранение. Квантование мгновенных значений сигнала, ошибка и шум, неравномерное квантование.
25. Передача данных по телефонным сетям. Модем. Бод, бодовый интервал, бодовая скорость.
26. МЧРК, ассиметричная дуплексная связь, эхоподавление, полудуплескная связь, V.34.
27. Системы телеграфной связи. Оконечный телеграфный аппарат, кодовый метод. Равномерное и неравномерное кодирование.
28. Способы передачи двоичных кодов. Синхронизация. Фазирование. Стартстопы системы телеграфной связи.
29. Телевизионные системы. Передающая и приемная трубка. Линейно-строчная и черезстрочная развертки. PAL, SECAM, NTSC.
30. Системы подвижной радиосвязи. Тракинговые системы.
31. Сотовая связь. Принцип повторного использования частот. Поколения сотовых передатчиков.
32. Сетевые карты – принцип действия, виды, модели.
33. Сетевой кабель – скорости передачи, физические виды, наименования, конструкция, полоса пропускания.
34. Хабы, свичи, коммутаторы – основные определения.
35. Классификация коммутатров – общие характеристики, сравнение моделей (DLINK, TPLINK).
36. Интеллектуальные коммутаторы 2-го и 3-го уровней – модели, характеристики, цены (как показатель функциональности).
37. Точки доступа, маршрутизаторы – классификация, виды, характеристики. NAT.
38. ADSL-модемы, принт-серверы, межсетевые экраны.
39. Термины и определения компьютерных сетй.

40. Пассивное сетевое оборудование.
41. Состав сетевого оборудования, размещаемого в сетевых шкафах и стойках; серверные и коммутационные стойки.
42. Порядок расположения сетевого оборудования в сетевых шкафах, кроссирование, патч-корды, органайзеры. Кабель-каналы.
43. Классификация и модели сетевых серверов, особенности организации их дисковых массивов. Горячее резервирование. Лезвия.
44. Стэк протоколов TCP/IP: типы адресов стека, формат IP-адреса, классы IP-адресов.
45. Адресация в сетях TCP/IP: использование масок, порядок назначения, технология CIDR.
46. Протокол ARP. Доменные имена. Система DNS.

8.4. Планируемые уровни сформированности компетенций обучающихся и критерии оценивания

Уровни	Содержательное описание уровня	Основные признаки выделения уровня (этапы формирования компетенции, критерии оценки сформированности)	Пятибалльная шкала (академическая) оценка	Двухбалльная шакала, зачет	БРС, % освоения (рейтинговая оценка)
Повышенный	Творческая деятельность	*Включает нижестоящий уровень.* Умение самостоятельно принимать решение, решать проблему/задачу теоретического и прикладного характера на основе изученных методов, приемов, технологий	отлично	зачтено	86-100
Базовый	Применение знаний и умений в более широких контекстах учебной и профессиональной деятельности, нежели по образцу с большей степени самостоятельности и инициативы	*Включает нижестоящий уровень.* Способность собирать, систематизировать, анализировать и грамотно использовать информацию из самостоятельно найденных теоретических источников и иллюстрировать ими теоретические положения или обосновывать практику применения	хорошо		71-85
Удовлетворительный	Репродуктивная	Изложение в пределах задач курса	удовлетворительно		55-70

(достаточный)	деятельность	теоретически и практически контролируемого материала			
Недостаточный	Отсутствие признаков удовлетворительного уровня		неудовлетворительно	не зачтено	Менее 55

9. Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины.

Основная литература

1. Каганов, В. И. Радиотехнические цепи и сигналы. Компьютеризированный курс : учебное пособие / В.И. Каганов. — 4-е изд., перераб. и доп. — Москва : ФОРУМ : ИНФРА-М, 2021. — 498 с. — (Высшее образование: Магистратура). — DOI 10.12737/textbook_5a86b8b1ee58d8.44881391. - ISBN 978-5-00091-447-2. - Текст : электронный. - URL: https://znanium.com/catalog/product/1413304 (дата обращения: 28.04.2022). – Режим доступа: по подписке.

Дополнительная литература

2. Гребешков, А. Ю. Вычислительная техника, сети телекоммуникации: Учебное пособие для ВУЗов / Гребешков А.Ю., Попова Н.А. - Москва : Гор. линия-Телеком, 2015. - 190 с. (Учебник для высших учебных заведений) ISBN 978-5-9912-0492-7. - Текст : электронный. - URL: https://znanium.com/catalog/product/524144 (дата обращения: 28.04.2022). – Режим доступа: по подписке.
3. Кузьмич, Р.И. Вычислительные системы, сети и телекоммуникации : учеб. пособие / Р.И. Кузьмич, А.Н. Пупков, Л.Н. Корпачева. - Красноярск : Сиб. федер. ун-т, 2018. - 120 с. - ISBN 978-5-7638-3943-2. - Текст : электронный. - URL: https://znanium.com/catalog/product/1032192 (дата обращения: 28.04.2022). – Режим доступа: по подписке.

10. Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины (модуля).

- НЭБ Национальная электронная библиотека, диссертации и прочие издания
- eLIBRARY.RU Научная электронная библиотека, книги, статьи, тезисы докладов конференций
- Гребенников Электронная библиотека ИД журналы
- ЭБС ZNANIUM.COM
- РГБ Информационное обслуживание по МБА
- БЕН РАН
- Электронно-библиотечная система (ЭБС) Кантитана (https://elib.kantiana.ru/)

11. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине.

Программное обеспечение обучения включает в себя:

- система электронного образовательного контента БФУ им. И. Канта – www.lms-3.kantiana.ru, обеспечивающую разработку и комплексное использование электронных образовательных ресурсов;

- серверное программное обеспечение, необходимое для функционирования сервера и связи с системой электронного обучения через Интернет;
- корпоративная платформа Microsoft Teams;
- установленное на рабочих местах обучающихся ПО: Microsoft Windows 7, Microsoft Office Standart 2010, антивирусное программное обеспечение Kaspersky Endpoint Security.
- СУБД PostgreSQL (Свободное ПО, лицензия - Freeware).
- MongoDB (Свободное ПО, лицензия - Freeware).

12. Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине.

Для проведения занятий лекционного типа, практических и семинарских занятий используются специальные помещения (учебные аудитории), оборудованные техническими средствами обучения – мультимедийной проекционной техникой. Для проведения занятий лекционного типа используются наборы демонстрационного оборудования.

Для проведения лабораторных работ, (практических занятий – при необходимости) используются специальные помещения (учебные аудитории), оснащенные специализированным лабораторным оборудованием: персональными компьютерами с возможностью выхода в интернет и с установленным программным обеспечением, заявленным в п.11.

Для проведения групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации используются специальные помещения (учебные аудитории), оборудованные специализированной мебелью (для обучающихся), меловой / маркерной доской.

Для организации самостоятельной работы обучающимся предоставляются помещения, оснащенные компьютерной техникой с возможностью подключения к сети «Интернет» и обеспечением доступа в электронную информационно-образовательную среду университета.

Для обучения инвалидов и лиц с ограниченными возможностями здоровья университетом могут быть представлены специализированные средства обучения, в том числе технические средства коллективного и индивидуального пользования.

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
федеральное государственное автономное образовательное учреждение высшего образования «Балтийский федеральный университет имени Иммануила Канта»
Институт физико-математических наук и информационных технологий

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

«Системы управления базами данных»

Шифр: 10.05.01
Специальность: «Компьютерная безопасность»
Специализация: «Математические методы защиты информации»
Квалификация (степень) выпускника: специалист по защите информации

Калининград
2022

Лист согласования

Составитель: Каратаева Полина Михайловна, старший преподаватель

Рабочая программа утверждена на заседании учебно-методического совета института физико-математических наук и информационных технологий

Протокол № 01/22 от «01» февраля 2022 г.

Председатель учебно-методического
совета института физико-
математических наук и информационных
технологий

Первый заместитель директора Шпилевой А. А
ИФМНиИТ, к. ф.-м. н., доцент

Ведущий менеджер Е.П.Ставицкая

Содержание

1.Наименование дисциплины: «Системы управления базами данных».

Целью курса «Системы управления базами данных» является обучение студентов фундаментальным знаниям в области теории баз данных и выработка практических навыков применения этих знаний при создании программных продуктов для обработки информации с помощью систем управления базами данных.

2. Перечень планируемых результатов обучения по дисциплине, соотнесенных с планируемыми результатами освоения образовательной программы

Код компетенции	Результаты освоения образовательной программы (ИДК)	Результаты обучения по дисциплине
ОПК-14 - Способность проектировать базы данных, администрировать системы управления базами данных в соответствии с требованиями по защите информации;	ОПК-14.1. Знает методы, алгоритмы и инструменты для проектирования баз данных, администрирования систем управления базами данных в соответствии с требованиями по защите информации. ОПК-14.2. Умеет проектировать базы данных, администрировать системы управления базами данных в соответствии с требованиями по защите информации. ОПК-14.3. Владеет навыками проектирования баз данных, администрирования систем управления базами данных в соответствии с требованиями по защите информации.	В результате формирования данной компетенции обучающийся должен: -знать: основы теории построения баз данных; методику анализа предметной области при построении базы данных информационной системы; современные СУБД и языки, связанные с созданием и обработкой информации в базах данных, методы и подходы к оценке эффективности баз данных и СУБД; -уметь проводить даталогическое, инфологическое проектирование базы данных, осуществлять разработку физической реализации базы данных на основе современных СУБД; обнаруживать и исправлять ошибки при работе с базами данных; администрировать СУБД; -владеть практическими навыками разработки клиент-серверных систем, проверки соответствия существующих информационных систем актуальным стандартам хранения и обработки информации, требованиям заказчика, работы в современных СУБД.

3. Место дисциплины в структуре образовательной программы

«Системы управления базами данных» представляет собой дисциплину обязательной части Блока 1 Дисциплины (модули) подготовки обучающихся, входит в Модуль 4. Компьютерные технологии (Б1.О.08.02).

4. Виды учебной работы по дисциплине.

Виды учебной работы по дисциплине зафиксированы учебным планом основной профессиональной образовательной программы по указанному направлению и профилю, выражаются в академических часах. Часы контактной работы и самостоятельной работы обучающегося и часы, отводимые на процедуры контроля, могут различаться в учебных планах ОПОП по формам обучения. Объем контактной работы включает часы контактной аудиторной работы (лекции/практические занятия/ лабораторные работы), контактной внеаудиторной работы (контроль самостоятельной работы), часы контактной работы в период аттестации. Контактная работа, в том числе может проводиться посредством электронной информационно-образовательной среды университета с использованием ресурсов сети Интернет и дистанционных технологий

5. Содержание дисциплины, структурированное по темам (разделам)

Исходя из рамок, установленных учебным планом по трудоемкости и видам учебной работы по дисциплине, преподаватель самостоятельно выбирает тематику занятий по формам и количеству часов проведения контактной работы: лекции и иные учебные занятия, предусматривающие преимущественную передачу учебной информации преподавателем и (или) занятия семинарского типа (семинары, практические занятия, практикумы, лабораторные работы, коллоквиумы и иные аналогичные занятия), и (или) групповые консультации, и (или) индивидуальную работу обучающихся с преподавателем, в том числе индивидуальные консультации (по курсовым работам/проектам – при наличии курсовой работы/проекта по данной дисциплине в учебном плане). Рекомендуемая тематика занятий максимально полно реализуется в контактной работе с обучающимися очной формы обучения. В случае реализации образовательной программы в заочной / очно-заочной форме трудоемкость дисциплины сохраняется, однако объем учебного материала в значительной части осваивается обучающимися в форме самостоятельной работы. При этом требования к ожидаемым образовательным результатам обучающихся по данной дисциплине не зависят от формы реализации образовательной программы.

№	Наименование раздела	Содержание раздела
1	Информационные системы. Базы данных и системы управления базой данных	Информационные системы. Информационные процессы. Информация. Представление информации. Документирование информации. Данные. Основы информационного обеспечения и информационные системы. Структура и классификация информационных систем. Система представления и обработки данных фактографических, документальных и геоинформационных ИС. Системы управления базами данных.
2	Модели данных. Инфологическое и даталогическое моделирование. Этапы проектирования БД.	Классификация моделей. Иерархическая, сетевая, реляционная, объектно-ориентированная и многомерная модели организации данных. Концептуальное и схемно-структурное проектирование. Основные понятия и этапы даталогического моделирования. Организация программного и информационного обеспечения с использованием БД и СУБД. Жизненный цикл базы

		данных. Основные понятия и этапы инфологического моделирования. Проектирование на физическом уровне.
3	Реляционная модель данных. Нормирование. Средства и методы проектирования БД	Задачи, решаемые реляционной моделью данных. Реляционные типы данных. Проектирование схемы базы данных. Нормирование. Проектирование и создание таблиц. Внутренняя схема базы данных. Физическая структура данных. Проектирование с условием нормализации. Семантическое моделирование данных, ER-диаграммы.
4	Языковые средства современных СУБД. Реляционные БД и СУБД. Язык SQL	Функции, классификация и структура СУБД. Языки программирования. Реляционные БД и СУБД. Логическая схема базы данных. Сильные и слабы стороны данных СУБД. Язык структурированных запросов SQL. Команды Insert, Modify, Update. Создание БД и объектов СУБД. Индексирование данных.
5	Реляционные БД. Организация процессов обработки данных в БД. Запросы на языке SQL	Организация процессов обработки данных в БД. Поиск, фильтрация и сортировка данных. Запросы на языке SQL. Команда Select. Создание запросов с условием, из нескольких таблиц, агрегированных запросов. Подзапросы. Нетривиальные запросы.
6	Реляционные БД. Ограничения целостности	Организация процессов хранения данных в БД. Ограничения целостности Триггеры, правила, ограничения.
7	Реляционные БД. Особенности построение интерфейса.	Реляционные БД. Механизмы разработки приложений баз данных Особенности построение интерфейса. Обработка данных на стороне клиента.
8	Коммерческие БД и СУБД.	Типы коммерческих БД и СУБД. Гипертекстовые и мультимедийные БД. СУБД на инвертированных файлах. СУБД на правилах. Дедуктивные и темпоральные БД.
9	Обзор развития современных БД и СУБД	Обзор развития современных БД и СУБД. Рейтинг СУБД. Современные направления развития.
10	Объектно-реляционные БД и СУБД.	Типы данных. Внутренняя схема базы данных. Физическая структура данных. Сильные и слабы стороны объектно-реляционных СУБД. Создания и применения объектных типов, использование пакетов, реализация внешних процедур. Особенности обработки данных в объектно-реляционных БД и СУБД. Объекты СУБД: представления, хранимые процедуры, функции пользователя, вычисляемые поля. Методы связи с SQL-ориентированными БД.
11	Динамический и встроенный SQL.	Вопросы встраивания операторов языка SQL в основной язык программирования и применение операторов SQL, создание и использование SQL-дескрипторов и динамических курсоров..
12	Организация многопользовательского режима работы в СУБД.	Организация процессов доступа к данных в БД через СУБД. Команды языка SQL. Вопросы использования различных уровней изоляции и применение транзакций. Управление транзакциями.

		Методы сериализация транзакций. Метод временных меток. Вопросы назначения и снятия привилегий на объекты баз данных. Журнализация
13	Распределенные БД.	Понятие распределенных информационных систем, принципы их создания и функционирования.
14	Технология клиент - сервер	Режимы работы с БД. Технологии и модели «Клиент-сервер». Модели файлового сервера, удаленного доступа к данным, сервера базы данных, сервера приложений. Мониторы транзакций. Архитектуры построения серверов БД.
15	Технологии доступа к данным.	Подходы к реализации доступа к источникам данных, приводится анализ различных методов доступа к данным, включая ODBC, DAO, RDO, OLE DB и ADO, рассматриваются механизмы публикации удаленных источников данных в Inernet.
16	Технология реплицирования данных.	Реплика. Виды технологий реплицирования данных. Проблемы и пути их решения.
17	Анализ данных. Технология NoSQL	История появления баз NoSQL. Агрегированные модели данных. Графовые базы данных. Неструктурированные базы данных. Модели распределения. Отображения - свертка. Базы данных типа "ключ - значение". База данных PostgreSQL. Технология NoSQL
18	Хранилища данных.	Хранилища данных: виды и способы создания. Технология оперативной обработки транзакций (OLTP – технология). Информационные хранилища. OLAP – технология.
19	Документационные информационные системы. Публикация баз данных в Интернете	Общая характеристика и виды документальных информационных систем. Информационно-поисковые каталоги и тезариусы. Полнотекстовые информационно-поисковые системы. Гипертекстовые информационно-поисковые системы. Применение БД для хранения информации в сети Интернет. Особенности проектирования структуры базы данных и визуализации в Интернете. СУБД, позволяющие осуществлять публикацию данных в сети Интернет.
20	XML-серверы	XML – серверы. Взаимодействие пользовательских приложений с БД через СУБД. Задачи, решаемые XML-сервером. Обработка данных в формате XML.
21	Интеллектуальный анализ данных (Data Mining)	Задачи Data Mining. Задачи классификации и регрессии. Задача классификации. Задача поиска ассоциативных правил и последовательностей. Модели Data Mining. Деревья решений. Нейронные сети. Нечеткая логика. Генетические алгоритмы. Стандарты Data Mining. Роли в Data Mining. Рынок инструментов Data Mining. Классификация инструментов Data Mining. SAS Enterprise Data Mining. PolyAnalyst. WebAnalyst
22	Определение больших данных. Обзор технологий хранения	Основные вызовы больших данных. Определение термина "большие данные". Характеристика больших данных. Большие данные как одна из

	больших данных	глобальных проблем современности. Свойства больших данных и ограничения RDBMS. ACID требования, CAP-теорема, BASE архитектура. Подход MapReduce: Map-задачи, Reduce-задачи. Алгоритмы, использующие MapReduce и их приложения. Матрично-векторное умножение, операции реляционной алгебры, операции на базах данных, группировка и агрегирование.

6. Рекомендуемая тематика учебных занятий в форме контактной работы

Рекомендуемая тематика учебных занятий *лекционного* типа (предусматривающих преимущественную передачу учебной информации преподавателями):

№	Наименование раздела	Тема лекции
1	Информационные системы. Базы данных и системы управления базой данных	Лекция 1. Информационные системы. Информационные процессы. Информация. Представление информации. Системы управления базами данных.
2	Модели данных. Инфологическое и даталогическое моделирование. Этапы проектирования БД.	Лекция 2. Классификация моделей. Иерархическая, сетевая, реляционная, объектно-ориентированная и многомерная модели организации данных.
3	Реляционная модель данных. Нормирование. Средства и методы проектирования БД	Лекция 3. Задачи, решаемые реляционной моделью данных. Реляционные типы данных. Проектирование схемы базы данных. Нормирование. Лекция 4. Проектирование и создание таблиц. Внутренняя схема базы данных. Физическая структура данных.
4	Языковые средства современных СУБД. Реляционные БД и СУБД. Язык SQL	Лекция 5. Функции, классификация и структура СУБД. Языки программирования. Лекция 6. Реляционные БД и СУБД. Логическая схема базы данных. Лекция 7. Язык структурированных запросов SQL. Команды Insert, Modify, Update.
5	Реляционные БД. Организация процессов обработки данных в БД. Запросы на языке SQL	Лекция 8. Организация процессов обработки данных в БД. Поиск, фильтрация и сортировка данных. Лекция 9. Запросы на языке SQL. Команда Select.
6	Реляционные БД. Ограничения целостности	Лекция 10. Организация процессов хранения данных в БД. Лекция 11. Ограничения целостности Триггеры, правила, ограничения.
7	Реляционные БД. Особенности построение интерфейса.	Лекция 12. Механизмы разработки приложений баз данных Лекция 13. Особенности построение интерфейса. Обработка данных на стороне клиента.
8	Коммерческие БД и СУБД.	Лекция 14. Типы коммерческих БД и СУБД.

9	Обзор развития современных БД и СУБД	Лекция 15. Обзор развития современных БД и СУБД. Рейтинг СУБД. Современные направления развития.
10	Объектно-реляционные БД и СУБД.	Лекция 16. Внутренняя схема базы данных. Физическая структура данных. Сильные и слабы стороны объектно-реляционных СУБД. Лекция 17. Создания и применения объектных типов, использование пакетов, реализация внешних процедур. Особенности обработки данных в объектно-реляционных БД и СУБД. Лекция 18. Объекты СУБД: представления, хранимые процедуры, функции пользователя, вычисляемые поля. Методы связи с SQL-ориентированными БД.
11	Динамический и встроенный SQL.	Лекция 19. Вопросы встраивания операторов языка SQL в основной язык программирования и применение операторов SQL. Лекция 20. Создание и использование SQL-дескрипторов и динамических курсоров..
12	Организация многопользовательского режима работы в СУБД.	Лекция 21. Организация процессов доступа к данных в БД через СУБД. Управление транзакциями.
13	Распределенные БД.	Лекция 22. Понятие распределенных информационных систем, принципы их создания и функционирования.
14	Технология клиент - сервер	Лекция 23. Режимы работы с БД. Технологии и модели «Клиент-сервер».
15	Технологии доступа к данным.	Лекция 24. Подходы к реализации доступа к источникам данных, приводится анализ различных методов доступа к данным, включая ODBC, DAO, RDO, OLE DB и ADO.
16	Технология реплицирования данных.	Лекция 25. Реплика. Виды технологий реплицирования данных. Проблемы и пути их решения.
17	Анализ данных. Технология NoSQL	Лекция 26. История появления баз NoSQL. Агрегированные модели данных. Лекция 27. Графовые базы данных. Неструктурированные базы данных. Базы данных типа "ключ - значение".
18	Хранилища данных.	Лекция 28. Хранилища данных: виды и способы создания.
19	Документационные информационные системы. Публикация баз данных в Интернете	Лекция 29. Общая характеристика и виды документальных информационных систем. Информационно-поисковые каталоги и тезариусы.
20	XML-серверы	Лекция 30. XML – серверы. Взаимодействие пользовательских приложений с БД через СУБД.
21	Интеллектуальный анализ данных (Data Mining)	Лекция 31. Задачи Data Mining. Задачи классификации и регрессии. Задача классификации.
22	Определение больших данных. Обзор	Лекция 32. Основные вызовы больших данных. Определение термина "большие данные".

	технологий хранения больших данных	Характеристика больших данных.

Рекомендуемая тематика *практических* занятий:

№ п/п	**Наименование Темы**	**Содержание темы**
1	Информационные системы. Базы данных и системы управления базой данных	Определение информации, документирование информации и данных. Обзор систем представления и обработки данных фактографических, документальных и геоинформационных
2	Модели данных. Инфологическое и даталогическое моделирование. Этапы проектирования БД.	Правила анализа функциональных требований. Определение объектов проектируемой области, их свойств и взаимосвязей. Основные принципы инфологического моделирования. Принципы даталогического моделирования.
3	Реляционная модель данных. Нормирование. Средства и методы проектирования БД	Логическое проектирование схемы базы данных. Нормирование. Проектирование физической схемы БД с условием нормализации. Построение ER-диаграммы
4	Языковые средства современных СУБД. Реляционные БД и СУБД. Язык SQL	Создание БД и объектов СУБД Язык структурированных запросов SQL. Команды Create, Alter, Drop, Insert, Modify, Update. Индексирование данных.
5	Реляционные БД. Организация процессов обработки данных в БД. Запросы на языке SQL	Организация процессов обработки данных в БД. Поиск, фильтрация и сортировка данных. Запросы на языке SQL. Команда Select. Создание запросов с условием, из нескольких таблиц, агрегированных запросов. Подзапросы. Нетривиальные запросы.
6	Реляционные БД. Ограничения целостности	Организация процессов хранения данных в БД. Ограничения целостности Триггеры, правила, ограничения.
7	Реляционные БД. Особенности построение интерфейса.	Разработка приложений баз данных Особенности построение интерфейса. Обработка данных на стороне клиента.
8	Объектно-реляционные БД и СУБД	Создания и применения объектных типов, использование пакетов, реализация внешних процедур. Обработка данных в объектно-реляционных БД и СУБД (представления, хранимые процедуры, функции пользователя, вычисляемые поля).
9	Динамический и встроенный SQL.	Встраивание операторов языка SQL в основной язык программирования, создание и использование SQL-дескрипторов и динамических курсоров
10	Технологии доступа к данным	Изучение различных методов доступа к данным, включая ODBC, DAO, RDO, OLE DB и ADO, в том числе механизмы публикации удаленных источников данных в Inernet.
11	Технология	Создание реплики БД. Изучение технологии

	реплицирования данных	реплицирования данных.
12	Анализ данных. Технология NoSQL	Создание и изучение графовых базы данных. Неструктурированные базы данных. Технология NoSQL
13	Хранилища данных.	Создание хранилища. Обработка данных.
14	XML-серверы	Обработка данных в формате XML.
15	Интеллектуальный анализ данных (Data Mining)	Обзор задач Data Mining.

На практических занятиях решаются задачи по теме занятия.

Требования к самостоятельной работе обучающихся

1. Работа с лекционным материалом, предусматривающая проработку конспекта лекций и учебной литературы, по всем темам из п. 6 настоящей рабочей программы.

2. Выполнение домашнего задания, предусматривающего решение задач, выполнение упражнений, выдаваемых на практических занятиях, по всем темам из п. 6 настоящей рабочей программы.

Руководствуясь положениями статьи 47 и статьи 48 Федерального закона от 29 декабря 2012 г. N 273-ФЗ «Об образовании в Российской Федерации» научно-педагогические работники и иные лица, привлекаемые университетом к реализации данной образовательной программы, пользуются предоставленными академическими правами и свободами в части свободы преподавания, свободы от вмешательства в профессиональную деятельность; свободы выбора и использования педагогически обоснованных форм, средств, методов обучения и воспитания; права на творческую инициативу, разработку и применение авторских программ и методов обучения и воспитания в пределах реализуемой образовательной программы и отдельной дисциплины.

Исходя из рамок, установленных учебным планом по трудоемкости и видам учебной работы по дисциплине, преподаватель самостоятельно выбирает тематику занятий по формам и количеству часов проведения контактной работы: лекции и иные учебные занятия, предусматривающие преимущественную передачу учебной информации преподавателем и (или) занятия семинарского типа (семинары, практические занятия, практикумы, лабораторные работы, коллоквиумы и иные аналогичные занятия), и (или) групповые консультации, и (или) индивидуальную работу обучающихся с преподавателем, в том числе индивидуальные консультации (по курсовым работам/проектам – при наличии курсовой работы/проекта по данной дисциплине в учебном плане).

Рекомендуемая тематика занятий максимально полно реализуется в контактной работе с обучающимися очной формы обучения. В случае реализации образовательной программы в заочной / очно-заочной форме трудоемкость дисциплины сохраняется, однако объем учебного материала в значительной части осваивается обучающимися в форме самостоятельной работы. При этом требования к ожидаемым образовательным результатам обучающихся по данной дисциплине не зависят от формы реализации образовательной программы.

7. Методические рекомендации по видам занятий

Лекционные занятия.

В ходе лекционных занятий обучающимся рекомендуется выполнять следующие действия. Вести конспектирование учебного материала. Обращать внимание на категории, формулировки, раскрывающие содержание тех или иных явлений и процессов, научные

выводы и практические рекомендации по их применению. Задавать преподавателю уточняющие вопросы с целью уяснения теоретических положений, разрешения спорных ситуаций.

Желательно оставить в рабочих конспектах поля, на которых во внеаудиторное время можно сделать пометки из рекомендованной литературы, дополняющие материал прослушанной лекции, а также подчеркивающие особую важность тех или иных теоретических положений.

Практические и семинарские занятия.

На практических и семинарских занятиях в зависимости от темы занятия выполняется поиск информации по решению проблем, практические упражнения, контрольные работы, выработка индивидуальных или групповых решений, итоговое обсуждение с обменом знаниями, участие в круглых столах, разбор конкретных ситуаций, командная работа, представление портфолио и т.п.

Самостоятельная работа.

Самостоятельная работа осуществляется в виде изучения литературы, эмпирических данных по публикациям и конкретных ситуаций из практики, подготовке индивидуальных работ, работа с лекционным материалом, самостоятельное изучение отдельных тем дисциплины; поиск и обзор литературы и электронных источников; чтение и изучение учебника и учебных пособий.

8. Фонд оценочных средств

8.1. Перечень компетенций с указанием этапов их формирования в процессе освоения образовательной программы в рамках учебной дисциплины

Основными этапами формирования указанных компетенций при изучении обучающимися дисциплины являются последовательное изучение содержательно связанных между собой тем учебных занятий. Изучение каждой темы предполагает овладение обучающимися необходимыми компетенциями. Результат аттестации обучающихся на различных этапах формирования компетенций показывает уровень освоения компетенций.

Контролируемые разделы (темы) дисциплины	Индекс контролируемой компетенции (или её части)	Оценочные средства по этапам формирования компетенций
		текущий контроль по дисциплине
Тема 1. Информационные системы. Базы данных и системы управления базой данных	ОПК-14	Лабораторная работа
Тема 2. Модели данных. Инфологическое и даталогическое моделирование. Этапы проектирования БД.	ОПК-14	Лабораторная работа
Тема 3. Реляционная модель данных. Нормирование. Средства и методы проектирования БД	ОПК-14	Лабораторная работа
Тема 4. Языковые средства современных СУБД. Реляционные БД и СУБД.	ОПК-14	Лабораторная работа

Контролируемые разделы (темы) дисциплины	Индекс контролируемой компетенции (или её части)	Оценочные средства по этапам формирования компетенций
		текущий контроль по дисциплине
Язык SQL		
Тема 5. Реляционные БД. Организация процессов обработки данных в БД. Запросы на языке SQL	ОПК-14	Лабораторная работа
Тема 6. Реляционные БД. Ограничения целостности	ОПК-14	Лабораторная работа
Тема 7. Реляционные БД. Особенности построение интефейса.	ОПК-14	Лабораторная работа
Тема 8. Коммерческие БД и СУБД	ОПК-14	Доклад
Тема 9. Обзор развития современных БД и СУБД	ОПК-14	Лабораторная работа
Тема 10. Объектно-реляционные БД и СУБД	ОПК-14	Лабораторная работа
Тема 11. Динамический и встроенный SQL.	ОПК-14	Тест
Тема 12. Организация многопользовательского режима работы в СУБД.	ОПК-14	Тест
Тема 13. Распределенные БД	ОПК-14	Тест
Тема 14. Технология клиент - сервер	ОПК-14	Тест
Тема 15. Технологии доступа к данным.	ОПК-14	Лабораторная работа
Тема 16. Технология реплицирования данных	ОПК-14	Лабораторная работа
Тема 17. Анализ данных. Технология NoSQL	ОПК-14	Лабораторная работа
Тема 18. Хранилища данных.	ОПК-14	Лабораторная работа
Тема 19. Документационные информационные системы. Публикация баз данных в Интернете	ОПК-14	Тест
Тема 20. XML-серверы	ОПК-14	Лабораторная работа
Тема 21. Интеллектуальный анализ данных (Data Mining)	ОПК-14	Лабораторная работа
Тема 22. Определение больших данных. Обзор технологий хранения больших данных	ОПК-14	Тест

8.2. Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений и навыков и (или) опыта деятельности процессе текущего контроля

Тема 3. Реляционная модель данных. Нормирование.
Средства и методы проектирования БД

1.	Реляционная модель организации данных представлена только наборами данных, которые имеют:	А) строго древовидную структуру Б) сетевую структуру Г) распределенную структуру Д) табличную структуру
2.	Информация в реляционной базе данных может хранится с помощью:	А) представлений Б) индексов В) таблиц Г) схемы Д) физической схемы
3.	Нормализация баз данных нужна для:	А) минимизации дублирования информации Б) для усложнения базы данных В) рациональное введение ключевых полей
4.	важным отличием реляционных баз данных являются:	• четкая граница между логическим и физическим представлениями объектов • мощные и гибкие средства структуризации данных
5.	Реляционная модель поддерживает следующие типы отношений:	• Многие к одному • Кратные • Один ко одному • Неопределенные • Предок / потомок
6.	Поля кортежей могут содержать:	Г) атомарные значения Д) множественные значения
7.	В наиболее общей и классической постановке реляционный подход базируется на следующих концепциях:	А) объекта и идентификатора объекта; Б) атрибутов и методов; В) классов; Г) иерархии и наследования классов.
8.	при проектировании реляционной БД вся информация разбивается на:	А) множество двумерных объектов. Б) множество двумерных массивов. В) множество двумерных связей.
9.	Ограничение на атомарность атрибутов означает:	• что в реляционной базе данных атрибут каждой записи может содержать только одно значение. • что в реляционной базе данных ключевое поле каждой записи может содержать несколько значений.
10.	Основными понятиями реляционных баз данных являются.	• тип данных, • домен • атрибут • кортеж • первичный ключ • внешний ключ • отношение
11.	Ограничением первой нормальной формы является:	• каждый неключевой атрибут таблицы полностью зависит от первичного ключа • каждый неключевой атрибут не зависит от первичного

1.	Иерархическая модель организации данных представлена только наборами данных, которые имеют:	А) строго древовидную структуру Б) сетевую структуру В) Одноуровневую структуру Г) распределенную структуру Д) табличную структуру

		ключа • каждый неключевой атрибут нетранзитивно зависит от первичного ключа.
12.	Таблица-отношение находится во второй нормальной форме:	• если все ее неключевые атрибуты функционально полно зависят от составного ключа. • если осуществляется взаимная независимость неключевых атрибутов и их полная функциональная зависимость от первичного ключа.

2.	Существуют следующие функции, реализуемые СУБД	А) организация и поддержание программной структуры данных Б) организация и поддержание физической структуры данных В) организация доступа к данным и их обработке в оперативной и внешней памяти Г) обработка и передача данных файловой системой Д) организация, размещение и оперирование данными во внешней памяти Е) организация и поддержание логической структуры данных Ж) размещение и обработка больших объемов данных в оперативной памяти
3.	Триггер это-	А) специальный файл СУБД Б) элемент системы обеспечение целостности базы данных В) хранимая процедура Г) специальный программный код, вызываемый СУБД при определенных условиях
4.	БД по типу хранимой информации бывает	• Информационными • Фактографическими • Распределенными • Документационными • Структурными • Геоинформационными
5.	Реляционная модель поддерживает следующие типы отношений:	А) Многие к одному Б) Один ко многим В) Кратные Г) Один ко одному Д) Многие ко многим Е) Неопределенные Ж) Предок / потомок
6.	OLE-объекты нужны для:	Е) Для доступа к данным во внешних библиотеках Ж) Для передачи данных в программе З) Для использования в программе внешних модулей
7.	Логическая модель базы данных нужна для:	А) определяет размещение данных, метод доступа и технику индексирования (иногда называется внутренней моделью системы) Б) отражает логические связи между элементами данных вне зависимости от их содержания и среде хранения
8.	Транзакция – это:	А) Механизм удаления записей Б) Механизм сохранения записей в базу В) Механизм возможности возврата в любую точку работы Г) Механизм возможности возврата в сохраненную точку
9.	в структуре СУБД можно выделить следующие функциональные блоки	А) • монитор транзакций Б) • интерфейс выдачи сведений В) • процессор описания и поддержания структуры базы данных Г) • генератор отчетов Д) • интерфейс запросов Е) • интерфейс ввода данных Ж) • процессор запросов к базе данных
10.	Хранимая процедура используется в случаях	Г) Обработки данных на стороне сервера Д) Используется для обработки данных на стороне клиента Е) Необходима для реализации интерфейса программы Ж) Для реализации триггеров
11.	Клиент-серверная	А) Способ отображения данных

	технология – это	Б) Технология организации доступа к данным В) Способ организации данных Г) Технология поддержки данных Д) Реализация принципа распределенной информации

8.3. Перечень вопросов и заданий для промежуточной аттестации по дисциплине

Вопросы для промежуточного контроля (зачет)

1.. Основные понятия базы данных.
2. Жизненный цикл базы данных.
3. Уровни моделей и этапы проектирования.
4. Даталогическое проектирование.
5. Средства проектирования базы данных
6. Методы проектирования базы данных
7. Проектирование базы данных на физическом уровне
8. Виды баз данных
9. Распределенные базы данных
10. Коммерческие базы данных: сходства и различия
11. Выбор СУБД.
12. Сетевые СУБД.
13. Реляционные СУБД
14. Языковые средства манипулирования данными в реляционных СУБД.
15. Средства реализации диалогового интерфейса и подготовки отчётов в языках СУБД.
16. Основы автоматического проектирования баз данных.

Вопросы для промежуточного контроля (экзамен)

1. Разъяснить соотношение и взаимосвязь понятий «информация», «знания», «сведения» и «данные».
2. Каково соотношение понятий банка данных и базы данных?
3. К какому типу информационных систем можно отнести картотеку личных дел сотрудников организации?
4. Чем отличается инфологическая схема предметной области информационной системы от схемы ее базы данных?
5. Перечислить основные функции, реализуемые СУБД, и охарактеризовать их с точки зрения системного или прикладного характера решаемых задач.
6. Перечислить основные понятия структурной составляющей реляционной мо-дели данных.
7. Сформулировать, в чем заключается и каким образом обеспечивается целост-ность в реляционной модели данных.
8. В чем заключается концептуальное проектирование?
9. Этапы проектирование схемы реляционной базы данных?
10. Нормализация таблиц. Декомпозиция схемы базы данных в третьей нормальной форме.
11. В каких целях применяется язык SQL в реляционных СУБД?
12. Структура запроса и условия поиска в языке SQL.
13. В чем преимущества и недостатки представления и отображения дан-ных в табличном виде и виде экранных форм?
14. Индексные методы доступа, индексно последовательные методы до-ступа, организация индекса, методы поиска в индексе.
15. Виртуальная память и иерархия в организации памяти.

16. Что «распределено» в распределенных информационных системах и каковы основные принципы создания и функционирования распределенных информационных систем?
17. На какие компоненты подразделяется программное обеспечение си-стем «Клиент-сервер»?
18. Охарактеризуйте роль и место монитора транзакций в СУБД систем «Клиент-сервер».
19. XML-серверы.
20. Основные отличия фактографических и документальных информаци-онных систем по форме предоставления данных и способам удовлетворения информационных потребностей пользователей.
21. Какие функции администратора связаны с проектированием и вводом АИС в эксплуатацию?
22. Цели, задачи и суть процессов журнализации в базах данных.
23. Какие функции обеспечивают языки безопасности баз данных?

8.4. Планируемые уровни сформированности компетенций обучающихся и критерии оценивания

Уровни	Содержательное описание уровня	Основные признаки выделения уровня (этапы формирования компетенции, критерии оценки сформированности)	Пятибалльная шкала (академическая) оценка	Двухбалльная шакала, зачет	БРС, % освоения (рейтинговая оценка)
Повышенный	Творческая деятельность	*Включает нижестоящий уровень.* Умение самостоятельно принимать решение, решать проблему/задачу теоретического и прикладного характера на основе изученных методов, приемов, технологий	отлично	зачтено	86-100
Базовый	Применение знаний и умений в более широких контекстах учебной и профессиональной деятельности, нежели по образцу с большей степени самостоятельности и	*Включает нижестоящий уровень.* Способность собирать, систематизировать, анализировать и грамотно использовать информацию из самостоятельно найденных теоретических источников и иллюстрировать ими теоретические положения или обосновывать практику применения	хорошо		71-85

	инициативы				
Удовлетворительный (достаточный)	Репродуктивная деятельность	Изложение в пределах задач курса теоретически и практически контролируемого материала	удовлетворительно		55-70
Недостаточный	Отсутствие признаков удовлетворительного уровня		неудовлетворительно	не зачтено	Менее 55

9. Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины.

Основная литература

1. Голицына, О. Л. Базы данных : учебное пособие / О. Л. Голицына, Н. В. Максимов, И. И. Попов. — 4-е изд., перераб. и доп. — Москва : ФОРУМ : ИНФРА-М, 2020. — 400 с. — (Высшее образование: Бакалавриат). - ISBN 978-5-00091-516-5. - Текст : электронный. - URL: https://znanium.com/catalog/product/1053934 (дата обращения: 11.01.2022). – Режим доступа: по подписке.

Дополнительная литература

1. Агальцов, В. П. Базы данных : в 2 книгах. Книга 2. Распределенные и удаленные базы данных : учебник / В.П. Агальцов. — Москва : ФОРУМ : ИНФРА-М, 2021. — 271 с. — (Высшее образование: Бакалавриат). - ISBN 978-5-8199-0713-9. - Текст : электронный. - URL: https://znanium.com/catalog/product/1514118 (дата обращения: 11.01.2022). – Режим доступа: по подписке.

10. Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины (модуля).

- НЭБ Национальная электронная библиотека, диссертации и прочие издания
- eLIBRARY.RU Научная электронная библиотека, книги, статьи, тезисы докладов конференций
- Гребенников Электронная библиотека ИД журналы
- ЭБС ZNANIUM.COM
- РГБ Информационное обслуживание по МБА
- БЕН РАН
- Электронно-библиотечная система (ЭБС) Кантитана (https://elib.kantiana.ru/)

11. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине.

Программное обеспечение обучения включает в себя:

- система электронного образовательного контента БФУ им. И. Канта – www.lms-3.kantiana.ru, обеспечивающую разработку и комплексное использование электронных образовательных ресурсов;
- серверное программное обеспечение, необходимое для функционирования сервера и связи с системой электронного обучения через Интернет;
- корпоративная платформа Microsoft Teams;

- установленное на рабочих местах обучающихся ПО: Microsoft Windows 7, Microsoft Office Standart 2010, антивирусное программное обеспечение Kaspersky Endpoint Security.
- СУБД PostgreSQL (Свободное ПО, лицензия - Freeware).
- MongoDB (Свободное ПО, лицензия - Freeware).

12. Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине.

Для проведения занятий лекционного типа, практических и семинарских занятий используются специальные помещения (учебные аудитории), оборудованные техническими средствами обучения – мультимедийной проекционной техникой. Для проведения занятий лекционного типа используются наборы демонстрационного оборудования.

Для проведения лабораторных работ, (практических занятий – при необходимости) используются специальные помещения (учебные аудитории), оснащенные специализированным лабораторным оборудованием: персональными компьютерами с возможностью выхода в интернет и с установленным программным обеспечением, заявленным в п.11.

Для проведения групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации используются специальные помещения (учебные аудитории), оборудованные специализированной мебелью (для обучающихся), меловой / маркерной доской.

Для организации самостоятельной работы обучающимся предоставляются помещения, оснащенные компьютерной техникой с возможностью подключения к сети «Интернет» и обеспечением доступа в электронную информационно-образовательную среду университета.

Для обучения инвалидов и лиц с ограниченными возможностями здоровья университетом могут быть представлены специализированные средства обучения, в том числе технические средства коллективного и индивидуального пользования.

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
федеральное государственное автономное образовательное учреждение высшего образования «Балтийский федеральный университет имени Иммануила Канта»
Институт физико-математических наук и информационных технологий

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

«Операционные системы»

Шифр: 10.05.01
Специальность: «Компьютерная безопасность»
Специализация: «Математические методы защиты информации»
Квалификация (степень) выпускника: специалист по защите информации

Калининград
2022

Лист согласования

Составитель: Зубков Евгений Вячеславович, старший преподаватель

Рабочая программа утверждена на заседании учебно-методического совета института физико-математических наук и информационных технологий

Протокол № 01/22 от «01» февраля 2022 г.

Председатель учебно-методического
совета института физико-
математических наук и информационных
технологий

Первый заместитель директора Шпилевой А. А
ИФМНиИТ, к. ф.-м. н., доцент

Ведущий менеджер Е.П.Ставицкая

Содержание

1. Наименование дисциплины: «Операционные системы»

Цель дисциплины: целью освоения дисциплины «Операционные системы» является развитие у студентов компетенций, связанных с изучением базовых понятий, компонентов и средств взаимодействия пользователя в операционной системе Linux (ОС).

2. Перечень планируемых результатов обучения по дисциплине, соотнесенных с планируемыми результатами освоения образовательной программы

Код компетенции	Результаты освоения образовательной программы (ИДК)	Результаты обучения по дисциплине
ОПК-12. Способен администрировать операционные системы и выполнять работы по восстановлению работоспособности прикладного и системного программного обеспечения	ОПК-12.1. Знает принципы и способы администрирования операционных систем, методы и алгоритмы восстановления работоспособности прикладного и системного программного обеспечения. ОПК-12.2. Способен администрировать операционные системы и выполнять работы по восстановлению работоспособности прикладного и системного программного обеспечения. ОПК-12.3. Владеет навыками администрирования операционных систем и восстановления работоспособности прикладного и системного программного обеспечения.	- **знать** понятия идентификатора и дескриптора процесса; понятия приоритета и очереди процессов; понятие событийного программирования; - **уметь** устанавливать иерархию процессов; задавать приоритет процессам; использовать системные прерывания; - **владеть** практическими навыками использования интерфейса прикладного программирования (API) для разработки прикладных приложений; разработки формальных моделей политик безопасности, политик управления доступом и информационными потоками в компьютерных системах с учетом угроз безопасности информации.

3. Место дисциплины в структуре образовательной программы

Дисциплина «Операционные системы» представляет собой дисциплину обязательной части блока дисциплин подготовки обучающихся.

4. Виды учебной работы по дисциплине

Виды учебной работы по дисциплине зафиксированы учебным планом основной профессиональной образовательной программы по указанному направлению и профилю, выражаются в академических часах. Часы контактной работы и самостоятельной работы обучающегося и часы, отводимые на процедуры контроля, могут различаться в учебных

планах ОПОП по формам обучения. Объем контактной работы включает часы контактной аудиторной работы (лекции/практические занятия/лабораторные работы), контактной внеаудиторной работы (контроль самостоятельной работы), часы контактной работы в период аттестации. Контактная работа, в том числе может проводиться посредством электронной информационно-образовательной среды университета с использованием ресурсов сети Интернет и дистанционных технологий.

5. Содержание дисциплины, структурированное по темам (разделам)

Исходя из рамок, установленных учебным планом по трудоемкости и видам учебной работы по дисциплине, преподаватель самостоятельно выбирает тематику занятий по формам и количеству часов проведения контактной работы: лекции и иные учебные занятия, предусматривающие преимущественную передачу учебной информации преподавателем и (или) занятия семинарского типа (семинары, практические занятия, практикумы, лабораторные работы, коллоквиумы и иные аналогичные занятия), и (или) групповые консультации, и (или) индивидуальную работу обучающихся с преподавателем, в том числе индивидуальные консультации (по курсовым работам/проектам – при наличии курсовой работы/проекта по данной дисциплине в учебном плане). Рекомендуемая тематика занятий максимально полно реализуется в контактной работе с обучающимися очной формы обучения. В случае реализации образовательной программы в заочной / очно-заочной форме трудоемкость дисциплины сохраняется, однако объем учебного материала в значительной части осваивается обучающимися в форме самостоятельной работы. При этом требования к ожидаемым образовательным результатам обучающихся по данной дисциплине не зависят от формы реализации образовательной программы.

№	Наименование раздела	Содержание раздела
1	Сеанс работы в Linux	Пользователи системы. Регистрация в системе. Одновременный доступ к системе. Простейшие команды. Выход из системы.
2	Терминал и командная строка	Терминал. Командная строка. Подсистема помощи. Ключи. Интерпретатор командной строки (shell).
3	Структура файловой системы	Организация файловой системы. Размещение компонентов системы: Стандарт FHS.
4	Работа с файловой системой	Текущий каталог. Домашний каталог. Информация о каталоге. Перемещение по дереву каталогов. Создание каталогов. Копирование и перемещение файлов. Файл и его имена: ссылки. Удаление файлов и каталогов.
5	Доступ процессов к файлам и каталогам	Процессы. Доступ к файлу и каталогу.
6	Права доступа. Особые биты атрибутов	Права доступа.
7	Работа с текстовыми данными	Ввод и вывод. Перенаправление ввода и вывода. Обработка данных в потоке. Примеры задач.
8	Возможности командной оболочки	Редактирование ввода. Генерация имён файлов. Окружение. Настройка командного интерпретатора.
9	Пользователи и безопасность	Управление базой данных пользователей и групп. Аутентификация и авторизация пользователей. Повышение привилегий в системе. Пакет sudo.
10	Использование	Лист контроля доступа (ACL). Примеры

	возможностей ACL	использования ACL
11	Работа с SSH. Туннелирование траффика	Подключение к системе по протоколу ssh. Генерация ключей ssh. Туннелирование траффика для графического интерфейса.
12	Установка ПО и сервисы	Установка ПО из пакетов (rpm). Использование менеджеров пакетов и репозиториев (yum, dnf). Обновление системы и ПО. Регистрация действий сервисов (rsyslog).
13	Резервное копирование	Стратегии резервного копирования. Управление файловыми системами (fdisk, parted, gparted). Утилиты резервного копирования (tar, dd, gzip, rsync). Управление периодическими заданиями (cron, at).
14	Использование LVM	Принцип работы LVM. Физические и логические тома, группы. Снапшоты.
15	Шифрование дисков	Принцип работы LUKS (технология). Создание зашифрованного диска. Монтирование зашифрованного диска.
16	Использование виртуальных систем	Виртуализация KVM (гипервизор). Установка среды виртуализации. Создание виртуальной машины с помощью GUI и консольного интерфейса.
17	Система инициализации systemd	Обзор системы systemd. Изучение юнитов системы. Запуск и остановка сервисов. Создание собственного сервиса.

6. Рекомендуемая тематика учебных занятий в форме контактной работы

Рекомендуемая тематика учебных занятий *лекционного* типа (предусматривающих преимущественную передачу учебной информации преподавателями):

№	Наименование раздела	Темы лекций
1	Сеанс работы в Linux	Лекция 1. Пользователи системы. Регистрация в системе. Одновременный доступ к системе. Лекция 2. Простейшие команды. Выход из системы.
2	Терминал и командная строка	Лекция 3. Терминал. Командная строка. Подсистема помощи. Лекция 4. Ключи. Интерпретатор командной строки (shell).
3	Структура файловой системы	Лекция 5. Организация файловой системы. Лекция 6. Размещение компонентов системы: Стандарт FHS.
4	Работа с файловой системой	Лекция 7. Текущий каталог. Домашний каталог. Информация о каталоге. Перемещение по дереву каталогов. Создание каталогов. Копирование и перемещение файлов. Лекция 8. Файл и его имена: ссылки. Удаление файлов и каталогов.
5	Доступ процессов к файлам и каталогам	Лекция 9. Процессы. Лекция 10. Доступ к файлу и каталогу.

6	Права доступа. Особые биты атрибутов	Лекция 11. Права доступа.
7	Работа с текстовыми данными	Лекция 12. Ввод и вывод. Перенаправление ввода и вывода. Лекция 13. Обработка данных в потоке. Примеры задач.
8	Возможности командной оболочки	Лекция 14. Редактирование ввода. Генерация имён файлов. Лекция 15. Окружение. Настройка командного интерпретатора.
9	Пользователи и безопасность	Лекция 16. Управление базой данных пользователей и групп. Аутентификация и авторизация пользователей. Лекция 17. Повышение привилегий в системе. Пакет sudo.
10	Использование возможностей ACL	Лекция 18. Лист контроля доступа (ACL). Лекция 19. Примеры использования ACL.
11	Работа с SSH. Туннелирование траффика	Лекция 20. Подключение к системе по протоколу ssh. Генерация ключей ssh. Лекция 21. Туннелирование траффика для графического интерфейса.
12	Установка ПО и сервисы	Лекция 22. Установка ПО из пакетов (rpm/yum). Использование менеджеров пакетов и репозиториев (yum, dnf). Лекция 23. Обновление системы и ПО. Регистрация действий сервисов (rsyslog).
13	Резервное копирование	Лекция 24. Стратегии резервного копирования. Управление файловыми системами (fdisk, parted, gparted). Утилиты резервного копирования (tar, dd, gzip, rsync). Лекция 25. Управление периодическими заданиями (cron, at).
14	Использование LVM	Лекция 26. Принцип работы LVM. Физические и логические тома, группы. Лекция 27. Снапшоты.
15	Шифрование дисков	Лекция 28. Принцип работы LUKS (технология). Лекция 29. Создание зашифрованного диска. Монтирование зашифрованного диска.
16	Использование виртуальных систем	Лекция 30. Виртуализация KVM (гипервизор). Установка среды виртуализации. Лекция 31. Создание виртуальной машины с помощью GUI и консольного интерфейса.
17	Система инициализации systemd	Лекция 32. Обзор системы systemd. Изучение юнитов системы. Запуск и остановка сервисов. Лекция 33. Создание собственного сервиса.

Рекомендуемая тематика *лабораторных* занятий:

1. Базовые терминальные команды в ОС Linux
2. Взаимодействие с процессами
3. Права доступа у файлов и каталогов
4. Расширенные терминальные команды. Фильтрация. Конвейер

5. Работа с дисками и разделами диска
6. Создание файловых систем
7. Монтирование файловых систем
8. RSYSLOG
9. Резервное копирование и восстановление
10. LVM
11. Создание и монтирование зашифрованного диска
12. Установка и первичная настройка гипервизора (KVM)
13. Система инициализации. Запуск и остановка сервисов

На лабораторных занятиях решаются задачи по теме занятия.

Требования к самостоятельной работе обучающихся

1. Работа с лекционным материалом, предусматривающая проработку конспекта лекций и учебной литературы, по всем темам из п. 6 настоящей рабочей программы.
2. Выполнение домашнего задания, предусматривающее решение задач, выполнение практических упражнений, выдаваемых на лабораторных занятиях, по всем темам из п. 6 настоящей рабочей программы.

Руководствуясь положениями статьи 47 и статьи 48 Федерального закона от 29 декабря 2012 г. N 273-ФЗ «Об образовании в Российской Федерации» научно-педагогические работники и иные лица, привлекаемые университетом к реализации данной образовательной программы, пользуются предоставленными академическими правами и свободами в части свободы преподавания, свободы от вмешательства в профессиональную деятельность; свободы выбора и использования педагогически обоснованных форм, средств, методов обучения и воспитания; права на творческую инициативу, разработку и применение авторских программ и методов обучения и воспитания в пределах реализуемой образовательной программы и отдельной дисциплины.

7. Методические рекомендации по видам занятий

Лекционные занятия.

В ходе лекционных занятий обучающимся рекомендуется выполнять следующие действия. Вести конспектирование учебного материала. Обращать внимание на категории, формулировки, раскрывающие содержание тех или иных явлений и процессов, научные выводы и практические рекомендации по их применению. Задавать преподавателю уточняющие вопросы с целью уяснения теоретических положений, разрешения спорных ситуаций.

Желательно оставить в рабочих конспектах поля, на которых во внеаудиторное время можно сделать пометки из рекомендованной литературы, дополняющие материал прослушанной лекции, а также подчеркивающие особую важность тех или иных теоретических положений.

Лабораторные занятия.

На лабораторных занятиях в зависимости от темы занятия выполняется поиск информации по решению проблем, практические упражнения, выработка индивидуальных или групповых решений, итоговое обсуждение с обменом знаниями, участие в круглых столах, разбор конкретных ситуаций, командная работа, представление портфолио и т.п.

Самостоятельная работа.

Самостоятельная работа осуществляется в виде изучения литературы, эмпирических данных по публикациям и конкретных ситуаций из практики, подготовке лабораторных работ, работа с лекционным материалом, самостоятельное изучение отдельных тем дисциплины; поиск и обзор литературы и электронных источников; чтение и изучение учебника и учебных пособий.

8. Фонд оценочных средств

8.1. Перечень компетенций с указанием этапов их формирования в процессе освоения образовательной программы в рамках учебной дисциплины

Основными этапами формирования указанных компетенций при изучении обучающимися дисциплины являются последовательное изучение содержательно связанных между собой тем учебных занятий. Изучение каждой темы предполагает овладение обучающимися необходимыми компетенциями. Результат аттестации обучающихся на различных этапах формирования компетенций показывает уровень освоения компетенций.

Контролируемые разделы (темы) дисциплины	Индекс контроли-руемой компетенции (или её части)	Оценочные средства по этапам формирования компетенций
		текущий контроль по дисциплине
1. Сеанс работы в Linux	ОПК-12	
2. Терминал и командная строка	ОПК-12	лабораторная работа
3. Структура файловой системы	ОПК-12	лабораторная работа
4. Работа с файловой системой	ОПК-12	лабораторная работа
5. Доступ процессов к файлам и каталогам	ОПК-12	лабораторная работа
6. Права доступа. Особые биты атрибутов	ОПК-12	лабораторная работа
7. Работа с текстовыми данными	ОПК-12	лабораторная работа
8. Возможности командной оболочки	ОПК-12	лабораторная работа
9. Пользователи и безопасность	ОПК-12	лабораторная работа
10. Использование возможностей ACL	ОПК-12	
11. Работа с SSH. Туннелирование траффика	ОПК-12	лабораторная работа
12. Установка ПО и сервисы	ОПК-12	
13. Резервное копирование	ОПК-12	лабораторная работа
14. Использование LVM	ОПК-12	лабораторная работа
15. Шифрование дисков	ОПК-12	лабораторная работа
16. Использование виртуальных систем	ОПК-12	

Контролируемые разделы (темы) дисциплины	Индекс контроли-руемой компетенции (или её части)	Оценочные средства по этапам формирования компетенций
		текущий контроль по дисциплине
17. Система инициализации systemd	ОПК-12	лабораторная работа

8.2. Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений и навыков и (или) опыта деятельности процессе текущего контроля

Примеры лабораторной работы:

По Теме 2. Терминал и командная строка

1. Создайте каталог в текущей директории со своей фамилией.
2. Скопируйте в созданный каталог - каталог /sbin.
3. Используя команду ls, создайте файл с содержимым каталога.
4. Используя программы tar, gzip создайте архив с каталогом.
5. Создайте ссылку на полученный архив со своим именем.
6. Удалите каталог.
7. Используя программы tar, gzip, распакуйте файл по ссылке с вашем именем.
8. Используя команду ls, создайте файл с содержимым каталога.
9. Используя команду diff, сравните списки файлов.

По Теме 5. Доступ процессов к файлам и каталогам

1. Создайте три каталога в домашнем каталоге.
2. Какие права доступа по умолчанию установлены для этих каталогов?
3. Создайте по одному файлу внутри каждого каталога.
4. Установите права для первого каталога «drwxrwxrwx», для второго - «d---------», для третьего - «drwx------».
5. Какие права доступа по умолчанию установлены для файлов внутри каталогов?
6. Измените содержимое файлов, записав туда информацию о трех различных пользователях системы.
7. Сделайте один из каталогов «разделяемым».
8. Установите для любого файла атрибут SetUID.

8.3. Перечень вопросов и заданий для промежуточной аттестации по дисциплине

Вопросы для промежуточного контроля (зачета)

1. Терминал. Его свойства. Требования к терминалу.
2. Ключи. Типы ключей.
3. Стандарт FHS. Дерево каталогов.
4. Путь. Виды путей.
5. Файл и его имена. Ссылки.
6. Процесс. Запуск дочерних. Фоновые и активные.
7. Сигналы.

8. Доступы к файлу. Доступы к каталогам.
9. Сценарии.
10. Права доступа у пользователя. UID. GID.
11. Разделяемые каталоги. Подмена идентификатора.
12. Дескрипторы. Перенаправление ввода и вывода. Конвейер.
13. Окружение. Переменные окружения.

Вопросы для промежуточного контроля (экзамена)

1. Пользователи и безопасность.
2. Использование возможностей ACL.
3. Работа с SSH. Туннелирование траффика.
4. Установка ПО и сервисы.
5. Резервное копирование.
6. Использование LVM.
7. Шифрование дисков.
8. Использование виртуальных систем.
9. Система инициализации systemd.

8.4. Планируемые уровни сформированности компетенций обучающихся и критерии оценивания

Уровни	Содержательное описание уровня	Основные признаки выделения уровня (этапы формирования компетенции, критерии оценки сформированности)	Пятибалльная шкала (академическая) оценка	Двухбалльная шакала, зачет	БРС, % освоения (рейтинговая оценка)
Повышенный	Творческая деятельность	*Включает нижестоящий уровень.* Умение самостоятельно принимать решение, решать проблему/задачу теоретического и прикладного характера на основе изученных методов, приемов, технологий	отлично	зачтено	86-100
Базовый	Применение знаний и умений в более широких контекстах учебной и профессиональной деятельности, нежели по образцу с большей	*Включает нижестоящий уровень.* Способность собирать, систематизировать, анализировать и грамотно использовать информацию из самостоятельно найденных теоретических источников и иллюстрировать ими теоретические	хорошо		71-85

	степени самостоятельности и инициативы	положения или обосновывать практику применения			
Удовлетворительный (достаточный)	Репродуктивная деятельность	Изложение в пределах задач курса теоретически и практически контролируемого материала	удовлетворительно		55-70
Недостаточный	Отсутствие признаков удовлетворительного уровня		неудовлетворительно	не зачтено	Менее 55

9. Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины

Основная литература

1. Петцке, К. LINUX. От понимания к применению [Электронный ресурс] / К. Петцке; Пер. с нем. - Москва: ДМК, 2008. - 576 с.: ил. - ISBN 5-93700-004-8. - Текст: электронный. - URL: https://znanium.com/catalog/product/407336 (дата обращения: 03.03.2022). – Режим доступа: по подписке.
2. Зубков, С. В. Linux. Русские версии [Электронный ресурс] / С. В. Зубков. - Москва: ДМК Пресс, 2007. - 347 с.: ил. - ISBN 5-94074-013-8. - Текст: электронный. - URL: https://znanium.com/catalog/product/407420 (дата обращения: 03.03.2022). – Режим доступа: по подписке.

Дополнительная литература

1. Аленичев, Д. ALT Linux изнутри [Электронный ресурс] / Д. Аленичев, А. Боковой, А. Бояршинов и др. - Москва: ALT Linux; ДМК пресс, 2009. - 416 с.: ил. - (В серии: «Библиотека ALT Linux»). - ISBN 5-9706-0029-6. - Текст: электронный. - URL: https://znanium.com/catalog/product/407225 (дата обращения: 03.03.2022). – Режим доступа: по подписке.
2. Войтов, Н. М. Основы работы с Linux [Электронный ресурс]: учебный курс / Н. М. Войтов. - Москва: ДМК Пресс, 2010. - 216 с.: ил. - ISBN 978-5-94074-148-0. - Текст: электронный. - URL: https://znanium.com/catalog/product/407269 (дата обращения: 03.03.2022). – Режим доступа: по подписке.

10. Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины (модуля)

- НЭБ Национальная электронная библиотека, диссертации и прочие издания
- eLIBRARY.RU Научная электронная библиотека, книги, статьи, тезисы докладов конференций
- ЭБС Лань книги, журналы
- ЭБС Консультант студента
- ПРОСПЕКТ ЭБС
- ЭБС ZNANIUM.COM

- РГБ Информационное обслуживание по МБА
- БЕН РАН
- Электронно-библиотечная система (ЭБС) Кантиана

11. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине

Программное обеспечение обучения включает в себя:

- система электронного образовательного контента БФУ им. И. Канта – www.lms-3.kantiana.ru, обеспечивающую разработку и комплексное использование электронных образовательных ресурсов;
- серверное программное обеспечение, необходимое для функционирования сервера и связи с системой электронного обучения через Интернет;
- корпоративная платформа Microsoft Teams;
- ОС Microsoft Windows 10;
- Гипервизор VMware Workstation или VirtualBox;
- ОС Linux, установленная на гипервизоре или самостоятельно.

12. Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине

Для проведения занятий лекционного типа, лабораторных занятий используются специальные помещения (учебные аудитории), оборудованные техническими средствами обучения – мультимедийной проекционной техникой. Для проведения занятий лекционного типа используются наборы демонстрационного оборудования.

Для проведения лабораторных работ используются специальные помещения (учебные аудитории), оснащенные специализированным лабораторным оборудованием: персональными компьютерами с возможностью выхода в интернет и с установленным программным обеспечением, заявленным в п. 11.

Для проведения групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации используются специальные помещения (учебные аудитории), оборудованные специализированной мебелью (для обучающихся), меловой/маркерной доской.

Для организации самостоятельной работы обучающимся предоставляются помещения, оснащенные компьютерной техникой с возможностью подключения к сети «Интернет» и обеспечением доступа в электронную информационно-образовательную среду университета.

Для обучения инвалидов и лиц с ограниченными возможностями здоровья университетом могут быть представлены специализированные средства обучения, в том числе технические средства коллективного и индивидуального пользования.

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
федеральное государственное автономное образовательное учреждение высшего образования «Балтийский федеральный университет имени Иммануила Канта»
Институт физико-математических наук и информационных технологий

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

«Компьютерные сети»

Шифр: 10.05.01
Специальность: «Компьютерная безопасность»
Специализация: «Математические методы защиты информации»
Квалификация (степень) выпускника: специалист по защите информации

Калининград
2022

Лист согласования

Составитель: Мищук Богдан Ростиславович, к.ф.-м.н., доцент

Рабочая программа утверждена на заседании учебно-методического совета института физико-математических наук и информационных технологий

Протокол № 01/22 от «01» февраля 2022 г.

Председатель учебно-методического совета института физико-математических наук и информационных технологий

Первый заместитель директора ИФМНиИТ, к. ф.-м. н., доцент — Шпилевой А. А

Ведущий менеджер — Е.П.Ставицкая

Содержание

1.Наименование дисциплины: «Компьютерные сети».

Цель дисциплины: целью освоения дисциплины «Компьютерные сети» освоение базовых знаний по вопросам построения компьютерных сетей различной модификации.

2. Перечень планируемых результатов обучения по дисциплине, соотнесенных с планируемыми результатами освоения образовательной программы

Код компетенции	Результаты освоения образовательной программы (ИДК)	Результаты обучения по дисциплине
ОПК-15. Способен администрировать компьютерные сети и контролировать корректность их функционирования;	ОПК-15.1. Знает устройство, порядок администрирования и контроля функционирования компьютерных сетей. ОПК-15.2. Умеет осуществлять администрирование и контроль корректности функционирования компьютерных сетей. ОПК-15.3. Владеет навыками администрирования и контроля функционирования компьютерных сетей	• ***Знать***: базовые понятия и терминологию курса, основные характеристики сред передачи данных в компьютерных сетях; способы коммутаций компьютерных сетей; механизм реализации виртуальной памяти; принципы построения и защита от сбоев и несанкционированного доступа; • ***Уметь*** объединять компьютеры в сеть, включать и исключать узлы в сети; управлять топологией и конфигурацией сети; • ***Владеть*** **навыками** вычислениями маски сети, маски подсетей; вычислением диапазона адресов компьютеров, их количество;

3. Место дисциплины в структуре образовательной программы

Дисциплина «Компьютерные сети» представляет собой дисциплину обязательной части блока дисциплин подготовки обучающихся.

4. Виды учебной работы по дисциплине.

Виды учебной работы по дисциплине зафиксированы учебным планом основной профессиональной образовательной программы по указанному направлению и профилю, выражаются в академических часах. Часы контактной работы и самостоятельной работы обчающегося и часы, отводимые на процедуры контроля, могут различаться в учебных планах ОПОП по формам обучения. Объем контактной работы включает часы контактной аудиторной работы (лекции/практические занятия/ лабораторные работы), контактной внеаудиторной работы (контроль самостоятельной работы), часы контактной работы в период аттестации. Контактная работа, в том числе может проводиться посредством

электронной информационно-образовательной среды университета с использованием ресурсов сети Интернет и дистанционных технологий

5. Содержание дисциплины, структурированное по темам (разделам)

Исходя из рамок, установленных учебным планом по трудоемкости и видам учебной работы по дисциплине, преподаватель самостоятельно выбирает тематику занятий по формам и количеству часов проведения контактной работы: лекции и иные учебные занятия, предусматривающие преимущественную передачу учебной информации преподавателем и (или) занятия семинарского типа (семинары, практические занятия, практикумы, лабораторные работы, коллоквиумы и иные аналогичные занятия), и (или) групповые консультации, и (или) индивидуальную работу обучающихся с преподавателем, в том числе индивидуальные консультации (по курсовым работам/проектам – при наличии курсовой работы/проекта по данной дисциплине в учебном плане). Рекомендуемая тематика занятий максимально полно реализуется в контактной работе с обучающимися очной формы обучения. В случае реализации образовательной программы в заочной / очно-заочной форме трудоемкость дисциплины сохраняется, однако объем учебного материала в значительной части осваивается обучающимися в форме самостоятельной работы. При этом требования к ожидаемым образовательным результатам обучающихся по данной дисциплине не зависят от формы реализации образовательной программы.

№	Наименование раздела	Содержание раздела
1	Эволюция и основы компьютерных сетей. Требования, предъявляемые при разработке и функционировании сети.	Эволюция развития компьютерных сетей. Первые компьютерные сети. Появление БИС. Понятие сетевой технологии. Классификация сетей по масштабу. Классификация сетей по наличию сервера. Достоинства и недостатки одно ранговых сетей. Достоинства и недостатки сетей с выделенным сервером. Определение информационных потоков. Определение маршрутов. Оповещение сети о найденных маршрутах. Мультиплексирование и демультиплексирование. Основные механизмы коммутации. Схема коммутации каналов. Достоинства и недостатки. Схема коммутации пакетов. Достоинства и недостатки. Методы QoS.
2	Модель взаимодействия открытых систем OSI. Стандартные стеки протоколов. Стек протоколов TCP/IP. Маршрутизация. Разработка инфраструктуры корпоративной сети.	Управление процессами учета ресурсов ИС и вопросы обеспечения информационной безопасности. Основные задачи учета, наиболее типичные виды угроз безопасности, средства, мероприятия и нормы защиты безопасности. Организация удаленного доступа к сети предприятия на основе безопасной VPN-технологии, типы частных виртуальных сетей и технология IPSec. Firewall аппаратный и программный его настройка администрирование. Администрирование корпоративных антивирусных программ. Общая характеристика модели OSI. Уровни модели OSI. Прохождение сообщения по уровням модели. Физический уровень и его функции. Канальный уровень и его функции. Связь канального уровня с топологией сети. Сетевой уровень и его функции. Проблемы маршрутизации. Виды протоколов сетевого уровня. Транспортный протокол и его функции. Транспортная подсистема. Сеансовый уровень и его функции. Представительный уровень и его функции. Прикладной уровень и его функции. Сетезависимые и сетенезависимые уровни. Спецификация IEEE 802.

		Стандартизация стека протоколов TCP/IP. Уровни TCP/IP. Физический и канальный уровень. Уровень межсетевого взаимодействия. Основной уровень. Прикладной уровень. Некоторые протоколы прикладного уровня: FTP, telnet, SNMP. Типы адресов в сети TCP/IP. Локальные адреса. IP-адрес. Символьный идентификатор. Номер сети и номер узла. Маска подсети. Протоколы разрешения адресов. Маршрутизация в IP сетях. Протокол ARP. Протокол DNS. Доменные имена. Протокол DHCP. Протокол IP. Алгоритмы маршрутизации. Протоколы TCP и UDP. .Протоколы vIP6, их характеристики, необходимость реализации. Разработка инфраструктуры корпоративной сети.
3	Беспроводные сети и стандарты. Вызов удалённых процедур. Динамическое связывание. Нити и RPC. Виртуализация, кластеры.	Стандарт IEEE 802.11. Топологии беспроводных сетей. Зона доступа. Множественный доступ с предотвращением коллизий. Спецификация 802.11a. Спецификация 802.11b. Промежуточные спецификации стандарта. Спецификация 802.11g. Спецификация 802.11n. Типы сервисов беспроводных ЛВС. Сервисы распределения. Станционные сервисы. Архитектура сетевой Windows Server. Состав и основные компоненты сетевой операционной системы Windows Server. Сетевая операционная система Unix и её потомки, их свойства Вызов удалённых процедур: асимметричность, синхронность. Динамическое связывание. Семантика RPC в случае отказов. Нити и RPC. Распределенные файловые системы. Виртуализация. Кластеры

6. Рекомендуемая тематика учебных занятий в форме контактной работы

Рекомендуемая тематика учебных занятий *лекционного* типа (предусматривающих преимущественную передачу учебной информации преподавателями):

№	Наименование раздела	Темы лекций
1	Эволюция и основы компьютерных сетей. Требования, предъявляемые при разработке и функционировании сети.	Лекция 1. Базовые архитектуры и топологии сетей. Лекция 2. Требования, предъявляемые при разработке и функционировании сети и базовые параметры и характеристики сетей..

2	Модель взаимодействия открытых систем OSI. Стандартные стеки протоколов. Стек протоколов TCP/IP. Маршрутизация. Разработка инфраструктуры корпоративной сети.	Лекция 3. Модель OSI. Лекция 4. Стек протоколов TCP/IP . Лекция 5-6. Протоколы IP v.4,6. Лекция 7. Протоколы ARP, SNMP, DHCP. Лекция 8-9. Маршрутизация. Протоколы маршрутизации Лекция 10. Протоколы транспортного уровня Лекция 11. Прикладные протоколы
3	Беспроводные сети и стандарты. Вызов удалённых процедур. Динамическое связывание. Нити и RPC. Виртуализация, кластеры.	Лекция 12 Стандарт IEEE 802.11. Топологии беспроводных сетей. Bluetooth. Лекция 13. Спецификация 802.11. Лекция 14. Вызов удалённых процедур: асимметричность, синхронность. Динамическое связывание. Лекция 15. Распределенные файловые системы. Виртуализация. Кластеры.

Рекомендуемая тематика лабораторных занятий:

№ п/п	**Наименование темы**	**Содержание темы**
1	Эволюция и основы компьютерных сетей. Требования, предъявляемые при разработке и функционировании сети.	Локальные вычислительные сети. DHCP-сервер: установка, настройка и управление. DNS-сервер: установка, настройка и управление. Аппаратное обеспечение компьютерных сетей. Изучение пакета NetEmul, создание проектов согласно варианту задания.
2	Модель взаимодействия открытых систем OSI. Стандартные стеки протоколов. Стек протоколов TCP/IP. Маршрутизация. Разработка инфраструктуры корпоративной сети.	Маршрутизация в разных IP-подсетях. Сетевые протоколы. FTP-сервер: установка, настройка и управление. Web-сервер: установка, настройка и управление. Разработка и реализация корпоративной компьютерной сети.
3	Беспроводные сети и стандарты. Вызов удалённых процедур. Динамическое связывание. Нити и	Беспроводные сети Wi-Fi. Технологии защиты компьютерных сетей. Антивирусное ПО. Инсталляция, настройка. Сетевой анализатор Network Monitor и сети VPN. Прямое соединение компьютеров.

	RPC. Виртуализация, кластеры.	

Требования к самостоятельной работе обучающихся

1. Работа с лекционным материалом, предусматривающая проработку конспекта лекций и учебной литературы, по всем темам из п. 6 настоящей рабочей программы.
2. Выполнение домашнего задания, предусматривающего решение задач, выполнение упражнений, выдаваемых на практических занятиях, по всем темам из п. 6 настоящей рабочей программы.

Руководствуясь положениями статьи 47 и статьи 48 Федерального закона от 29 декабря 2012 г. N 273-ФЗ «Об образовании в Российской Федерации» научно-педагогические работники и иные лица, привлекаемые университетом к реализации данной образовательной программы, пользуются предоставленными академическими правами и свободами в части свободы преподавания, свободы от вмешательства в профессиональную деятельность; свободы выбора и использования педагогически обоснованных форм, средств, методов обучения и воспитания; права на творческую инициативу, разработку и применение авторских программ и методов обучения и воспитания в пределах реализуемой образовательной программы и отдельной дисциплины.

Исходя из рамок, установленных учебным планом по трудоемкости и видам учебной работы по дисциплине, преподаватель самостоятельно выбирает тематику занятий по формам и количеству часов проведения контактной работы: лекции и иные учебные занятия, предусматривающие преимущественную передачу учебной информации преподавателем и (или) занятия семинарского типа (семинары, практические занятия, практикумы, лабораторные работы, коллоквиумы и иные аналогичные занятия), и (или) групповые консультации, и (или) индивидуальную работу обучающихся с преподавателем, в том числе индивидуальные консультации (по курсовым работам/проектам – при наличии курсовой работы/проекта по данной дисциплине в учебном плане).

Рекомендуемая тематика занятий максимально полно реализуется в контактной работе с обучающимися очной формы обучения. В случае реализации образовательной программы в заочной / очно-заочной форме трудоемкость дисциплины сохраняется, однако объем учебного материала в значительной части осваивается обучающимися в форме самостоятельной работы. При этом требования к ожидаемым образовательным результатам обучающихся по данной дисциплине не зависят от формы реализации образовательной программы.

7. Методические рекомендации по видам занятий

Лекционные занятия.

В ходе лекционных занятий обучающимся рекомендуется выполнять следующие действия. Вести конспектирование учебного материала. Обращать внимание на категории, формулировки, раскрывающие содержание тех или иных явлений и процессов, научные выводы и практические рекомендации по их применению. Задавать преподавателю уточняющие вопросы с целью уяснения теоретических положений, разрешения спорных ситуаций.

Желательно оставить в рабочих конспектах поля, на которых во внеаудиторное время можно сделать пометки из рекомендованной литературы, дополняющие материал

прослушанной лекции, а также подчеркивающие особую важность тех или иных теоретических положений.

Лабораторные занятия.

На лабораторных занятиях в зависимости от темы занятия выполняется поиск информации по решению проблем, практические упражнения, контрольные работы, выработка индивидуальных или групповых решений, итоговое обсуждение с обменом знаниями, участие в круглых столах, разбор конкретных ситуаций, командная работа, представление портфолио и т.п.

Самостоятельная работа.

Самостоятельная работа осуществляется в виде изучения литературы, эмпирических данных по публикациям и конкретных ситуаций из практики, подготовке индивидуальных работ, работа с лекционным материалом, самостоятельное изучение отдельных тем дисциплины; поиск и обзор литературы и электронных источников; чтение и изучение учебника и учебных пособий.

8. Фонд оценочных средств

8.1. Перечень компетенций с указанием этапов их формирования в процессе освоения образовательной программы в рамках учебной дисциплины

Основными этапами формирования указанных компетенций при изучении обучающимися дисциплины являются последовательное изучение содержательно связанных между собой тем учебных занятий. Изучение каждой темы предполагает овладение обучающимися необходимыми компетенциями. Результат аттестации обучающихся на различных этапах формирования компетенций показывает уровень освоения компетенций.

Контролируемые разделы (темы) дисциплины	Индекс контроли-руемой компетенции (или её части)	Оценочные средства по этапам формирования компетенций
		текущий контроль по дисциплине
Эволюция и основы компьютерных сетей. Требования, предъявляемые при разработке и функционировании сети.	ОПК-12	Опрос, выполнение лабораторных работ.
Модель взаимодействия открытых систем OSI. Стандартные стеки протоколов. Стек протоколов TCP/IP. Маршрутизация. Разработка инфраструктуры корпоративной сети.	ОПК-12	Опрос, выполнение лабораторных работ.
Беспроводные сети и стандарты. Вызов удалённых процедур. Динамическое связывание. Нити и RPC. Виртуализация, кластеры.	ОПК-12	Опрос, выполнение лабораторных работ.

8.2. Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений и навыков и (или) опыта деятельности процессе текущего контроля

Примеры вопросов для устного опроса:

Тема 1. Эволюция и основы компьютерных сетей. Требования, предъявляемые при разработке и функционировании сети.

1. Эволюция развития компьютерных сетей. Первые компьютерные сети.
2. Появление БИС. Понятие сетевой технологии.
3. Классификация сетей по масштабу. Классификация сетей по наличию сервера. Достоинства и недостатки одно ранговых сетей. Достоинства и недостатки сетей с выделенным сервером.
4. Определение информационных потоков. Определение маршрутов. Оповещение сети о найденных маршрутах.
5. Мультиплексирование и демультиплексирование. Основные механизмы коммутации.
6. Схема коммутации каналов. Достоинства и недостатки.
7. Схема коммутации пакетов. Достоинства и недостатки. Методы QoS.
8. Маршрутизация и мониторинг компьютерной сети.
9. Архитектура сетевых клиентов DOS. Архитектура сетевой подсистемы Windows.
10. Взаимодействие систем многоуровневой архитектуры.
11. Неэкранированная витая пара. Экранированная витая пара. Коаксиальный кабель.
12. Оптоволоконный кабель. Беспроводные технологии. Беспроводная связь.
13. Сетевой адаптер. Трансивер и конвертор. Повторители и усилители.
14. Концентраторы. Мост. Маршрутизатор. Шлюз.

Типовая лабораторная работа:

Тема: «IP адресация в компьютерных сетях»

Задание 1. Определить, находятся ли два узла A и B в одной подсети или в разных подсетях.

1. IP-адрес компьютера A: 94.235.16.59;
   IP-адрес компьютера B: 94.235.23.240;
   Маска подсети: 255.255.240.0.
2. IP-адрес компьютера A: 131.189.15.6;
   IP-адрес компьютера B: 131.173.216.56;
   Маска подсети: 255.248.0.0.
3. IP-адрес компьютера A: 215.125.159.36;
   IP-адрес компьютера B: 215.125.153.56;
   Маска подсети: 255.255.224.0.

Задание 2. Определить количество и диапазон адресов узлов в подсети, если известны номер подсети и маска подсети.
Номер подсети: 192.168.1.0, маска подсети: 255.255.255.0.
Номер подсети: 110.56.0.0, маска подсети: 255.248.0.0.
Номер подсети: 88.217.0.0, маска подсети: 255.255.128.0.

Задание 3. Определить маску подсети, соответствующую указанному диапазону IP-адресов.

1. 119.38.0.1 – 119.38.255.254.
2. 75.96.0.1 – 75.103.255.254.
3. 48.192.0.1 – 48.255.255.254.

Задание 4. Организации выделена сеть класса B: 185.210.0.0/16. Определить маски и количество возможных адресов новых подсетей в каждом из следующих вариантов разделения на подсети:

1. Число подсетей – 256, число узлов – не менее 250.
2. Число подсетей – 16, число узлов – не менее 4000.
3. Число подсетей – 5, число узлов – не менее 4000. В этом варианте укажите не менее двух способов решения.

8.3. Перечень вопросов и заданий для промежуточной аттестации по дисциплине

Вопросы для промежуточного контроля (зачет)

1. Клиент-серверные приложения, логическая структура сети, некоторые типы серверов. Удаленное управление.
2. Распределенные вычисления. Координация деятельности.
3. Архитектура сетевой системы, модель ISO/OSI.
4. Монолитная архитектура. Многоуровневая архитектура.
5. Архитектура сетевых клиентов DOS. Архитектура сетевой подсистемы Windows.
6. Драйверы NIC, сетевые протоколы и сетевые сервисы. Привязка.
7. Взаимодействие систем многоуровневой архитектуры.
8. Передача и прием данных.
9. Особенности модели ISO/OSI.
10. Назначение и функции физического уровня. Назначение и функции канального уровня. Назначение и функции сетевого уровня. Назначение и функции транспортного уровня.
11. Кадры, MAC-адреса.
12. Логические адреса. Маршрутизация, таблица маршрутизации. Необходимость разрешения адресов.
13. Мультиплексирование потоков данных. Надежная доставка.
14. Назначение и функции уровня сессии. Назначение и функции уровня представления. Прикладной уровень.
15. Проект IEEE 802.Цель проекта. Разделы проекта.
16. Структура и характеристики кабелей различных типов. Примеры спецификаций, использующих данные кабели. Структурированная кабельная система.
17. Архитектура, терминология, стандарты. Передача данных на физическом уровне.
18. Методы кодирования. Аналоговая модуляция. Цифровое кодирование (методы NRZ, NRZi, MLT-3, RZ, 2B1Q, Манчестерский код). Логическое кодирование.
19. Методы доступа ALOHA, CSMA/CD, CSMA/CA, CDMA, маркерный доступ.
20. Технология Ethernet. Численные характеристики. Параметры CSMA/CD. Спецификации физического уровня. Формат кадра Ethernet.
21. Технология Token Ring. Численные характеристики. Параметры маркерного доступа. Формат кадра. Технология Fast Ethernet. Численные характеристики.
22. Параметры CSMA/CD. Спецификации физического уровня.

23. Особенности и численные характеристики. Спецификации физического уровня. Технология FDDI. Особенности и численные характеристики. Сетевой адаптер (NIC).
24. Классификации NIC. Параметры NIC. Структура MAC-адреса.
25. Классификация устройств с несколькими подключениями.
26. Повторитель. Мост. Маршрутизатор. Шлюз.
27. Обзор архитектуры TCP/IP. Организационные структуры Интернет. Архитектура TCP/IP. Уровень доступа к сети.
28. Назначение и функции межсетевого уровня и протокола IP.Назначение и функции уровня хост-хост и протоколов UDP и TCP.
29. Прикладной уровень. Назначение некоторых протоколов прикладного уровня: FTP, TELNET, SMTP, DNS, NFS, SNMP.Межсетевой уровень архитектуры TCP/IP и протокол IP. Адресация IP.
30. Формат IP-адреса. Классы IP-адресов. Специальные адреса. Частные адреса. Маска подсети. Подсети и надсети. Деление сети на несколько подсетей. Маршрутизация IP.
31. Таблица маршрутизации IP. Алгоритм выбора маршрута. Автоматически генерируемые маршруты.
32. Действия источника, маршрутизатора и приемника при обработке IP-пакета. Протокол ARP. Назначение и алгоритм работы протокола ARP. Динамическая маршрутизация.
33. Понятия динамической маршрутизации. Автономные системы, классы протоколов маршрутизации. Дистанционно-векторные протоколы. Протоколы состояния канала связи.
34. Назначение полей IP-пакета. Фрагментация IP-пакетов. Протокол RARP. Протокол ICMP.
35. Уровень хост-хост архитектуры TCP/IP и протоколы UDP и TCP. Мультиплексирование и механизм портов. Формат UDP-датаграммы. Свойства протокола TCP. Логическое соединение. Механизм окон TCP. Формат TCP-сегмента.
36. Типы сокетов. Коммуникационные домены.
37. Взаимодействие процессов с установлением соединения. Domain Name System (DNS).
38. Структура доменных имен. Авторизованные серверы и делегирование ответственности. Понятия сервера и ресолвера DNS, зоны, записи ресурса.
39. Алгоритм разрешения имен. Прямое и обратное разрешение имен. Формат записи ресурса. Типы записей SOA, NS, A, CNAME, PTR, MX, SRV.
40. Реализации сервера DNS для UNIX и Windows.
41. Понятия область, исключаемый диапазон, пул адресов, аренда, резервирование. Параметры, настраиваемые на DHCP-сервере. Получение и продление лицензии DHCP-клиентом.
42. Компоненты доставки почты. Конфигурация sendmail. Типовые случаи настройки почтового сервера. Проблема сетевой безопасности и терминология. Механизмы безопасности.
43. Сервисы безопасности: неотрекаемость, целостность, конфиденциальность, аутентификация, защита от повторений, контроль доступа. IPSec. VPN.
44. Фильтрация пакетов на примере iptables. Правила, цепочки правил, таблицы. Условия отбора пакетов, действия над пакетами. Трансляция сетевых адресов.

8.4. Планируемые уровни сформированности компетенций обучающихся и критерии оценивания

Уровни	Содержательное описание уровня	Основные признаки выделения уровня (этапы формирования компетенции, критерии оценки сформированности)	Пятибалльная шкала (академическая) оценка	Двухбалльная шакала, зачет	БРС, % освоения (рейтинговая оценка)
Повышенный	Творческая деятельность	*Включает нижестоящий уровень.* Умение самостоятельно принимать решение, решать проблему/задачу теоретического и прикладного характера на основе изученных методов, приемов, технологий	отлично	зачтено	86-100
Базовый	Применение знаний и умений в более широких контекстах учебной и профессиональной деятельности, нежели по образцу с большей степени самостоятельности и инициативы	*Включает нижестоящий уровень.* Способность собирать, систематизировать, анализировать и грамотно использовать информацию из самостоятельно найденных теоретических источников и иллюстрировать ими теоретические положения или обосновывать практику применения	хорошо		71-85
Удовлетворительный (достаточный)	Репродуктивная деятельность	Изложение в пределах задач курса теоретически и практически контролируемого материала	удовлетворительно		55-70
Недостаточный	Отсутствие признаков удовлетворительного уровня		неудовлетворительно	не зачтено	Менее 55

9. Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины.

Основная литература

1. Ибе, О. Компьютерные сети и службы удаленного доступа [Электронный ресурс] / О. Ибе; Пер. с англ. - Москва : ДМК Пресс, 2007. - 336 с.: ил. - ISBN 5-94074-080-4. - Текст : электронный. - URL: https://znanium.com/catalog/product/407717 (дата обращения: 23.03.2022). – Режим доступа: по подписке.
2. Широков, А. И. Операционные системы и среды: основные понятия теории : учебник / А. И. Широков, Ф. Г. Кирдяшов, С. Э. Мурадханов ; под ред. Е. А. Калашникова, Л. П. Рябова. - Москва : Изд. Дом НИТУ «МИСиС», 2018. - 192 с. - ISBN 978-5-906953-49-0. - Текст : электронный. - URL: https://znanium.com/catalog/product/1232238 (дата обращения: 23.03.2022). – Режим доступа: по подписке.

Дополнительная литература

1. Топорков, С. С. Компьютерные сети для продвинутых пользователей [Электронный ресурс] / С. С. Топорков. - Москва : ДМК Пресс, 2009. - 192 с. : ил. - (Серия «С компьютером на ты!»). - ISBN 5-94074-093-6. - Текст : электронный. - URL: https://znanium.com/catalog/product/408222 (дата обращения: 23.03.2022). – Режим доступа: по подписке.
2. Шелухин, О. И. Обнаружение вторжений в компьютерные сети (сетевые аномалии): Учебное пособие для вузов / О.И. Шелухин, Д.Ж. Сакалема, А.С. Филинова. - Москва : Гор. линия-Телеком, 2013. - 220 с.: ил.; . ISBN 978-5-9912-0323-4, 500 экз. - Текст : электронный. - URL: https://znanium.com/catalog/product/421968 (дата обращения: 23.03.2022). – Режим доступа: по подписке.

10. Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины (модуля).

- НЭБ Национальная электронная библиотека, диссертации и прочие издания
- eLIBRARY.RU Научная электронная библиотека, книги, статьи, тезисы докладов конференций
- Гребенников Электронная библиотека ИД журналы
- ЭБС Лань книги, журналы
- ЭБС Консультант студента
- ПРОСПЕКТ ЭБС
- ЭБС ZNANIUM.COM
- РГБ Информационное обслуживание по МБА
- БЕН РАН
- Электронно-библиотечная система (ЭБС) Кантитана (https://elib.kantiana.ru/)

11. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине.

Программное обеспечение обучения включает в себя:

- система электронного образовательного контента БФУ им. И. Канта – www.lms-3.kantiana.ru, обеспечивающую разработку и комплексное использование электронных образовательных ресурсов;
- серверное программное обеспечение, необходимое для функционирования сервера и связи с системой электронного обучения через Интернет;
- корпоративная платформа Microsoft Teams;
- установленное на рабочих местах обучающихся ПО: Microsoft Windows 10, Microsoft Office Standart 2010, антивирусное программное обеспечение Kaspersky Endpoint Security.
- специализированное ПО: NetEmul, VirtualBox.

12. Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине.

Для проведения занятий лекционного типа, практических и семинарских занятий используются специальные помещения (учебные аудитории), оборудованные техническими средствами обучения – мультимедийной проекционной техникой. Для проведения занятий лекционного типа используются наборы демонстрационного оборудования.

Для проведения лабораторных работ, (практических занятий – при необходимости) используются специальные помещения (учебные аудитории), оснащенные специализированным лабораторным оборудованием: персональными компьютерами с возможностью выхода в интернет и с установленным программным обеспечением, заявленным в п.11.

Для проведения групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации используются специальные помещения (учебные аудитории), оборудованные специализированной мебелью (для обучающихся), меловой / маркерной доской.

Для организации самостоятельной работы обучающимся предоставляются помещения, оснащенные компьютерной техникой с возможностью подключения к сети «Интернет» и обеспечением доступа в электронную информационно-образовательную среду университета.

Для обучения инвалидов и лиц с ограниченными возможностями здоровья университетом могут быть представлены специализированные средства обучения, в том числе технические средства коллективного и индивидуального пользования.

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
федеральное государственное автономное образовательное учреждение высшего образования «Балтийский федеральный университет имени Иммануила Канта»
Институт физико-математических наук и информационных технологий

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

«Теория кодирования, сжатия и восстановления информации»

Шифр: 10.05.01
Специальность: «Компьютерная безопасность»
Специализация: «Математические методы защиты информации»
Квалификация (степень) выпускника: специалист по защите информации т

Калининград
2022

Лист согласования

Составитель: Киршанова Е.А., PhD., доцент.

Рабочая программа утверждена на заседании учебно-методического совета института физико-математических наук и информационных технологий

Протокол № 01/22 от «01» февраля 2022 г.

Председатель учебно-методического
совета института физико-
математических наук и информационных
технологий

Первый заместитель директора ИФМНиИТ, к. ф.-м. н., доцент — Шпилевой А. А

Ведущий менеджер — Е.П.Ставицкая

Содержание

1.Наименование дисциплины: «Теория кодирования, сжатия и восстановления информации».

Цель дисциплины: изучение основных понятий, теорем и алгоритмов теории кодирования, сжатия и восстановления информации, методикой построения эффективных помехоустойчивых кодов и алгоритмов их декодирования, практической реализацией этих алгоритмов

2. Перечень планируемых результатов обучения по дисциплине, соотнесенных с планируемыми результатами освоения образовательной программы

Код компетенции	Результаты освоения образовательной программы (ИДК)	Результаты обучения по дисциплине
ОПК-7 Способен создавать программы на языках высокого и низкого уровня, применять методы и инструментальные средства программирования для решения профессиональных задач, осуществлять обоснованный выбор инструментария программирования и способов организации программ.	ОПК-7.1. Разрабатывает программы на языках высокого и низкого уровня. ОПК-7.2. Применяет известные методы программирования и возможности базового языка программирования для решения типовых профессиональных задач. ОПК-7.3. Осуществляет обоснованный выбор инструментария программирования и способов организации программ.	**Знать** базовый синтаксис языка Python для выполнения лабораторных работ по курсу. **Уметь** моделировать алгоритмическую задачу, связанную с теорией кодирования, и переносить её в машинный код языка Python. **Владеть** навыками программирования задач из линейной алгебры и теории кодирования.
ОПК-9 Способен решать задачи профессиональной деятельности с учетом текущего состояния и тенденций развития методов защиты информации в операционных системах, компьютерных сетях и системах управления базами данных, а также методов и средств защиты информации от утечки по техническим каналам, сетей и систем передачи информации	ОПК-9.1. Знает методы защиты информации в операционных системах, компьютерных сетях и системах управления базами данных, а также методы и средства защиты информации от утечки по техническим каналам, сетей и систем передачи информации. ОПК-9.2. Умеет решать задачи профессиональной деятельности с учетом текущего состояния и тенденций развития методов защиты информации в операционных системах, компьютерных сетях и системах управления базами данных, а также методов и средств защиты информации от утечки по техническим каналам, сетей и систем передачи информации. ОПК-9.3. Владеет навыками	**Знать** основные понятия дисциплины (код, линейный код, дуальный код, алгоритм декодирования по синдрому, Граница Гильберта-Варшамова. Неравенство МакЭлис, коды Рида-Соломон, БЧХ коды, коды Гоппы, LDPC коды) и алгоритмы на кодирования/декодирования вышеперечисленных кодов, знать как строится криптосистемы на кодах. **Уметь** вычислять порождающие/проверочные матрицы, строить таблицу синдромов, вычислять дуальный код, оценивать минимальное расстояние кода.

	решения задач профессиональной деятельности с учетом текущего состояния и тенденций развития методов защиты информации в операционных системах, компьютерных сетях и системах управления базами данных, а также методов и средств защиты информации от утечки по техническим каналам, сетей и систем передачи информации.	**Владеть** методами построения линейных кодов, вычисления основных параметров кода, алгоритмами кодирования и декодирования основных линейных кодов.
ОПК-2.1 Способен разрабатывать алгоритмы, реализующие современные математические методы защиты информации.	ОПК-2.1.1. Знает алгоритмы, реализующие современные математические методы защиты информации. ОПК-2.1.2. Разрабатывает рекомендации и предложения по совершенствованию и повышению эффективности защиты информации. ОПК-2.1.3. Владеет методами отладки создаваемых средств защиты.	**Знать** принципы работы алгоритмов кодирования и декодирования популярных кодов (Рида-Соломона, БЧХ, кодов Гоппы, LDPC кодов) **Уметь** анализировать сложность алгоритмов декодирования. **Владеть** навыками реализации алгоритмов, связанных с теорией кодирования, тестировать полученные алгоритмы.

3. Место дисциплины в структуре образовательной программы

Дисциплина «Теория кодирования, сжатия и восстановления информации» представляет собой дисциплину обязательной части блока дисциплин подготовки студентов.

4. Виды учебной работы по дисциплине.

Виды учебной работы по дисциплине зафиксированы учебным планом основной профессиональной образовательной программы по указанному направлению и профилю, выражаются в академических часах. Часы контактной работы и самостоятельной работы студента и часы, отводимые на процедуры контроля, могут различаться в учебных планах ОПОП по формам обучения. Объем контактной работы включает часы контактной аудиторной работы (лекции/практические занятия/ лабораторные работы), контактной внеаудиторной работы (контроль самостоятельной работы), часы контактной работы в период аттестации. Контактная работа, в том числе может проводиться посредством электронной информационно-образовательной среды университета с использованием ресурсов сети Интернет и дистанционных технологий

5. Содержание дисциплины, структурированное по темам (разделам)

Исходя из рамок, установленных учебным планом по трудоемкости и видам учебной работы по дисциплине, преподаватель самостоятельно выбирает тематику занятий по формам и количеству часов проведения контактной работы: лекции и иные учебные занятия, предусматривающие преимущественную передачу учебной информации преподавателем и (или) занятия семинарского типа (семинары, практические занятия, практикумы, лабораторные работы, коллоквиумы и иные аналогичные занятия), и (или) групповые консультации, и (или) индивидуальную работу обучающихся с преподавателем, в том числе индивидуальные консультации (по курсовым работам/проектам – при наличии курсовой работы/проекта по данной дисциплине в учебном плане). Рекомендуемая тематика занятий максимально полно реализуется в контактной работе со студентами очной формы обучения. В случае реализации образовательной программы в заочной / очно-заочной форме трудоемкость дисциплины сохраняется, однако объем учебного материала в значительной части осваивается студентами в форме самостоятельной работы. При этом требования к ожидаемым образовательным результатам студентов по данной дисциплине не зависят от формы реализации образовательной программы.

№	Наименование раздела	Содержание раздела
1	Основные понятия теории кодирования	Основные определения: код, длина кода, размерность, расстояние Хэмминга, минимальное расстояние кода, нижняя граница минимального расстояния, дуальный код. Проверочная/порождающая матрица.
2	Линейные коды. Декодирование по синдрому	Определение синдрома, таблица синдромов, два алгоритма декодирования по синдрому, их сложность.
3	Граница Гильберта-Варшамова. Неравенство МакЭлис	Граница Гильберта-Варшамова, граница Синглтона, доказательства. Граница Плоткина. Неравенства МакЭлис, доказательства.
4	Код Рида-Соломона	Основные определения расширения конечного поля. Определение кода Рида-Соломона, его минимальное расстояние. Алгоритм декодирования кода, его сложность. Применение кода в задачах биологии.
5	БЧХ-код, код Гоппы	Определения подкода подполя. БЧХ-код. Размер кода. Минимальное расстояние. Алгоритм декодирования. Определения кода Гоппы. Его размер и минимальное расстояние. Алгоритм декодирования. Сложность.
6	Коды конкатенации	Определение кода конкатенации, внешнего и внутреннего кодов.

		Границы минимального расстояния кода конкатенации. Алгоритм декодирования.
7	LDPC код	Понятие двудольного графа. Коды на графах. Код с малой плотностью проверок на четность. Алгоритм декодирования.
8	Списочное декодирование	Декодирование за границей минимального расстояния. Алгоритм списочного декодирования Гурусвами-Судана для кода Рида-Соломона.

6. Рекомендуемая тематика учебных занятий в форме контактной работы

Рекомендуемая тематика учебных занятий *лекционного* типа (предусматривающих преимущественную передачу учебной информации преподавателями):

№	Наименование раздела	Содержание раздела
1	Основные понятия теории кодирования	Лекция № 1. Основные определения:
2	Линейные коды. Декодирование по синдрому	Лекция № 2. Алгоритмы декодирование: по таблице смежности, по синдрому,
3	Граница Гильберта-Варшамова. Неравенство МакЭлис	Лекция № 3: Граница Гильберта-Варшамова. Лекция №4: Граница Плоткина. Лекция : Лекция № 5. Неравенства МакЭлис, дуальный кода.
4	Код Рида-Соломона	Лекция № 6. Определение кода Рида-Соломона, его минимальное расстояние. Лекция №7. Алгоритмы декодирования кода Рида-Соломона Лекция №8. Применение кода в задачах биологии.
5	БЧХ-код, код Гоппы, код Рида-Маллера	Лекция №9. БЧХ-код. Лекция №10. Код Гоппы. Лекция №11. Код Рида-Маллера
6	Коды конкатенации	Лекция №12. Коды контакетанации: определение, мин. рассмтояние. Лекция №13. Алгоритм декодирования кодов конкатенации.
7	LDPC код	Лекция № 14. Коды на графах. Код с малой плотностью проверок на четность.
8	Списочное декодирование	Лекция №15. Алгоритм списочного декодирования Гурусвами-Судана для кода Рида-Соломона.

Рекомендуемая тематика *практических* занятий:

№ п/п	**Наименование Темы**	**Содержание темы**
1	Основные понятия теории кодирования	Систематическая форма порождающей/проверочной матриц кода. Дуальный код. Количество порождающих матриц кода над конечным полем.
2	Линейные коды. Декодирование по синдрому	Декодирование по таблице классов смежности. Декодирование бинарного кода Хэмминга.
3	Граница Гильберта-Варшамова. Неравенство МакЭлис	Доказательство свойств границы Граница Синглтона. Альтернативное доказательство границы Гильберта-Варшамова. Уточнение границы ГВ для линейных кодов.Минимальное расстояние совершенного кода. Обобщенный код Хэмминга.
4	Код Рида-Соломона	Формула Форней. Пример алгоритма декодирования кода Рида-Соломона алгоритмом Петерсона.
5	БЧХ-код. Код Гоппы	Минимальное расстояние кода Рида-Маллера. Алгоритм декодирования кода Гоппы
6	Коды конкатенации	Алгоритм Walsh-Berlekemp для кода Рида-Соломона
7	LDPC код	Пример декодирования LDPC кода.
8	Списочное декодирование	Списочный алгоритм декодирования для кода Рида-Соломона

Рекомендуемый перечень тем *лабораторных* работ *(при наличии)*

№ п/п	Наименование раздела дисциплины	Тема лабораторной работы
1	Основные понятия теории кодирования	Код Адамара
2	Линейные коды. Декодирование по синдрому	Доказательства свойств линейного кода. Задание на программирование: расширенный код Хэмминга
3	Граница Гильберта-Варшамова. Неравенство МакЭлис	Совершенный код
4	Код Рида-Соломона	Реализация алгоритма декодирования кода Рида-Соломона на Python
5	Коды конкатенации	Реализация алгоритма декодирования кода конкатенации на Python
6	LDPC код	Мажоритарное декодирование LDPC кода

Требования к самостоятельной работе студентов

1. Работа с лекционным материалом, предусматривающая проработку конспекта лекций и учебной литературы, по всем лабораторным работам, описанным выше.
2. Выполнение некоторых индивидуальных практических работ.
3. Изучение семейств кодов в ходе домашних работ, а именно обобщенного кода Хэмминга, кода Адамара, кода Голея, циклических кодов.

Руководствуясь положениями статьи 47 и статьи 48 Федерального закона от 29 декабря 2012 г. N 273-ФЗ «Об образовании в Российской Федерации» научно-педагогические работники и иные лица, привлекаемые университетом к реализации

данной образовательной программы, пользуются предоставленными академическими правами и свободами в части свободы преподавания, свободы от вмешательства в профессиональную деятельность; свободы выбора и использования педагогически обоснованных форм, средств, методов обучения и воспитания; права на творческую инициативу, разработку и применение авторских программ и методов обучения и воспитания в пределах реализуемой образовательной программы и отдельной дисциплины.

Исходя из рамок, установленных учебным планом по трудоемкости и видам учебной работы по дисциплине, преподаватель самостоятельно выбирает тематику занятий по формам и количеству часов проведения контактной работы: лекции и иные учебные занятия, предусматривающие преимущественную передачу учебной информации преподавателем и (или) занятия семинарского типа (семинары, практические занятия, практикумы, лабораторные работы, коллоквиумы и иные аналогичные занятия), и (или) групповые консультации, и (или) индивидуальную работу обучающихся с преподавателем, в том числе индивидуальные консультации (по курсовым работам/проектам – при наличии курсовой работы/проекта по данной дисциплине в учебном плане).

Рекомендуемая тематика занятий максимально полно реализуется в контактной работе со студентами очной формы обучения. В случае реализации образовательной программы в заочной / очно-заочной форме трудоемкость дисциплины сохраняется, однако объем учебного материала в значительной части осваивается студентами в форме самостоятельной работы. При этом требования к ожидаемым образовательным результатам студентов по данной дисциплине не зависят от формы реализации образовательной программы.

7. Методические рекомендации по видам занятий

Лекционные занятия.

В ходе лекционных занятий обучающимся рекомендуется выполнять следующие действия. Вести конспектирование учебного материала. Обращать внимание на категории, формулировки, раскрывающие содержание тех или иных явлений и процессов, научные выводы и практические рекомендации по их применению. Задавать преподавателю уточняющие вопросы с целью уяснения теоретических положений, разрешения спорных ситуаций.

Желательно оставить в рабочих конспектах поля, на которых во внеаудиторное время можно сделать пометки из рекомендованной литературы, дополняющие материал прослушанной лекции, а также подчеркивающие особую важность тех или иных теоретических положений.

Практические и семинарские занятия.

На практических и семинарских занятиях в зависимости от темы занятия выполняется поиск информации по решению проблем, практические упражнения, контрольные работы, выработка индивидуальных или групповых решений, итоговое обсуждение с обменом знаниями, участие в круглых столах, разбор конкретных ситуаций, командная работа, представление портфолио и т.п.

Самостоятельная работа.

Самостоятельная работа осуществляется в виде изучения литературы, эмпирических данных по публикациям и конкретных ситуаций из практики, подготовке индивидуальных работ, работа с лекционным материалом, самостоятельное изучение отдельных тем дисциплины; поиск и обзор литературы и электронных источников; чтение и изучение учебника и учебных пособий.

8. Фонд оценочных средств

8.1. Перечень компетенций с указанием этапов их формирования в процессе освоения образовательной программы в рамках учебной дисциплины

Основными этапами формирования указанных компетенций при изучении обучающимися дисциплины являются последовательное изучение содержательно связанных между собой тем учебных занятий. Изучение каждой темы предполагает овладение обучающимися необходимыми компетенциями. Результат аттестации обучающихся на различных этапах формирования компетенций показывает уровень освоения компетенций.

Контролируемые разделы (темы) дисциплины	Индекс контролируемой компетенции (или её части)	Оценочные средства по этапам формирования компетенций
		текущий контроль по дисциплине
Тема 1. Основные понятия теории кодирования	ОПК-2.1 ОПК-9	Решение задач
Тема 2. Линейные коды. Декодирование по синдрому	ОПК-2.1 ОПК-7 ОПК-9	Решение задач
Тема 3. Граница Гильберта-Варшамова. Неравенство МакЭлис	ОПК-9 ОПК-2.1	Решение задач
Тема 4. Код Рида-Соломона	ОПК-2.1 ОПК-7 ОПК-9	Решение задач, Индивидуальная работа
Тема 5. БЧХ-код. Код Гоппы	ОПК-9 ОПК-2.1	Решение задач, Индивидуальная работа
Тема 6. Коды конкатенации	ОПК-2.1 ОПК-7 ОПК-9	Решение задач, Индивидуальная работа
Тема 7. LDPC код	ОПК-9 ОПК-2.1	Решение задач
Тема 8. Списочное декодирование	ОПК-9 ОПК-2.1	Решение задач

8.2. Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений и навыков и (или) опыта деятельности процессе текущего контроля

Тема 1. Основные понятия теории кодирования

Пример задач на оценку “удовлетворительно”:

1. Напишите порождающие и проверочные матрицы для [n, n − 1, 2]_2 – кода проверки на четность и для [n, 1, n]_2 кода с повторением

2. Покажите, что минимальное расстояние любого линейного кода C равно минимальному весу Хэмминга ненулевого слова в C.

3. Пусть G = [Id_k|A] - порождающая матрица [n, k]_q−кода C в систематической форме, где Id_k− единичная матрица k × k, A - матрицу размерности k×(n-k) над конечным полем. Опишите проверочную матрицу для C.

4. Пусть G - порождающая матрица C. Докажите эквивалентность определений дуального кода: C^\perp = {x \in Fq : <x, c> = 0 : c \in C} = {x \in Fq : xG^t = 0}.

Тема 2. Линейные коды. Декодирование по синдрому

Задание. Для линейного кода C, заданного над F_3 с порождающей матрицей

$$G = \begin{pmatrix} 2 & 1 & 2 & 1 \\ 1 & 1 & 1 & 0 \end{pmatrix}$$

1. привести G к систематической форме,
2. определить мин. расстояние кода,
3. построить таблицу классов смежности и декодировать y = (1 1 1 1),
4. построить таблицу синдромов

Тема 3. Граница Гильберта-Варшамова. Неравенство МакЭлис

Задание. Докажите, что для q > 1, n, d \in N, таких что $2 \leq d \leq n$, выполняются

$$A_q(n,d) \leq q^{n-d+1},$$

$$A_q(n,d) \geq \frac{q^{n-1}}{Vol\ _q^{n-1}(d-2)}$$

Тема 4. Код Рида-Соломона

Задание. Пример кода Рида-Соломона.
Код Рида-Соломона $R_F{}^S(n,k)$ размерности $k = 4$ определён над $F = GF(3^2) = F_3[x] = (x^2 + x + 2)$. Обозначим α −корень $f(x) = (x^2 + x + 2)$ и положим $S = \{1, \alpha, \alpha^2, \ldots, \alpha^7\}$.

1. Каково минимальное расстояние $R_F{}^S(n,k)$?
2. Закодируйте сообщение m = [2, 0, α + 1, 1]
3. Докажите, что c = [2, 1, 2α + 2, 0, α, α + 1, 2α, α + 2] принадлежит коду

4. Восстановите исходное сообщение по полученному слову c = [?, 1, ?, 0, α, ?, 2α, ?], где ? означает, что символ кодового слова был стёрт

Тема 5. БЧХ-код. Код Гоппы

1. Для двоичного БЧХ-кода длины n = 9 над F_3 с минимальным расстоянием d = 3 построить порождающий многочлен и порождающую матрицу. Вычислить размерность, минимальное расстояние кода и число исправляемых ошибок. Продемонстрировать корректность алгоритма декодирования.

2. Для кода Гоппы, заданного параметрами g(x) = x^2 + x + 1, q = 2, L = F_2^3 =F_2[x]/(x^3+ x + 1) ={0, 1, α, α^2, α^3 = α + 1, α^4 = α^2 + α, α5 = α^2 + α + 1, α6 = α^2 + 1}, с помощью алгоритма декодирования кода Гоппы декодируйте y = [1 0 1 1 1 1 1 1].

Тема 6. Коды конкатенации

Покажите, что алгоритм Walsh-Berlekemp для кода Рида-Соломона RS(n, k), успешен в случае wt(e) ошибочных символов и s удаленных символов, если 2wt(e) + s < n − k + 1.

Тема 7. LDPC код

LDPC код задан проверочной матрицей

$$H = \begin{pmatrix} 0 & 1 & 0 & 1 & 1 & 0 & 0 & 1 \\ 1 & 1 & 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 & 1 & 1 \\ 1 & 0 & 0 & 1 & 1 & 0 & 1 & 0 \end{pmatrix}$$

1. Опишите граф, соответствующий коду.
2. Декодируйте слово y = [1 1 0 1 0 1 0 1], используя в алгоритме декодирования мажоритарное голосование при выборе бита.

8.3. Перечень вопросов и заданий для промежуточной аттестации по дисциплине

1. Определение линейного кода, порождающей/проверочной матриц, минимального расстояния, размерности\длины линейного кода.
2. Понятие синдрома слова, алгоритм декодирования линейного кода по синдрому.
3. Граница Гильберта-Варшамова, доказательство.
4. Граница Синглтона, доказательство.
5. Граница Плоткина, доказательство.
6. Тождества МакВильямса, основные определения, связанные с тождеством.
7. Код Рида-Соломона, его размерность, минимальное расстояние.
8. Алгоритмы декодирования кода Рида-Соломона, их сложность.

9. BCH код.
10. Код Рида-Маллера.
11. Код Гоппы
12. Коды конкатенации
13. Списочное декодирование
14. LDPC коды

8.4. Планируемые уровни сформированности компетенций обучающихся и критерии оценивания

Уровни	Содержательное описание уровня	Основные признаки выделения уровня (этапы формирования компетенции, критерии оценки сформированности)	Пятибалльная шкала (академическая) оценка	Двухбалльная шакала, зачет	БРС, % освоения (рейтинговая оценка)
Повышенный	Творческая деятельность	*Включает нижестоящий уровень.* Умение самостоятельно принимать решение, решать проблему/задачу теоретического и прикладного характера на основе изученных методов, приемов, технологий	отлично	зачтено	86-100
Базовый	Применение знаний и умений в более широких контекстах учебной и профессиональной деятельности, нежели по образцу с большей степени самостоятельности и	*Включает нижестоящий уровень.* Способность собирать, систематизировать, анализировать и грамотно использовать информацию из самостоятельно найденных теоретических источников и иллюстрировать ими теоретические положения или обосновывать практику	хорошо		71-85

	инициативы	применения			
Удовлетвори тельный (достаточный)	Репродуктив ная деятельность	Изложение в пределах задач курса теоретически и практически контролируемого материала	удовлетвор ительно		55-70
Недостаточн ый	Отсутствие признаков удовлетворительного уровня		неудовлетв орительно	не зачтено	Менее 55

9. Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины.

Основная литература

1. Березкин, Е. Ф. Основы теории информации и кодирования: Учебное пособие / Березкин Е.Ф. - Москва :НИЯУ "МИФИ", 2010. - 312 с. ISBN 978-5-7262-1294-4. - Текст : электронный. - URL: https://znanium.com/catalog/product/560066 (дата обращения: 26.04.2022). – Режим доступа: по подписке.

Дополнительная литература

1. Каганов, В. И. Радиотехнические цепи и сигналы. Компьютеризированный курс : учебное пособие / В.И. Каганов. — 4-е изд., перераб. и доп. — Москва : ФОРУМ : ИНФРА-М, 2021. — 498 с. — (Высшее образование: Магистратура). — DOI 10.12737/textbook_5a86b8b1ee58d8.44881391. - ISBN 978-5-00091-447-2. - Текст : электронный. - URL: https://znanium.com/catalog/product/1413304 (дата обращения: 26.04.2022). – Режим доступа: по подписке.

Интернет-ресурсы:

1. Лекции Проф. Др. В. Гурусвами. NUY. Находятся в открытом доступе по адресу http://www.cs.cmu.edu/~venkatg/teaching/codingtheory/

2. Лекции Проф. Др. М. Судана. Находятся в открытом доступе по адресу http://people.csail.mit.edu/madhu/FT01/course.html

10. Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины (модуля).

- НЭБ Национальная электронная библиотека, диссертации и прочие издания
- eLIBRARY.RU Научная электронная библиотека, книги, статьи, тезисы докладов конференций

- Гребенников Электронная библиотека ИД журналы
- ЭБС Лань книги, журналы
- ЭБС Консультант студента
- ПРОСПЕКТ ЭБС
- ЭБС ZNANIUM.COM
- РГБ Информационное обслуживание по МБА
- БЕН РАН
- Электронно-библиотечная система (ЭБС) Кантитана (https://elib.kantiana.ru/)

11. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине.

Программное обеспечение обучения включает в себя:

- система электронного образовательного контента БФУ им. И. Канта – www.lms-3.kantiana.ru, обеспечивающую разработку и комплексное использование электронных образовательных ресурсов;
- серверное программное обеспечение, необходимое для функционирования сервера и связи с системой электронного обучения через Интернет;
- корпоративная платформа Microsoft Teams;
- установленное на рабочих местах студентов ПО: Microsoft Windows 7, Microsoft Office Standart 2010, антивирусное программное обеспечение Kaspersky Endpoint Security.
- специализированное ПО (при наличии): система компьютерной алгебры Sage

12. Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине.

Для проведения занятий лекционного типа, практических и семинарских занятий используются специальные помещения (учебные аудитории), оборудованные техническими средствами обучения – мультимедийной проекционной техникой. Для проведения занятий лекционного типа используются наборы демонстрационного оборудования.

Для проведения лабораторных работ, (практических занятий – при необходимости) используются специальные помещения (учебные аудитории), оснащенные специализированным лабораторным оборудованием: персональными компьютерами с возможностью выхода в интернет и с установленным программным обеспечением, заявленным в п.11.

Для проведения групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации используются специальные помещения (учебные аудитории), оборудованные специализированной мебелью (для обучающихся), меловой / маркерной доской.

Для организации самостоятельной работы обучающимся предоставляются помещения, оснащенные компьютерной техникой с возможностью подключения к сети «Интернет» и обеспечением доступа в электронную информационно-образовательную среду университета.

Для обучения инвалидов и лиц с ограниченными возможностями здоровья университетом могут быть представлены специализированные средства обучения, в том числе технические средства коллективного и индивидуального пользования.

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
федеральное государственное автономное образовательное учреждение высшего образования «Балтийский федеральный университет имени Иммануила Канта»
Институт физико-математических наук и информационных технологий

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

«Теория информации»

Шифр: 10.05.01
Специальность: «Компьютерная безопасность»
Специализация: «Математические методы защиты информации»
Квалификация (степень) выпускника: специалист по защите информации

Калининград
2022

Лист согласования

Составитель: Колесников Никита Сергеевич, мл. науч. сотрудник лаборатории «Математические методы защиты и обработки информации»

Рабочая программа утверждена на заседании учебно-методического совета института физико-математических наук и информационных технологий

Протокол № 01/22 от «01» февраля 2022 г.

Председатель учебно-методического
совета института физико-
математических наук и информационных
технологий

Первый заместитель директора Шпилевой А. А
ИФМНиИТ, к. ф.-м. н., доцент

Ведущий менеджер Е.П.Ставицкая

Содержание

1.Наименование дисциплины: «Теория информации».

Цель дисциплины: формирование у обучающихся чёткого понимания предмета теории информации и её основных концепций, а также развитие навыков применять методы теории информации для решения проблем, связанных с хранением, обработкой и передачей информации.

2. Перечень планируемых результатов обучения по дисциплине, соотнесенных с планируемыми результатами освоения образовательной программы

Код компетенции	Результаты освоения образовательной программы (ИДК)	Результаты обучения по дисциплине
ОПК-2.1. Способен разрабатывать алгоритмы, реализующие современные математические методы защиты информации.	ОПК-2.1.1. Знает алгоритмы, реализующие современные математические методы защиты информации. ОПК-2.1.2. Разрабатывает рекомендации и предложения по совершенствованию и повышению эффективности защиты информации. ОПК-2.1.3. Владеет методами отладки создаваемых средств защиты.	- **знать** современные методы исследований из различных областей математики, физики, электроники, и других; знать методологические принципы применения этих методов в задачах защиты информации; - **уметь** корректно формулировать задачи обеспечения информационной безопасности, строить план их решения, разрабатывать подходящие алгоритмы для решения прикладных задач, применять современные математические методы защиты информации в профессиональной деятельности; - **владеть** навыками применения теоретических и экспериментальных методов для решения задач обеспечения информационной безопасности.
ОПК-3. Способен на основании совокупности математических методов разрабатывать, обосновывать и реализовывать процедуры решения задач профессиональной деятельности.	ОПК-3.1. Знает необходимые математические методы для решения задач обеспечения защиты информации. ОПК-3.2. Применяет совокупность необходимых математических методов для решения задач обеспечения защиты информации. ОПК-3.3. Разрабатывает, обосновывает и реализует на практике процедуры решения задач обеспечения защиты информации.	- ***знать*** фундаментальные понятия теории информации (энтропия, взаимная информация, источники сообщений, каналы связи); свойства энтропии и взаимной информации; основные результаты о кодировании дискретных источников сообщений при наличии и отсутствии шума; основные методы оптимального кодирования источников информации; понятие пропускной способности канала связи, прямую и обратную теоремы кодирования; - ***уметь*** вычислять теоретико-информационные характеристики источников сообщений и каналов связи (энтропия, взаимная информации, пропускная способность); применять математические методы и модели для

		формализации, исследования и решения простейших задач обеспечения информационной безопасности; - ***владеть*** основами построения математических моделей текстовой информации и моделей систем передачи информации; навыками применения математического аппарата для решения прикладных теоретико-информационных задач.

3. Место дисциплины в структуре образовательной программы

«*Теория информации*» представляет собой обязательную дисциплину Блока 1 «Дисциплины (модули)», входит в модуль 5 «Дополнительные разделы дискретной математики» (Б1.О.09) дисциплин специальности 10.05.01 «Компьютерная безопасность», специализация «Математические методы защиты информации».

4. Виды учебной работы по дисциплине.

Виды учебной работы по дисциплине зафиксированы учебным планом основной профессиональной образовательной программы по указанному направлению и профилю, выражаются в академических часах. Часы контактной работы и самостоятельной работы обучающегося и часы, отводимые на процедуры контроля, могут различаться в учебных планах ОПОП по формам обучения. Объем контактной работы включает часы контактной аудиторной работы (лекции/практические занятия/ лабораторные работы), контактной внеаудиторной работы (контроль самостоятельной работы), часы контактной работы в период аттестации. Контактная работа, в том числе может проводиться посредством электронной информационно-образовательной среды университета с использованием ресурсов сети Интернет и дистанционных технологий

5. Содержание дисциплины, структурированное по темам (разделам)

Исходя из рамок, установленных учебным планом по трудоемкости и видам учебной работы по дисциплине, преподаватель самостоятельно выбирает тематику занятий по формам и количеству часов проведения контактной работы: лекции и иные учебные занятия, предусматривающие преимущественную передачу учебной информации преподавателем и (или) занятия семинарского типа (семинары, практические занятия, практикумы, лабораторные работы, коллоквиумы и иные аналогичные занятия), и (или) групповые консультации, и (или) индивидуальную работу обучающихся с преподавателем, в том числе индивидуальные консультации (по курсовым работам/проектам – при наличии курсовой работы/проекта по данной дисциплине в учебном плане). Рекомендуемая тематика занятий максимально полно реализуется в контактной работе с обучающимися очной формы обучения. В случае реализации образовательной программы в заочной / очно-заочной форме трудоемкость дисциплины сохраняется, однако объем учебного материала в значительной части осваивается обучающимися в форме самостоятельной работы. При этом требования к ожидаемым образовательным результатам обучающихся по данной дисциплине не зависят от формы реализации образовательной программы.

№	Наименование раздела	Содержание раздела

1	Энтропия и взаимная информация	Задачи и программа курса. Место курса «Теория информации» в ряду других математических и прикладных дисциплин. Формы самостоятельной работы студентов по изучению курса. Литература к курсу. Предмет теории информации. Основные свойства вероятности, известные из курса теории вероятностей (обзорно). Дискретные случайные величины и их основные свойства (обзорно). Собственная, условная и взаимная информация. Энтропия дискретной случайной величины (вероятностной схемы). Свойства энтропии: симметричность, непрерывность, нижняя и верхняя границы, выпуклость. Совместная энтропия двух и более дискретных случайных величин, условная энтропия и их свойства: аддитивность, правило цепочки, основные неравенства, полуаддитивность, невозрастание при отображении. Средняя взаимная информация: определение, простейшие свойства. Условная средняя взаимная информация: определение, неотрицательность, условие равенства нулю. Сравнение различных подходов к определению понятия энтропии. Аксиомы об энтропии по Шеннону. Аксиомы Хинчина и Фаддеева. Теорема о единственности функции, удовлетворяющей системе аксиом об энтропии по Шеннону.
2	Дискретные источники сообщений	Математическая модель источника сообщений – случайный процесс с дискретным временем и конечным множеством состояний. Цилиндрические множества, условия согласованности и теорема существования продолжения вероятностной меры (без доказательства). Примеры источников сообщений: источник без памяти, простой марковский источник, марковский источник с заданной глубиной зависимости. Энтропия H_k, приходящаяся на одну букву сообщения, и условная энтропия $H^{(k)}$ последней буквы сообщения: определение и основные свойства, связывающие эти величины. Предельная энтропия H_∞. Энтропия H_k, $H^{(k)}$ и H_∞ для простого источника без памяти. Стационарные источники. Стационарность источника без памяти. Условие стационарности простого марковского источника. Теорема о

		существовании предельной энтропии для стационарного источника. Предельная энтропия для простого стационарного марковского источника. Свойство асимптотической равнораспределённости: определение, оценка мощности множества ε-типичных последовательностей, примеры. Теорема об асимптотической равнораспределённости для источника без памяти. Эргодические источники. Эргодическая теорема для регулярного простого марковского источника (без доказательства). Закон больших чисел для частот биграмм в последовательностях, порождаемых стационарным и регулярным простым марковским источником. Теорема об асимптотической равнораспределённости для стационарного и регулярного простого марковского источника. Информационная дивергенция. Граница Симмонса. Теорема об асимптотической оценке числа высоковероятных последовательностей, порождаемых источником со свойством асимптотической равнораспределённости. Сжимающее кодирование последовательностей, порождаемых источником со свойством асимптотической равнораспределённости.
3	Кодирование дискретных источников сообщений	Алфавитное кодирование. Однозначно декодируемые, префиксные и суффиксные коды. Теорема о соответствии между префиксными кодами и кодовыми деревьями. Необходимое и достаточное условие существования префиксного кода с заданными длинами кодовых слов – неравенство Крафта. Необходимое и достаточное условие однозначного декодирования – неравенство Мак-Миллана. Задача оптимального кодирования. Теорема об оценке средней длины оптимального префиксного кода. Теорема о пределе средней длины кодового слова при кодировании длинных блоков. Алгоритмы Фано и Хаффмана. Леммы о строении оптимального кода. Теорема об оптимальности кода Хаффмана.
4	Дискретные каналы связи	Математическая модель канала связи и его информационные характеристики. Дискретный стационарный канал без памяти (ДСКБП). Примеры ДСКБП: двоичный симметричный канал, двоичный

		канал со стиранием. Определение пропускной способности канала. Пропускная способность ДСКБП. Оценка пропускной способности в остальных случаях. Симметричные каналы связи и их разновидности. Пропускная способность для различных видов симметричных каналов. Примеры симметричных каналов. Последовательное и параллельное соединение и сумма двух ДСКБП. Оценка пропускной способности результирующего канала при различных видах соединения.
5	Теоремы кодирования для дискретных каналов связи без памяти	Скорость передачи информации. Декодер общего вида и решающие области. Ошибочное декодирование, условная и средняя вероятности ошибочного декодирования. Неравенство Фано. Свойства функции Фано. Обратная теорема кодирования для ДКБП. Типичные входные и выходные векторы и пары векторов. Декодер типичных пар. Леммы о совместной асимптотической равнораспределённости. Прямая теорема кодирования для ДКБП.

6. Рекомендуемая тематика учебных занятий в форме контактной работы

Рекомендуемая тематика учебных занятий *лекционного* типа (предусматривающих преимущественную передачу учебной информации преподавателями):

№	Наименование раздела	Темы лекций
1	Энтропия и взаимная информация	Лекция 1. Предмет и понятие теории информации. Энтропия. Лекция 2. Свойства энтропии. Совместная и условная энтропия. Лекция 3. Взаимная информация и условная взаимная информация.
2	Дискретные источники сообщений	Лекция 4. Дискретные источники сообщений (ДИС). Лекция 5. Стационарные источники сообщений.
3	Кодирование дискретных источников сообщений	Лекция 6. Кодирование ДИС. Лекция 7. Оптимальное кодирование. Коды Фано и Хаффмана. Лекция 8. Алгоритм Хаффмана.

4	Дискретные каналы связи	Лекция 9. Дискретные каналы связи. Лекция 10. Симметричные каналы связи.
5	Теоремы кодирования для дискретных каналов связи без памяти	Лекция 11. Декодер общего вида и решающие области. Лекция 12. Прямая теорема кодирования ДКБП.

Рекомендуемая тематика *практических* занятий:

1. Измерение количества информации и энтропии случайных величин.
2. Вычисление энтропии и оценка на её основе различных информационных систем.
3. Вычисление совместной и условной энтропии и взаимной информации для зависимых случайных величин.
4. Вычисление энтропии для различных источников сообщений.
5. Построение однозначно декодируемого кода. Использование алгоритмов Фано и Хаффмана.
6. Применение неравенства Крафта и теоремы МакМиллана.
7. Проверка однозначной декодируемости линейного кода.
8. Стационарность ДИС.
9. Применение свойства асимптотической равнораспределённости.
10. Алгоритмы сжимающего кодирования для дискретного источника без памяти.
11. Оценка средней длины оптимального кода.
12. Вычисление пропускной способности и иных вероятностных характеристик для различных ДСКБП и их соединений.
13. Оценка вероятности ошибочного декодирования.

На практических занятиях решаются задачи по теме занятия.

Требования к самостоятельной работе обучающихся

1. Работа с лекционным материалом, предусматривающая проработку конспекта лекций и учебной литературы, по всем темам из п. 6 настоящей рабочей программы.
2. Выполнение домашнего задания, предусматривающего решение задач, выполнение упражнений, выдаваемых на практических занятиях, по всем темам из п. 6 настоящей рабочей программы.

Руководствуясь положениями статьи 47 и статьи 48 Федерального закона от 29 декабря 2012 г. N 273-ФЗ «Об образовании в Российской Федерации» научно-педагогические работники и иные лица, привлекаемые университетом к реализации данной образовательной программы, пользуются предоставленными академическими правами и свободами в части свободы преподавания, свободы от вмешательства в профессиональную деятельность; свободы выбора и использования педагогически обоснованных форм, средств, методов обучения и воспитания; права на творческую инициативу, разработку и применение авторских программ и методов обучения и воспитания в пределах реализуемой образовательной программы и отдельной дисциплины.

Исходя из рамок, установленных учебным планом по трудоемкости и видам учебной работы по дисциплине, преподаватель самостоятельно выбирает тематику занятий по формам и количеству часов проведения контактной работы: лекции и иные

учебные занятия, предусматривающие преимущественную передачу учебной информации преподавателем и (или) занятия семинарского типа (семинары, практические занятия, практикумы, лабораторные работы, коллоквиумы и иные аналогичные занятия), и (или) групповые консультации, и (или) индивидуальную работу обучающихся с преподавателем, в том числе индивидуальные консультации (по курсовым работам/проектам – при наличии курсовой работы/проекта по данной дисциплине в учебном плане).

Рекомендуемая тематика занятий максимально полно реализуется в контактной работе с обучающимися очной формы обучения. В случае реализации образовательной программы в заочной / очно-заочной форме трудоемкость дисциплины сохраняется, однако объем учебного материала в значительной части осваивается обучающимися в форме самостоятельной работы. При этом требования к ожидаемым образовательным результатам обучающихся по данной дисциплине не зависят от формы реализации образовательной программы.

7. Методические рекомендации по видам занятий

Лекционные занятия.

В ходе лекционных занятий обучающимся рекомендуется выполнять следующие действия. Вести конспектирование учебного материала. Обращать внимание на категории, формулировки, раскрывающие содержание тех или иных явлений и процессов, научные выводы и практические рекомендации по их применению. Задавать преподавателю уточняющие вопросы с целью уяснения теоретических положений, разрешения спорных ситуаций.

Желательно оставить в рабочих конспектах поля, на которых во внеаудиторное время можно сделать пометки из рекомендованной литературы, дополняющие материал прослушанной лекции, а также подчеркивающие особую важность тех или иных теоретических положений.

Практические и семинарские занятия.

На практических и семинарских занятиях в зависимости от темы занятия выполняется поиск информации по решению проблем, практические упражнения, контрольные работы, выработка индивидуальных или групповых решений, итоговое обсуждение с обменом знаниями, участие в круглых столах, разбор конкретных ситуаций, командная работа, представление портфолио и т.п.

Самостоятельная работа.

Самостоятельная работа осуществляется в виде изучения литературы, эмпирических данных по публикациям и конкретных ситуаций из практики, подготовке индивидуальных работ, работа с лекционным материалом, самостоятельное изучение отдельных тем дисциплины; поиск и обзор литературы и электронных источников; чтение и изучение учебника и учебных пособий.

8. Фонд оценочных средств

8.1. Перечень компетенций с указанием этапов их формирования в процессе освоения образовательной программы в рамках учебной дисциплины

Основными этапами формирования указанных компетенций при изучении обучающимися дисциплины являются последовательное изучение содержательно связанных между собой тем учебных занятий. Изучение каждой темы предполагает овладение обучающимися необходимыми компетенциями. Результат аттестации обучающихся на различных этапах формирования компетенций показывает уровень освоения компетенций.

Контролируемые разделы (темы) дисциплины	Индекс контроли-руемой компетенции (или её части)	Оценочные средства по этапам формирования компетенций
		текущий контроль по дисциплине
1. Энтропия и взаимная информация	ОПК-3	Опрос, решение задач.
2. Дискретные источники сообщений	ОПК-3	Опрос, решение задач
3. Кодирование дискретных источников сообщений	ОПК-3 ОПК-2.1	Опрос, решение задач
4. Дискретные каналы связи	ОПК-3 ОПК-2.1	Опрос, решение задач
5. Теоремы кодирования для дискретных каналов без памяти	ОПК-3 ОПК-2.1	Опрос, решение задач

8.2. Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений и навыков и (или) опыта деятельности процессе текущего контроля

Примеры вопросов для устного опроса:

По Теме 1. Энтропия и взаимная информация

1. Как измеряется количество информации?
2. Что такое условная информация?
3. Что такое взаимная информация?
4. Что такое энтропия дискретной случайной величины?
5. Сформулировать основные свойства функции энтропии.
6. Что такое совместная энтропия нескольких дискретных случайных величин?
7. Что такое условная энтропия?
8. Что такое средняя взаимная информация?
9. В чём сущность аксиоматического определения энтропии?

По Теме 2. Дискретные источники сообщений

1. В чём заключаются условия согласованности цилиндрических множеств?
2. Сформулировать теорему Колмогорова о продолжении вероятностной меры.
3. Какова математическая модель дискретного источника сообщений без памяти?
4. Какова математическая модель простого марковского источника сообщений?
5. Дать определение стационарного источника сообщений
6. Каковы условия стационарности простого Марковского источника?
7. Что такое энтропия, приходящаяся на одну букву сообщения?
8. Что такое энтропия источника сообщений?
9. Сформулировать определение асимптотической равнораспределённости дискретного источника сообщений.
10. Какие источники обладают свойством асимптотической равнораспределённости?
11. Сформулировать эргодическую теорему для регулярного простого марковского источника.

Типовые контрольные задания:

Тема 1: Энтропия и взаимная информация

1. Совместное распределение случайных величин ξ и η задано матрицей

$$\frac{1}{48}\cdot\begin{pmatrix} 5 & 11 & 1 & 2 & 9 \\ 3 & 1 & 2 & 2 & 1 \\ 1 & 0 & 0 & 1 & 0 \\ 3 & 1 & 2 & 0 & 3 \end{pmatrix}.$$

Вычислить $H(\xi)$, $H(\eta)$, $H(\xi|\eta)$, $H(\eta|\xi)$, $H(\xi, \eta)$ и $\mathbf{I}(\xi, \eta)$.

2. Случайная величина ξ имеет ряд распределения

ξ	-2	-1	0	2
$\mathbf{P}_\xi$	¼	3/8	¼	1/8

а случайная величина η – ряд распределения

η	-1	0	1
$\mathbf{P}_\eta$	2/9	1/9	2/3

Величины ξ и η не зависят друг от друга. Значение случайной величины χ определяется по формуле $\chi = (2\xi + \eta)^2$. Вычислить $H(\chi|\xi)$, $H(\chi|\eta)$, $\mathbf{I}(\chi, \xi)$ и $\mathbf{I}(\chi, \eta)$.

Тема 2: Дискретные источники сообщений

1. Дискретный источник генерирует сообщения из символов алфавита $\mathcal{A} = \{0, 1\}$. Вероятность появления символа на первой позиции сообщения такова:

A_1	0	1
$\mathbf{P}(A_1)$	¼	3/4

Вероятность появления символа на второй позиции сообщения описывается следующей таблицей переходных вероятностей:

A_1 \ A_2	0	1
0	1/2	½
1	3/8	5/8

Таблица переходных вероятностей для третьего символа сообщения такова:

A_1, A_2 \ A_3	0	1
00	1/8	7/8
10	½	½
01	1	0
11	¾	1/4

Вычислить H_1, H_2, H_3, $H^{(1)}$, $H^{(2)}$ и $H^{(3)}$.

2. Для простого марковского источника, у которого матрица переходных вероятностей

$$Q = \begin{pmatrix} 5/6 & 0 & 1/6 \\ 2/9 & 7/18 & 7/18 \\ 1/6 & 4/9 & 7/18 \end{pmatrix},$$

найти такое распределение начальных вероятностей $\vec{p} = (p_1, p_2, p_3)$, при котором этот источник является стационарным, и вычислить для него H_1, H_2, H_3, H_4, $H^{(1)}$, $H^{(2)}$, $H^{(3)}$, $H^{(4)}$ и H_∞.

8.3. Перечень вопросов и заданий для промежуточной аттестации по дисциплине

Вопросы для промежуточного контроля (зачета)

1. Предмет теории информации. Дискретные случайные величины.
2. Собственная, условная и взаимная информация.
3. Энтропия дискретной случайной величины.
4. Аксиомы Хинчина и Фаддеева. Энтропия вероятностной схемы.
5. Свойства энтропии: симметричность, непрерывность, нижняя и верхняя границы, выпуклость.
6. Совместная энтропия двух и более дискретных случайных величин.
7. Условная энтропия и её свойства: аддитивность, правило цепочки, основные неравенства, полуаддитивность, невозрастание при отображении.
8. Взаимная информация и её свойства.
9. Средняя взаимная информация: определение, простейшие свойства.
10. Условная средняя взаимная информация: определение, неотрицательность, условие равенства нулю.
11. Сопоставление различных подходов к определению энтропии.
12. Система аксиом об энтропии по Шеннону. Теорема о единственности функции, удовлетворяющей шенноновской системе аксиом об энтропии.
13. Математическая модель источника сообщений: случайный процесс с дискретным временем и конечным множеством состояний.
14. Цилиндрические множества, условия согласованности и теорема существования продолжения вероятностной меры (без доказательства).

15. Примеры дискретных источников сообщения: источник без памяти, простой марковский источник, марковский источник с заданной глубиной зависимости.
16. Энтропия H_k, приходящаяся на одну букву сообщения, и условная энтропия $H^{(k)}$ последней буквы сообщения: определение и основные свойства. Предельная энтропия H_∞.
17. Энтропия H_k, $H^{(k)}$ и H_∞ для простого источника без памяти.
18. Стационарные источники. Стационарность источника без памяти. Условие стационарности простого марковского источника.
19. Свойства энтропии H_k и $H^{(k)}$ для стационарных источников. Существование предельной энтропии H_∞ для стационарных источников.
20. Значение энтропии H_k, $H^{(k)}$ и H_∞ для простого стационарного марковского источника.
21. Свойство асимптотической равнораспределённости: определение, оценка мощности множества типичных ε-последовательностей, примеры.
22. Теорема об асимптотической равнораспределённости для источника без памяти.
23. Эргодическая теорема для регулярного простого марковского источника (без доказательства).
24. Закон больших чисел для частот биграмм в последовательностях, порождаемых стационарным и регулярным простым марковским источником.
25. Теорема об асимптотической равнораспределённости для стационарного и регулярного простого марковского источника.
26. Теорема об асимптотической оценке числа высоковероятных последовательностей, порождаемых источником со свойством асимптотической равнораспределённости.
27. Сжимающее кодирование последовательностей, порождаемых источником со свойством асимптотической равнораспределённости.
28. Алфавитное кодирование. Однозначно декодируемые, префиксные и суффиксные коды.
29. Теорема о соответствии между префиксными кодами и кодовыми деревьями.
30. Необходимое и достаточное условие существования префиксного кода с заданными длинами кодовых слов – неравенство Крафта.
31. Необходимое и достаточное условие однозначного декодирования – неравенство Мак-Миллана.
32. Граница Симмонса. Оптимальное кодирование. Задача оптимального кодирования.
33. Теорема об оценке средней длины оптимального префиксного кода.
34. Теорема о пределе средней длины кодового слова при кодировании длинных блоков.
35. Алгоритмы Фано и Хаффмана. Леммы о строении оптимального кода.
36. Теорема об оптимальности кода Хаффмана.
37. Математическая модель канала связи и его информационные характеристики.
38. Дискретный стационарный канал без памяти (ДСКБП). Примеры: двоичный симметричный канал, канал со стиранием.
39. Определение пропускной способности. Теоремы о пропускной способности последовательного соединения, параллельного соединения и суммы двух ДСКБП.
40. Симметричные каналы связи. Утверждения о пропускной способности симметричных каналов. Примеры вычисления пропускной способности.
41. Скорость передачи информации.
42. Декодер общего вида и решающие области.
43. Ошибочное декодирование, условная и средняя вероятности ошибочного декодирования.
44. Неравенство Фано. Свойства функции Фано.
45. Обратная теорема кодирования для ДСКБП.
46. Типичные входные и выходные векторы и пары векторов.

47. Декодер типичных пар. Леммы о совместной асимптотической равнораспределённости.
48. Прямая теорема кодирования для ДКБП.

8.4. Планируемые уровни сформированности компетенций обучающихся и критерии оценивания

Уровни	Содержательное описание уровня	Основные признаки выделения уровня (этапы формирования компетенции, критерии оценки сформированности)	Пятибалльная шкала (академическая) оценка	Двухбалльная шакала, зачет	БРС, % освоения (рейтинговая оценка)
Повышенный	Творческая деятельность	*Включает нижестоящий уровень.* Умение самостоятельно принимать решение, решать проблему/задачу теоретического и прикладного характера на основе изученных методов, приемов, технологий	отлично	зачтено	86-100
Базовый	Применение знаний и умений в более широких контекстах учебной и профессиональной деятельности, нежели по образцу с большей степени самостоятель	*Включает нижестоящий уровень.* Способность собирать, систематизировать, анализировать и грамотно использовать информацию из самостоятельно найденных теоретических	хорошо		71-85

	ности и инициативы	источников и иллюстрировать ими теоретические положения или обосновывать практику применения			
Удовлетворительный (достаточный)	Репродуктивная деятельность	Изложение в пределах задач курса теоретически и практически контролируемого материала	удовлетворительно		55-70
Недостаточный	Отсутствие признаков удовлетворительного уровня		неудовлетворительно	не зачтено	Менее 55

9. Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины.

Основная литература

1. Котенко В.В., Румянцев К.Е. Теория информации. Учебное пособие ВО: специалитет, изд-во ЮФУ, 2018г., 239 с. Имеются экземпляры в отделах / There are copies in departments: ЭБС «Znanium» (https://znanium.com/catalog/document?id=343835)

Дополнительная литература

1. Исаев, С.В. Интеллектуальные системы : учеб. пособие / С.В. Исаев, О.С. Исаева. - Красноярск : Сиб. федер. ун-т, 2017. - 120 с. - ISBN 978-5-7638-3781-0. - Текст : электронный. - URL: https://znanium.com/catalog/product/1032129 (дата обращения: 26.04.2022). – Режим доступа: по подписке.

10. Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины (модуля).

- ЭБС Кантиана (https://lib.kantiana.ru/).
- Научная электронная библиотека eLIBRARY.RU (https://elibrary.ru/defaultx.asp).
- Электронно-библиотечная система «Знаниум» (https://znanium.com/)
- Учебно-методический комплекс по теории информации, размещенный на портале БФУ им. И.Канта (https://kantiana.ru/).

11. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине.

Программное обеспечение обучения включает в себя:

- система электронного образовательного контента БФУ им. И. Канта – www.lms-3.kantiana.ru, обеспечивающую разработку и комплексное использование электронных образовательных ресурсов;
- серверное программное обеспечение, необходимое для функционирования сервера и связи с системой электронного обучения через Интернет;
- корпоративная платформа Microsoft Teams;
- установленное на рабочих местах обучающихся ПО: Microsoft Windows 7, Microsoft Office Standart 2010, антивирусное программное обеспечение Kaspersky Endpoint Security.
- специализированное ПО не требуется.

12. Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине.

Для проведения занятий лекционного типа, практических и семинарских занятий используются специальные помещения (учебные аудитории), оборудованные техническими средствами обучения – мультимедийной проекционной техникой. Для проведения занятий лекционного типа используются наборы демонстрационного оборудования.

Для проведения лабораторных работ, (практических занятий – при необходимости) используются специальные помещения (учебные аудитории), оснащенные специализированным лабораторным оборудованием: персональными компьютерами с возможностью выхода в интернет и с установленным программным обеспечением, заявленным в п. 11.

Для проведения групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации используются специальные помещения (учебные аудитории), оборудованные специализированной мебелью (для обучающихся), меловой / маркерной доской.

Для организации самостоятельной работы обучающимся предоставляются помещения, оснащенные компьютерной техникой с возможностью подключения к сети «Интернет» и обеспечением доступа в электронную информационно-образовательную среду университета.

Для обучения инвалидов и лиц с ограниченными возможностями здоровья университетом могут быть представлены специализированные средства обучения, в том числе технические средства коллективного и индивидуального пользования.

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

федеральное государственное автономное образовательное учреждение высшего образования «Балтийский федеральный университет имени Иммануила Канта»

Институт физико-математических наук и информационных технологий

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

«Организационное и правовое обеспечение информационной безопасности»

Шифр: 10.05.01

Специальность: «Компьютерная безопасность»

Специализация: «Математические методы защиты информации»

Квалификация (степень) выпускника: Специалист по защите информации

Калининград

2022

Лист согласования

Составитель: Ветров Игорь Анатольевич, к.т.н., доцент

Рабочая программа утверждена на заседании учебно-методического совета института физико-математических наук и информационных технологий
Протокол № 01/22 от «01» февраля 2022 г.

Председатель учебно-методического
совета института физико-
математических наук и
информационных технологий
Первый заместитель директора Шпилевой А. А
ИФМНиИТ, к. ф.-м. н., доцент

Ведущий менеджер
Е.П.Ставицкая

Содержание

1. Наименование дисциплины «Организационное и правовое обеспечение информационной безопасности»

Целью изучения дисциплины «*Организационное и правовое обеспечение информационной безопасности*» является получение знаний по изучению основ правового регулирования отношений в информационной сфере; конституционных гарантий прав граждан на получение информации и механизма их реализации; понятий и видов защищаемой информации по законодательству РФ; системы защиты государственной тайны; основ правового регулирования отношений в области интеллектуальной собственности и способов защиты этой собственности; понятий и видов компьютерных преступлений, а также приобретение студентами знаний по организационному обеспечению защиты информации и обеспечение освоения студентами практических навыков работы с нормативными правовыми актами в области обеспечения информационной безопасности компьютерных систем, в том числе нормативными методическими документами ФСБ России и ФСТЭК России, и применения их положений в профессиональной деятельности

2. Перечень планируемых результатов обучения по дисциплине, соотнесенных с планируемыми результатами освоения образовательной программы

Код компетенции	Результаты освоения образовательной программы (ИДК)	Результаты обучения по дисциплине
ОПК – 5: Способность применять нормативные правовые акты, нормативные и методические документы, регламентирующие деятельность по защите информации	ОПК-5.1. Демонстрирует знание нормативных правовых актов, нормативных и методических документов, регламентирующих деятельность по защите информации в организации; классифицирует и оценивает угрозы информационной безопасности для объекта информатизации. ОПК-5.2. Формулирует основные требования по защите конфиденциальной информации, персональных данных и охране результатов интеллектуальной деятельности в организации ОПК-5.3. Анализирует и разрабатывает проекты локальных правовых актов, инструкций, регламентов и организационно-распорядительных документов, регламентирующих работу по обеспечению информационной безопасности в организации.	***знать:*** - правовые основы и нормативные документы по организации защиты государственной тайны и конфиденциальной информации, задачи органов защиты государственной тайны; - правовые нормы и стандарты по лицензированию в области обеспечения защиты государственной тайны и сертификации средств защиты информации; - основные отечественные и зарубежные стандарты в области компьютерной безопасности; - терминологию, основные руководящие и регламентирующие документы в области ЭВМ, комплексов и систем; - принципы формирования политики информационной безопасности в компьютерной сфере; ***уметь:*** - применять действующую законодательную базу в области обеспечения компьютерной безопасности; - классифицировать защищаемую

		информацию по видам тайн и степеням конфиденциальности; ***владеть:*** - навыками работы с нормативными правовыми актами; - навыками работы с технической документацией на ЭВМ и вычислительных системах; - навыками работы с технической документацией на компонентах информационных систем на русском и иностранном языках.
ОПК – 6: Способность при решении профессиональных задач организовывать защиту информации ограниченного доступа в компьютерных системах и сетях в соответствии с нормативными правовыми актами и нормативными методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю	ОПК-6.1. Понимает угрозы безопасности информации и возможные пути их реализации, нормативные правовые акты, нормативные и методические документы Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю. ОПК-6.2. Способен организовать защиту информации ограниченного доступа в соответствии с нормативными правовыми актами, нормативными и методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю. ОПК-6.3. Обладает навыками организации защиты информации ограниченного доступа в соответствии с нормативными правовыми актами, нормативными и методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю.	***Знать:*** - направления создания правовой базы в области информационной безопасности; - области применения полученных навыков в рамках реальной практической деятельности с пониманием границ их применимости; - особенности обеспечения информационной безопасности компьютерных систем при обработке информации, составляющей государственную тайну; - программные и аппаратные средства обеспечения информационной безопасности в типовых компьютерных сетях, операционных системах, системах управления базами данных; - современные подходы к построению систем защиты информации в компьютерных системах; - нормативную базу эксплуатации и эксплуатационную документацию компьютерных систем; ***Уметь:*** - разрабатывать, реализовывать, оценивать и корректировать процессы менеджмента информационной безопасности; разрабатывать предложения по совершенствованию системы управления информационной безопасностью компьютерных систем; - пользоваться современной научно-технической информацией по исследуемым проблемам и задачам; - отыскивать необходимые нормативные правовые акты и информационно-правовые нормы в системе действующего законодательства, в том числе с помощью систем правовой

		информации; - разрабатывать проекты нормативных материалов, регламентирующих работу по защите информации, а также положений, инструкций и других организационно-распорядительных документов; - применять действующую законодательную базу в области компьютерной безопасности; - проводить выбор программно-аппаратных средств обеспечения информационной безопасности для использования их в составе компьютерной системы с целью обеспечения требуемого уровня защищенности информационных систем; - выбирать и анализировать эксплуатационные показатели качества и критерии оценки подсистемы безопасности, а также отдельных методов и средств защиты информации. ***Владеть:*** - навыками работы с нормативными правовыми актами; с проектной и технической документацией на ЭВМ и вычислительные системы; - с технической документацией на компоненты компьютерных систем на русском и иностранном языках; - навыками поиска, систематизации, обобщения проектной, справочной, нормативно-технической информации, составления кратких отчетов, рефератов; - разработке специализированной проектной и технической документации; - навыками обоснования, выбора, реализации и контроля результатов управленческого решения; - навыками эксплуатации и администрирования (в части, касающейся разграничения доступа, аутентификации и аудита) баз данных, локальных компьютерных сетей, программных систем с учетом требований по обеспечению информационной безопасности; - навыками оценки надёжности и технической диагностики программно-аппаратных средств подсистем информационной

		безопасности компьютерных сетей.

3. Место дисциплины в структуре образовательной программы

«*Организационное и правовое обеспечение информационной безопасности*» представляет собой дисциплину обязательной части блока 1 «Дисциплины (модули)» (Б1.О.09.03), входит в Модуль 5 «Дополнительные разделы дискретной математики» дисциплин специальности 10.05.01 «Компьютерная безопасность», специализация «Математические методы защиты информации».

4. Виды учебной работы по дисциплине

Виды учебной работы по дисциплине зафиксированы учебным планом основной профессиональной образовательной программы по указанному направлению и профилю, выражаются в академических часах. Часы контактной работы и самостоятельной работы обучающегося и часы, отводимые на процедуры контроля, могут различаться в учебных планах ОПОП по формам обучения. Объем контактной работы включает часы контактной аудиторной работы (лекции/практические занятия/ лабораторные работы), контактной внеаудиторной работы (контроль самостоятельной работы), часы контактной работы в период аттестации. Контактная работа, в том числе может проводиться посредством электронной информационно-образовательной среды университета с использованием ресурсов сети Интернет и дистанционных технологий

5. Содержание дисциплины, в том числе практической подготовки в рамках дисциплины, структурированное по темам

Исходя из рамок, установленных учебным планом по трудоемкости и видам учебной работы по дисциплине, преподаватель самостоятельно выбирает тематику занятий по формам и количеству часов проведения контактной работы: лекции и иные учебные занятия, предусматривающие преимущественную передачу учебной информации преподавателем и (или) занятия семинарского типа (семинары, практические занятия, практикумы, лабораторные работы, коллоквиумы и иные аналогичные занятия), и (или) групповые консультации, и (или) индивидуальную работу обучающихся с преподавателем, в том числе индивидуальные консультации (по курсовым работам/проектам – при наличии курсовой работы/проекта по данной дисциплине в учебном плане). Рекомендуемая тематика занятий максимально полно реализуется в контактной работе с обучающимися очной формы обучения. В случае реализации образовательной программы в заочной / очно-заочной форме трудоемкость дисциплины сохраняется, однако объем учебного материала в значительной части осваивается обучающимися в форме самостоятельной работы. При этом требования к ожидаемым образовательным результатам обучающихся по данной дисциплине не зависят от формы реализации образовательной программы.

№ п/п	Наименование Темы	Содержание темы
1	Информационные отношения как объект правового регулирования.	Структура информационной сферы и характеристика ее элементов. Информация как объект правоотношений. Категории информации по условиям доступа к ней и распространения. Конституционные гарантии прав граждан в информационной сфере и механизм их реализации.

	Законодательство РФ в области информационной безопасности	Понятие информационной безопасности. Субъекты и объекты правоотношений в области информационной безопасности. Система нормативных правовых актов, регулирующих обеспечение информационной безопасности в Российской Федерации Понятие и виды защищаемой информации по законодательству РФ. Перспективы развития законодательства в области информационной безопасности.
2	Правовой режим защиты государственной тайны. Правовые режимы защиты информации конфиденциального характера	Государственная тайна как особый вид защищаемой информации и ее характерные признаки. Понятие правового режима защиты государственной тайны. Система нормативных правовых актов, регламентирующих обеспечение сохранности сведений, составляющих государственную тайну в Российской Федерации. Принципы и механизмы отнесения сведений к государственной тайне, их засекречивания и рассекречивания. Органы защиты государственной тайны и их компетенция. Организационные меры, направленные на защиту государственной тайны. Порядок допуска и доступа к государственной тайне. Иные меры по обеспечению сохранности сведений, составляющих государственную тайну (режим секретности как основной порядок деятельности в сфере защиты государственной тайны). Система контроля за состоянием защиты государственной тайны. Юридическая ответственность за нарушения правового режима защиты государственной тайны (уголовная, административная, дисциплинарная). Понятие «конфиденциальной» информации по российскому законодательству. Основные виды «конфиденциальной» информации: персональные данные, служебная тайна, коммерческая тайна, банковская тайна, тайна следствия и судопроизводства, профессиональная тайна. Правовые режимы «конфиденциальной» информации: содержание и особенности. Основные требования, предъявляемые к организации защиты конфиденциальной информации. Юридическая ответственность за нарушения правовых режимов конфиденциальной информации (уголовная, административная, гражданско-правовая, дисциплинарная).
3	Государственное регулирование деятельности в области защиты информации. Нормы международного права в информационной сфере	Понятие лицензирования по российскому законодательству. Виды деятельности, подлежащие лицензированию. Правовая регламентация лицензионной деятельности в области обеспечения информационной безопасности. Объекты лицензирования и участники лицензионных отношений в сфере защиты информации. Органы лицензирования и их полномочия. Организация лицензирования в сфере обеспечения информационной безопасности. Контроль за соблюдением лицензиатами условий ведения деятельности. Понятие сертификации по российскому законодательству. Правовая регламентация сертификационной деятельности в области обеспечения информационной безопасности. Режимы сертификации. Объекты сертификационной деятельности (сертификации). Органы сертификации и их полномочия. Понятие международного информационного обмена. Законодательство РФ об участии в международном информационном обмене. Правовой режим участия в международном обмене. Субъекты и объекты международного информационного обмена. Международное право в сфере телекоммуникаций и связи. Международно-правовые нормы в деятельности средств массовой информации. Международно-правовые

		аспекты защиты прав и свобод личности в связи с применением современных информационных технологий. Международное сотрудничество в области борьбы с преступностью в сфере высоких технологий.
4	Правовая охрана результатов интеллектуальной деятельности	Законодательство РФ об интеллектуальных правах. Интеллектуальные права: понятие, виды. Авторское право. Объекты и субъекты авторского права. Исключительные авторские права. Правовая охрана программ для ЭВМ, баз данных, топологий интегральных микросхем и единых технологий. Лицензии операционных систем (Unix, Linux, Windows).Защита интеллектуальных прав.
5	Преступления в сфере компьютерной информации	Преступления в сфере компьютерной информации. Признаки и элементы состава преступления. Криминалистическая характеристика преступлений в сфере компьютерной информации. Расследование преступлений в сфере компьютерной информации. Особенности основных следственных действий. Криминалистические аспекты проведения расследования. Сбор доказательств. Экспертиза преступлений в сфере компьютерной информации. Проблемы судебного преследования за преступления в сфере компьютерной информации.
6	Понятие организационной защиты информации	Сущность организационных методов защиты информации. Соотношение организационных методов защиты информации с правовыми и техническими. Понятие «режим защиты информации». Режим защиты информации как составная часть организационной защиты информации. Модели систем и процессов обеспечения информационной безопасности. Анализ и оценка угроз информации. Понятие системы защиты информации. Анализ риска. Защита информации от стихийных бедствий. Наводнение. Землетрясение. Ураган. Противопожарная защита. Отключение коммуникаций: электроэнергия, канализация, газ, телефон, вода, каналы связи.
7	Политика информационной безопасности. Методы обеспечения физической безопасности.	Составляющие политики информационной безопасности предприятий. Объекты обеспечения физической безопасности: сооружения, предметы, люди. Проектирование здания. Охрана территории. Охрана здания. Сигнализация. Противостояние взлому: двери, замки, запоры, ограждения. Безопасность при транспортировке носителей информации. Личная безопасность сотрудников и членов их семей. Защита документов от подделок. Обнаружение фальсификации документов. Предварительная защита документов. Приборы и методы контроля документов. Хранилища. Сейфы. Запирающие устройства. Физическая защита неподвижных объектов. Пропускной режим.
8	Технологические методы поддержания безопасности	Проблема безопасности технологии. Организация работы персонала. Резервирование оборудования и дублирование информации. Система инструкций и правил. Администрирование технологического процесса. Контроль доступа и средства поиска и досмотра. Системы контроля доступа. Технология считывания ключей. Средства поиска и досмотра. Обнаружение металлов и взрывчатки. Обнаружители наркотиков. Обнаружители газов и отравляющих веществ. Обнаружители радиоактивных веществ.
9	Организация режима секретности	Организационные меры, направленные на защиту государственной тайны. Режим секретности как основной порядок деятельности в сфере защиты государственной тайны. Виды представления информации. Пути прохождения информации. Учет получения, перемещения, преобразования, хранения и уничтожения информации. Секретариаты. Первые отделы. Служба собственной безопасности. Категорирование объектов. Подбор и расстановка кадров.
10	Допуск к	Порядок допуска и доступа к государственной тайне. Основные принципы

	государственной тайне	допускной работы. Номенклатура должностей работников, подлежащих оформлению на допуск и порядок ее составления и утверждения. Документальное оформление для отправки на согласование. Процедура оформления и переоформления допусков и ее документирование, подлежащие согласованию с органами государственной безопасности. Особенности инструктажа и документальное оформление контракта об оформлении допуска к государственной тайне.
11	Защита компьютерной информации. Основные каналы утечки информации при обработке на компьютерах.	Технологическая схема обработки информации. Основные каналы утечки информации при обработке на компьютерах. Аппаратные закладки. Виброаккустический канал утечки информации. Визуальный канал утечки информации. Программные и аппаратные средства защиты от несанкционированного доступа. Парольная система доступа. Защита на различных уровнях: операционная система, прикладные программы. Программные закладки. Разграничение доступа. Регистрация. Остаточная информация. Защита от копирования. Вирусы. Антивирусные программы и основные способы защиты от вирусов.

6. Рекомендуемая тематика учебных занятий в форме контактной работы

Учебно-методическое обеспечение для самостоятельной работы обучающихся составляют:

1. Материалы лекций.
2. Материалы практических занятий.
3. Информационные ресурсы «Интернет» (сайты ФСТЭК России, ФСБ России, Консультант плюс и др.)
4. Методические рекомендации и указания.
5. Фонды оценочных средств.
6. Учебники и учебно-методические пособия.

Рекомендуемая тематика учебных занятий *лекционного* типа (предусматривающих преимущественную передачу учебной информации преподавателями):

№ п/п	**Наименование Темы**	**Содержание темы**
1	Информационные отношения как объект правового регулирования. Законодательство РФ в области информационной безопасности	Структура информационной сферы и характеристика ее элементов. Информация как объект правоотношений. Категории информации по условиям доступа к ней и распространения. Конституционные гарантии прав граждан в информационной сфере и механизм их реализации. Понятие информационной безопасности. Субъекты и объекты правоотношений в области информационной безопасности. Система нормативных правовых актов, регулирующих обеспечение информационной безопасности в Российской Федерации Понятие и виды защищаемой информации по законодательству РФ. Перспективы развития законодательства в области информационной безопасности.
2	Правовой режим защиты государственной тайны. Правовые	Государственная тайна как особый вид защищаемой информации и ее характерные признаки. Понятие правового режима защиты государственной тайны. Система нормативных правовых актов, регламентирующих обеспечение сохранности сведений, составляющих

	режимы защиты информации конфиденциального характера	государственную тайну в Российской Федерации. Принципы и механизмы отнесения сведений к государственной тайне, их засекречивания и рассекречивания. Органы защиты государственной тайны и их компетенция. Организационные меры, направленные на защиту государственной тайны. Порядок допуска и доступа к государственной тайне. Иные меры по обеспечению сохранности сведений, составляющих государственную тайну (режим секретности как основной порядок деятельности в сфере защиты государственной тайны). Система контроля за состоянием защиты государственной тайны. Юридическая ответственность за нарушения правового режима защиты государственной тайны (уголовная, административная, дисциплинарная). Понятие «конфиденциальной» информации по российскому законодательству. Основные виды «конфиденциальной» информации: персональные данные, служебная тайна, коммерческая тайна, банковская тайна, тайна следствия и судопроизводства, профессиональная тайна. Правовые режимы «конфиденциальной» информации: содержание и особенности. Основные требования, предъявляемые к организации защиты конфиденциальной информации. Юридическая ответственность за нарушения правовых режимов конфиденциальной информации (уголовная, административная, гражданско-правовая, дисциплинарная).
3	Государственное регулирование деятельности в области защиты информации. Нормы международного права в информационной сфере	Понятие лицензирования по российскому законодательству. Виды деятельности, подлежащие лицензированию. Правовая регламентация лицензионной деятельности в области обеспечения информационной безопасности. Объекты лицензирования и участники лицензионных отношений в сфере защиты информации. Органы лицензирования и их полномочия. Организация лицензирования в сфере обеспечения информационной безопасности. Контроль за соблюдением лицензиатами условий ведения деятельности. Понятие сертификации по российскому законодательству. Правовая регламентация сертификационной деятельности в области обеспечения информационной безопасности. Режимы сертификации. Объекты сертификационной деятельности (сертификации). Органы сертификации и их полномочия. Понятие международного информационного обмена. Законодательство РФ об участии в международном информационном обмене. Правовой режим участия в международном обмене. Субъекты и объекты международного информационного обмена. Международное право в сфере телекоммуникаций и связи. Международно-правовые нормы в деятельности средств массовой информации. Международно-правовые аспекты защиты прав и свобод личности в связи с применением современных информационных технологий. Международное сотрудничество в области борьбы с преступностью в сфере высоких технологий.
4	Правовая охрана результатов интеллектуальной деятельности	Законодательство РФ об интеллектуальных правах. Интеллектуальные права: понятие, виды. Авторское право. Объекты и субъекты авторского права. Исключительные авторские права. Правовая охрана программ для ЭВМ, баз данных, топологий интегральных микросхем и единых технологий. Лицензии операционных систем (Unix, Linux, Windows).Защита интеллектуальных прав.

5	Преступления в сфере компьютерной информации	Преступления в сфере компьютерной информации. Признаки и элементы состава преступления. Криминалистическая характеристика преступлений в сфере компьютерной информации. Расследование преступлений в сфере компьютерной информации. Особенности основных следственных действий. Криминалистические аспекты проведения расследования. Сбор доказательств. Экспертиза преступлений в сфере компьютерной информации. Проблемы судебного преследования за преступления в сфере компьютерной информации.
6	Понятие организационной защиты информации	Сущность организационных методов защиты информации. Соотношение организационных методов защиты информации с правовыми и техническими. Понятие «режим защиты информации». Режим защиты информации как составная часть организационной защиты информации. Модели систем и процессов обеспечения информационной безопасности. Анализ и оценка угроз информации. Понятие системы защиты информации. Анализ риска. Защита информации от стихийных бедствий. Наводнение. Землетрясение. Ураган. Противопожарная защита. Отключение коммуникаций: электроэнергия, канализация, газ, телефон, вода, каналы связи.
7	Политика информационной безопасности. Методы обеспечения физической безопасности.	Составляющие политики информационной безопасности предприятий. Объекты обеспечения физической безопасности: сооружения, предметы, люди. Проектирование здания. Охрана территории. Охрана здания. Сигнализация. Противостояние взлому: двери, замки, запоры, ограждения. Безопасность при транспортировке носителей информации. Личная безопасность сотрудников и членов их семей. Защита документов от подделок. Обнаружение фальсификации документов. Предварительная защита документов. Приборы и методы контроля документов. Хранилища. Сейфы. Запирающие устройства. Физическая защита неподвижных объектов. Пропускной режим.
8	Технологические методы поддержания безопасности	Проблема безопасности технологии. Организация работы персонала. Резервирование оборудования и дублирование информации. Система инструкций и правил. Администрирование технологического процесса. Контроль доступа и средства поиска и досмотра. Системы контроля доступа. Технология считывания ключей. Средства поиска и досмотра. Обнаружение металлов и взрывчатки. Обнаружители наркотиков. Обнаружители газов и отравляющих веществ. Обнаружители радиоактивных веществ.
9	Организация режима секретности	Организационные меры, направленные на защиту государственной тайны. Режим секретности как основной порядок деятельности в сфере защиты государственной тайны. Виды представления информации. Пути прохождения информации. Учет получения, перемещения, преобразования, хранения и уничтожения информации. Секретариаты. Первые отделы. Служба собственной безопасности. Категорирование объектов. Подбор и расстановка кадров.
10	Допуск к государственной тайне	Порядок допуска и доступа к государственной тайне. Основные принципы допускной работы. Номенклатура должностей работников, подлежащих оформлению на допуск и порядок ее составления и утверждения. Документальное оформление для отправки на согласование. Процедура оформления и переоформления допусков и ее документирование, подлежащие согласованию с органами государственной безопасности. Особенности инструктажа и документальное оформление контракта об оформлении допуска к государственной тайне.
11	Защита компьютерной информации.	Технологическая схема обработки информации. Основные каналы утечки информации при обработке на компьютерах. Аппаратные закладки. Виброаккустический канал утечки информации. Визуальный канал утечки информации. Программные и аппаратные средства защиты от несанкциони-

	Основные каналы утечки информации при обработке на компьютерах.	рованного доступа. Парольная система доступа. Защита на различных уровнях: операционная система, прикладные программы. Программные закладки. Разграничение доступа. Регистрация. Остаточная информация. Защита от копирования. Вирусы. Антивирусные программы и основные способы защиты от вирусов.

Тематика практических занятий

№ п/п	**Наименование Темы**	**Содержание темы**
1	Информационные отношения как объект правового регулирования. Законодательство РФ в области информационной безопасности	Структура информационной сферы и характеристика ее элементов. Информация как объект правоотношений. Категории информации по условиям доступа к ней и распространения. Конституционные гарантии прав граждан в информационной сфере и механизм их реализации. Понятие информационной безопасности. Субъекты и объекты правоотношений в области информационной безопасности. Система нормативных правовых актов, регулирующих обеспечение информационной безопасности в Российской Федерации Понятие и виды защищаемой информации по законодательству РФ. Перспективы развития законодательства в области информационной безопасности.
2	Правовой режим защиты государственной тайны. Правовые режимы защиты информации конфиденциального характера	Государственная тайна как особый вид защищаемой информации и ее характерные признаки. Понятие правового режима защиты государственной тайны. Система нормативных правовых актов, регламентирующих обеспечение сохранности сведений, составляющих государственную тайну в Российской Федерации. Принципы и механизмы отнесения сведений к государственной тайне, их засекречивания и рассекречивания. Органы защиты государственной тайны и их компетенция. Организационные меры, направленные на защиту государственной тайны. Порядок допуска и доступа к государственной тайне. Иные меры по обеспечению сохранности сведений, составляющих государственную тайну (режим секретности как основной порядок деятельности в сфере защиты государственной тайны). Система контроля за состоянием защиты государственной тайны. Юридическая ответственность за нарушения правового режима защиты государственной тайны (уголовная, административная, дисциплинарная). Понятие «конфиденциальной» информации по российскому законодательству. Основные виды «конфиденциальной» информации: персональные данные, служебная тайна, коммерческая тайна, банковская тайна, тайна следствия и судопроизводства, профессиональная тайна. Правовые режимы «конфиденциальной» информации: содержание и особенности. Основные требования, предъявляемые к организации защиты конфиденциальной информации. Юридическая ответственность за нарушения правовых режимов конфиденциальной информации (уголовная, административная, гражданско-правовая, дисциплинарная).
3	Государственное регулирование деятельности в области защиты	Понятие лицензирования по российскому законодательству. Виды деятельности, подлежащие лицензированию. Правовая регламентация лицензионной деятельности в области обеспечения информационной безопасности. Объекты лицензирования и участники лицензионных

	информации. Нормы международного права в информационной сфере	отношений в сфере защиты информации. Органы лицензирования и их полномочия. Организация лицензирования в сфере обеспечения информационной безопасности. Контроль за соблюдением лицензиатами условий ведения деятельности. Понятие сертификации по российскому законодательству. Правовая регламентация сертификационной деятельности в области обеспечения информационной безопасности. Режимы сертификации. Объекты сертификационной деятельности (сертификации). Органы сертификации и их полномочия. Понятие международного информационного обмена. Законодательство РФ об участии в международном информационном обмене. Правовой режим участия в международном обмене. Субъекты и объекты международного информационного обмена. Международное право в сфере телекоммуникаций и связи. Международно-правовые нормы в деятельности средств массовой информации. Международно-правовые аспекты защиты прав и свобод личности в связи с применением современных информационных технологий. Международное сотрудничество в области борьбы с преступностью в сфере высоких технологий.
4	Правовая охрана результатов интеллектуальной деятельности	Законодательство РФ об интеллектуальных правах. Интеллектуальные права: понятие, виды. Авторское право. Объекты и субъекты авторского права. Исключительные авторские права. Правовая охрана программ для ЭВМ, баз данных, топологий интегральных микросхем и единых технологий. Лицензии операционных систем (Unix, Linux, Windows).Защита интеллектуальных прав.
5	Преступления в сфере компьютерной информации	Преступления в сфере компьютерной информации. Признаки и элементы состава преступления. Криминалистическая характеристика преступлений в сфере компьютерной информации. Расследование преступлений в сфере компьютерной информации. Особенности основных следственных действий. Криминалистические аспекты проведения расследования. Сбор доказательств. Экспертиза преступлений в сфере компьютерной информации. Проблемы судебного преследования за преступления в сфере компьютерной информации.
6	Понятие организационной защиты информации	Сущность организационных методов защиты информации. Соотношение организационных методов защиты информации с правовыми и техническими. Понятие «режим защиты информации». Режим защиты информации как составная часть организационной защиты информации. Модели систем и процессов обеспечения информационной безопасности. Анализ и оценка угроз информации. Понятие системы защиты информации. Анализ риска. Защита информации от стихийных бедствий. Наводнение. Землетрясение. Ураган. Противопожарная защита. Отключение коммуникаций: электроэнергия, канализация, газ, телефон, вода, каналы связи.
7	Политика информационной безопасности. Методы обеспечения физической безопасности.	Составляющие политики информационной безопасности предприятий. Объекты обеспечения физической безопасности: сооружения, предметы, люди. Проектирование здания. Охрана территории. Охрана здания. Сигнализация. Противостояние взлому: двери, замки, запоры, ограждения. Безопасность при транспортировке носителей информации. Личная безопасность сотрудников и членов их семей. Защита документов от подделок. Обнаружение фальсификации документов. Предварительная защита документов. Приборы и методы контроля документов. Хранилища. Сейфы. Запирающие устройства. Физическая защита неподвижных объектов. Пропускной режим.

8	Технологические методы поддержания безопасности	Проблема безопасности технологии. Организация работы персонала. Резервирование оборудования и дублирование информации. Система инструкций и правил. Администрирование технологического процесса. Контроль доступа и средства поиска и досмотра. Системы контроля доступа. Технология считывания ключей. Средства поиска и досмотра. Обнаружение металлов и взрывчатки. Обнаружители наркотиков. Обнаружители газов и отравляющих веществ. Обнаружители радиоактивных веществ.
9	Организация режима секретности	Организационные меры, направленные на защиту государственной тайны. Режим секретности как основной порядок деятельности в сфере защиты государственной тайны. Виды представления информации. Пути прохождения информации. Учет получения, перемещения, преобразования, хранения и уничтожения информации. Секретариаты. Первые отделы. Служба собственной безопасности. Категорирование объектов. Подбор и расстановка кадров.
10	Допуск к государственной тайне	Порядок допуска и доступа к государственной тайне. Основные принципы допускной работы. Номенклатура должностей работников, подлежащих оформлению на допуск и порядок ее составления и утверждения. Документальное оформление для отправки на согласование. Процедура оформления и переоформления допусков и ее документирование, подлежащие согласованию с органами государственной безопасности. Особенности инструктажа и документальное оформление контракта об оформлении допуска к государственной тайне.
11	Защита компьютерной информации. Основные каналы утечки информации при обработке на компьютерах.	Технологическая схема обработки информации. Основные каналы утечки информации при обработке на компьютерах. Аппаратные закладки. Виброаккустический канал утечки информации. Визуальный канал утечки информации. Программные и аппаратные средства защиты от несанкционированного доступа. Парольная система доступа. Защита на различных уровнях: операционная система, прикладные программы. Программные закладки. Разграничение доступа. Регистрация. Остаточная информация. Защита от копирования. Вирусы. Антивирусные программы и основные способы защиты от вирусов.

Тематика самостоятельных работ

№ п/п	**Наименование Темы**	**Содержание темы**
1	Информационные отношения как объект правового регулирования. Законодательство РФ в области информационной безопасности	Повторение теоретического материала, ознакомление с законодательной базой. Доработка конспекта. Ответы на контрольные вопросы по тематике занятия, подготовка к практическим занятиям.
2	Правовой режим защиты государственной тайны. Правовые режимы защиты информации	Повторение теоретического материала, ознакомление с законодательной базой. Доработка конспекта. Ответы на контрольные вопросы по тематике занятия, подготовка к практическим занятиям.

	конфиденциального характера	
3	Государственное регулирование деятельности в области защиты информации. Нормы международного права в информационной сфере	Повторение теоретического материала, ознакомление с законодательной базой. Доработка конспекта. Ответы на контрольные вопросы по тематике занятия, подготовка к практическим занятиям.
4	Правовая охрана результатов интеллектуальной деятельности	Повторение теоретического материала, ознакомление с законодательной базой. Доработка конспекта. Ответы на контрольные вопросы по тематике занятия, подготовка к практическим занятиям.
5	Преступления в сфере компьютерной информации	Повторение теоретического материала, ознакомление с законодательной базой. Доработка конспекта. Ответы на контрольные вопросы по тематике занятия, подготовка к практическим занятиям.
6	Понятие организационной защиты информации	Повторение теоретического материала, ознакомление с законодательной базой. Доработка конспекта. Ответы на контрольные вопросы по тематике занятия, подготовка к практическим занятиям.
7	Политика информационной безопасности. Методы обеспечения физической безопасности.	Повторение теоретического материала, ознакомление с законодательной базой. Доработка конспекта. Ответы на контрольные вопросы по тематике занятия, подготовка к практическим занятиям.
8	Технологические методы поддержания безопасности	Повторение теоретического материала, ознакомление с законодательной базой. Доработка конспекта. Ответы на контрольные вопросы по тематике занятия, подготовка к практическим занятиям.
9	Организация режима секретности	Повторение теоретического материала, ознакомление с законодательной базой. Доработка конспекта. Ответы на контрольные вопросы по тематике занятия, подготовка к практическим занятиям.
10	Допуск к государственной тайне	Повторение теоретического материала, ознакомление с законодательной базой. Доработка конспекта. Ответы на контрольные вопросы по тематике занятия, подготовка к практическим занятиям.
11	Защита компьютерной информации. Основные каналы утечки информации при обработке на компьютерах.	Повторение теоретического материала, ознакомление с законодательной базой. Доработка конспекта. Ответы на контрольные вопросы по тематике занятия, подготовка к практическим занятиям.

7. Методические рекомендации по видам занятий

Лекционные занятия.

В ходе лекционных занятий обучающимся рекомендуется выполнять следующие действия. Вести конспектирование учебного материала. Обращать внимание на категории, формулировки, раскрывающие содержание тех или иных явлений и процессов, научные выводы и практические рекомендации по их применению. Задавать преподавателю уточняющие вопросы с целью уяснения теоретических положений, разрешения спорных ситуаций.

Желательно оставить в рабочих конспектах поля, на которых во внеаудиторное время можно сделать пометки из рекомендованной литературы, дополняющие материал прослушанной лекции, а также подчеркивающие особую важность тех или иных теоретических положений.

Практические и семинарские занятия.

На практических и семинарских занятиях в зависимости от темы занятия выполняется поиск информации по решению проблем, практические упражнения, контрольные работы, выработка индивидуальных или групповых решений, итоговое обсуждение с обменом знаниями, участие в круглых столах, разбор конкретных ситуаций, командная работа, представление портфолио и т.п.

Самостоятельная работа.

Самостоятельная работа осуществляется в виде изучения литературы, эмпирических данных по публикациям и конкретных ситуаций из практики, подготовке индивидуальных работ, работа с лекционным материалом, самостоятельное изучение отдельных тем дисциплины; поиск и обзор литературы и электронных источников; чтение и изучение учебника и учебных пособий.

8. Фонд оценочных средств

8.1. Перечень компетенций с указанием этапов их формирования в процессе освоения образовательной программы в рамках учебной дисциплины

Код компетенции	Содержание компетенций
ОПК-5	Способность применять нормативные правовые акты, нормативные и методические документы, регламентирующие деятельность по защите информации
ОПК-6	Способность участвовать в разработке проектной и технической документации

Основными этапами формирования указанных компетенций при изучении студентами дисциплины являются последовательное изучение содержательно связанных между собой *разделов* (*тем*) учебных занятий. Изучение каждого раздела (темы) предполагает овладение студентами необходимыми компетенциями. Результат аттестации студентов на различных этапах формирования компетенций показывает уровень освоения компетенций студентами.

Паспорт фонда оценочных средств по дисциплине «*Организационно-правовое обеспечение информационной безопасности*»

Контролируемые модули, разделы (темы) дисциплины	**Индекс контролируемой компетенции (или ее части)**	**Оценочные средства по этапам формирования компетенций**
		текущий контроль по дисциплине

Тема 1. Информационные отношения как объект правового регулирования. Законодательство РФ в области информационной безопасности	ОПК-5 ОПК-6	Тестирование, устный опрос
Тема 2. Правовой режим защиты государственной тайны. Правовые режимы защиты информации конфиденциального характера	ОПК-5 ОПК-6	Тестирование, устный опрос
Тема 3. Государственное регулирование деятельности в области защиты информации. Нормы международного права в информационной сфере	ОПК-5 ОПК-6	Тестирование, устный опрос
Тема 4. Правовая охрана результатов интеллектуальной деятельности	ОПК-5 ОПК-6	Тестирование, устный опрос
Тема 5. Преступления в сфере компьютерной информации	ОПК-5 ОПК-6	Тестирование, устный опрос
Тема 6. Понятие организационной защиты информации	ОПК-5 ОПК-6	Тестирование, устный опрос
Тема 7. Политика информационной безопасности. Методы обеспечения физической безопасности.	ОПК-5 ОПК-6	Тестирование, устный опрос
Тема 8. Технологические методы поддержания безопасности	ОПК-5 ОПК-6	Тестирование, устный опрос
Тема 9. Организация режима секретности	ОПК-5 ОПК-6	Тестирование, устный опрос
Тема 10. Допуск к государственной тайне	ОПК-5 ОПК-6	Тестирование, устный опрос
Тема 11. Защита компьютерной информации. Основные каналы утечки информации при обработке на компьютерах.	ОПК-5 ОПК-6	Тестирование, устный опрос

8.2. Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений и навыков и (или) опыта деятельности процессе текущего контроля

8.2.1. Тестовые задания для самоконтроля

Целью тестирования является закрепление, углубление и систематизация знаний студентов, полученных на лекциях и в процессе самостоятельной работы; проведение тестирования позволяет ускорить контроль за усвоением знаний и объективизировать процедуру оценки знаний студента.

Тема 1. Информационные отношения как объект правового регулирования. Законодательство РФ в области информационной безопасности

	Вопрос теста	Варианты ответов
Оценка «удовлетворительно» (зачтено) или низкой уровень освоения компетенции	К основным видам информации по форме представления, способам кодирования и хранения относятся:	Графическая, звуковая, текстовая, числовая и видеоинформация
		Изобразительная, акустическая, текстовая, числовая и видеоинформация
		Графическая, звуковая, текстовая и числовая
		Изобразительная, звуковая, текстовая и видеоинформация
Оценка «хорошо» (зачтено) или повышенный уровень освоения компетенции	Какова основная цель защиты информации	Исключение её утечки
		Обеспечение её безопасности
		Выполнение требования обладателя информации
		Исключение или снижение возможного ущерба
Оценка «отлично» (зачтено) или высокий уровень освоения компетенции	Основными свойствами безопасности информации являются:	Конфиденциальность, целостность, доступность
		Актуальность, значимость, оперативность
		Точность, важность, полнота
		Защищённость, надёжность, устойчивость

Тема 2. Правовой режим защиты государственной тайны. Правовые режимы защиты информации конфиденциального характера

	Вопрос теста	Варианты ответов
Оценка «удовлетворительно» (зачтено) или низкой уровень освоения компетенции	Перечень сведений, отнесённых к государственной тайне предназначен для	Определения степени секретности сведений, дате и условиях их рассекречивания
		Определения степени секретности сведений, месте, дате и условиях их рассекречивания
		Определения категорий сведений, отнесённых к государственной тайне
		Определения категорий сведений, отнесённых к государственной тайне, и распределения полномочий между министерствами и ведомствами по распоряжению сведениями
Оценка «хорошо» (зачтено) или повышенный уровень освоения компетенции	Федеральным законом, регулирующим отношения, возникающие при применении информационных технологий и обеспечения защиты информации является:	ФЗ «Об участии в международном информационном обмене»
		ФЗ «Об информации, информационных технологиях и о защите информации»
		ФЗ «Об информации, информатизации и защите информации»
		ФЗ «О техническом регулировании»
Оценка «отлично» (зачтено) или высокий уровень освоения компетенции	Информация по категории доступа классифицируется как	Конфиденциальная
		Общедоступная
		Особо конфиденциальная
		Широкого доступа
		Ограниченного доступа

Тема 3. Государственное регулирование деятельности в области защиты информации. Нормы международного права в информационной сфере

	Вопрос теста	Варианты ответов
Оценка «удовлетворительно» (зачтено) или низкой уровень освоения компетенции	Необходимость получения лицензии на осуществление работ, связанных с использованием сведений, составляющих государственную тайну, определяет:	Закон РФ «О государственной тайне» ФЗ «О лицензировании отдельных видов деятельности» ФЗ «Об информации, информатизации и защите информации» ФЗ «О техническом регулировании»
Оценка «хорошо» (зачтено) или повышенный уровень освоения компетенции	Регулирование деятельности в области защиты информации криптографическими методами является основной задачей	ФСТЭК Российской Федерации МВД Российской Федерации Службы внешней разведки РФ Министерства обороны РФ ФСБ Российской Федерации
Оценка «отлично» (зачтено) или высокий уровень освоения компетенции	Маркёр для «Служебного пользования» является	Грифом секретности Ограничительной пометкой Степенью конфиденциальности Степенью секретности

4. Правовая охрана результатов интеллектуальной деятельности

	Вопрос теста	Варианты ответов
Оценка «удовлетворительно» (зачтено) или низкой уровень освоения компетенции	Перечислите виды информации как объекта права собственности	Государственная, муниципальная, частная Государственная, муниципальная, акционерная (корпоративная) Государственная, муниципальная, акционерная (корпоративная), общественная Государственная, муниципальная, частная, акционерная (корпоративная), общественная
Оценка «хорошо» (зачтено) или повышенный уровень освоения компетенции	Перечислите все виды владельцев информации	Государство, физические лица Государство, негосударственные (юридические лица), граждане (физические лица) Государство, общественные организации и объединения (юридические лица), граждане (физические лица) Государство, негосударственные (юридические лица), общественные организации и объединения (юридические лица), граждане (физические лица)
Оценка «отлично» (зачтено) или высокий уровень освоения компетенции	Носители защищаемой информации это:	Человек, документы, изделия (предметы) Человек, документы, изделия (предметы), вещества и материалы Документы, изделия (предметы), вещества и материалы, электромагнитные, тепловые радиационные и др. излучения Человек, документы, изделия (предметы), вещества и материалы, электромагнитные, тепловые радиационные и др. излучения

Тема 5. Преступления в сфере компьютерной информации

	Вопрос теста	Варианты ответов
Оценка	Какими статьями глава	литературным, художественным и научным

«удовлетворительно» (зачтено) или низкой уровень освоения компетенции	№ 28 Уголовного кодекса РФ определяет ответственность за компьютерные преступления:	произведениям, изобретениям и открытиям
		Статья 272 предусматривает наказание за неправомерный доступ к компьютерной информации. Наказание – от штрафа 200 МРОТ до 5 лет лишения свободы
		Статья 273 устанавливает ответственность за создание, использование и распространение вредоносных программ для ЭВМ. Наказание – до 7 лет лишения свободы.
		Статья 274 определяет ответственность за нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети. Наказание – до 5 лет лишения свободы
		Только ***статья 272 и 274***
		Все выше перечисленные
Оценка «хорошо» (зачтено) или повышенный уровень освоения компетенции	Что относится к следственным действиям	Осмотр, освидетельствование, следственный эксперимент, обыск, выемка, наложение ареста на почтово-телеграфные отправления, контроль и запись переговоров, допрос, очная ставка, предъявление для опознания, проверка показаний на месте, производство судебной экспертизы
		Обыск, выемка, наложение ареста на почтово-телеграфные отправления, контроль и запись переговоров
		Допрос, очная ставка, предъявление для опознания, проверка показаний на месте, производство судебной экспертизы
		Производство судебной экспертизы
Оценка «отлично» (зачтено) или высокий уровень освоения компетенции	Какие наказания предусмотрены УК РФ по статье 159.6. «Мошенничество в сфере компьютерной информации (п. 1)»	Штраф в размере до 120 тыс. руб. или в размере з/п, или иного дохода осужденного за период до 1 года
		Обязательные работы на срок до 360 часов или исправительные работы на срок до 1 года, или принудительные работы на срок до 2 лет
		Ограничение свободы на срок до 2 лет либо арест на срок до 4 месяцев
		Все используются

Тема 6. Понятие организационной защиты информации

	Вопрос теста	**Варианты ответов**
Оценка «удовлетворительно» (зачтено) или низкой уровень освоения компетенции	Что включает в себя система защиты информации	Совокупность органов защиты информации, используемых ими средств и методов защиты информации, объектов защиты информации и организационно-распорядительных документах (локальных актах) по защите информации, а также мероприятий, планируемых и проводимых в этих целях
		Совокупность органов защиты информации, используемых ими средств и методов защиты информации и объектов защиты информации
		Совокупность органов защиты информации

		(структурных подразделений или должностных лиц организации), используемых ими средств и методов защиты информации и объектов защиты информации
		Совокупность органов защиты информации, объектов защиты информации, а также мероприятий, планируемых и проводимых в этих целях
Оценка «хорошо» (зачтено) или повышенный уровень освоения компетенции	Приведите порядок и последовательность построения комплексной защиты информации	Определить состав защищаемой информации; круг лиц, имеющий доступ к защищаемой информации; определить угрозы безопасности; определить и внедрить меры защиты информации; оценить эффективность принятых мер
		Определить круг лиц, имеющий доступ к защищаемой информации; определить угрозы безопасности; состав защищаемой информации; определить и внедрить меры защиты информации; оценить эффективность принятых мер
		Определить угрозы безопасности; состав защищаемой информации; определить и внедрить меры защиты информации; определить круг лиц, имеющий доступ к защищаемой информации; оценить эффективность принятых мер
Оценка «отлично» (зачтено) или высокий уровень освоения компетенции	Что относится к методам защиты информации на объектах информатизации	Поиск, препятствие, резервирование, маскировка, работа с персоналом
		Препятствие, резервирование, маскировка, работа с персоналом
		Поиск, резервирование, работа с персоналом
		Резервирование, маскировка, работа с персоналом, пренятствие

Тема 7. Политика информационной безопасности. Методы обеспечения физической безопасности.

	Вопрос теста	**Варианты ответов**
Оценка «удовлетворительно» (зачтено) или низкой уровень освоения компетенции	Дайте определение «Субъект доступа»	Единица информационного ресурса автоматизированной системы, доступ к которой регламентируется правилами разграничения доступа
		Лицо или процесс, действия которого регламентируются правилами разграничения доступа
		Пользователь автоматизированной системы обработки информации (в том числе Администратор безопасности), действия которого регламентируются правилами разграничения доступа
Оценка «хорошо» (зачтено) или повышенный уровень освоения компетенции	Основные технические средства и системы (ОТСС) это:	Технические средства и системы, а также их коммуникации, используемые для обработки, хранения и передачи секретной информации
		Технические средства и системы, не предназначенные для передачи, обработки и хранения секретной информации, устанавливаемые на объектах вычислительной техники или в

		выделенных помещениях
Оценка «отлично» (зачтено) или высокий уровень освоения компетенции	Границей контролируемой зоны может являться:	Ограждающие конструкции охраняемого здания, охраняемой части здания, выделенного помещения
		Периметр охраняемой территории предприятия (учреждения)
		Все варианты

Тема 8. Технологические методы поддержания безопасности

	Вопрос теста	**Варианты ответов**
Оценка «удовлетворительно» (зачтено) или низкой уровень освоения компетенции	К основным функциям систем анализа защищённости относятся:	Инвентаризация ресурсов - составление перечня всех узлов сети, выявление их базовых настроек
		Выполнение аудита безопасности - проверки заданных политик безопасности с существующими.
		Все вышеперечисленные
Оценка «хорошо» (зачтено) или повышенный уровень освоения компетенции	Какие технические средства могут использоваться злоумышленником для ведения акустической речевой разведки по вибрационному каналу утечки?	Лазерные акустические средства разведки
		Электронные стетоскопы
		Направленные микрофоны
		Все перечисленные
Оценка «отлично» (зачтено) или высокий уровень освоения компетенции	Технический канал утечки информации это:	Совокупность приёмника и среды распространения сигнала
		Совокупность передатчика, среды распространения сигнала и приёмника
		Совокупность передатчика и среды распространения сигнала
		Правильного ответа нет

Тема 9. Организация режима секретности

	Вопрос теста	**Варианты ответов**
Оценка «удовлетворительно» (зачтено) или низкой уровень освоения компетенции	Что является обязательными условия допуска к государственной тайне	Добровольность
		Проведение проверочных мероприятий
		Оформление по месту работы или военкомат
		Оформление в соответствии с номенклатурой должностей
		Все мероприятия вместе
Оценка «хорошо» (зачтено) или повышенный уровень освоения компетенции	Найдите ошибку в определении форм допуска к государственной тайне	Первая форма «А» - для граждан, допускаемых к сведениям особой важности (допуск – руководитель организации по согласованию с ТО ФСБ РФ)
		Вторая форма «Б» – для граждан, допускаемых к совершенно секретным сведениям (допуск – руководитель организации по согласованию с ТО ФСБ РФ)
		Третья форма «Д» – для граждан, допускаемых к секретным сведениям (1. Допуск – руководитель организации. 2. Допуск - руководитель организации

		по согласованию с ТО ФСБ РФ.) Все варианты правильные
Оценка «отлично» (зачтено) или высокий уровень освоения компетенции	Кто определяет формы допуска в соответствии с номенклатурой должностей	Режимно - секретное подразделение Кадровый орган Руководитель организации Правильного ответа нет

Тема 10. Допуск к государственной тайне

	Вопрос теста	**Варианты ответов**
Оценка «удовлетворительно» (зачтено) или низкой уровень освоения компетенции	Кто проводит оформление документов на допуск к государственной тайне гражданина	Режимно - секретное подразделение Руководитель организации Кадровый орган Правильного ответа нет
Оценка «хорошо» (зачтено) или повышенный уровень освоения компетенции	Кто принимает решения о допуске гражданина к государственной тайне	Территориальный орган ФСБ Руководитель организации Руководитель режимно-секретного подразделения
Оценка «отлично» (зачтено) или высокий уровень освоения компетенции	Какие документы должен представить гражданин, командируемый в другую организацию для доступа к сведениям, составляющим государственную тайну;;	Предписание на выполнение задания по установленной форме Документы, удостоверяющие личность (паспорт или удостоверение личности офицера) Справка о допуске по соответствующей форме Все вышеперечисленные

Тема 11. Защита компьютерной информации. Основные каналы утечки информации при обработке на компьютерах.

	Вопрос теста	**Варианты ответов**
Оценка «удовлетворительно» (зачтено) или низкой уровень освоения компетенции	Что не относится из перечисленного к видам компьютерных преступлений	Компьютерное мошенничество Подделка компьютерной информации Повреждение данных ЭВМ или программ ЭВМ Компьютерный саботаж Несанкционированный доступ Всё относится
Оценка «хорошо» (зачтено) или повышенный уровень освоения компетенции	Какое определение правильно устанавливает понятие «Компьютерный вирус»?	Компьютерный вирус – это небольшая программа, написанная программистом высокой квалификации, способная к саморазмножению и выполнению разных вредоносных действий Компьютерный вирус – это специальная программа, наносящая заведомый вред компьютеру, на котором она запускается на выполнение, или другим компьютерам в сети. Основной функцией вируса

		является его размножение
		Оба правильно
Оценка «отлично» (зачтено) или высокий уровень освоения компетенции	Какие вирусы относятся к классификации «по среде обитания»?	Файловые вирусы
		Загрузочные вирусы
		Макро-вирусы
		Сетевые вирусы
		Резидентные и нерезидентные вирусы
		Все относятся

8.2.2. Групповое задание

Для развития у обучающихся навыков командной работы, межличностной коммуникации, принятия решений, лидерских качеств, развития навыков творческой исследовательской деятельности студентам предлагается выполнить групповое задание.

Групповое задание – творческая практическая работа, направленная на формирования практических навыков в области применения методов теории чисел в компьютерном моделировании теоретико-числовых объектов и программирования.

Для развития у обучающихся навыков командной работы, межличностной коммуникации, принятия решений, лидерских качеств задание получает группа из 2-3 человек.

Защита группового задания происходит в виде публичного выступления с презентаций (по требованию преподавателя).

Темы практических групповых заданий

1. Сформировать и обосновать перспективы развития законодательства в области информационной безопасности.
2. Представить анализ системы контроля за состоянием защиты государственной тайны.
3. Сформировать и обосновать основные требования, предъявляемые к организации защиты конфиденциальной информации.
4. Представить анализ правовой охраны программ для ЭВМ, баз данных, топологий интегральных микросхем и единых технологий, а также защиты интеллектуальных прав.
5. Обозначить основные проблемы судебного преследования за преступления в сфере компьютерной информации и способы их решения.

8.3. Перечень вопросов и заданий для промежуточной аттестации по дисциплине

Промежуточный контроль по дисциплине служит для оценки работы студента в течение семестра и призван выявить уровень, прочность и систематичность полученных им теоретических и практических знаний, приобретения навыков самостоятельной работы, развития творческого

мышления, умение синтезировать полученные знания и применять их в решении практических задач.

Вопросы предполагают контроль общих методических знаний и умений, способность студентов проиллюстрировать их примерами, индивидуальными материалами, составленными студентами в течение курса.

Промежуточный контроль проводится в форме устного собеседования, по результатам которого ставится «зачтено» или «не зачтено» на основе следующих критериев: полноты, структурированности и правильности ответа по сути поставленных вопросов.

Вопросы для промежуточного контроля (зачета)

1. Вопросы по правовому обеспечению ИБ

1. Как трактуется понятие «информационная безопасность» в Доктрине информационной безопасности Российской Федерации?
2. Раскройте структуру информационной безопасности.
3. Назовите основные методы и направления ведения информационной войны.
4. Сформулируйте типы отношений в сфере права информационной собственности, возникающих при реализации информационных процессов.
5. Назовите основные принципы правового регулирования отношений, возникающих в сфере информации, информационных технологий и защиты информации.
6. Дайте определение и обоснуйте понятие «информация».
7. Проведите классификацию источников конфиденциальной информации.
8. Проведите классификацию угроз конфиденциальной информации.
9. В чем особенности информации как объекта юридической защиты?
10. Проведите классификацию видов защищаемой информации.

2. Вопросы по организационному обеспечению ИБ

1. Что включают организационные методы защиты информации?
2. На что направлена деятельность по защите информации?
3. Какие задачи обеспечения информационной безопасности решаются на организационном уровне?
4. Что такое система безопасности предприятия?
5. На основе каких принципов осуществляется функционирование системы безопасности предприятия?
6. Каким требованиям должна удовлетворять система безопасности предприятия?
7. Что является компонентами комплексной модели информационной безопасности?
8. Перечислите виды объектов защиты.
9. Раскройте суть понятия безопасности предприятия (организации).
10. Перечислите основные объекты безопасности предприятия.

8.4. Планируемые уровни сформированности компетенций обучающихся и критерии оценивания

Уровни	Содержательное описание уровня	Основные признаки выделения уровня (этапы формирования компетенции, критерии оценки сформированности)	Пятибалльная шкала (академическая) оценка	Двухбалльная шакала, зачет	БРС, % освоения (рейтинговая оценка)
Повышенный	Творческая деятельность	*Включает нижестоящий уровень.* Умение самостоятельно принимать решение, решать проблему/задачу теоретического и прикладного характера на основе изученных методов, приемов, технологий	отлично	зачтено	86-100
Базовый	Применение знаний и умений в более широких контекстах учебной и профессиональной деятельности, нежели по образцу с большей степени самостоятельности и инициативы	*Включает нижестоящий уровень.* Способность собирать, систематизировать, анализировать и грамотно использовать информацию из самостоятельно найденных теоретических источников и иллюстрировать ими теоретические положения или обосновывать практику применения	хорошо		71-85
Удовлетворительный (достаточный)	Репродуктивная деятельность	Изложение в пределах задач курса теоретически и практически контролируемого материала	удовлетворительно		55-70
Недостаточный	Отсутствие признаков удовлетворительного уровня		неудовлетворительно	не зачтено	Менее 55

9. Перечень основной и дополнительной литературы, необходимой для освоения дисциплины

9.1. Основная литература:

1. Новиков, В. К. Организационно-правовые основы информационной безопасности (защиты информации). Юридическая ответственность за правонарушения в области ...: Уч. пос./Новиков В.К. - Москва : Гор. линия-Телеком, 2015.- 176с. (О)ISBN 978-5-9912-0525-2, 500 экз. - Текст : электронный. - URL: https://znanium.com/catalog/product/536932 (дата обращения: 13.01.2022). – Режим доступа: по подписке.
2. Костин, В. Н. Методы и средства защиты компьютерной информации: законодательные и нормативные акты по защите информации : учебное пособие / В. Н. Костин. - Москва : Изд. Дом НИТУ «МИСиС», 2017. - 26 с. - ISBN 978-5-906846-87-7. - Текст : электронный. - URL: https://znanium.com/catalog/product/1232204 (дата обращения: 13.01.2022). – Режим доступа: по подписке.
3. Малюк, А. А. Теория защиты информации / А.А. Малюк. - Москва : Гор. линия-Телеком, 2012. - 184 с.: ил.; . ISBN 978-5-9912-0246-6, 500 экз. - Текст : электронный. - URL: https://znanium.com/catalog/product/367555 (дата обращения: 13.01.2022). – Режим доступа: по подписке.

9.2. Дополнительная литература:

1. Аверченков, В. И. Защита персональных данных в организации : монография / В. И. Аверченков, М. Ю. Рытов, Т. Р. Гайнулин. - 4-е изд., стер. - Москва : ФЛИНТА, 2021. - 124 с. - ISBN 978-5-9765-1273-3. - Текст : электронный. - URL: https://znanium.com/catalog/product/1843194 (дата обращения: 13.01.2022). – Режим доступа: по подписке.
2. Девянин, П. Н. Модели безопасности компьютерных систем. Управление доступом и информац. потоками:Учебное пособие для вузов/П.Н.Девянин-2-е изд., испр. и доп.-Москва :Гор.линия-Телеком,2013-338с.:ил.;. - (Специальность). ISBN 978-5-9912-0328-9, 100 экз. - Текст : электронный. - URL: https://znanium.com/catalog/product/436878 (дата обращения: 13.01.2022). – Режим доступа: по подписке.
3. Милославская, Н. Г. Технические, организационные и кадровые аспекты управления информационной безопасностью: Учебное пособие для вузов / Милославская Н.Г., Сенаторов М.Ю., Толстой А.И. - Москва :Гор. линия-Телеком, 2013. - 214 с.: . - (Вопросы управления информационной безопасностью)ISBN 978-5-9912-0274-9. - Текст : электронный. - URL: https://znanium.com/catalog/product/560783 (дата обращения: 13.01.2022). – Режим доступа: по подписке.

10. Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины

- НЭБ Национальная электронная библиотека, диссертации и прочие издания
- eLIBRARY.RU Научная электронная библиотека, книги, статьи, тезисы докладов конференций

– Гребенников Электронная библиотека ИД журналы
– ЭБС Лань книги, журналы
– ЭБС Консультант студента
– ПРОСПЕКТ ЭБС
– ЭБС ZNANIUM.COM
– РГБ Информационное обслуживание по МБА
– БЕН РАН
– Электронно-библиотечная система (ЭБС) Кантитана (https://elib.kantiana.ru/)

11. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине

Программное обеспечение обучения включает в себя:

– система электронного образовательного контента БФУ им. И. Канта – www.lms-3.kantiana.ru, обеспечивающую разработку и комплексное использование электронных образовательных ресурсов;

– серверное программное обеспечение, необходимое для функционирования сервера и связи с системой электронного обучения через Интернет;

– корпоративная платформа Microsoft Teams;

– установленное на рабочих местах студентов ПО: Microsoft Windows 7, Microsoft Office Standart 2010, антивирусное программное обеспечение Kaspersky Endpoint Security.

12. Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине

Для проведения занятий лекционного типа, практических и семинарских занятий используются специальные помещения (учебные аудитории), оборудованные техническими средствами обучения – мультимедийной проекционной техникой. Для проведения занятий лекционного типа используются наборы демонстрационного оборудования.

Для проведения лабораторных работ, (практических занятий – при необходимости) используются специальные помещения (учебные аудитории), оснащенные специализированным лабораторным оборудованием: персональными компьютерами с возможностью выхода в интернет и с установленным программным обеспечением, заявленным в п.11.

Для проведения групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации используются специальные помещения (учебные аудитории), оборудованные специализированной мебелью (для обучающихся), меловой / маркерной доской.

Для организации самостоятельной работы обучающимся предоставляются помещения, оснащенные компьютерной техникой с возможностью подключения к сети «Интернет» и обеспечением доступа в электронную информационно-образовательную среду университета.

Для обучения инвалидов и лиц с ограниченными возможностями здоровья университетом могут быть представлены специализированные средства обучения, в том числе технические средства коллективного и индивидуального пользования.

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ
федеральное государственное автономное образовательное учреждение высшего образования «Балтийский федеральный университет имени Иммануила Канта»

Институт физико-математических наук и информационных технологий

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

«Модели безопасности компьютерных систем»

Шифр: 10.05.01
Специальность: «Компьютерная безопасность»
Специализация: «Математические методы защиты информации»
Квалификация (степень) выпускника: специалист по защите информации

Калининград
2022

Лист согласования

Составитель: Олефиренко Денис Олегович, ассистент Института физико-математических наук и информационных технологий.

Рабочая программа утверждена на заседании учебно-методического совета института физико-математических наук и информационных технологий
Протокол № 01/22 от «01» февраля 2022 г.

Председатель учебно-методического совета института физико-математических наук и информационных технологий
Первый заместитель директора ИФМНиИТ, к. ф.-м. н., доцент — Шпилевой А. А

Ведущий менеджер — Е.П.Ставицкая

СОДЕРЖАНИЕ

1. Наименование дисциплины: «Модели безопасности компьютерных систем».

Целью изучения дисциплины «Модели безопасности компьютерных систем» является формирование чётких знаний об основных формальных моделях безопасности современных КС, адекватных условиям их функционирования; овладение навыками по формальному моделированию и анализу безопасности КС.

Необходимость изучения дисциплины заключается в подготовке студентов для научной и практической деятельности в области обеспечения защиты компьютерных систем от постоянно растущего числа угроз безопасности и хакерских атак.

Основные **задачи** изучения дисциплины:

- изучить основные формальные модели дискреционного, мандатного, ролевого управления доступом, изолированной программной среды и изолированных информационных потоков;
- изучить подходы, применяемые для разработки формальных моделей безопасности современных КС.

2. Перечень планируемых результатов обучения по дисциплине, соотнесенных с планируемыми результатами освоения образовательной программы

В результате освоения ООП специалитета обучающийся должен овладеть следующими результатами обучения по дисциплине:

Код компетенции	Результаты освоения образовательной программы (ИДК)	Результаты обучения по дисциплине
ОПК-8. Способен применять методы научных исследований при проведении разработок в области обеспечения безопасности компьютерных систем и сетей;	**ОПК-8.1.** Знает принципы работы с научной литературой, методы поиска научно-технической информации. **ОПК-8.2.** Способен осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических документов. **ОПК-8.3.** Обладает навыками решения профессиональных задач с широким использованием актуальной научно-технической литературы.	Студент, изучивший модели безопасности компьютерных систем, должен: ***знать*:** основные формальные модели безопасности компьютерных систем; угрозы безопасности информации; основные виды политик управления доступом. ***уметь:*** анализировать угрозы безопасности КС; разрабатывать формальные модели политик безопасности, политик управления доступом и информационными потоками. ***владеть:*** навыками построения моделей защищаемых систем и систем обеспечения безопасности КС.
ОПК-11. Способен разрабатывать политики безопасности, политики управления доступом и информационными потоками в компьютерных системах с учетом	**ОПК-11.1.** Знает меры по обеспечению информационной безопасности и методы управления процессом их реализации на объекте защиты. **ОПК-11.2.** Способен формировать политику информационной безопасности,	Студент должен: ***знать*:** основные формальные модели дискреционного, мандатного, ролевого управления доступом, модели изолированной программной среды и безопасности информационных потоков; ***уметь:*** формализовывать задачи по безопасности КС; разрабатывать модели нарушителя

угроз безопасности информации и требований по защите информации;	организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности. **ОПК-11.3.** Владеет навыками управления процессом реализации политики информационной безопасности, организации и поддержки выполнения комплекса мер по обеспечению информационной безопасности на объекте защиты.	безопасности КС; разрабатывать политики безопасности КС. ***владеть:*** навыками разработки и анализа моделей безопасности КС.

3. Место дисциплины в структуре ООП ВО

«Модели безопасности компьютерных систем» представляет собой дисциплину обязательной части блока 1 «Дисциплины (модули)», входит в модуль 5 «Дополнительные разделы дискретной математики» дисциплин специальности 10.05.01 «Компьютерная безопасность», специализация «Математические методы защиты информации».

4. Виды учебной работы по дисциплине

Виды учебной работы по дисциплине зафиксированы учебным планом основной профессиональной образовательной программы по указанному направлению и профилю, выражаются в академических часах. Часы контактной работы и самостоятельной работы студента и часы, отводимые на процедуры контроля, могут различаться в учебных планах ОПОП по формам обучения. Объем контактной работы включает часы контактной аудиторной работы (лекции/практические занятия/ лабораторные работы), контактной внеаудиторной работы (контроль самостоятельной работы), часы контактной работы в период аттестации. Контактная работа, в том числе может проводиться посредством электронной информационно-образовательной среды университета с использованием ресурсов сети Интернет и дистанционных технологий

5. Содержание дисциплины, структурированное по темам (разделам)

№ п/п	Наименование раздела	Содержание раздела

1	Основные понятия	Сущность, объект, доступ, информационный поток. Основные элементы теории компьютерной безопасности: сущность, субъект, доступ, право доступа, информационные потоки по памяти и по времени. Основная аксиома безопасности КС. Проблема построения защищённой КС. Модели ценности информации: аддитивная модель, порядковая шкала, решётка многоуровневой безопасности. Архитектура электронных систем обработки данных. Угрозы информационной безопасности. Политика безопасности. Классификация угроз информационной безопасности. Угрозы конфиденциальности, целостности, доступности информации. Угроза раскрытия параметров КС. Понятие политики безопасности. Модель нарушителя. Основные виды политики управления доступом и информационными потоками. Политики дискреционного, мандатного, ролевого управления доступом, изолированной программной среды и безопасности информационных потоков. Формальные модели. Модели безопасности. Критерии и классы защищённости средств вычислительной техники и автоматизированных информационных систем. Стандарты по оценке защищённых систем. Примеры практической реализации. Построение парольных систем. Особенности применения криптографических методов. Способы реализации криптографической подсистемы. Особенности реализации систем с симметричными и несимметричными ключами. Концепция защищённого ядра. Методы верификации. Защищённые домены
2	Модели КС с дискреционным разграничением доступа.	Модель матрицы доступа Харрисона – Руззо – Ульмана (ХРУ). Анализ безопасности систем ХРУ. Монооперационные системы ХРУ. Алгоритмическая неразрешимость задачи проверки безопасности систем ХРУ. Модель типизированной матрицы доступа (ТМД). Монотонные системы ТМД и их каноническая форма. Ациклические монотонные ТМД и алгоритм проверки их безопасности. Классическая модель Take-Grant. Условия передачи прав доступа при отсутствии ограничений на кооперацию субъектов. Расширенная модель Take-Grant. Условия реализации информационных потоков. Алгоритм построения замыкания графа доступов и информационных потоков. Представление систем Take-Grant системами ХРУ и ТМД.
3	Модели КС с мандатным разграничением доступа	Модель Белла – ЛаПадулы. Классическая модель Белла – ЛаПадулы. Базовая теорема безопасности. Интерпретации модели Белла – ЛаПадулы: модель реализации политики low-watermark, безопасность переходов, модель мандатной политики целостности информации Биба. Недостатки модели Белла – ЛаПадулы. Примеры реализации запрещённых информационных потоков. Модель системы военных сообщений (СВС). Неформальное и формальное описание модели СВС. Безопасное состояние. Безопасность переходов. Потенциальная модификация сущности с источником. Смысл безопасности функции переходов.
4	Модели безопасности информационных потоков	Автоматная, программная и вероятностная модели безопасности информационных потоков. Автоматная модель безопасности информационных потоков. Программная модель контроля информационных потоков. Контролирующий механизм защиты. Вероятностная модель безопасности информационных потоков. Информационное невлияние. Субъектно-ориентированная модель изолированной программной среды (ИПС). Объекты, функционально ассоциированные с субъектами. Мониторы безопасности обращений и порождения субъектов. Базовая теорема ИПС.

5	Модели КС с ролевым разграничением доступа	Базовая модель ролевого разграничения доступа. Описание базовой модели ролевого разграничения доступа. Иерархия ролей. Применение иерархического метода для построения защищённой операционной системы. Механизм ограничений. Расширение базовой ролевой модели. Модель администрирования ролевого управления доступом. Администрирование множества авторизованных ролей пользователей и прав доступа, которыми обладают роли, а также иерархии ролей. Модель мандатного ролевого управления доступом. Защита от угроз конфиденциальности и целостности информации.
6	Развитие формальных моделей безопасности КС	Взаимосвязь моделей безопасности КС и основные направления их развития. Обзор семейства формальных моделей управления доступом и информационными потоками (ДП-моделей) КС с дискреционным, мандатным и ролевым разграничением доступа. Проблема адекватности реализации модели безопасности в реальной КС. Исследование корректности системы защиты. Методология обследования и проектирования системы защиты. Модель политики контроля целостности.

6. Рекомендуемая тематика учебных занятий в форме контактной работы

Рекомендуемая тематика учебных занятий *лекционного* типа (предусматривающих преимущественную передачу учебной информации преподавателями):

№ п/п	**Наименование раздела**	**Содержание раздела**
1	Основные понятия	Лекции 1-2. Сущность, объект, доступ, информационный поток. Основные элементы теории компьютерной безопасности: сущность, субъект, доступ, право доступа, информационные потоки по памяти и по времени. Основная аксиома безопасности КС. Проблема построения защищённой КС. Модели ценности информации: аддитивная модель, порядковая шкала, решётка многоуровневой безопасности. Архитектура электронных систем обработки данных. Лекции 3-4. Угрозы информационной безопасности. Политика безопасности. Классификация угроз информационной безопасности. Угрозы конфиденциальности, целостности, доступности информации. Угроза раскрытия параметров КС. Понятие политики безопасности. Модель нарушителя. Основные виды политики управления доступом и информационными потоками. Политики дискреционного, мандатного, ролевого управления доступом, изолированной программной среды и безопасности информационных потоков. Формальные модели. Модели безопасности. Критерии и классы защищённости средств вычислительной техники и автоматизированных информационных систем. Стандарты по оценке защищённых систем. Примеры практической реализации. Построение парольных систем. Особенности применения криптографических методов. Способы реализации криптографической подсистемы. Особенности реализации систем с симметричными и несимметричными ключами. Концепция защищённого ядра. Методы верификации. Защищённые домены
2	Модели КС с дискреционным разграничением доступа.	Лекция 5. Модель матрицы доступа Харрисона – Руззо – Ульмана (ХРУ). Анализ безопасности систем ХРУ. Монооперационные системы ХРУ. Алгоритмическая неразрешимость задачи проверки безопасности систем ХРУ. Лекция 6. Модель типизированной матрицы доступа (ТМД). Монотонные системы ТМД и их каноническая форма. Ациклические монотонные ТМД и алгоритм проверки их безопасности. Лекции 7-8. Классическая модель Take-Grant. Условия передачи прав доступа при отсутствии ограничений на кооперацию субъектов. Расширенная модель Take-Grant. Условия реализации информационных потоков. Алгоритм построения замыкания графа доступов и информационных потоков. Представление систем Take-Grant системами ХРУ и ТМД.

3	Модели КС с мандатным разграничением доступа	Лекции 9-10. Модель Белла – ЛаПадулы. Классическая модель Белла – ЛаПадулы. Базовая теорема безопасности. Интерпретации модели Белла – ЛаПадулы: модель реализации политики low-watermark, безопасность переходов, модель мандатной политики целостности информации Биба. Недостатки модели Белла – ЛаПадулы. Примеры реализации запрещённых информационных потоков. Лекции 11-12. Модель системы военных сообщений (СВС). Неформальное и формальное описание модели СВС. Безопасное состояние. Безопасность переходов. Потенциальная модификация сущности с источником. Смысл безопасности функции переходов.
4	Модели безопасности информационных потоков	Лекции 13-14. Автоматная, программная и вероятностная модели безопасности информационных потоков. Автоматная модель безопасности информационных потоков. Программная модель контроля информационных потоков. Контролирующий механизм защиты. Вероятностная модель безопасности информационных потоков. Информационное невлияние. Лекции 15-16. Субъектно-ориентированная модель изолированной программной среды (ИПС). Объекты, функционально ассоциированные с субъектами. Мониторы безопасности обращений и порождения субъектов. Базовая теорема ИПС.
5	Модели КС с ролевым разграничением доступа	Лекции 17-18. Базовая модель ролевого разграничения доступа. Описание базовой модели ролевого разграничения доступа. Иерархия ролей. Применение иерархического метода для построения защищённой операционной системы. Механизм ограничений. Лекции 19-20. Расширение базовой ролевой модели. Модель администрирования ролевого управления доступом. Администрирование множества авторизованных ролей пользователей и прав доступа, которыми обладают роли, а также иерархии ролей. Модель мандатного ролевого управления доступом. Защита от угроз конфиденциальности и целостности информации.
6	Развитие формальных моделей безопасности КС	Лекции 21-23. Взаимосвязь моделей безопасности КС и основные направления их развития. Обзор семейства формальных моделей управления доступом и информационными потоками (ДП-моделей) КС с дискреционным, мандатным и ролевым разграничением доступа. Проблема адекватности реализации модели безопасности в реальной КС. Исследование корректности системы защиты. Методология обследования и проектирования системы защиты. Модель политики контроля целостности.

Рекомендуемая тематика *практических* занятий:

№ п/п	**Наименование Темы**	**Содержание темы**
1	Основные понятия	Моделирование различных угроз информационной безопасности с использованием субъектно-ориентированного подхода.
2	Модели КС с дискреционным разграничением доступа.	Элементы дискреционной модели в подсистеме управления доступом операционной системы Windows: список прав доступа (access control list, ACL). Элементы дискреционной модели в подсистеме управления доступом в операционных системах семейства UNIX: биты доступа. Построение замыкания графа доступов в классической модели Take-Grant.
3	Модели КС с мандатным разграничением	Классическая модель Белла-ЛаПадулы и её интерпретации. Модель СВС.

	доступа	
4	Модели безопасности информационных потоков	Построение автоматной модели безопасности информационных потоков. Построение программной модели контроля информационных потоков. Исследование вопросов информационной невыводимости и информационного невлияния для схемы КС.
5	Модели КС с ролевым разграничением доступа	Ролевая модель управления доступом в СУБД SQL Server, Oracle и MySQL.
6	Развитие формальных моделей безопасности КС	Обоснование политики безопасного администрирования ОС Windows.

Рекомендуемая тематика *самостоятельных* работ:

№ п/п	**Наименование раздела**	**Тематика самостоятельных работ**
1	Основные понятия	1. Программные закладки, взаимодействующие с операционной системой по принципу «наблюдатель»: формализация модели с точки зрения субъектно-ориентированного подхода. 2. Программные закладки, взаимодействующие с операционной системой по принципу «перехват»: формализация модели с точки зрения субъектно-ориентированного подхода. 3. Программные закладки, взаимодействующие с операционной системой по принципу «искажение»: формализация модели с точки зрения субъектно-ориентированного подхода.
2	Модели КС с дискреционным разграничением доступа.	4. Модель АДЕПТ-50. 5. Пятимерное пространство безопасности Хартсона.
3	Модели КС с мандатным разграничением доступа	6. Модель Лендвера.
4	Модели безопасности информационных потоков	7. Применение ФАС ДП-модели для анализа безопасности веб-систем.
5	Модели КС с ролевым разграничением доступа	8. Система Феррайоло – Куна. 9. Метод Куна для построения ролевой модели доступа на основе мандатной. 10. Метод Санти для построения мандатной модели доступа на основе ролевой.
6	Развитие формальных моделей безопасности КС	11. Доверенные и недоверенные субъекты. Анализ информационных потоков по памяти и по времени. Функционально и параметрически ассоциированные с субъектами сущности.

Требования к самостоятельной работе обучающихся

Учебно-методическое обеспечение для самостоятельной работы обучающихся составляют:

1. Материалы лекций.
2. Материалы практических занятий.
3. Информационные ресурсы «Интернета».

4. Методические рекомендации и указания.
5. Фонды оценочных средств.
6. Учебники и учебно-методические пособия.

7. Методические рекомендации по видам занятий

Лекционные занятия.

В ходе лекционных занятий обучающимся рекомендуется выполнять следующие действия. Вести конспектирование учебного материала. Обращать внимание на категории, формулировки, раскрывающие содержание тех или иных явлений и процессов, научные выводы и практические рекомендации по их применению. Задавать преподавателю уточняющие вопросы с целью уяснения теоретических положений, разрешения спорных ситуаций.

Желательно оставить в рабочих конспектах поля, на которых во внеаудиторное время можно сделать пометки из рекомендованной литературы, дополняющие материал прослушанной лекции, а также подчеркивающие особую важность тех или иных теоретических положений.

Практические и семинарские занятия.

На практических и семинарских занятиях в зависимости от темы занятия выполняется поиск информации по решению проблем, практические упражнения, контрольные работы, выработка индивидуальных или групповых решений, итоговое обсуждение с обменом знаниями, участие в круглых столах, разбор конкретных ситуаций, командная работа, представление портфолио и т.п.

Самостоятельная работа.

Самостоятельная работа осуществляется в виде изучения литературы, эмпирических данных по публикациям и конкретных ситуаций из практики, подготовке индивидуальных работ, работа с лекционным материалом, самостоятельное изучение отдельных тем дисциплины; поиск и обзор литературы и электронных источников; чтение и изучение учебника и учебных пособий.

8. Фонд оценочных средств

8.1. Перечень компетенций с указанием этапов их формирования в процессе освоения образовательной программы в рамках учебной дисциплины

Основными этапами формирования указанных компетенций при изучении обучающимися дисциплины являются последовательное изучение содержательно связанных между собой тем учебных занятий. Изучение каждой темы предполагает овладение обучающимися необходимыми компетенциями. Результат аттестации обучающихся на различных этапах формирования компетенций показывает уровень освоения компетенций.

Контролируемые модули, разделы (темы) дисциплины	Индекс контролируемой компетенции (или её части)	Оценочные средства по этапам формирования компетенций
		текущий контроль по дисциплине
Тема 1. Основные понятия	ОПК-8	Устный опрос
Тема 2. Модели КС с дискреционным разграничением доступа	ОПК-8, ОПК-11	Устный опрос, решение задач
Тема 3. Модели КС с мандатным разграничением доступа	ОПК-8, ОПК-11	Устный опрос, решение задач
Тема 4. Модели безопасности	ОПК-8, ОПК-11	Устный опрос, решение задач

информационных потоков		
Тема 5. Модели КС с ролевым разграничением доступа	ОПК-8, ОПК-11	Устный опрос, решение задач
Тема 6. Развитие формальных моделей безопасности КС	ОПК-8, ОПК-11	Устный опрос, решение задач, реферат или групповое задание

8.2. Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений и навыков и (или) опыта деятельности процессе текущего контроля

Тема 1. Основные понятия

Задание 1. Моделирование поведения пользователя в операционной системе с точки зрения субъектно-ориентированного подхода.

Тема 2. Модели КС с дискреционным разграничением доступа.

Задание 1. Элементы дискреционной модели в подсистеме управления доступом операционной системы Windows: список прав доступа (access control list, ACL).

Задание 2. Элементы дискреционной модели в подсистеме управления доступом в операционных системах семейства UNIX: биты доступа.

Задание 3. Доказать, что для общего случая систем ХРУ не существует возможности утечки права доступа для заданной пары субъект-объект.

Задание 4. Представить произвольную систему ТМД системой ХРУ.

Задание 5. Классическая модель Take-Grant. Проверить является ли мостом заданный граф доступов.

Задание 6. Классическая модель Take-Grant. Проверить истинен ли предикат can_share для заданных графа доступов и параметров.

Тема 3. Модели КС с мандатным разграничением доступа.

Задание 1. Описать состояния системы Белла-ЛаПадулы с заданными параметрами. Подсчитать количество различных состояний, если в системе требуется выполнение только ss-свойства.

Задание 2. Показать каким образом десять свойств модели СВС реализуются в её формальном описании.

Тема 4. Модели безопасности информационных потоков.

Задание 1. Описать требования информационного невлияния, позволяющие в автоматной модели реализовать мандатную политику безопасности для заданной решетки уровней конфиденциальности.

Задание 2. Пусть заданы компьютеры и сетевые информационные каналы, определяемые как совокупность команд сетевых интерфейсов. Для заданной схемы КС, описать её с использованием семи требований информационного невлияния автоматной модели безопасности информационных потоков.

Тема 5. Модели КС с ролевым разграничением доступа.

Задание 1. Мандатная сущностно-ролевая ДП-модель управления доступом и информационными потоками в операционных системах семейства Linux.

Задание 2. Анализ безопасности информационных потоков в операционных системах семейства GNU/Linux.

Тема 6. Развитие формальных моделей безопасности КС.

Задание 1. Обоснование политики безопасного администрирования ОС Windows. Контроль целостности в ОС Windows.

Устные опросы

Тема 1. Основные понятия

1. В чем состоит важность основной аксиомы теории компьютерной безопасности?
2. Какие основные угрозы безопасности информации рассматриваются в теории компьютерной безопасности?
3. Какие основные виды политик безопасности рассматриваются в теории компьютерной безопасности?
4. Приведите примеры наиболее распространённых в современных ОС и СУБД запрещенных информационных потоков по памяти и по времени.

Тема 2. Модели КС с дискреционным разграничением доступа.

1. Модель матрицы доступа Харрисона – Руззо – Ульмана.
2. Анализ безопасности систем ХРУ.
3. Модель типизированной матрицы доступа (ТМД).
4. Классическая модель Take-Grant.
5. Представление систем Take-Grant системами ХРУ и ТМД.

Тема 3. Модели КС с мандатным разграничением доступа.

1. Классическая модель Белла – ЛаПадулы.
2. Интерпретации модели Белла – ЛаПадулы: модель реализации политики low-watermark, безопасность переходов
3. Модель мандатной политики целостности информации Биба.
4. Недостатки модели Белла – ЛаПадулы.
5. Модель системы военных сообщений (СВС).

Тема 4. Модели безопасности информационных потоков.

1. Автоматная модель безопасности информационных потоков.
2. Программная модель контроля информационных потоков.
3. Вероятностная модель безопасности информационных потоков.
4. Субъектно-ориентированная модель изолированной программной среды (ИПС).

Тема 5. Модели КС с ролевым разграничением доступа.

1. Базовая модель ролевого разграничения доступа. Применение иерархического метода для построения защищённой операционной системы.
2. Расширение базовой ролевой модели. Модель администрирования ролевого управления доступом. Администрирование множества авторизованных ролей пользователей и прав доступа, которыми обладают роли, а также иерархии ролей.

3. Модель мандатного ролевого управления доступом.

Тема 6. Развитие формальных моделей безопасности КС.

1. Взаимосвязь моделей безопасности КС и основные направления их развития.
2. Проблема адекватности реализации модели безопасности в реальной КС.
3. Модель политики контроля целостности.

8.3. Перечень вопросов и заданий для промежуточной аттестации по дисциплине

Вопросы для промежуточного контроля (зачёта):

1. Основные понятия теории компьютерной безопасности: сущность, субъект, доступ, право доступа, информационные потоки по памяти и по времени.
2. Основная аксиома безопасности КС. Проблема построения защищённой КС.
3. Понятие политики безопасности.
4. Основные виды политик управления доступом и информационными потоками.
5. Модель матрицы доступов Харрисона–Руззо–Ульмана (ХРУ).
6. Анализ безопасности систем ХРУ. Монооперационные системы ХРУ.
7. Алгоритмическая неразрешимость задачи проверки безопасности систем ХРУ.
8. Модель типизированной матрицы доступов (ТМД).
9. Монотонные системы ТМД и их каноническая форма.
10. Ациклические монотонные ТМД и алгоритм проверки их безопасности.
11. Классическая модель Take-Grant. Условия передачи прав доступа при отсутствии ограничений на кооперацию субъектов.
12. Расширенная модель Take-Grant. Условия реализации информационных потоков.
13. Алгоритм построения замыкания графа доступов и информационных потоков.
14. Представление систем Take-Grant системами ХРУ и ТМД.
15. Классическая модель Белла – ЛаПадулы. Базовая теорема безопасности.
16. Модель реализации политики low-watermark.
17. Безопасность переходов.
18. Модель мандатной политики целостности информации Биба.
19. Недостатки модели Белла – ЛаПадулы. Примеры реализации запрещённых информационных потоков.
20. Неформальное и формальное описание модели систем военных сообщений.
21. Безопасное состояние. Безопасность переходов. Потенциальная модификация сущности с источником. Смысл безопасности функции переходов.
22. Автоматная модель безопасности информационных потоков.
23. Программная модель контроля информационных потоков. Контролирующий механизм защиты.
24. Вероятностная модель безопасности информационных потоков. Информационное невлияние.
25. Описание базовой модели ролевого управления доступом. Иерархия ролей. Механизм ограничений.
26. Модель администрирования при ролевом управлении доступом. Администрирование множества авторизованных ролей пользователей и прав доступа, которыми обладают роли, а также иерархии ролей.
27. Модель мандатного ролевого управления доступом. Защита от угроз конфиденциальности и целостности информации.

8.4. Планируемые уровни сформированности компетенций обучающихся и критерии оценивания

Уровни	Содержательное описание уровня	Основные признаки выделения уровня (этапы формирования компетенции, критерии оценки сформированности)	Пятибалльная шкала (академическая) оценка	Двухбалльная шакала, зачет	БРС, % освоения (рейтинговая оценка)
Повышенный	Творческая деятельность	*Включает нижестоящий уровень.* Умение самостоятельно принимать решение, решать проблему/задачу теоретического и прикладного характера на основе изученных методов, приемов, технологий	отлично	зачтено	86-100
Базовый	Применение знаний и умений в более широких контекстах учебной и профессиональной деятельности, нежели по образцу с большей степени самостоятельности и инициативы	*Включает нижестоящий уровень.* Способность собирать, систематизировать, анализировать и грамотно использовать информацию из самостоятельно найденных теоретических источников и иллюстрировать ими теоретические положения или обосновывать практику применения	хорошо		71-85
Удовлетворительный (достаточный)	Репродуктивная деятельность	Изложение в пределах задач курса теоретически и практически контролируемого материала	удовлетворительно		55-70
Недостаточный	Отсутствие признаков удовлетворительного уровня		неудовлетворительно	не зачтено	Менее 55

9. Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины.

Основная литература

1. Казарин, О. В. Надежность и безопасность программного обеспечения [Электронный ресурс]: учеб. пособие для бакалавриата и магистратуры/ О. В. Казарин, И. Б. Шубинский; Рос. гос. гуманитар. ун-т, Моск. гос. ун-т им. М. В. Ломоносова. - Москва: Юрайт, 2019. - 1 on-line, 342 с.. - (Бакалавр и магистр. Модуль). - ISBN 978-5-534-05142-1: Б.ц. Имеются экземпляры в отделах /There are copies in departments: ЭБС Юрайт(1)

Дополнительная литература

1. Богульская, Н. А. Модели безопасности компьютерных систем : учебное пособие / Н. А. Богульская, М. М. Кучеров. - Красноярск : Сиб. федер. ун-т, 2019. - 206 с. - ISBN 978-5-7638-4008-7. - Текст : электронный. - URL: https://znanium.com/catalog/product/1819309 (дата обращения: 26.04.2022). – Режим доступа: по подписке.

10. Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины (модуля).

- НЭБ Национальная электронная библиотека, диссертации и прочие издания
- eLIBRARY.RU Научная электронная библиотека, книги, статьи, тезисы докладов конференций
- Гребенников Электронная библиотека ИД журналы
- ЭБС Лань книги, журналы
- ЭБС Консультант студента
- ПРОСПЕКТ ЭБС
- ЭБС ZNANIUM.COM
- РГБ Информационное обслуживание по МБА
- БЕН РАН
- Электронно-библиотечная система (ЭБС) Кантитана (https://elib.kantiana.ru/)

11. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине.

Программное обеспечение обучения включает в себя:

- система электронного образовательного контента БФУ им. И. Канта – www.lms-3.kantiana.ru, обеспечивающую разработку и комплексное использование электронных образовательных ресурсов;
- серверное программное обеспечение, необходимое для функционирования сервера и связи с системой электронного обучения через Интернет;
- корпоративная платформа Microsoft Teams;
- установленное на рабочих местах обучающихся ПО: Microsoft Windows 7, Microsoft Office Standart 2010, антивирусное программное обеспечение Kaspersky Endpoint Security.
- специализированное ПО не требуется.

12. Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине.

Для проведения занятий лекционного типа, практических и семинарских занятий используются специальные помещения (учебные аудитории), оборудованные техническими средствами обучения – мультимедийной проекционной техникой. Для проведения занятий лекционного типа используются наборы демонстрационного оборудования.

Для проведения лабораторных работ, (практических занятий – при необходимости) используются специальные помещения (учебные аудитории), оснащенные специализированным лабораторным оборудованием: персональными компьютерами с возможностью выхода в интернет и с установленным программным обеспечением, заявленным в п.11.

Для проведения групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации используются специальные помещения (учебные аудитории), оборудованные специализированной мебелью (для обучающихся), меловой / маркерной доской.

Для организации самостоятельной работы обучающимся предоставляются помещения, оснащенные компьютерной техникой с возможностью подключения к сети «Интернет» и обеспечением доступа в электронную информационно-образовательную среду университета.

Для обучения инвалидов и лиц с ограниченными возможностями здоровья университетом могут быть представлены специализированные средства обучения, в том числе технические средства коллективного и индивидуального пользования.

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
федеральное государственное автономное образовательное учреждение высшего образования «Балтийский федеральный университет имени Иммануила Канта»
Институт физико-математических наук и информационных технологий

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

«Физика»

Шифр: 10.05.01
Специальность: «Компьютерная безопасность»
Специализация: «Математические методы защиты информации»
Квалификация (степень) выпускника: специалист по защите информации

Калининград
2022

Лист согласования

Составитель: Корнев Константин Петрович, к.ф.-м.н. , доцент

Рабочая программа утверждена на заседании учебно-методического совета института физико-математических наук и информационных технологий

Протокол № 01/22 от «01» февраля 2022 г.

Председатель учебно-методического
совета института физико-
математических наук и информационных
технологий

Первый заместитель директора Шпилевой А. А
ИФМНиИТ, к. ф.-м. н., доцент

Ведущий менеджер Е.П.Ставицкая

Содержание

1.Наименование дисциплины: «Физика».

Цель дисциплины: целью освоения дисциплины «Физика» является фундаментальная подготовка обучающихся в области физики.

2. Перечень планируемых результатов обучения по дисциплине, соотнесенных с планируемыми результатами освоения образовательной программы

Код компетенции	Результаты освоения образовательной программы (ИДК)	Результаты обучения по дисциплине
ОПК-4 Способность анализировать физическую сущность явлений и процессов, лежащих в основе функционирования микроэлектронной техники, применять основные физические законы и модели для решения задач профессиональной деятельности.	ОПК-4.1. Демонстрирует знание физических законов и моделей, необходимых при решении задач обеспечения защиты информации. ОПК-4.2. Применяет необходимые физические законы и модели для решения обеспечения защиты информации. ОПК-4.3. Владеет навыками моделирования для решения задач обеспечения защиты информации.	- **знать** фундаментальную базу теоретических знаний по физике,. иметь представление о физической картине, связывающей все изучаемые явления, теории и модели их описания. - **уметь** понять поставленную задачу и использовать базу теоретических знаний и практических навыков по физике в процессе ее решения; на основе анализа увидеть и корректно сформулировать результат; использовать полученные знания в профессиональной деятельности; ориентироваться в постановках задач; на основе анализа увидеть и корректно сформулировать результат; передавать результат проведенных физико-математических и прикладных исследований в виде конкретных рекомендаций, выраженных в терминах предметной области изучавшегося явления; - **владеть** полученными знаниями и навыками при освоении других дисциплин, которые связаны с физическими явлениями и понятиями.

3. Место дисциплины в структуре образовательной программы

Дисциплина «Физика» представляет собой дисциплину обязательной части блока 1 «Дисциплины (модули)».

4. Виды учебной работы по дисциплине.

Виды учебной работы по дисциплине зафиксированы учебным планом основной профессиональной образовательной программы по указанному направлению и профилю, выражаются в академических часах. Часы контактной работы и самостоятельной работы обчающегося и часы, отводимые на процедуры контроля, могут различаться в учебных планах ОПОП по формам обучения. Объем контактной работы включает часы контактной аудиторной работы (лекции/практические занятия/ лабораторные работы), контактной внеаудиторной работы (контроль самостоятельной работы), часы контактной работы в период аттестации. Контактная работа, в том числе может проводиться посредством электронной информационно-образовательной среды университета с использованием ресурсов сети Интернет и дистанционных технологий

5. Содержание дисциплины, структурированное по темам (разделам)

Исходя из рамок, установленных учебным планом по трудоемкости и видам учебной работы по дисциплине, преподаватель самостоятельно выбирает тематику занятий по формам и количеству часов проведения контактной работы: лекции и иные учебные занятия, предусматривающие преимущественную передачу учебной информации преподавателем и (или) занятия семинарского типа (семинары, практические занятия, практикумы, лабораторные работы, коллоквиумы и иные аналогичные занятия), и (или) групповые консультации, и (или) индивидуальную работу обучающихся с преподавателем, в том числе индивидуальные консультации (по курсовым работам/проектам – при наличии курсовой работы/проекта по данной дисциплине в учебном плане). Рекомендуемая тематика занятий максимально полно реализуется в контактной работе с обучающимися очной формы обучения. В случае реализации образовательной программы в заочной / очно-заочной форме трудоемкость дисциплины сохраняется, однако объем учебного материала в значительной части осваивается обучающимися в форме самостоятельной работы. При этом требования к ожидаемым образовательным результатам обучающихся по данной дисциплине не зависят от формы реализации образовательной программы.

Наименование раздела	**Содержание дисциплины**
1. Физические основы механики.	Предмет физики. Направления развития современной физики
	1. **Механика.**
2. Кинематика материальной точки	Понятие состояния в классической механике. Уравнения движения. Описание движения материальной точки. Системы отсчета. Кинематические уравнения. Прямолинейное движение. Криволинейное движение. Ускорение при криволинейном движении. Движение по окружности, центростремительное ускорение. Основы релятивистской механики.
3. Динамика материальной точки	Инерциальные и неинерциальные системы отсчёта. Первый закон Ньютона. Фундаментальные взаимодействия. Силы в механике. Масса. Инертная и гравитационная масса. Второй закон Ньютона.

	Третий закон Ньютона.
4. Законы сохранения в механике.	Импульс тела. Закон сохранения импульса в механике. Энергия и работа. Закон сохранения механической энергии.
5. Вращательное движение	Угол поворота, угловая скорость, угловое ускорение. Момент импульса тела и системы тел. Моменты сил. Закон сохранения момента импульса.
6. Статика	Виды равновесия тел. Момент силы. Условия равновесия тел. Центр масс тела.
7. Кинематика движения твёрдого тела, жидкостей и газов.	Кинематические уравнения, описывающие движение твердых тел. Поступательное, вращательное и сложное движение твердого тела.
8. Динамика твёрдого тела, жидкостей и газов.	Основные законы динамики поступательного и вращательного движение твердого тела.
9. Момент инерции тел.	Момент инерции тел относительно оси, проходящей через центр масс. Момент инерции тел относительно произвольной оси. Теорема Штейнера. Кинетическая энергия при сложном движении твердого тела.
10.Относительность в классической механике	Принцип относительности в классической механике. Преобразования Галилея. Эквивалентность инерциальных систем отсчета.
11. Основы специальной теории относительности	Постулаты специальной теории относительности Эйнштейна. Преобразования Лоренца. Время в подвижной и неподвижной системах отсчета. Формула Эйнштейна для связи массы и энергии.
	2. Молекулярная физика и термодинамика
1. Молекулярно-кинетическая теория	Основы МКТ. Экспериментальное подтверждение основных положений МКТ. Броуновское движение, диффузия, несжимаемость жидкости, теплота парообразования.
2. Уравнение состояния идеального газа	Параметры, описывающие состояние идеального газа. Уравнение Клапейрона-Менделеева. Уравнение Клапейрона. Изопроцессы и адиабатный процесс. Графики. Основное уравнение МКТ для идеального газа.
3. Состояние термодинамической системы	Виды термодинамических систем. Внутренняя энергия термодинамической системы. Работа, совершаемая при изменении состояния системы.
4. Три начала термодинамики.	Теплота, теплопередача. Первое начало термодинамики как закон сохранения энергии. Внутренняя энергия и теплоёмкость идеального газа. Классическая теория теплоёмкости идеального газа. Термодинамические функции состояния. Фазовые равновесия и фазовые превращения. Элементы неравновесной термодинамики. Классическая и квантовые статистики. Кинетические явления. Системы заряженных частиц. Конденсированное состояние.
5. Работа, совершаемая идеальным газом	Работа, совершаемая идеальным газом в разных процессах. Работа в изобарном процессе. Работа в изохорном процессе. Работа в изотермическом процессе.

6. Циклы в термодинамике.	Циклы в термодинамике. Работа, совершаемая рабочим телом в цикле. Работа на диаграмме $p-V$. КПД циклов. Цикл Карно.
	3. **Электричество и магнетизм.**
1.Взаимодействие зарядов.	Взаимодействие точечных зарядов. Закон Кулона. Взаимодействие системы точечных зарядов.
2.Электростати-ческое поле	Напряженность электрического поля. Силовые линии электростатического поля. Принцип суперпозиции полей. Однородное электростатическое поле.
3.Потенциальная энергия и потенциал	Потенциальная энергия взаимодействия двух точечных зарядов. Потенциал электростатического поля. Связь потенциала и напряженности электрического поля. Потенциал, создаваемый системой зарядов. Потенциальная энергия системы зарядов.
4. Теорема Остроградского-Гаусса для электростатического поля.	Поток вектора напряженности электрического поля через площадку. Теорема Остроградского-Гаусса для электростатического поля.
5. Проводники в электрическом поле. Электроёмкость	Проводники в электрическом поле. Поверхностная плотность зарядов. Электроёмкость. Емкость уединенного проводника, емкость шара. Конденсатор. Типы конденсаторов. Соединение конденсаторов.
6. Постоянный электрический ток.	Постоянный электрический ток. Закон Ома для участка цепи. Электрическое сопротивление. Соединение сопротивлений. Электродвижущая сила. Закон Ома для полной цепи. Сложные цепи. Правила Кирхгофа.
7. Магнитное поле	Магнитное поле. Вектор индукции магнитного поля. Силовые линии магнитного поля. Действие магнитного поля на движущийся заряд. Сила Лоренца.
8. Закон Ампера.	Взаимодействие проводников с током. Действие магнитного поля на проводник с током. Закон Ампера.
9. Закон Био-Савара-Лапласа	Магнитное поле, создаваемое проводником с током. Закон Био-Савара-Лапласа.
10. Теорема о циркуляции и теорема Остроградского-Гаусса для магнитного поля	Понятие циркуляция вектора магнитной индукции. Теорема о циркуляции вектора магнитной индукции. Элементарный поток вектора магнитной индукции. Поток вектора магнитной индукции через площадку. Теорема Остроградского-Гаусса для магнитного поля.
11. Магнитное поле в веществе.	Магнитные моменты атомов. Магнитное поле в веществе. Напряженность магнитного поля. Диамагнетики, парамагнетики и ферромагнетики. Петля гистерезиса. Электростатика и магнитостатика в вакууме и веществе.
12.Электромагнитная индукция.	Явление электромагнитной индукции. Правило Ленца. Явление самоиндукции. Индуктивность. Явление взаимной индукции.
13. Уравнения Максвелла в интегральной и дифференциальной форме.	Первое уравнение Максвелла. Токи смещения. Второе уравнение Максвелла. Третье и четвертое уравнения Максвелла. Материальные уравнения. Квазистационарные токи. Принцип относительности в электродинамике.
	4. Оптика. Квантовая физика
1. Оптика. Физика колебаний и волн.	Гармонический и ангармонический осциллятор, физический смысл спектрального разложения, кинематика волновых процессов, нормальные моды, интерференция и дифракция волн, элементы Фурье-оптики. Основы геометрической оптики. Волновые свойства света. Спектроскоп, критерий Релея. Рентгеноструктурный анализ.

	Взаимодействия света с веществом (дисперсия, поглощение и рассеяние света). Поляризация света.
2. Тепловое излучение	Закон Кирхгофа. Правило Прево. Излучение абсолютно черного тела. Формула Релея-Джинса. Ультрафиолетовая катастрофа. Формула Планка. Законы Стефана-Больцмана и Вина.
3. Волновые и корпускулярные свойства частиц	Гипотеза де Бройля. Корпускулярно-волновой дуализм. Опыт Дэвиссона-Джермера.
4. Строение атома	Модели строения по Томпсону, Резерфорду. Постулаты Бора. Квантование энергии и моменты импульса. Радиусы разрешенных орбит.
5. Основные понятия квантовой механики атомов и молекул	Принцип неопределенности. Квантовые состояния. Волновая функция и ее интерпретация. Уравнение Шредингера. Соотношение неопределенностей Гейзенберга. Квантовые числа. Принцип Паули. Принцип суперпозиции. Квантовые уравнения движения. Операторы физических величин. Энергетический спектр атомов и молекул. Природа химической связи.
6. Основные понятия ядерной физики	Строение ядра. Нуклоны. Изотопы. Радионуклиды. Сильное взаимодействие. Закон радиоактивного распада. Метод радиоактивного датирования.
7. Основы физики элементарных частиц	Типы взаимодействий. Классификация элементарных частиц. Кварки.

6. Рекомендуемая тематика учебных занятий в форме контактной работы

Рекомендуемая тематика учебных занятий *лекционного* типа (предусматривающих преимущественную передачу учебной информации преподавателями):

Наименование раздела	**Темы и содержание лекций**
1. Физические основы механики.	Предмет физики. Направления развития современной физики
	1. **Механика.**
2. Кинематика материальной точки	Понятие состояния в классической механике. Уравнения движения. Описание движения материальной точки. Системы отсчета. Кинематические уравнения. Прямолинейное движение. Криволинейное движение. Ускорение при криволинейном движении. Движение по окружности, центростремительное ускорение. Основы релятивистской механики.
3. Динамика материальной точки	Инерциальные и неинерциальные системы отсчёта. Первый закон Ньютона. Фундаментальные взаимодействия. Силы в механике. Масса. Инертная и гравитационная масса. Второй закон Ньютона. Третий закон Ньютона.
4. Законы сохранения в механике.	Импульс тела. Закон сохранения импульса в механике. Энергия и работа. Закон сохранения механической энергии.
5. Вращательное движение	Угол поворота, угловая скорость, угловое ускорение. Момент импульса тела и системы тел. Моменты сил. Закон

	сохранения момента импульса.
6. Статика	Виды равновесия тел. Момент силы. Условия равновесия тел. Центр масс тела.
7. Кинематика движения твёрдого тела, жидкостей и газов.	Кинематические уравнения, описывающие движение твердых тел. Поступательное, вращательное и сложное движение твердого тела.
8. Динамика твёрдого тела, жидкостей и газов.	Основные законы динамики поступательного и вращательного движение твердого тела.
9. Момент инерции тел.	Момент инерции тел относительно оси, проходящей через центр масс. Момент инерции тел относительно произвольной оси. Теорема Штейнера. Кинетическая энергия при сложном движении твердого тела.
10.Относительность в классической механике	Принцип относительности в классической механике. Преобразования Галилея. Эквивалентность инерциальных систем отсчета.
11. Основы специальной теории относительности	Постулаты специальной теории относительности Эйнштейна. Преобразования Лоренца. Время в подвижной и неподвижной системах отсчета. Формула Эйнштейна для связи массы и энергии.
	2. Молекулярная физика и термодинамика
1. Молекулярно-кинетическая теория	Основы МКТ. Экспериментальное подтверждение основных положений МКТ. Броуновское движение, диффузия, несжимаемость жидкости, теплота парообразования.
2. Уравнение состояния идеального газа	Параметры, описывающие состояние идеального газа. Уравнение Клапейрона-Менделеева. Уравнение Клапейрона. Изопроцессы и адиабатный процесс. Графики. Основное уравнение МКТ для идеального газа.
3. Состояние термодинамической системы	Виды термодинамических систем. Внутренняя энергия термодинамической системы. Работа, совершаемая при изменении состояния системы.
4. Три начала термодинамики.	Теплота, теплопередача. Первое начало термодинамики как закон сохранения энергии. Внутренняя энергия и теплоёмкость идеального газа. Классическая теория теплоёмкости идеального газа. Термодинамические функции состояния. Фазовые равновесия и фазовые превращения. Элементы неравновесной термодинамики. Классическая и квантовые статистики. Кинетические явления. Системы заряженных частиц. Конденсированное состояние.
5. Работа, совершаемая идеальным газом	Работа, совершаемая идеальным газом в разных процессах. Работа в изобарном процессе. Работа в изохорном процессе. Работа в изотермическом процессе.
6. Циклы в термодинамике.	Циклы в термодинамике. Работа, совершаемая рабочим телом в цикле. Работа на диаграмме $p-V$. КПД циклов. Цикл Карно.
	3. Электричество и магнетизм.
1.Взаимодействие	Взаимодействие точечных зарядов. Закон Кулона. Взаимодействие

зарядов.	системы точечных зарядов.
2.Электростати-ческое поле	Напряженность электрического поля. Силовые линии электростатического поля. Принцип суперпозиции полей. Однородное электростатическое поле.
3.Потенциальная энергия и потенциал	Потенциальная энергия взаимодействия двух точечных зарядов. Потенциал электростатического поля. Связь потенциала и напряженности электрического поля. Потенциал, создаваемый системой зарядов. Потенциальная энергия системы зарядов.
4. Теорема Остроградского-Гаусса для электростатического поля.	Поток вектора напряженности электрического поля через площадку. Теорема Остроградского-Гаусса для электростатического поля.
5. Проводники в электрическом поле. Электроёмкость	Проводники в электрическом поле. Поверхностная плотность зарядов. Электроёмкость. Емкость уединенного проводника, емкость шара. Конденсатор. Типы конденсаторов. Соединение конденсаторов.
6. Постоянный электрический ток.	Постоянный электрический ток. Закон Ома для участка цепи. Электрическое сопротивление. Соединение сопротивлений. Электродвижущая сила. Закон Ома для полной цепи. Сложные цепи. Правила Кирхгофа.
7. Магнитное поле	Магнитное поле. Вектор индукции магнитного поля. Силовые линии магнитного поля. Действие магнитного поля на движущийся заряд. Сила Лоренца.
8. Закон Ампера.	Взаимодействие проводников с током. Действие магнитного поля на проводник с током. Закон Ампера.
9. Закон Био-Савара-Лапласа	Магнитное поле, создаваемое проводником с током. Закон Био-Савара-Лапласа.
10. Теорема о циркуляции и теорема Остроградского-Гаусса для магнитного поля	Понятие циркуляция вектора магнитной индукции. Теорема о циркуляции вектора магнитной индукции. Элементарный поток вектора магнитной индукции. Поток вектора магнитной индукции через площадку. Теорема Остроградского-Гаусса для магнитного поля.
11. Магнитное поле в веществе.	Магнитные моменты атомов. Магнитное поле в веществе. Напряженность магнитного поля. Диамагнетики, парамагнетики и ферромагнетики. Петля гистерезиса. Электростатика и магнитостатика в вакууме и веществе.
12.Электромагнитная индукция.	Явление электромагнитной индукции. Правило Ленца. Явление самоиндукции. Индуктивность. Явление взаимной индукции.
13. Уравнения Максвелла в интегральной и дифференциальной форме.	Первое уравнение Максвелла. Токи смещения. Второе уравнение Максвелла. Третье и четвертое уравнения Максвелла. Материальные уравнения. Квазистационарные токи. Принцип относительности в электродинамике.
	4. Оптика. Квантовая физика
2. Оптика. Физика колебаний и волн.	Гармонический и ангармонический осциллятор, физический смысл спектрального разложения, кинематика волновых процессов, нормальные моды, интерференция и дифракция волн, элементы Фурье-оптики. Основы геометрической оптики. Волновые свойства света. Спектроскоп, критерий Релея. Рентгеноструктурный анализ. Взаимодействия света с веществом (дисперсия, поглощение и рассеяние света). Поляризация света.
2. Тепловое излучение	Закон Кирхгофа. Правило Прево. Излучение абсолютно черного тела. Формула Релея-Джинса. Ультрафиолетовая катастрофа. Формула Планка. Законы Стефана-Больцмана и Вина.
3. Волновые и корпускулярные	Гипотеза де Бройля. Корпускулярно-волновой дуализм. Опыт Дэвиссона-Джермера.

свойства частиц	
4. Строение атома	Модели строения по Томпсону, Резерфорду. Постулаты Бора. Квантование энергии и моменты импульса. Радиусы разрешенных орбит.
5. Основные понятия квантовой механики атомов и молекул	Принцип неопределенности. Квантовые состояния. Волновая функция и ее интерпретация. Уравнение Шредингера. Соотношение неопределенностей Гейзенберга. Квантовые числа. Принцип Паули. Принцип суперпозиции. Квантовые уравнения движения. Операторы физических величин. Энергетический спектр атомов и молекул. Природа химической связи.
6. Основные понятия ядерной физики	Строение ядра. Нуклоны. Изотопы. Радионуклиды. Сильное взаимодействие. Закон радиоактивного распада. Метод радиоактивного датирования.
7. Основы физики элементарных частиц	Типы взаимодействий. Классификация элементарных частиц. Кварки.

Тематика лабораторных работ

№ п/п	Наименование темы лабораторной работы
1	Исследование прямолинейного движения тел в поле тяжести на машине Атвуда
2	Определение момента инерции и проверка теоремы Штейнера методом крутильных колебаний..
3	Определение скорости пули методом физического маятника
4	Изучение движении тел в жидкости . Формула Стокса.
5	Изучение статистических закономерностей.
6	Изучение осциллографа
7	Определение удельного зарада электрона
8	Изучение влияния сопротивления амперметра и вольтметра на погрешность измерений.
9	Изучение контактных явлений. Термопара.
10	Определение фокусного расстояния собирающей и рассеивающей линз
11	Определение длины световой волны с помощью бипризмы Френеля и щелей Юнг
12	Изучение дифракционной решетки и определение длины световой волны
13	Изучение поляризации света

Тематика практических занятий

№ п/п	№ темы	Темы практических занятий
1.	1,2	Введение. Кинематика материальной точки.
2.	3	Динамика материальной точки.
3.	4	Вращательное движение
4.	5	Законы сохранения в механике.
5.	6	Статика
6.	7	Гидростатика
7.	8	Кинематика движения твёрдого тела
8	9	Динамика твёрдого тела.

9	10	Момент инерции тел.
10	11,12	Относительность в классической механике. Основы специальной теории относительности
11	13	Молекулярно-кинетическая теория.
12	14	Уравнение состояния идеального газа
13	15	Состояние термодинамической системы
14	16	Первое начало термодинамики
15	17	Работа, совершаемая идеальным газом в разных процессах
16	18	Циклы в термодинамике
17	19	Взаимодействие зарядов.
18	20	Электростатическое поле
19	21	Потенциал электростатическое поле
20	22	Теорема Остроградского-Гаусса для электростатического поля.
21	23	Проводники в электрическом поле. Электроёмкость
22	24	Постоянный электрический ток.
23	25	Магнитное поле
24	26	Закон Ампера.
25	27	Закон Био-Савара-Лапласа
26	28	Теорема о циркуляции и теорема Остроградского-Гаусса для магнитного поля
27	29	Магнитное поле в веществе.
28	30	Электромагнитная индукция.
29	31	Уравнения Максвелла.
30	32	Электромагнитные колебания и волны
31	33	Фотометрия и геометрическая оптика
32	34	Интерференция, ее виды. Методы осуществления интерференции
33	35	Дифракция света. Виды дифракции. Дифракционная решетка
34	36	Дисперсия света. Поглощение и рассеяние света
35	37	Отражение и преломление света.

Требования к самостоятельной работе обучающихся

1. Работа с лекционным материалом, предусматривающая проработку конспекта лекций и учебной литературы, по всем темам из п. 6 настоящей рабочей программы.

2. Выполнение домашнего задания, предусматривающего решение задач, выполнение упражнений, выдаваемых на практических занятиях, по всем темам из п. 6 настоящей рабочей программы.

Руководствуясь положениями статьи 47 и статьи 48 Федерального закона от 29 декабря 2012 г. N 273-ФЗ «Об образовании в Российской Федерации» научно-педагогические работники и иные лица, привлекаемые университетом к реализации данной образовательной программы, пользуются предоставленными академическими правами и свободами в части свободы преподавания, свободы от вмешательства в профессиональную деятельность; свободы выбора и использования педагогически обоснованных форм, средств, методов обучения и воспитания; права на творческую инициативу, разработку и применение авторских программ и методов обучения и воспитания в пределах реализуемой образовательной программы и отдельной дисциплины.

Исходя из рамок, установленных учебным планом по трудоемкости и видам учебной работы по дисциплине, преподаватель самостоятельно выбирает тематику

занятий по формам и количеству часов проведения контактной работы: лекции и иные учебные занятия, предусматривающие преимущественную передачу учебной информации преподавателем и (или) занятия семинарского типа (семинары, практические занятия, практикумы, лабораторные работы, коллоквиумы и иные аналогичные занятия), и (или) групповые консультации, и (или) индивидуальную работу обучающихся с преподавателем, в том числе индивидуальные консультации (по курсовым работам/проектам – при наличии курсовой работы/проекта по данной дисциплине в учебном плане).

Рекомендуемая тематика занятий максимально полно реализуется в контактной работе с обучающимися очной формы обучения. В случае реализации образовательной программы в заочной / очно-заочной форме трудоемкость дисциплины сохраняется, однако объем учебного материала в значительной части осваивается обучающимися в форме самостоятельной работы. При этом требования к ожидаемым образовательным результатам обучающихся по данной дисциплине не зависят от формы реализации образовательной программы.

7. Методические рекомендации по видам занятий

Лекционные занятия.

В ходе лекционных занятий обучающимся рекомендуется выполнять следующие действия. Вести конспектирование учебного материала. Обращать внимание на категории, формулировки, раскрывающие содержание тех или иных явлений и процессов, научные выводы и практические рекомендации по их применению. Задавать преподавателю уточняющие вопросы с целью уяснения теоретических положений, разрешения спорных ситуаций.

Желательно оставить в рабочих конспектах поля, на которых во внеаудиторное время можно сделать пометки из рекомендованной литературы, дополняющие материал прослушанной лекции, а также подчеркивающие особую важность тех или иных теоретических положений.

Практические и семинарские занятия.

На практических и семинарских занятиях в зависимости от темы занятия выполняется поиск информации по решению проблем, практические упражнения, контрольные работы, выработка индивидуальных или групповых решений, итоговое обсуждение с обменом знаниями, участие в круглых столах, разбор конкретных ситуаций, командная работа, представление портфолио и т.п.

Самостоятельная работа.

Самостоятельная работа осуществляется в виде изучения литературы, эмпирических данных по публикациям и конкретных ситуаций из практики, подготовке индивидуальных работ, работа с лекционным материалом, решение задач, самостоятельное изучение отдельных тем дисциплины; поиск и обзор литературы и электронных источников; чтение и изучение учебника и учебных пособий.

Тематика самостоятельных работ.

№	Содержание вопроса
1.	Элементы векторной алгебры.
2.	Теорема Штейнера и ее применение.
3.	Законы Кеплера.
4.	Законы сохранения и симметрии пространства и времени.

5.	Закон Гука. Растяжение и сжатие стержней.
6.	Распределение Гиббса.
7.	Фазовые переходы. Эффект Джоуля-Томсона.
8.	Правила Кирхгофа.
9.	Импеданс. Цепи переменного тока.
10.	Автоколебания. Релаксационные колебания.
11.	Стоячие волны. Ударные волны.
12.	Применение интерференции.
13.	Твердотельные и газоразрядные лазеры.
14.	Сверхпроводимость.
15.	Элементарные частицы, их классификация и взаимопревращаемость.

8. Фонд оценочных средств

8.1. Перечень компетенций с указанием этапов их формирования в процессе освоения образовательной программы в рамках учебной дисциплины

Основными этапами формирования указанных компетенций при изучении обучающимися дисциплины являются последовательное изучение содержательно связанных между собой тем учебных занятий. Изучение каждой темы предполагает овладение обучающимися необходимыми компетенциями. Результат аттестации обучающихся на различных этапах формирования компетенций показывает уровень освоения компетенций.

Контролируемые разделы (темы) дисциплины	Индекс контроли-руемой компетенции (или её части)	Оценочные средства по этапам формирования компетенций
		текущий контроль по дисциплине
1. Механика материальной точки	ОПК-4	Опрос, решение задач.
2. Механика твердого тела	ОПК-4	Опрос, решение задач, контрольная работа
3. Статика и гидростатика	ОПК-4	Опрос, решение задач
4. Молекулярно-кинетическая теория	ОПК-4	Опрос, решение задач
5. Уравнение состояния идеального газа	ОПК-4	Опрос, решение задач
6. Основные законы термодинамики Циклы в термодинамике. Работа, совершаемая идеальным газом.	ОПК-4	Опрос, решение задач решение задач, контрольная работа
7. Электростатика.	ОПК-4	Опрос, решение задач,
8. Постоянный электрический ток.	ОПК-4	Опрос,
9. .Магнитное поле. Сила	ОПК-4	Опрос, решение задач

Контролируемые разделы (темы) дисциплины	Индекс контроли-руемой компетенции (или её части)	Оценочные средства по этапам формирования компетенций
		текущий контроль по дисциплине
Лоренца. Закон Ампера.Закон Био-Савара-Лапласа		
10. Электромагнитная индукция.	ОПК-4	Опрос, решение задач
11. Уравнения Максвелла.	ОПК-4	Опрос, решение задач решение задач, контрольная работа
12. Геометрическая оптика	ОПК-4	Опрос, решение задач
13. Волновая оптика.	ОПК-4	Опрос, решение задач
14. Волновые и корпускулярные свойства частиц.	ОПК-4	Опрос, решение задач
15. Строение атома. Основные понятия квантовой механики атомов и молекул	ОПК-4	Опрос, решение задач
16. Основные понятия и законы ядерной физики	ОПК-4	Опрос, решение задач
17. Основы физики элементарных частиц	ОПК-4	Опрос, решение задач решение задач, контрольная работа

8.2. Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений и навыков и (или) опыта деятельности процессе текущего контроля

Тематика контрольных работ

1. Кинематика и динамика материальной точки, законы сохранения в механике.

2. Кинематика и динамика твёрдого тела.

3. Состояние термодинамической системы. Первое начало термодинамики.

4. Работа, совершаемая идеальным газом. Циклы в термодинамике.

5. Электростатика. Проводники в электрическом поле. Электроёмкость.

6. Постоянный электрический ток.

7. Магнитное поле. Закон Ампера. Закон Био-Савара-Лапласа.

8. Строение атома по Резерфорду. Постулаты Бора.

9. Строение ядра. Нуклоны. Изотопы.

10. Закон радиоактивного распада.

Вопросы для зачета по разделу «Механика и молекулярная физика»

1. Описание движения материальной точки.
2. Криволинейное движение. Ускорение при криволинейном движении.
3. Инерциальная и неинерциальная системы отсчёта. Фундаментальные взаимодействия.
4. Второй закон Ньютона. Третий закон Ньютона. Силы в механике.
5. Закон сохранения импульса в механике.
6. Энергия и работа.
7. Потенциальная энергия. Кинетическая энергия.
8. Закон сохранения механической энергии.
9. Закон сохранения момента импульса.
10. Условие равновесия тела, имеющего ось вращения.
11. Кинематика движения твёрдого тела.
12. Динамика твёрдого тела.
13. Момент инерции.
14. Теорема Штейнера.
15. Кинетическая энергия при вращательном движении тела.
16. Принцип относительности в механике. Преобразования Галилея.
17. Постулаты специальной теории относительности. Преобразования Лоренца.
18. Основы МКТ. Экспериментальное подтверждение основных положений МКТ.
19. Уравнение состояния идеального газа. Изопроцессы и адиабатный процесс. Графики.
20. Основное уравнение МКТ для идеального газа.
21. Внутренняя энергия и работа, совершаемая при изменении состояния системы.
22. Первое начало термодинамики.
23. Внутренняя энергия и теплоёмкость идеального газа.
24. Уравнение адиабаты.
25. Работа, совершаемая идеальным газом в разных процессах.
26. Классическая теория теплоёмкости идеального газа в термодинамике.
27. Циклы в термодинамике. Цикл Карно. КПД циклов.

Вопросы для зачета по разделу «Электричество и магнетизм. Оптика. Квантовая физика»

1. Закон Кулона. Границы применимости закона Кулона.
2. Электростатическое поле и его свойства. Графическое изображение электростатических полей. Напряженность электростатического поля.
3. Теорема Остроградского-Гаусса для электростатического поля в вакууме и ее применение к расчету полей.
4. Циркуляция вектора напряженности электростатического поля. Работа сил поля при перемещении заряда.

5. Потенциал электростатического поля. Эквипотенциальные поверхности. Напряженность как градиент потенциала.
6. Электрическая емкость уединенного проводника, проводящей сферы.
7. Электрическая емкость конденсаторов: плоского, сферического цилиндрического. Соединение конденсаторов.
8. Энергия системы зарядов, заряженного проводника, заряженного конденсатора.
9. Постоянный электрический ток. Условия появления и существования тока. Сила и плотность тока.
10. Сторонние силы. Электродвижущая сила и напряжение.
11. Сопротивление проводников. Закон Ома в интегральной и дифференциальной формах: для однородного и неоднородного участков цепи, для замкнутой цепи.
12. Магнитное поле в вакууме и его характеристики. Вектор магнитной индукции. Графическое изображение магнитных полей.
13. Закон Био-Савара-Лапласа и его применение к расчету магнитного поля. Расчет по выбору: магнитное поле прямого тока, в центре и на оси кругового тока.
14. Действие магнитного поля на проводник с током. Сила Ампера.
15. Взаимодействие параллельных токов. Закон Ампера.
16. Действие магнитного поля на движущийся заряд. Сила Лоренца.
17. Циркуляция вектора магнитной индукции в вакууме. Закон полного тока для магнитного поля в вакууме.
18. Поток вектора магнитной индукции. Теорема Остроградского-Гаусса для магнитного поля в вакууме.
19. Диа- и парамагнетики, ферромагнетики.
20. Явление электромагнитной индукции. Опыты Фарадея. Закон Фарадея. Правило Ленца.
21. Индуктивность контура. Самоиндукция. Потокосцепление. ЭДС самоиндукции.
22. Система уравнений Максвелла для электромагнитного поля в интегральной и дифференциальной формах и их физический смысл.
23. Основы геометрической оптики. Законы отражения и преломления света. Полное внутреннее отражение.
24. Волновые свойства света. Электромагнитная волна. Вектор Умова-Пойнтинга.
25. Интерференция света. Условие временной когерентности волн и их источников.
26. Расчет интерференционной картины для двух зеркал Френеля, бипризмы Френеля и щелей Юнга.
27. Применение интерференции света. Просветление оптики.
28. Дифракция света. Принцип Гюйгенса-Френеля.
29. Метод зон Френеля. Дифракция на круглом отверстии. Дифракция на непрозрачном диске.
30. Дифракция Фраунгофера на плоской дифракционной решетке.
31. Основные характеристики спектральных приборов-дисперсия и разрешающая способность. Критерий Рэлея.
32. Дифракция рентгеновских лучей. Формула Брэгга-Вульфа. Рентгено-структурный анализ.
33. Взаимодействие света с веществом. Дисперсия и поглощение света.
34. Поляризация света. Естественный и поляризованный свет. Виды поляризации.
35. Закон Малюса. Закон Брюстера.
36. Тепловое излучение и его свойства.
37. Законы Кирхгофа, Стефана-Больцмана и Вина.
38. Формула Рэлея-Джинса. Ультрафиолетовая катастрофа.
39. Гипотеза Планка. Фотон и его свойства.
40. Гипотеза де Бройля. Корпускулярно-волновой дуализм вещества.
41. Модели строения атома по Томпсону, Резерфорду.

42. Постулаты Бора. Квантование энергии и момента импульса, радиусы разрешенных орбит в теории атома по Бору.
43. Соотношение неопределенностей Гейзенберга.
44. Волновая функция и ее интерпретация. Уравнение Шредингера.
45. Строение ядра. Сильное взаимодействие. Закон радиоактивного распада.
46. Типы взаимодействий. Классификация элементарных частиц. Кварки.

8.4. Планируемые уровни сформированности компетенций обучающихся и критерии оценивания

Уровни	Содержательное описание уровня	Основные признаки выделения уровня (этапы формирования компетенции, критерии оценки сформированности)	Пятибалльная шкала (академическая) оценка	Двухбалльная шакала, зачет	БРС, % освоения (рейтинговая оценка)
Повышенный	Творческая деятельность	содержание ответа на *первый* и *второй* вопрос представляет собой связный рассказ, в котором используются все необходимые понятия по данной теме; рассказ сопровождается правильной записью математических формул и пояснением физического смысла входящих в них величин; в ответе отсутствуют ошибки.	отлично	зачтено	86-100
Базовый	Применение знаний и умений в более широких контекстах учебной и профессиональной деятельности, нежели по образцу с большей степени самостоятельности и инициативы	В случае правильного, но неполного ответа на вопросы, если: отсутствуют некоторые несущественные элементы содержания; присутствуют все понятия, составляющие основу содержания темы, но при их раскрытии допущены неточности или незначительные ошибки, которые свидетельствуют о недостаточном уровне овладения отдельными	хорошо		71-85

		умениями (ошибки при написании определений, математических формул, в толковании физического смысла использующихся в формулах величин).			
Удовлетворительный (достаточный)	Репродуктивная деятельность	в ответе на вопросы отсутствуют некоторые понятия, которые необходимы для раскрытия вопроса билета, нарушается логика изложения материала	удовлетворительно		55-70
Недостаточный	Отсутствие признаков удовлетворительного уровня		неудовлетворительно	не зачтено	Менее 55

9. Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины.

Основная литература

1. Андреева, Н. А. Физика : часть 2. :курс лекций / Н. А. Андреева, С. В. Белокуров, Е. В. Корчагина. - Воронеж : Воронежский институт ФСИН России, 2019. - 157 с. - Текст : электронный. - URL: https://znanium.com/catalog/product/1086194 (дата обращения: 07.04.2022). – Режим доступа: по подписке.
2. Демидченко, В. И. Физика : учебник / В.И. Демидченко, И.В. Демидченко. — 6-е изд., перераб. и доп. — Москва : ИНФРА-М, 2021. — 581 с. + Доп. материалы [Электронный ресурс]. — (Высшее образование: Бакалавриат). - ISBN 978-5-16-010079-1. - Текст : электронный. - URL: https://znanium.com/catalog/product/1541963 (дата обращения: 07.04.2022). – Режим доступа: по подписке.

Дополнительная литература

1. Андреева, Н. А. Физика : сборник задач : практическое пособие / Н. А. Андреева, Е. В. Корчагина. - Воронеж : Воронежский институт ФСИН России, 2019. - 188 с. - Текст : электронный. - URL: https://znanium.com/catalog/product/1086249 (дата обращения: 07.04.2022). – Режим доступа: по подписке.
2. Ильюшонок, А. В. Физика : учеб. пособие / А.В. Ильюшонок [и др.]. - Минск : Новое знание ; Москва : ИНФРА-М, 2013. — 600 с. - (Высшее образование). - ISBN 978-985-475-548-9 (Новое знание) ; ISBN 978-5-16-006556-4 (ИНФРА-М). - Текст : электронный. - URL: https://znanium.com/catalog/product/397226 (дата обращения: 07.04.2022). – Режим доступа: по подписке.

10. Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины (модуля).

- НЭБ Национальная электронная библиотека, диссертации и прочие издания
- eLIBRARY.RU Научная электронная библиотека, книги, статьи, тезисы докладов конференций
- Гребенников Электронная библиотека ИД журналы
- ЭБС Лань книги, журналы
- ЭБС Консультант студента
- ПРОСПЕКТ ЭБС
- ЭБС ZNANIUM.COM
- РГБ Информационное обслуживание по МБА
- БЕН РАН
- Электронно-библиотечная система (ЭБС) Кантитана (https://elib.kantiana.ru/)

11. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине.

Программное обеспечение обучения включает в себя:

- система электронного образовательного контента БФУ им. И. Канта – www.lms-3.kantiana.ru, обеспечивающую разработку и комплексное использование электронных образовательных ресурсов;
- серверное программное обеспечение, необходимое для функционирования сервера и связи с системой электронного обучения через Интернет;
- корпоративная платформа Microsoft Teams;
- установленное на рабочих местах обучающихся ПО: Microsoft Windows 7, Microsoft Office Standart 2010, антивирусное программное обеспечение Kaspersky Endpoint Security.
- специализированное ПО не требуется.

12. Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине.

Для проведения занятий лекционного типа, практических и семинарских занятий используются специальные помещения (учебные аудитории), оборудованные техническими средствами обучения – мультимедийной проекционной техникой. Для проведения занятий лекционного типа используются наборы демонстрационного оборудования.

Для проведения лабораторных работ, (практических занятий – при необходимости) используются специальные помещения (учебные аудитории), оснащенные специализированным лабораторным оборудованием: персональными компьютерами с возможностью выхода в интернет и с установленным программным обеспечением, заявленным в п.11.

Для проведения групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации используются специальные помещения (учебные аудитории), оборудованные специализированной мебелью (для обучающихся), меловой / маркерной доской.

Для организации самостоятельной работы обучающимся предоставляются помещения, оснащенные компьютерной техникой с возможностью подключения к сети «Интернет» и обеспечением доступа в электронную информационно-образовательную среду университета.

Для обучения инвалидов и лиц с ограниченными возможностями здоровья университетом могут быть представлены специализированные средства обучения, в том числе технические средства коллективного и индивидуального пользования.

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
федеральное государственное автономное образовательное учреждение высшего образования «Балтийский федеральный университет имени Иммануила Канта»
Институт физико-математических наук и информационных технологий

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

«Электроника и схемотехника»

Шифр: 10.05.01
Специальность: «Компьютерная безопасность»
Специализация: «Математические методы защиты информации»
Квалификация (степень) выпускника: специалист по защите информации

Калининград
2022

Лист согласования

Составитель: Горбачев Андрей Александрович к.т.н., доцент

Рабочая программа утверждена на заседании учебно-методического совета института физико-математических наук и информационных технологий

Протокол № 01/22 от «01» февраля 2022 г.

Председатель учебно-методического
совета института физико-
математических наук и информационных
технологий

Первый заместитель директора Шпилевой А. А
ИФМНиИТ, к. ф.-м. н., доцент

Ведущий менеджер Е.П.Ставицкая

Содержание

1.Наименование дисциплины: «Электроника и схемотехника».

Цель дисциплины: формирование необходимых знаний в области основ построения современной электронной техники, используемой в построении компьютерных информационных систем и технических средствах защиты информации.

2. Перечень планируемых результатов обучения по дисциплине, соотнесенных с планируемыми результатами освоения образовательной программы

Код компетенции	Результаты освоения образовательной программы (ИДК)	Результаты обучения по дисциплине
ОПК-4 Способность анализировать физическую сущность явлений и процессов, лежащих в основе функционирования микроэлектронной техники, применять основные физические законы и модели для решения задач профессиональной деятельности.	ОПК-4.1. Демонстрирует знание физических законов и моделей, необходимых при решении задач обеспечения защиты информации. ОПК-4.2. Применяет необходимые физические законы и модели для решения обеспечения защиты информации. ОПК-4.3. Владеет навыками моделирования для решения задач обеспечения защиты информации.	***Знать***: физические принципы работы базовых элементов современной радиоэлектронной аппаратуры и физические процессы, протекающие в них; основы анализа базовых элементов и устройств радиоэлектронной аппаратуры, используемых в современных информационных системах; назначение и состав основных аналоговых и цифровых устройств, используемых в современных информационных системах. ***Уметь***: работать с современной элементной базой электронной аппаратуры; применять основные методы анализа радиоэлектронных систем обработки информации; использовать современную измерительную аппаратуру при экспериментальном исследовании систем обработки информации; пользоваться современной научно-технической информацией по радиоэлектронике. ***Владеть***: навыками инженерного количественного анализа узловых элементов и устройств современной радиоэлектронной аппаратуры; навыками использования СВТ для машинного анализа аналоговых и цифровых элементов и узлов радиоэлектронной аппаратуры; навыками экспериментального анализа узловых элементов и

		устройств радиоэлектронной аппаратуры с применением современной измерительной техники.

3. Место дисциплины в структуре образовательной программы

Дисциплина "Электроника и схемотехника" представляет собой дисциплину обязательной части блока 1 «Дисциплины (модули)».

4. Виды учебной работы по дисциплине.

Виды учебной работы по дисциплине зафиксированы учебным планом основной профессиональной образовательной программы по указанному направлению и профилю, выражаются в академических часах. Часы контактной работы и самостоятельной работы обучающегося и часы, отводимые на процедуры контроля, могут различаться в учебных планах ОПОП по формам обучения. Объем контактной работы включает часы контактной аудиторной работы (лекции/практические занятия/лабораторные работы), контактной внеаудиторной работы (контроль самостоятельной работы), часы контактной работы в период аттестации. Контактная работа, в том числе может проводиться посредством электронной информационно-образовательной среды университета с использованием ресурсов сети Интернет и дистанционных технологий

5. Содержание дисциплины, структурированное по темам (разделам)

Исходя из рамок, установленных учебным планом по трудоемкости и видам учебной работы по дисциплине, преподаватель самостоятельно выбирает тематику занятий по формам и количеству часов проведения контактной работы: лекции и иные учебные занятия, предусматривающие преимущественную передачу учебной информации преподавателем и (или) занятия семинарского типа (семинары, практические занятия, практикумы, лабораторные работы, коллоквиумы и иные аналогичные занятия), и (или) групповые консультации, и (или) индивидуальную работу обучающихся с преподавателем, в том числе индивидуальные консультации (по курсовым работам/проектам – при наличии курсовой работы/проекта по данной дисциплине в учебном плане). Рекомендуемая тематика занятий максимально полно реализуется в контактной работе с обучающимися очной формы обучения. В случае реализации образовательной программы в заочной / очно-заочной форме трудоемкость дисциплины сохраняется, однако объем учебного материала в значительной части осваивается обучающимися в форме самостоятельной работы. При этом требования к ожидаемым образовательным результатам обучающихся по данной дисциплине не зависят от формы реализации образовательной программы.

№	Наименование раздела	Содержание раздела
1	Физические основы полупроводников.	Энергетические уровни и зоны. Проводники, полупроводники и диэлектрики. Собственная проводимость полупроводников. Примесная проводимость полупроводников. Процессы переноса зарядов в полупроводниках. Электронно-дырочные переходы, их свойства, характеристики и виды.
2	Полупроводниковые диоды.	Принцип работы диода. Особенности вольт-амперных характеристик диодов. Выпрямительные

		диоды. Импульсные диоды. Туннельные диоды. Диоды Шотки. Варикапы. Стабилитроны.
3	Биполярные и полевые транзисторы.	Физические процессы в биполярном транзисторе. Схемы включения биполярных транзисторов. Режимы работы биполярных транзисторов. Физические процессы в полевых транзисторах с управляющим p-n-переходом. Физические процессы в полевых транзисторах с изолированным затвором со встроенным каналом. Физические процессы в полевых транзисторах с индуцированным каналом. Схемы включения полевых транзисторов.
4	Оптоэлектронные полупроводниковые приборы.	Оптоэлектронные приборы на основе внешнего фотоэффекта. Фотоэлементы. Фотоэлектронные умножители. Фотоэлектронные приборы на основе внутреннего фотоэффекта. Фоторезисторы. Фотодиоды. Фототранзисторы. Светодиоды. Оптроны. Люминесцентные индикаторы. Жидкокристаллические индикаторы. Полупроводниковые знакосинтезирующие индикаторы. Дисплеи.
5	Аналоговые устройства.	Однофазные выпрямители на диодах. Двухполупериодная схема выпрямления. Мостовая схема. Простейшие основные каскады усилителей на транзисторах для различных схем включения и их свойства. Обратная связь в усилителях и ее влияние на свойства исходных усилителей без обратной связи. Дифференциальный усилитель. Операционные усилители. Генераторы электрических колебаний. Мультивибраторы.
6	Основы теории логических функций.	Логические функции и их элементы. Основы булевой алгебры. Представление и преобразование логических функций. Минимизация логических функций. Структура и принцип действия логических элементов. Основные параметры и характеристики логических элементов.
7	Комбинационные логические устройства.	Шифраторы и дешифраторы. Мультиплексоры и демультиплексоры. Преобразователи кодов. Сумматоры. Компараторы. Арифметико-логическое устройство.
8	Последовательностные логические устройства.	Понятие триггера. RS-триггеры и их разновидности. JK-триггеры. D-триггеры. T-триггеры. Несимметричные триггеры. Понятие о цифровых автоматах. Понятие регистра. Сдвиговые регистры. Синхронные сдвиговые регистры с обратными связями. Функциональные узлы на базе регистров сдвига. Электронные счетчики.

6. Рекомендуемая тематика учебных занятий в форме контактной работы

Рекомендуемая тематика учебных занятий *лекционного* типа (предусматривающих преимущественную передачу учебной информации преподавателями):

№	Наименование раздела	Темы лекций
1	Физические основы полупроводников.	Лекция 1. Энергетические уровни и зоны. Лекция 2. Процессы переноса зарядов в полупроводниках. Лекция 3-4. Электронно-дырочные переходы и их свойства.
2	Полупроводниковые диоды.	Лекция 5. Принцип работы диода. ВАХ диода. Лекция 6. Основные виды диодов и их свойства.
3	Биполярные и полевые транзисторы.	Лекция 7. Физические процессы в биполярном транзисторе. Режимы и схемы работы биполярных транзисторов. Лекция 8. Физические процессы в полевых транзисторах. Схемы включения полевых транзисторов.
4	Оптоэлектронные полупроводниковые приборы.	Лекция 9-10. Оптоэлектронные приборы и их свойства.
5	Аналоговые устройства.	Лекции 11-12. Аналоговые устройства обработки сигналов.
6	Основы теории логических функций.	Лекция 13. Булева алгебра. Лекция 14. Логические элементы.
7	Комбинационные логические устройства.	Лекции 15-16. Комбинационные логические устройства.
8	Последовательностные логические устройства.	Лекции 17-18. Последовательностные логические устройства.

Рекомендуемый перечень *лабораторных* работ:

№	Наименование раздела	Темы лабораторной работы
1	Физические основы полупроводников.	1. Введение в среду компьютерного моделирования Multisim.
2	Полупроводниковые диоды.	1. Исследование диодов и стабилитронов.
3	Биполярные и полевые транзисторы.	1. Исследование принципа работы биполярного транзистора, включенного по схеме с общей базой и с общим эмиттером. 2. Исследование принципа работы полевого транзистора.
4	Оптоэлектронные полупроводниковые приборы.	1. Исследование вольт-амперной характеристики светодиода. 2. Исследование характеристик диодной оптопары.
5	Аналоговые устройства.	1. Исследование резистивного усилителя низкой частоты на биполярном транзисторе. 2. Исследование мультивибраторов на операционных усилителях.
6	Основы теории логических функций.	Лабораторные работы не предусмотрены
7	Комбинационные логические устройства.	1. Исследование работы шифраторов и дешифраторов. 2. Исследование мультиплексоров и демультиплексоров.

		3. Исследование преобразователей кодов.
8	Последовательностные логические устройства.	1. Исследование триггеров. 2. Исследование регистров памяти и регистров сдвига. 3. Исследование счетчиков.

Требования к самостоятельной работе обучающихся

1. Работа с лекционным материалом, предусматривающая проработку конспекта лекций и учебной литературы, по всем темам из п. 6 настоящей рабочей программы.

2. Обработка экспериментальных данных, полученных в ходе выполнения лабораторных работ по всем темам из п. 6 настоящей рабочей программы. Проработка теоретического материала к защите лабораторных работ.

Руководствуясь положениями статьи 47 и статьи 48 Федерального закона от 29 декабря 2012 г. N 273-ФЗ «Об образовании в Российской Федерации» научно-педагогические работники и иные лица, привлекаемые университетом к реализации данной образовательной программы, пользуются предоставленными академическими правами и свободами в части свободы преподавания, свободы от вмешательства в профессиональную деятельность; свободы выбора и использования педагогически обоснованных форм, средств, методов обучения и воспитания; права на творческую инициативу, разработку и применение авторских программ и методов обучения и воспитания в пределах реализуемой образовательной программы и отдельной дисциплины.

Исходя из рамок, установленных учебным планом по трудоемкости и видам учебной работы по дисциплине, преподаватель самостоятельно выбирает тематику занятий по формам и количеству часов проведения контактной работы: лекции и иные учебные занятия, предусматривающие преимущественную передачу учебной информации преподавателем и (или) занятия семинарского типа (семинары, практические занятия, практикумы, лабораторные работы, коллоквиумы и иные аналогичные занятия), и (или) групповые консультации, и (или) индивидуальную работу обучающихся с преподавателем, в том числе индивидуальные консультации (по курсовым работам/проектам – при наличии курсовой работы/проекта по данной дисциплине в учебном плане).

Рекомендуемая тематика занятий максимально полно реализуется в контактной работе с обучающимися очной формы обучения. В случае реализации образовательной программы в заочной / очно-заочной форме трудоемкость дисциплины сохраняется, однако объем учебного материала в значительной части осваивается обучающимися в форме самостоятельной работы. При этом требования к ожидаемым образовательным результатам обучающихся по данной дисциплине не зависят от формы реализации образовательной программы.

7. Методические рекомендации по видам занятий

Лекционные занятия.

В ходе лекционных занятий обучающимся рекомендуется выполнять следующие действия. Вести конспектирование учебного материала. Обращать внимание на категории, формулировки, раскрывающие содержание тех или иных явлений и процессов, научные выводы и практические рекомендации по их применению. Задавать преподавателю уточняющие вопросы с целью уяснения теоретических положений, разрешения спорных ситуаций.

Желательно оставить в рабочих конспектах поля, на которых во внеаудиторное время можно сделать пометки из рекомендованной литературы, дополняющие материал

прослушанной лекции, а также подчеркивающие особую важность тех или иных теоретических положений.

Лабораторные занятия.

На лабораторных занятиях в зависимости от темы занятия выполняется поиск информации по конкретной теме; подготовка теоретического материала к защите лабораторных работ на основе контрольных вопросов; обсуждение в круглых столах наиболее важных вопросов; разбор конкретных ошибок с группой студентов.

Самостоятельная работа.

Самостоятельная работа осуществляется в виде изучения литературы, эмпирических данных по публикациям и конкретных ситуаций из практики, подготовке индивидуальных работ, работа с лекционным материалом, самостоятельное изучение отдельных тем дисциплины; поиск и обзор литературы и электронных источников; чтение и изучение учебника и учебных пособий.

8. Фонд оценочных средств

8.1. Перечень компетенций с указанием этапов их формирования в процессе освоения образовательной программы в рамках учебной дисциплины

Основными этапами формирования указанных компетенций при изучении обучающимися дисциплины являются последовательное изучение содержательно связанных между собой тем учебных занятий. Изучение каждой темы предполагает овладение обучающимися необходимыми компетенциями. Результат аттестации обучающихся на различных этапах формирования компетенций показывает уровень освоения компетенций.

	Контролируемые разделы (темы) дисциплины	**Индекс контроли-руемой компетенции (или её части)**	**Оценочные средства по этапам формирования компетенций**
			текущий контроль по дисциплине
1	Физические основы полупроводников.	ОПК-4	Опрос
2	Полупроводниковые диоды.	ОПК-4	Выполнение и защита лабораторных работ
3	Биполярные и полевые транзисторы.	ОПК-4	Выполнение и защита лабораторных работ
4	Оптоэлектронные полупроводниковые приборы.	ОПК-4	Выполнение и защита лабораторных работ
5	Аналоговые устройства.	ОПК-4	Выполнение и защита лабораторных работ
6	Основы теории логических функций.	ОПК-4	Выполнение и защита лабораторных работ
7	Комбинационные логические устройства.	ОПК-4	Выполнение и защита лабораторных работ
8	Последовательностные логические устройства.	ОПК-4	Выполнение и защита лабораторных работ

8.2. Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений и навыков и (или) опыта деятельности процессе текущего контроля

Основные вопросы для защиты лабораторных работ и собеседования.

Тема 1. Физические основы полупроводников.

1) Назовите особенности полупроводникового материала.

2) Что называется донорной примесью?

3) Что называется акцепторной примесью?

4) Что называется p-n-переходом?

5) Почему p-n-переход часто называют запирающим слоем?

6) Дайте характеристику обратимому и необратимому пробою p-n перехода.

7) Объяснить назначение симулятора ***Multisim***.

8) Кратко описать функциональные возможности программ моделирования.

9) Что такое моделирование?

10) Объяснить назначение функционального генератора.

11) Объяснить назначение осциллографа и особенности его настройки.

12) Объяснить назначение ***Bode Plotter***, особенности настройки.

13) Каким образом можно запустить процесс моделирования.

14) Кратко описать суть метода, лежащего в основе моделирования ***Multisim***.

15) На чем основано компьютерное моделирование электронных устройств?

16) Привести примеры компьютерных программ, используемых для моделирования электронных устройств.

Тема 2. Полупроводниковые диоды.

1. Что такое полупроводниковый диод?

2. Из каких материалов изготавливаются диоды?

3. Сколько *p*-*n*-переходов содержит диод?

4. Чем отличаются диоды, изготовленные из различных материалов?

5. Какие приборы необходимы для снятия вольт-амперной характеристики диодов?

6. Изобразить вольт-амперную характеристику диода. Дать пояснения о процессах, соответствующих характерным участкам вольт-амперной характеристики.

7. Перечислить основные параметры диодов. Охарактеризовать каждый из них.

8. Как определить режим работы диода по нагрузочной прямой?

9. Указать разновидности полупроводниковых диодов. Пояснить их особенности и область применения.

Тема 3. Биполярные и полевые транзисторы.

1) Что такое биполярный транзистор и для чего он используется?

2) Объяснить сущность процессов инжекции и экстракции неосновных носителей заряда в транзисторе.

3) Как образуется ток базы?

4) Как образуется обратный ток коллектора и почему он сильно возрастает при повышении температуры?

5) Каков механизм влияния коллекторного напряжения на входную характеристику?

6) Что такое коэффициент передачи тока эмиттера?

7) Что такое коэффициент переноса неосновных носителей?

8) Какими достоинствами и недостатками обладает схема с общей базой?

9) Изобразить схемы включения биполярных транзисторов типов *p*-*n*-*p* и *n*-*p*-*n* в режимах отсечки, насыщения и активном. В каком из этих режимов возможно активное управление коллекторным током?

10) Почему схема с общим эмиттером чувствительна к изменениям температуры?

11) Какими преимуществами обладает схема с общим эмиттером?

12) Изобразить схемы включения с общим эмиттером транзисторов типа *p*-*n*-*p* и *n*-*p*-*n*.

13) В каком из режимов работы транзистора возможно активное управление коллекторным током?

14) Объяснить принцип работы полевого транзистора с управляющим *p*-*n*-переходом.

15) Объясните принцип работы полевого транзистора с изолированным затвором и индуцированным каналом.

16) Объясните принцип работы полевого транзистора с изолированным затвором и встроенным каналом.

17) Какие характеристики и параметры определяют основные свойства полевых транзисторов?

18) Почему большое входное сопротивление является достоинством электронного прибора?

19) Почему при изменении напряжения между стоком и истоком толщина канала вдоль его длины меняется неодинаково?

20) Что такое напряжение насыщения между стоком и стоком нас и напряжение отсечки между затвором и истоком?

Тема 4. Оптоэлектронные полупроводниковые приборы.

1) Что представляет собой светоизлучающий диод и для чего он используется?

2) Нарисовать световую характеристику и объясните ее.

3) Чем определяется цвет свечения светодиода?

4) Можно ли использовать инфракрасный светодиод в качестве фотоприемника инфракрасного излучения?

5) Указать основные достоинства и недостатки светодиодов.

6) Указать диапазон рабочих токов светодиодов.

7) Назовите основные типы оптопар.

8) Приведите основные достоинства и недостатки оптопар.

9) Назовите основные параметры и характеристики диодных оптопар.

10) Укажите области применения оптопар.

Тема 5. Аналоговые устройства.

1) Дать определение основным параметрам усилителя.

2) Как зависит коэффициент усиления по напряжению от режима работы каскада усиления по постоянному току? Дать качественный анализ.

3) Как обеспечивается стабилизация режима работы по постоянному току?

4) Как определяется коэффициент усиления транзистора?

5) Что происходит с фазами сигнала на входе и выходе схемы? Почему?

6) Как определить постоянную мощность, рассеиваемую на коллекторе транзистора?

7) Объясните, чем определяются режимы работы каскада усиления по постоянному и переменному току.

8) Объясните особенности прохождения импульсных сигналов через усилитель.

9) Что является причиной возникновения линейных (нелинейных) искажений

в усилителе?

10) Как определяются нелинейные искажения в усилительном каскаде?

11) Какие виды обратных связей используются в аналоговых электронных устройствах?

12) Как влияет обратная связь на основные показатели и характеристики усилителей?

13) Изобразите схемы усилительных каскадов с общим эмиттером, общей базой, общим коллектором.

14) Изобразите схемы усилительных каскадов с общим стоком, общим затвором, общим истоком.

15) Объяснить назначение элементов усилительного каскада.

16) Как можно добиться значительного усиления входного напряжения?

17) Объясните принцип работы симметричного мультивибратора на операционном усилителе.

18) Объясните принцип работы несимметричного мультивибратора на операционном усилителе.

19) Объясните принцип работы ждущего мультивибратора на операционном усилителе.

20) Чему равна скважность импульсов симметричного мультивибратора?

21) Способы регулирования длительности импульсов.

22) Какие изменения следует произвести в схеме ждущего мультивибратора, чтобы сформировать на выходе отрицательный перепад напряжения?

Тема 7. Комбинационные логические устройства.

1) Что называется базовым набором логических элементов?

2) Записать условное графическое обозначение, логическое уравнение и таблицу истинности логического элементов: И, НЕ, ИЛИ, ИЛИ-НЕ, И-НЕ.

3) Можно ли соединять между собой два (или более) выхода логических элементов?

4) Пояснить различия между комбинационным и последовательностным логическими устройствами.

5) Пояснить последовательность синтеза логического устройства.

6) Для каких целей используется минимизация логической функции?

7) Какие способы минимизации логических функций существуют?

8) Что называется шифратором, дешифратором? Привести условное графическое обознач шифратора, дешифратора и пояснить принцип их функционирования.

9) Что называется мультиплексором, демультиплексором? Привести условное графическое обозначение мультиплексора, демультиплексора и пояснить принцип их функционирования.

10) Что называется сумматором? Какие существуют разновидности сумматоров? Привести условное графическое обозначение и пояснить принцип функционирования одноразрядного асинхронного сумматора.

Тема 8. Последовательностные логические устройства.

1) Привести определение триггера, перечислить его отличительные особенности.
2) Какие признаки используют при классификации триггеров?
3) Какие триггеры называются асинхронными, а какие синхронными?
4) С какой целью ИС триггеров дополняют асинхронными входами?
5) В чем отличие синхронных триггеров, управляемых уровнем, от триггеров с динамическим управлением?
6) Какой тип триггеров называется «универсальным» и почему?
7) Приведите определение, схему, условное обозначение и принцип работы RS-триггера.
8) Приведите определение, схему, условное обозначение и принцип работы D-триггера.
9) Приведите определение, схему, условное обозначение и принцип работы JK-триггера.
10) Приведите определение, схему, условное обозначение и принцип работы T-триггера.

11) Назначение регистров.
12) По каким признакам классифицируются регистры?
13) Чем определяется разрядность регистров?
14) Назначение параллельного (статического) регистра.
15) Объяснить принцип работы последовательного регистра.
16) Объяснить принцип работы параллельного регистра.
17) Объяснить принцип работы последовательно-параллельного регистра.
18) Объяснить принцип работы параллельно-последовательного регистра.
19) Какие функции может выполнять регистр сдвига?
20) Пояснить принцип работы суммирующего асинхронного двоичного счетчика. Привести временные диаграммы.
21) Пояснить принцип работы вычитающего асинхронного двоичного счетчика. Привести временные диаграммы.
22) Почему при подключении счетных входов триггеров к инверсным выходам предыдущих каскадов счетчик на D-триггерах работает как суммирующий, а при подключении к прямым – как вычитающий?

23) В каком режиме будет работать счетчик на JK-триггерах при подключении счетных входов триггеров к прямым выходам предыдущих каскадов? Как изменится режим работы счетчика при подключении счетных входов триггеров к инверсным выходам?

24) Чем определяется разрядность цифровых счетчиков?

25) Какими способами можно изменить коэффициент пересчета счетчика?

8.3. Перечень вопросов и заданий для промежуточной аттестации по дисциплине

Вопросы для промежуточного контроля (экзамена)

1. Что понимается под разрешенными и запрещенными энергетическими зонами?
2. Что означает уровень Ферми? Как влияет концентрация примеси на положение уровня Ферми?
3. Собственная электропроводность полупроводника.
4. Диффузия и дрейф носителей заряда.
5. Температурная зависимость концентрации носителей заряда в полупроводнике.
6. Что такое примесная электропроводность полупроводника?
7. Механизм образования электронно-дырочного перехода и его вольт-амперная характеристика.
8. Барьерная и диффузионная ёмкости *p-n* –перехода.
9. Как влияет внешнее напряжение на высоту потенциального барьера и ширину *p-n*-перехода.
10. Полупроводниковый диод, принцип работы, вольт-амперная характеристика.
11. Как влияет повышение температуры на прямую ветвь вольт-амперной характеристики полупроводникового диода?
12. Стабилитрон, туннельный диод особенности работы, схемы включения.
13. Принцип работы варикапа. Почему в варикапах используется только барьерная ёмкость и не используется диффузионная ёмкость?
14. Принцип работы биполярного транзистора. Основные схемы включения.
15. Чем объясняется усиление электрических колебаний но мощности в биполярном транзисторе?
16. Влияние температуры на характеристики транзистора?
17. Принцип работы полевого транзистора с управляющим *p-n* – переходом.
18. Почему полевые транзисторы с управляющим *p-n* - переходом не должны работать при прямом напряжении на входе?
19. Почему при изменении напряжения толщина канала вдоль его длины меняется неодинаково?
20. Принцип работы полевого транзистора с изолированным затвором со встроенным каналом.
21. Принцип работы полевого транзистора с индуцированным каналом.
22. Внешний и внутренний фотоэффект.
23. Какие физические факторы влияют на световую характеристику фоторезистора при больших световых потоках?
24. Как в фотоэлементе происходит непосредственное преобразование световой энергии в электрическую?
25. Принцип работы светодиода, цветные светодиоды, характеристики, особенности.
26. Принцип и особенности работы оптрона.
27. Принцип работы фотоэлектронного умножителя.

28. Понятие и виды систем счисления. Алгоритмы перевода чисел из одной системы в другую.

29. При помощи, каких операций выполняется операция умножения двоичных чисел в цифровой технике?

30. Что называется булевыми константами и переменными в алгебре логики?

31. Привести основные операции булевой алгебры. Как они описываются с помощью таблиц истинности и с помощью алгебраических выражений.

32. Базовые логические элементы (НЕ, И, ИЛИ) и их электрические аналоги (ТТЛ-логика). Принципы работы, особенности.

33. Базовые логические элементы (НЕ, И, ИЛИ) и их электрические аналоги (ЭСЛ-логика). Принципы работы, особенности.

34. Как строится структурная схема логического устройства по функции алгебры логики?

35. В чем заключается принцип двойственности и каково его практическое значение для построения схем логических устройств?

36. Что такое функционально полная система и базис логических элементов?

37. В чем заключается цель и принципы минимизации логических устройств, реализуемых на ИС?

38. Каковы назначение и структурная схема мультиплексора?

39. Каково назначение демультиплексора? Привести его структурную схему.

40. Каково назначение преобразователя кодов?

41. Каковы назначение и логическая схема шифратора?

42. Приведите схему двоично-десятичного дешифратора.

43. Каковы назначение и логическая схема цифрового компаратора?

44. В чем основное отличие многоразрядных сумматоров параллельного и последовательного действий?

45. Назначение и состав триггерных устройств, их разновидности.

46. Привести определение, схему, условное обозначение и принцип работы RS-триггера.

47. Привести определение, схему, условное обозначение и принцип работы D-триггера.

48. Привести определение, схему, условное обозначение и принцип работы JK-триггера.

49. Привести определение, схему, условное обозначение и принцип работы T-триггера.

50. Назначение и классификация регистров, разрядность регистров.

51. Назначение параллельного (статического) регистра.

52. Принцип работы последовательного регистра.

53. Принцип работы параллельного регистра.

54. Принцип работы последовательно-параллельного регистра.

55. Принцип работы параллельно-последовательного регистра.

56. Регистр сдвига.

57. Параметры, назначение и классификация счетчиков.

58. Каким образом достигается повышение быстродействия счетчиков?

59. Как осуществляется предварительная установка счетчиков?

60. В чем сущность метода управляемого сброса?

8.4. Планируемые уровни сформированности компетенций обучающихся и критерии оценивания

Уровни	Содержательн	Основные признаки	Пятибалль	Двухба	БРС, %

	ое описание уровня	выделения уровня (этапы формирования компетенции, критерии оценки сформированности)	ная шкала (академическая) оценка	лльная шакала, зачет	освоения (рейтинговая оценка)
Повышенный	Творческая деятельность	*Включает нижестоящий уровень.* Умение самостоятельно принимать решение, решать проблему/задачу теоретического и прикладного характера на основе изученных методов, приемов, технологий	отлично	зачтено	86-100
Базовый	Применение знаний и умений в более широких контекстах учебной и профессиональной деятельности, нежели по образцу с большей степени самостоятельности и инициативы	*Включает нижестоящий уровень.* Способность собирать, систематизировать, анализировать и грамотно использовать информацию из самостоятельно найденных теоретических источников и иллюстрировать ими теоретические положения или обосновывать практику применения	хорошо		71-85
Удовлетворительный (достаточный)	Репродуктивная деятельность	Изложение в пределах задач курса теоретически и практически контролируемого материала	удовлетворительно		55-70
Недостаточный	Отсутствие признаков удовлетворительного уровня		неудовлетворительно	не зачтено	Менее 55

9. Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины.

Основная литература

1. Прянишников В. А. Электротехника и ТОЭ в примерах и задачах: практ. пособие/ В. А. Прянишников, Е. А. Петров, Ю. М. Осипов ; под ред. В. А. Прянишникова. – СПб.: КОРОНА-Век, 2008. - 334 с.: ил. (25 экз)
2. Морозова Н. Ю. Электротехника и электроника: учеб. для вузов/ Н. Ю. Морозова. - М.: Академия, 2007. - 255, с. (59 экз)

Дополнительная литература

1. Сорокин В. С. Материалы и элементы электронной техники: учеб. для вузов : в 2 т./ В. С. Сорокин, Б. Л. Антипов, Н. П. Лазарева. - М.: Академия, 2006.
Т.1: Проводники, полупроводники, диэлектрики. - 439, с. (19 экз)
Т.2: Активные диэлектрики, магнитные материалы, элементы электронной техники. - 376 с. (19 экз)
2. Основы электроники, радиотехники и связи: учеб. пособие для вузов / А. Д. Гуменюк [и др.], 2008. - 479, с. (14 экз)

10. Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины (модуля).

- НЭБ Национальная электронная библиотека, диссертации и прочие издания
- eLIBRARY.RU Научная электронная библиотека, книги, статьи, тезисы докладов конференций
- Гребенников Электронная библиотека ИД журналы
- ЭБС Лань книги, журналы
- ЭБС Консультант студента
- ПРОСПЕКТ ЭБС
- ЭБС ZNANIUM.COM
- РГБ Информационное обслуживание по МБА
- БЕН РАН
- Электронно-библиотечная система (ЭБС) Кантитана (https://elib.kantiana.ru/)

11. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине.

Программное обеспечение обучения включает в себя:

- система электронного образовательного контента БФУ им. И. Канта – www.lms-3.kantiana.ru, обеспечивающую разработку и комплексное использование электронных образовательных ресурсов;
- серверное программное обеспечение, необходимое для функционирования сервера и связи с системой электронного обучения через Интернет;
- корпоративная платформа Microsoft Teams;
- установленное на рабочих местах обучающихся ПО: Microsoft Windows 7, Microsoft Office Standart 2010, антивирусное программное обеспечение Kaspersky Endpoint Security.
- система схемотехнического проектирования Multisim

12. Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине.

Для проведения занятий лекционного типа, практических и семинарских занятий используются специальные помещения (учебные аудитории), оборудованные техническими

средствами обучения – мультимедийной проекционной техникой. Для проведения занятий лекционного типа используются наборы демонстрационного оборудования.

Для проведения лабораторных работ, (практических занятий – при необходимости) используются специальные помещения (учебные аудитории), оснащенные специализированным лабораторным оборудованием: персональными компьютерами с возможностью выхода в интернет и с установленным программным обеспечением, заявленным в п.11.

Для проведения групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации используются специальные помещения (учебные аудитории), оборудованные специализированной мебелью (для обучающихся), меловой / маркерной доской.

Для организации самостоятельной работы обучающимся предоставляются помещения, оснащенные компьютерной техникой с возможностью подключения к сети «Интернет» и обеспечением доступа в электронную информационно-образовательную среду университета.

Для обучения инвалидов и лиц с ограниченными возможностями здоровья университетом могут быть представлены специализированные средства обучения, в том числе технические средства коллективного и индивидуального пользования.

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
федеральное государственное автономное образовательное учреждение высшего образования «Балтийский федеральный университет имени Иммануила Канта»
Институт физико-математических наук и информационных технологий

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

«Аппаратные средства вычислительной техники»

Шифр: 10.05.01
Специальность: «Компьютерная безопасность»
Специализация: «Математические методы защиты информации»
Квалификация (степень) выпускника: специалист по защите информации

Калининград
2022

Лист согласования

Составитель: Горбачев Андрей Александрович к.т.н., доцент

Рабочая программа утверждена на заседании учебно-методического совета института физико-математических наук и информационных технологий

Протокол № 01/22 от «01» февраля 2022 г.

Председатель учебно-методического
совета института физико-
математических наук и информационных
технологий

Первый заместитель директора Шпилевой А. А
ИФМНиИТ, к. ф.-м. н., доцент

Ведущий менеджер Е.П.Ставицкая

Содержание

1.Наименование дисциплины: «Аппаратные средства вычислительной техники».

Цель дисциплины: изучение основных понятий архитектуры современного компьютера, устройства и принципа действия важнейших компонентов аппаратных средств компьютера, механизмов пересылки и управления информацией.

2. Перечень планируемых результатов обучения по дисциплине, соотнесенных с планируемыми результатами освоения образовательной программы

Код компетенции	Результаты освоения образовательной программы (ИДК)	Результаты обучения по дисциплине
ОПК-4 Способность анализировать физическую сущность явлений и процессов, лежащих в основе функционирования микроэлектронной техники, применять основные физические законы и модели для решения задач профессиональной деятельности.	ОПК-4.1. Демонстрирует знание физических законов и моделей, необходимых при решении задач обеспечения защиты информации. ОПК-4.2. Применяет необходимые физические законы и модели для решения обеспечения защиты информации. ОПК-4.3. Владеет навыками моделирования для решения задач обеспечения защиты информации.	***Знать***: - архитектуру основных типов современных компьютерных систем; - структуру и физические принципы работы современных и перспективных микропроцессоров; - физические принципы работы элементов и функциональных узлов электронной аппаратуры; - принципы построения и работы ПЭВМ; ***Уметь***: - определять состав компьютера: тип процессора и его параметры, тип модулей памяти и их характеристики, тип видеокарты, состав и параметры периферийных устройств; - работать с современной элементной базой электронной аппаратуры. - определять направления использования ЭВМ определенного класса для решения служебных задач; ***Владеть***: - навыками применения технических и программных средств тестирования с целью определения исправности компьютера и оценки его производительности; - навыками устранения неисправностей и технического обслуживания СВТ и периферийного оборудования; - навыками формирования структуры СВТ и выбора режимов их функционирования.

3. Место дисциплины в структуре образовательной программы

Дисциплина "Аппаратные средства вычислительной техники" представляет собой дисциплину обязательной части блока дисциплин подготовки студентов, входит в Модуль 6 «Техническая защита информации».

4. Виды учебной работы по дисциплине.

Виды учебной работы по дисциплине зафиксированы учебным планом основной профессиональной образовательной программы по указанному направлению и профилю, выражаются в академических часах. Часы контактной работы и самостоятельной работы обучающегося и часы, отводимые на процедуры контроля, могут различаться в учебных планах ОПОП по формам обучения. Объем контактной работы включает часы контактной аудиторной работы (лекции/практические занятия/лабораторные работы), контактной внеаудиторной работы (контроль самостоятельной работы), часы контактной работы в период аттестации. Контактная работа, в том числе может проводиться посредством электронной информационно-образовательной среды университета с использованием ресурсов сети Интернет и дистанционных технологий

5. Содержание дисциплины, структурированное по темам (разделам)

Исходя из рамок, установленных учебным планом по трудоемкости и видам учебной работы по дисциплине, преподаватель самостоятельно выбирает тематику занятий по формам и количеству часов проведения контактной работы: лекции и иные учебные занятия, предусматривающие преимущественную передачу учебной информации преподавателем и (или) занятия семинарского типа (семинары, практические занятия, практикумы, лабораторные работы, коллоквиумы и иные аналогичные занятия), и (или) групповые консультации, и (или) индивидуальную работу обучающихся с преподавателем, в том числе индивидуальные консультации (по курсовым работам/проектам – при наличии курсовой работы/проекта по данной дисциплине в учебном плане). Рекомендуемая тематика занятий максимально полно реализуется в контактной работе с обучающимися очной формы обучения. В случае реализации образовательной программы в заочной / очно-заочной форме трудоемкость дисциплины сохраняется, однако объем учебного материала в значительной части осваивается обучающимися в форме самостоятельной работы. При этом требования к ожидаемым образовательным результатам обучающихся по данной дисциплине не зависят от формы реализации образовательной программы.

№	Наименование раздела	Содержание раздела
1	Введение. История развития, классификация ЭВМ.	Практические потребности и технические предпосылки создания ЭВМ. Эволюция ЭВМ. Принцип фон-Неймана. Основные классы ЭВМ. Развитие элементной базы. Дискретные элементы радиоэлектроники. Интегральные схемы. Схемотехническая интеграция. Классификация ИС. Понятие МП. Поколения МП и их основные характеристики. Основные этапы производственного цикла ИС и МП. Виды технологии производства ИС и МП. Основные промышленные линии МП. Функциональная интеграция. Направления функциональной электроники. Перспективные МП.
2	Структурная организация ЭВМ.	Основные блоки ЭВМ и их назначение. Микропроцессор. Системная шина. Основная память.

		Внешняя память. Источник питания. Таймер. Внешние устройства. Мини- и микро-ЭВМ.
3	Командное управление.	Архитектура системы команд. Классификация по составу и сложности команд: CISC, RISC, VLIW. Классификация по месту хранения операндов: стековая, аккумуляторная, регистровая, с выделенным доступом к памяти. Их характеристики. Типы команд: пересылки данных, арифметической и логической обработки, работы со строками, команды SIMD, команды преобразования, команды ввода/вывода, команды управления потоком команд. Форматы команд. Система операций. Система прерываний.
4	Микропроцессоры.	Микропроцессорная техника: назначение и характеристики МП, функции МП, параметры МП, обобщенная структура МП. Физическая и функциональная структуры центрального процессора. Устройство управления. Арифметико-логическое устройство. Схема управления шиной и портами. Поколения МП и их основные характеристики. Обзор и характеристики МП типа CISC. Многоядерные МП.
5	Организация и структура памяти ЭВМ.	Общие принципы организации памяти. Иерархия памяти. Микропроцессорная память. Кэш-память. Постоянная память. Полупостоянная память. Буферная память. Основная память (ОЗУ). Виды модулей ОЗУ. Типы ОЗУ. Логическая структура памяти. Виртуальная память. Распределение памяти.
6	ПЭВМ.	Архитектура современных ПЭВМ. Системная плата, ее назначение, основные элементы и их взаимодействие в системе. Системная магистраль. Основные стандарты системных магистралей (шин). Буферизация шин. Управление системной магистралью. Подключение дополнительных и интерфейсных схем. Вопросы проектирования ПЭВМ.
7	Рабочие станции и серверы.	АРМ, средства обработки сигналов на базе ПЭВМ, архитектура, рабочих станций и серверов. Универсальные и специальные ЭВМ высокой производительности. Архитектура специализированных вычислительных комплексов. Архитектура комплексов, ориентированных на программное обеспечение, машины баз данных, объектно-ориентированная архитектура. Вопросы проектирования рабочих станций и серверов.
8	Периферийные устройства.	Назначение, состав и технические характеристики периферийных устройств и оборудования ЭВМ. Периферийное оборудование ПЭВМ. Средства ввода информации в ЭВМ. Клавиатура и графический манипулятор. Средства отображения информации. Видеомонитор. НГМД. НЖМД. Принтер. Устройство ввода информации CD-ROM. Аудиосистема. Коммуникационные устройства. Корпуса, источники питания, система охлаждения.

6. Рекомендуемая тематика учебных занятий в форме контактной работы

Рекомендуемая тематика учебных занятий *лекционного* типа (предусматривающих преимущественную передачу учебной информации преподавателями):

№	Наименование раздела	Темы лекций
1	Введение. История развития, классификация ЭВМ.	Лекция 1. История развития средств ВТ, современное состояние вопроса.
2	Структурная организация ЭВМ.	Лекция 2. Блочная структура ЭВМ. Лекция 3. Основные элементы ЭВМ.
3	Командное управление.	Лекция 4. Архитектура и классификация системы команд. Лекция 5. Типы и форматы команд, система прерываний.
4	Микропроцессоры.	Лекция 6. Назначение и характеристики МП, их структура. Лекция 7. Структура центрального процессора. Многоядерные МП.
5	Организация и структура памяти ЭВМ.	Лекция 8. Общие принципы организации памяти. Лекция 9. Виды памяти и их функции.
6	ПЭВМ.	Лекция 10. Архитектура современных ПЭВМ. Лекция 11. Назначение и функции основных элементов ПЭВМ.
7	Рабочие станции и серверы.	Лекция 12. Рабочие станции и серверы. Лекция 13. Специализированные вычислительные комплексы и их архитектура.
8	Периферийные устройства.	Лекция 14-15. Назначение, состав и характеристики периферийных устройств современных ЭВМ.

Рекомендуемый перечень *лабораторных* работ:

№	Наименование раздела	Темы лабораторной работы
1	Введение. История развития, классификация ЭВМ.	Лабораторные работы не предусмотрены.
2	Структурная организация ЭВМ.	Лабораторная работа 1. Создать на макете работающую модель ЭВМ, включающую в себя: задающий генератор; микроконтроллер; встроенный программатор; индикация состояния портов; источник питания TTL и CMOS. Лабораторная работа 2. Проверить взаимодействие внутренних компонент микроконтроллера: аналого-цифрового преобразователя, EEPROM памяти данных, таймера, EUSART протокола связи с периферией.
3	Командное управление.	Лабораторные работы 3-4. Исследование RISC архитектуры для создания программ реального времени. Написание простых программ на языке высокого уровня микро-Си для PIC контроллера. Лабораторная работа. Исследование организации пересылки данных в порт ввода-вывода, команды

		работы со стеком, АЛУ и регистром флагов.
4	Микропроцессоры.	Лабораторные работы 5-6. Логические и арифметические операции в ALU. Управление внутренней схемотехникой контроллера: настройка таймеров, портов, watch-dog реализация защиты от сбоев.
5	Организация и структура памяти ЭВМ.	Лабораторная работа 7. Исследование принципа работы динамической памяти данных, страничной организации регистровой памяти. Лабораторная работа 8. Защита программного кода от считывания.
6	ПЭВМ.	Лабораторная работа 9. Построение управления системной магистралью. Буферизация адресной шины. Назначение основных элементов макетной платы EasyPIC5.
7	Рабочие станции и серверы.	Лабораторные работы не предусмотрены.
8	Периферийные устройства.	Лабораторные работы 10-11. Исследование средств ввода данных макетной платы. Двухстрочный цифровой LCD экран. Работа USB порта. Информационный обмен с промышленным оборудованием RS232 и RS485. Расширение портов ввода-вывода методом буферизации.

Требования к самостоятельной работе обучающихся

1. Работа с лекционным материалом, предусматривающая проработку конспекта лекций и учебной литературы, по всем темам из п. 6 настоящей рабочей программы.

2. Обработка экспериментальных данных, полученных в ходе выполнения лабораторных работ по всем темам из п. 6 настоящей рабочей программы. Проработка теоретического материала к защите лабораторных работ.

Руководствуясь положениями статьи 47 и статьи 48 Федерального закона от 29 декабря 2012 г. N 273-ФЗ «Об образовании в Российской Федерации» научно-педагогические работники и иные лица, привлекаемые университетом к реализации данной образовательной программы, пользуются предоставленными академическими правами и свободами в части свободы преподавания, свободы от вмешательства в профессиональную деятельность; свободы выбора и использования педагогически обоснованных форм, средств, методов обучения и воспитания; права на творческую инициативу, разработку и применение авторских программ и методов обучения и воспитания в пределах реализуемой образовательной программы и отдельной дисциплины.

Исходя из рамок, установленных учебным планом по трудоемкости и видам учебной работы по дисциплине, преподаватель самостоятельно выбирает тематику занятий по формам и количеству часов проведения контактной работы: лекции и иные учебные занятия, предусматривающие преимущественную передачу учебной информации преподавателем и (или) занятия семинарского типа (семинары, практические занятия, практикумы, лабораторные работы, коллоквиумы и иные аналогичные занятия), и (или) групповые консультации, и (или) индивидуальную работу обучающихся с преподавателем, в том числе индивидуальные консультации (по курсовым работам/проектам – при наличии курсовой работы/проекта по данной дисциплине в учебном плане).

Рекомендуемая тематика занятий максимально полно реализуется в контактной работе с обучающимися очной формы обучения. В случае реализации образовательной

программы в заочной / очно-заочной форме трудоемкость дисциплины сохраняется, однако объем учебного материала в значительной части осваивается обучающимися в форме самостоятельной работы. При этом требования к ожидаемым образовательным результатам обучающихся по данной дисциплине не зависят от формы реализации образовательной программы.

7. Методические рекомендации по видам занятий

Лекционные занятия.

В ходе лекционных занятий обучающимся рекомендуется выполнять следующие действия. Вести конспектирование учебного материала. Обращать внимание на категории, формулировки, раскрывающие содержание тех или иных явлений и процессов, научные выводы и практические рекомендации по их применению. Задавать преподавателю уточняющие вопросы с целью уяснения теоретических положений, разрешения спорных ситуаций.

Желательно оставить в рабочих конспектах поля, на которых во внеаудиторное время можно сделать пометки из рекомендованной литературы, дополняющие материал прослушанной лекции, а также подчеркивающие особую важность тех или иных теоретических положений.

Лабораторные занятия.

На лабораторных занятиях в зависимости от темы занятия выполняется поиск информации по конкретной теме; подготовка теоретического материала к защите лабораторных работ на основе контрольных вопросов; обсуждение в круглых столах наиболее важных вопросов; разбор конкретных ошибок с группой студентов.

Самостоятельная работа.

Самостоятельная работа осуществляется в виде изучения литературы, эмпирических данных по публикациям и конкретных ситуаций из практики, подготовке индивидуальных работ, работа с лекционным материалом, самостоятельное изучение отдельных тем дисциплины; поиск и обзор литературы и электронных источников; чтение и изучение учебника и учебных пособий.

8. Фонд оценочных средств

8.1. Перечень компетенций с указанием этапов их формирования в процессе освоения образовательной программы в рамках учебной дисциплины

Основными этапами формирования указанных компетенций при изучении обучающимися дисциплины являются последовательное изучение содержательно связанных между собой тем учебных занятий. Изучение каждой темы предполагает овладение обучающимися необходимыми компетенциями. Результат аттестации обучающихся на различных этапах формирования компетенций показывает уровень освоения компетенций.

	Контролируемые разделы (темы) дисциплины	**Индекс контроли-руемой компетенции (или её части)**	**Оценочные средства по этапам формирования компетенций**
			текущий контроль по дисциплине
1	Введение. История развития, классификация ЭВМ.	ОПК-4	Опрос
2	Структурная организация ЭВМ.	ОПК-4	Выполнение и защита лабораторных работ

3	Командное управление.	ОПК-4	Выполнение и защита лабораторных работ
4	Микропроцессоры.	ОПК-4	Выполнение и защита лабораторных работ
5	Организация и структура памяти ЭВМ.	ОПК-4	Выполнение и защита лабораторных работ
6	ПЭВМ.	ОПК-4	Выполнение и защита лабораторных работ
7	Рабочие станции и серверы.	ОПК-4	Опрос
8	Периферийные устройства.	ОПК-4	Выполнение и защита лабораторных работ

8.2. Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений и навыков и (или) опыта деятельности процессе текущего контроля

Основные вопросы для защиты лабораторных работ и собеседования.

Тема 2. Структурная организация ЭВМ.
Учебные вопросы:

Характеристики быстродействия ЭВМ , задающий генератор
1. Какие типы задающих генераторов применяются в микропроцессорной технике?
2. Принцип работы кварцевых резонаторов
3. Принципы тактирования выполнения команд микроконтроллером.

Микроконтроллер
1. Назовите основные отличия микропроцессора от микроконтроллера.
2. Как взаимодействуют узлы управления микропроцессора при выполнении программ, последовательность операций?
3. Какие виды шин бывают в микроконтроллерах?

Встроенный программатор
1. Как осуществляется сохранение программ в памяти контроллера?
2. Какие виды памяти применяют для хранения программ и данных в микрочипе?
3. Существуют ли другие средства записи программ в память контроллера?
4. Каким способом защищают интеллектуальную собственность в готовых изделиях?

Индикация состояния портов
1. Что такое порты в МК и как их настроить?
2. Устройство и характеристики LED индикаторов применяемых в демо модели.
3. Для чего и чем ограничивают выходные токи МК портов?
4. Как организовано устранение неопределенности цифровых портов МК при чтении?
5. Какая разрядность и какое количество портов используется в PIC16F887?

Источники питания микроконтроллеров
1. Потребление энергии микроконтроллером в различных режимах работы? Чем достигается энергосбережение при питании от автономных источников?
2. Чем отличаются источники питания разных цифровых технологий (TTL , CMOS)?
3. Оцените нагрузочную способность МК в статическом и динамическом режимах. протоколы связи с периферией.

Передача данных по последовательному каналу RS232.
1. Протокол связи между устройствами USB
2. Асинхронная передача данных EUSART
3. Синхронный режим работы EUSART в чем разница?
4. Инфракрасный протокол связи IrDA где применяется повсеместно?
5. Протокол между автоматизированными системами управления?

Тема 3. Командное управление.
Учебные вопросы:
Применение RISC архитектуры
1. Каким количеством команд обладает RISK процессор PIC16F887?
2. Какие типы команд применяются практически?
3. Что такое язык низкого уровня?
4. Что записывается во FLASH память программ в виде инструкций и какой разрядности для PIC16F887?

Написание программ на языке высокого уровня
1. Что называют языком программирования высокого уровня?
2. Чем отличается интерпретатор от транслятора с языка высокого уровня (приведите примеры)?
3. Какие параметры указываются в проекте до создания программы, применительно к микроконтроллерам. Что такое инициализация внутренней архитектуры?
4. Какая команда не выполняет ни каких действий и для чего она применяется?

Организация пересылки данных в порт ввода-вывода
1. Нарисуйте схематично строение порта ввода вывода микроконтроллера PIC16F887.
2. В чем отличие команд работы с портами TRIS и PORT.
3. Что такое третье- или Z состояние порта ввода-вывода?
4. Как организовано аналого-цифровое преобразование в МК?

Команды работы со стеком
1. Для чего применяют специальную команду и специальный регистр SP?
2. Какова разрядность и глубина стека в PIC16F887?

Тема 4. Микропроцессоры
Структурное построение процессора PIC16F и средства обеспечения его связи с микропроцессорной системой
1. Перечислить логические и арифметические операции процессора
2. Логика работы одноразрядного двоичного сумматора.
3. Принцип построения матричного умножителя.
4. Мультиплексор и его роль в выполнении логических выражений
5. Основные свойства и область применения комбинационных схем.
6. Основные отличительные черты устройств последовательного типа (цифровых автоматов).
7. Признаки, по которым классифицируются триггеры. Разновидности триггеров.
8. Двоичные счетчики и их разновидности.
9. Регистры – их разновидности и структурный состав.
10. Принцип работы регистрового арифметическо-логического устройства.
Управление внутренней схемотехникой контроллера
1. Что понимается под режимами адресации, применяемыми в командах
2. Формат команд (ЦП).
3. Особенности формата команд для CISC и RISC архитектур.

4. Основные черты ЦП с регистрово ориентированной (RISC) архитектурой.
5. Конвейер операций и его реализация в RISC процессорах.
6. Микросистема на базе магистрального интерфейса. Машина фон-Неймана.
7. Микросистемы с гарвардской архитектурой. Структура цифрового процессора сигналов

Логические и арифметические операции в ALU
1. Выполнить арифметическое сложение смежных регистров и проверить регистр 2. флагов.
2. Выполнить логическое хэширование смежных регистров данных с выводом регистра флагов
3. Выполнить random заполнение области памяти данных программатором PICprog.

Настройка таймеров и watch-dog timer контроллера.
1. Настроить 16 битный таймер PIC16F887 на вывод импульса через 1 миллисекунду.
2. Рассчитать количество циклов для организации 1 секундного тайминга для частоты 8 Мгц.
3. Опишите работу программного предделителя таймера (prescaler programmable)
4. Опишите работу WDT и назначение этого узла.

Проверить взаимодействие внутренних компонент микроконтроллера
1. Проверить программно взаимодействие таймера и порта.

Аналого-цифровой преобразователь
1. Обьясните необходимость преобразования аналогового сигнала в цифровой
2. Опишите методы преобразователей и их свойства
3. Как метод преобразования влияет на скорость и точность обработки сигнала?

Тема 5. Организация и структура памяти ЭВМ.
Структурный состав оперативного запоминающего устройства (ОЗУ).
1. По каким адресам в контроллере находятся вектор сброса и вектор прерывания?
2. Опишите страничную организацию PIC контроллера
3. Статическое ОЗУ. Статические запоминающие элементы и структурное построение ОЗУ.
4. Какой алгоритм применяют для записи данных в EEPROM контроллера
5. К какому классу (статическая или динамическая) относится кеш память?

Принцип работы динамической памяти данных
1. Динамическое ОЗУ. Динамические элементы памяти и механизм использования в динамическом ОЗУ.
2. Обьясните необходимость регенерации информации в памяти.
3. Почему нельзя повышать скорость считывания из ячеек динамической памяти?
4. Чем отличаются технологии динамической памяти DDR DDR2 DDR3?

Защита программного кода от считывания
1. Для каких целей необходимо защищать данные контроллеров?
2. Опишите проблему незащищенного канала управления CRT мониторов.
3. Каким способом в PIC контроллерах защищают доступ к коду программы.
4. Возможно ли получить доступ к заблокированному коду опосредованно?
5. Опишите особенные способы взлома защит, известные на данный момент.

Тема 6. ПЭВМ

Назначение основных элементов макетной платы EasyPIC5
1. Опишите работу источника питания.
2. Назначение микропереключателей и перемычек, компонент ввода данных?

Буферизация адресной шины
1. Назначение и принцип работы microProg модуля
2. Построение АЦП на базе демо платы EasyPIC5
3. Запрограммировать USB порт платы на SLAVE режим.

Тема 8. Периферийные устройства.
Периферийное оборудование ПЭВМ.
1. Описать работу двух-строчного LCD индикатора.
2. Описать структуру и работу встроенного LED семисегментного индикатора.
3. Создать программу работы с цифровым термометром D18B20
4. Подключить к порту платы PS2 клавиатуру и настроить взаимодействие.

8.3. Перечень вопросов и заданий для промежуточной аттестации по дисциплине

Вопросы для промежуточного контроля (экзамена)

1. В чем сущность схемотехнической и функциональной интеграции?
2. Привести классификации ЭВМ по: принципу действия, по назначению, по вычислительной мощности.
3. Принципы фон-Неймановской архитектуры ЭВМ.
4. Какая система счисления и почему выбрана в фон-Неймановской ЭВМ для внутреннего представления чисел?
5. Кодирование информации в ЭВМ: стандарт IEEE 754, ASCII, Unicode
6. Общая структура ЭВМ и назначение ее узлов и элементов.
7. Общая структура центрального процессора, назначение и основные элементы.
8. Системная шина, ее состав и назначение.
9. Основные функции и параметры микропроцессора.
10. Физическая и функциональная структуры микропроцессора.
11. Структурная схема и назначение устройства управления.
12. Структурная схема и назначение арифметико-логического устройства.
13. Структурная схема и назначение схемы управления шиной и портами.
14. Микропроцессорная память. Основные регистры, их назначение и флаги.
15. Организация и типовая структура памяти ПК. Характеристики запоминающих устройств.
16. Назначение кэш-памяти, структурная схема, виды кэш-памяти, принципы записи данных.
17. Постоянная память. Назначение, технологии организации записи данных.
18. Флэш-память и полупостоянная память. Назначение, принципы записи данных.
19. Буферная память. Назначение, принципы записи данных.
20. ОЗУ. Назначение, виды, конструктивы.
21. Логическая структура памяти. Адресное пространство.
22. Виртуальная память. Назначение, технология организации.
23. Распределение памяти в ПК: непосредственно адресуемая (стандартная, верхняя); расширенная (высокая). Концепция унифицированной памяти.
24. Системы прерываний. Назначение, принцип работы и организация.
25. Типы команд ЭВМ: безадресные, одноадресные, двухадресные, трехадресные, четырехадресные. Структура командного кода. Формат команды.

26. Способы адресации операндов.
27. Режимы адресации с помощью регистров общего назначения.
28. Режимы адресации со ссылкой на регистр-счетчик команд.
29. Организация стека.
30. Системы ввода-вывода.
31. Назначение и возможности интерфейсов, основные интерфейсы ЭВМ.
32. Средства ввода информации в ЭВМ. Клавиатура и графический манипулятор. Назначение, возможности и принцип работы.
33. Средства отображения информации. Видеомонитор. Назначение, принцип работы и его технические характеристики.
34. НЖМД и НГМД. Назначение, принцип работы и технические характеристики.
35. Принтер. Назначение, принцип работы и его технические характеристики.
36. Устройство ввода информации CD-ROM. Назначение, виды, принципы работы и технические характеристики.
37. Коммуникационные устройства. Назначение, виды, принципы работы и технические характеристики.
38. Корпуса, источники питания ПЭВМ. Основные форм-факторы и параметры.
39. ПЭВМ. Архитектура современных ПЭВМ.
40. Системная плата, ее назначение, основные элементы и их взаимодействие в системе.
41. Системная магистраль. Основные стандарты системных магистралей (шин).
42. Буферизация шин. Управление системной магистралью. Подключение дополнительных и интерфейсных схем.
43. АРМ, средства обработки сигналов на базе ПЭВМ, архитектура, рабочих станций и серверов.
44. Универсальные и специальные ЭВМ высокой производительности.

8.4. Планируемые уровни сформированности компетенций обучающихся и критерии оценивания

Уровни	Содержательное описание уровня	Основные признаки выделения уровня (этапы формирования компетенции, критерии оценки сформированности)	Пятибалльная шкала (академическая) оценка	Двухбалльная шакала, зачет	БРС, % освоения (рейтинговая оценка)
Повышенный	Творческая деятельность	*Включает нижестоящий уровень.* Умение самостоятельно принимать решение, решать проблему/задачу теоретического и прикладного характера на основе изученных методов, приемов, технологий	отлично	зачтено	86-100
Базовый	Применение знаний и умений в	*Включает нижестоящий уровень.* Способность собирать,	хорошо		71-85

	более широких контекстах учебной и профессиональной деятельности, нежели по образцу с большей степени самостоятельности и инициативы	систематизировать, анализировать и грамотно использовать информацию из самостоятельно найденных теоретических источников и иллюстрировать ими теоретические положения или обосновывать практику применения			
Удовлетворительный (достаточный)	Репродуктивная деятельность	Изложение в пределах задач курса теоретически и практически контролируемого материала	удовлетворительно		55-70
Недостаточный	Отсутствие признаков удовлетворительного уровня		неудовлетворительно	не зачтено	Менее 55

9. Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины.

Основная литература

1. Федотова, Е. Л. Информатика : учебное пособие / Е.Л. Федотова. — 2-е изд., перераб. и доп. — Москва : ИНФРА-М, 2022. — 453 с. — (Высшее образование: Бакалавриат). — DOI 10.12737/1200564. - ISBN 978-5-16-016625-4. - Текст : электронный. - URL: https://znanium.com/catalog/product/1200564 (дата обращения: 26.04.2022). – Режим доступа: по подписке.
2. Гуров, В. В. Микропроцессорные системы : учебное пособие / В.В. Гуров. — Москва : ИНФРА-М, 2022. — 336 с. + Доп. материалы [Электронный ресурс]. — (Высшее образование: Бакалавриат). — DOI 10.12737/7788. - ISBN 978-5-16-009950-7. - Текст : электронный. - URL: https://znanium.com/catalog/product/1816816 (дата обращения: 25.03.2022). – Режим доступа: по подписке.

Дополнительная литература

1. Информатика : учебное пособие / Под ред. Б.Е. Одинцова, А.Н. Романова. — 2-е изд., перераб. и доп. — Москва : Вузовский учебник: ИНФРА-М, 2016. — 410 с. - ISBN 978-5-9558-0230-5. - Текст : электронный. - URL: https://znanium.com/catalog/product/538859 (дата обращения: 26.04.2022). – Режим доступа: по подписке.
2. Водовозов, А. М. Микроконтроллеры для систем автоматики: Учебное пособие / Водовозов А.М. - Вологда:Инфра-Инженерия, 2016. - 164 с.: ISBN 978-5-9729-0138-8. - Текст : электронный. - URL: https://znanium.com/catalog/product/760122 (дата обращения: 25.03.2022). – Режим доступа: по подписке.

10. Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины (модуля).

- НЭБ Национальная электронная библиотека, диссертации и прочие издания
- eLIBRARY.RU Научная электронная библиотека, книги, статьи, тезисы докладов конференций
- Гребенников Электронная библиотека ИД журналы
- ЭБС Лань книги, журналы
- ЭБС Консультант студента
- ПРОСПЕКТ ЭБС
- ЭБС ZNANIUM.COM
- РГБ Информационное обслуживание по МБА
- БЕН РАН
- Электронно-библиотечная система (ЭБС) Кантитана (https://elib.kantiana.ru/)

11. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине.

Программное обеспечение обучения включает в себя:

- система электронного образовательного контента БФУ им. И. Канта – www.lms-3.kantiana.ru, обеспечивающую разработку и комплексное использование электронных образовательных ресурсов;
- серверное программное обеспечение, необходимое для функционирования сервера и связи с системой электронного обучения через Интернет;
- корпоративная платформа Microsoft Teams;
- установленное на рабочих местах обучающихся ПО: Microsoft Windows 7, Microsoft Office Standart 2010, антивирусное программное обеспечение Kaspersky Endpoint Security.
- система схемотехнического проектирования Multisim

12. Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине.

Для проведения занятий лекционного типа, практических и семинарских занятий используются специальные помещения (учебные аудитории), оборудованные техническими средствами обучения – мультимедийной проекционной техникой. Для проведения занятий лекционного типа используются наборы демонстрационного оборудования.

Для проведения лабораторных работ, (практических занятий – при необходимости) используются специальные помещения (учебные аудитории), оснащенные специализированным лабораторным оборудованием: персональными компьютерами с возможностью выхода в интернет и с установленным программным обеспечением, заявленным в п.11.

Для проведения групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации используются специальные помещения (учебные аудитории), оборудованные специализированной мебелью (для обучающихся), меловой / маркерной доской.

Для организации самостоятельной работы обучающимся предоставляются помещения, оснащенные компьютерной техникой с возможностью подключения к сети «Интернет» и обеспечением доступа в электронную информационно-образовательную среду университета.

Для обучения инвалидов и лиц с ограниченными возможностями здоровья университетом могут быть представлены специализированные средства обучения, в том числе технические средства коллективного и индивидуального пользования.

Для выполнения демонстрационных и моделирующих лабораторных работ необходим компьютерный класс с моноблоком MSI AE 222 G в количестве не менее 7 шт с установленным программным обеспечением п 10.2.

1. Макетная плата EasyPic5 фирмы поставщика стендов Mikroelectronika укомплектованная средствами макетирования и кабелем соединения с основным компьютером моноблоком MSI AE 222 G - 7 шт.

2. Микроконтроллер в сокете типа PIC16F887 фирмы Microchip , кварцевый резонатор 8 МГц, микроперемычки.

3. Периферийное оборудование для макетной платы Mikroelectronika ; LCD цифровой двухстрочный дисплей , графический дисплей , IRDA, цифровой термометр D18B20 , потенциометры A\D, LED индикаторы, семисегментные LED с общим анодом.

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
федеральное государственное автономное образовательное учреждение высшего образования «Балтийский федеральный университет имени Иммануила Канта»
Институт физико-математических наук и информационных технологий

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

«Защита информации от утечки по техническим каналам»

Шифр: 10.05.01
Специальность: «Компьютерная безопасность»
Специализация: «Математические методы защиты информации»
Квалификация (степень) выпускника: специалист по защите информации

Калининград
2022

Лист согласования

Составитель: Горбачев Андрей Александрович к.т.н., доцент

Рабочая программа утверждена на заседании учебно-методического совета института физико-математических наук и информационных технологий

Протокол № 01/22 от «01» февраля 2022 г.

Председатель учебно-методического
совета института физико-
математических наук и информационных
технологий

Первый заместитель директора Шпилевой А. А
ИФМНиИТ, к. ф.-м. н., доцент

Ведущий менеджер Е.П.Ставицкая

Содержание

1.Наименование дисциплины: «Защита информации от утечки по техническим каналам».

Цель дисциплины: теоретическая и практическая подготовка обучающихся к организации и проведению мероприятий по защите информации от утечки по техническим каналам на объектах информатизации и защищаемых помещениях.

2. Перечень планируемых результатов обучения по дисциплине, соотнесенных с планируемыми результатами освоения образовательной программы

Код компетенции	Результаты освоения образовательной программы (ИДК)	Результаты обучения по дисциплине
ОПК-9. Способность решать задачи профессиональной деятельности с учетом текущего состояния и тенденций развития методов защиты информации в операционных системах, компьютерных сетях и системах управления базами данных, а также методов и средств защиты информации от утечки по техническим каналам, сетей и систем передачи информации.	ОПК-9.1. Знает методы защиты информации в операционных системах, компьютерных сетях и системах управления базами данных, а также методы и средства защиты информации от утечки по техническим каналам, сетей и систем передачи информации. ОПК-9.2. Умеет решать задачи профессиональной деятельности с учетом текущего состояния и тенденций развития методов защиты информации в операционных системах, компьютерных сетях и системах управления базами данных, а также методов и средств защиты информации от утечки по техническим каналам, сетей и систем передачи информации. ОПК-9.3. Владеет навыками решения задач профессиональной деятельности с учетом текущего состояния и тенденций развития методов защиты информации в операционных системах, компьютерных сетях и системах управления базами данных, а также методов и средств защиты информации от утечки по техническим каналам, сетей и систем передачи информации.	***Знать***: физические основы образования технических каналов утечки информации; физические явления и эффекты, лежащие в основе работы технических средств разведки и технических средств защиты информации; ***Уметь***: определять возможности и состав технических средств разведки в зависимости от специфики обрабатываемой информации на объектах информатизации; осуществлять подбор необходимых технических средств защиты информации в зависимости от физической природы потенциальных технических каналов утечки информации; ***Владеть***: способами выявления технических каналов утечки информации, а также способами их локализации в зависимости от физической природы потенциальных технических каналов утечки информации.

ОПК-13. Способность разрабатывать компоненты программных и программно-аппаратных средств защиты информации в компьютерных системах и проводить анализ их безопасности.	ОПК-13.1. Знает принципы функционирования программных и программно-аппаратных средств защиты информации в компьютерных системах, принципы и методы разработки их компонент, методики анализа их безопасности. ОПК-13.2. Способен разрабатывать компоненты программных и программно-аппаратных средств защиты информации в компьютерных системах. ОПК-13.3. Способен проводить анализ безопасности компонент программных и программно-аппаратных средств защиты информации в компьютерных системах.	***Знать***: технические каналы утечки информации; возможности различных видов технической разведки; виды технических средств, используемых при защите объектов информатизации; способы и средства защиты информации от утечки по техническим каналам; ***Уметь***: формировать требования по технической защите информации; применять наиболее эффективные методы и средства технической защиты информации; контролировать эффективность мер защиты информации. ***Владеть***: методами технической защиты информации; навыками расчета и инструментального контроля показателей технической защиты информации; методиками проверки защищенности объектов информатизации на соответствие требованиям нормативных документов.

3. Место дисциплины в структуре образовательной программы

Дисциплина "Защита информации от утечки по техническим каналам" представляет собой дисциплину обязательной части блока дисциплин подготовки студентов, входит в Модуль 6 «Техническая защита информации».

4. Виды учебной работы по дисциплине.

Виды учебной работы по дисциплине зафиксированы учебным планом основной профессиональной образовательной программы по указанному направлению и профилю, выражаются в академических часах. Часы контактной работы и самостоятельной работы обучающегося и часы, отводимые на процедуры контроля, могут различаться в учебных планах ОПОП по формам обучения. Объем контактной работы включает часы контактной аудиторной работы (лекции/практические занятия/лабораторные работы), контактной внеаудиторной работы (контроль самостоятельной работы), часы контактной работы в период аттестации. Контактная работа, в том числе может проводиться посредством электронной информационно-образовательной среды университета с использованием ресурсов сети Интернет и дистанционных технологий

5. Содержание дисциплины, структурированное по темам (разделам)

Исходя из рамок, установленных учебным планом по трудоемкости и видам учебной работы по дисциплине, преподаватель самостоятельно выбирает тематику занятий по формам и количеству часов проведения контактной работы: лекции и иные учебные занятия, предусматривающие преимущественную передачу учебной информации преподавателем и

(или) занятия семинарского типа (семинары, практические занятия, практикумы, лабораторные работы, коллоквиумы и иные аналогичные занятия), и (или) групповые консультации, и (или) индивидуальную работу обучающихся с преподавателем, в том числе индивидуальные консультации (по курсовым работам/проектам – при наличии курсовой работы/проекта по данной дисциплине в учебном плане). Рекомендуемая тематика занятий максимально полно реализуется в контактной работе с обучающимися очной формы обучения. В случае реализации образовательной программы в заочной / очно-заочной форме трудоемкость дисциплины сохраняется, однако объем учебного материала в значительной части осваивается обучающимися в форме самостоятельной работы. При этом требования к ожидаемым образовательным результатам обучающихся по данной дисциплине не зависят от формы реализации образовательной программы.

№	Наименование раздела	Содержание раздела
1	Концепция технической защиты информации.	1.1 *Системный подход к защите информации*. Концепция и методы инженерно-технической защиты информации. Основные проблемы технической защиты информации. Методы и средства защиты и технической охраны объектов. Представление сил и средств защиты информации в виде системы. Основные параметры системы защиты информации. Модели злоумышленника. 1.2 *Основные концептуальные положения технической защиты информации*. Цели и задачи защиты информации. Ресурсы, выделяемы на защиту информации. Принципы защиты информации техническими средствами. Основные направления технической защиты информации. Показатели эффективности технической защиты информации.
2	Организационные основы технической защиты информации.	2.1 *Государственная система защиты информации*. Нормативно-правовые акты по защите информации. Основные задачи, структура и характеристика государственной системы противодействия технической разведке. Основные руководящие, нормативные и методические документы по защите информации и противодействию технической разведке. Основные организационные и технические меры по защите информации. Аттестация объектов, лицензирование деятельности по защите информации и сертифицирование ее средств. 2.2 *Контроль эффективности технической защиты информации*. Виды контроля эффективности технической защиты информации. Виды зон безопасности. Принципы оценки размеров зон I и II. Оценка дальности перехвата сигналов. Методы технического контроля. Особенности инструментального контроля эффективности технической защиты информации.
3	Теоретические основы технической защиты информации.	3.1 *Информация как предмет защиты*. Особенности информации как предмета защиты. Свойства информации. Виды, источники и носители защищаемой информации. Демаскирующие

		признаки объектов наблюдения, сигналов и веществ. Понятие о текущей и эталонной признаковой структуре. 3.2 *Источники опасных сигналов.* Понятие об опасном сигнале. Основные и вспомогательные технические средства и системы как источники опасных сигналов. Состав и краткая характеристика основных и вспомогательных технических средств и систем. Образование опасных сигналов в результате побочных электромагнитных излучений и наводок. 3.3 *Технические каналы утечки информации.* Понятие и особенности утечки информации. Структура, классификация и основные характеристики технических каналов утечки информации. Оптические, акустические, радиоэлектронные и материально-вещественные каналы утечки информации, их характеристика и возможности.
4	Физические основы утечки информации по техническим каналам.	4.1 *Распространение сигналов в технических каналах утечки информации.* Распространение акустических сигналов в атмосфере, воде и в твердой среде. Особенности распространения акустических сигналов в помещениях. Распространение оптических сигналов в атмосфере и в световодах. Распространение радиосигналов различных диапазонов в пространстве и по направляющим линиям связи.. Характеристика среды распространения сигналов различных технических каналов утечки информации. 4.2 *Физические основы побочных излучений и наводок.* Акустоэлектрические преобразования. Источники побочных электромагнитных излучений и наводок. Характер электромагнитных излучений в ближней и дальней зонах. Виды паразитных связей и наводок. Утечка опасных сигналов по цепям электропитания и заземления. 4.3 *Физические процессы при подавлении опасных сигналов.* Подавление опасных сигналов акустоэлектрических преобразователей. Экранирование и компенсация информативных полей. Подавление информативных сигналов в цепях заземления и электропитания. Зашумление опасных сигналов помехами.
5	Технические средства добывания информации.	5.1 *Характеристика технической разведки.* Основные задачи и органы технической разведки. Принципы технической разведки. Основные этапы и процессы добывания информации технической разведкой. Классификация технической разведки. Возможности видов технической разведки.

		Основные направления развития технической разведки. 5.2 *Средства технической разведки*. Визуально-оптические приборы. Фотоаппараты. Возможности оценки видовых признаков объектов наблюдения. Оптоэлектрические приборы наблюдения в видимом и инфракрасном диапазонах. Акустические приемники. Направленные микрофоны. Структура комплексов перехвата. Особенности сканирующих радиоприемников. Закладные устройства, средства ВЧ-навязывания и лазерного подслушивания. Автономные средства разведки.
6	Технические средства защиты информации.	6.1 *Методы скрытия информации и ее носителей*. Пространственное скрытие объектов наблюдения и сигналов. Структурное и энергетическое скрытие объектов наблюдения. Методы технического скрытия речевой информации в каналах связи. Звукоизоляция и звукопоглощение. Энергетическое скрытие акустических информативных сигналов. Виды и условия зашумления. Энергетическое скрытие радио и электрических сигналов. Подходы к определению безопасности речевой информации в помещении. 6.2 *Средства предотвращения утечки информации по техническим каналам*. Средства маскировки и дезинформирования в оптическом и радиодиапазонах. Средства звукоизоляции из звукопоглощения. Средства обнаружения, локализации и подавления сигналов закладных устройств. Средства подавления опасных сигналов акустоэлектрических преобразователей, фильтрации и заземления. Генераторы линейного и пространственного зашумления. 6.3 *Средства защиты и технической охраны*. Основные инженерные конструкции, применяемые для предотвращения проникновения злоумышленника к источникам информации. Средства управления доступом. Средства видеоконтроля и видеоохраны. Средства нейтрализации угроз. Средства управления и передачи извещений. Автоматизированные интегральные системы охраны.

6. Рекомендуемая тематика учебных занятий в форме контактной работы

Рекомендуемая тематика учебных занятий *лекционного* типа (предусматривающих преимущественную передачу учебной информации преподавателями):

№	Наименование раздела	Темы лекций

1	Концепция технической защиты информации.	Лекция 1. Концепция и методы инженерно-технической защиты информации. Лекция 2. Модели злоумышленника. Лекция 3. Принципы и направления технической защиты информации.
2	Организационные основы технической защиты информации.	Лекция 4. Нормативно-правовые акты по защите информации. Лекция 5. Организационные и технические маары по защите информации. Лекция 6. Контроль эффективности технической защиты информации.
3	Теоретические основы технической защиты информации.	Лекция 7. Информация, как предмет защиты, свойства информации. Лекция 8. Источник опасных сигналов. Лекция 9. Технические каналы утечки информации.
4	Физические основы утечки информации по техническим каналам.	Лекция 10. Распространение сигналов в технических каналах утечки информации. Лекция 11. Физические основы побочных излучений и наводок. Лекция 12. Физические процессы при подавлении опасных сигналов.
5	Технические средства добывания информации.	Лекция 13. Характеристики технической разведки. Лекция 14. Средства технической разведки. Лекция 15. Направления развития технической разведки.
6	Технические средства защиты информации.	Лекция 16. Методы скрытия информации и ее носителей. Лекция 17. Средства предотвращения утечки по техническим каналам. Лекция 18. Средств азащиты и технической охраны.

Рекомендуемый перечень *лабораторных* работ:

№	Наименование раздела	Темы лабораторной работы
1	Концепция технической защиты информации.	Лабораторные работы не предусмотрены.
2	Организационные основы технической защиты информации.	Лабораторные работы не предусмотрены.
3	Теоретические основы технической защиты информации.	Лабораторная работа. Исследование работы помехоподавляющих фильтров нижних и верхних частот, полосовых и заграждающих фильтров. Лабораторная работа. Изучение влияния паразитных емкостных и индуктивных связей на утечку информации по проводным каналам.
4	Физические основы утечки информации по техническим каналам.	Лабораторная работа. Изучение анализатора проводных линий "Отклик-2" Лабораторная работа. Изучение локатора нелинейностей "Лорнет". Лабораторная работа. Изучение портативного измерителя частоты и мощности радиосигналов MFP-8000.

		Лабораторная работа. Изучение универсального поискового прибора для обнаружения устройств скрытого съема информации СРМ-700. Лабораторная работа. Изучение программно-аппаратного комплекса автоматического обнаружения подслушивающих устройств "Крона плюс".
5	Технические средства добывания информации.	Лабораторная работа. Изучение прибора ночного видения "Эдельвейс" и тепловизора "". Лабораторная работа. Изучение широкополосного сканирующего приемника "AR-8200"/
6	Технические средства защиты информации.	Лабораторная работа. Изучение работы портативного металлодетектора "ВМ-311". Лабораторная работа. Изучение работы блокиратора сотовых телефонов "Завеса", подавителя диктофонов "ЛГШ-104", линейных генераторов шума и устройств защиты аналоговых и цифровых телефонных АТС "МП-1А" и "МП-1Ц".

Требования к самостоятельной работе обучающихся

1. Работа с лекционным материалом, предусматривающая проработку конспекта лекций и учебной литературы, по всем темам из п. 6 настоящей рабочей программы.

2. Обработка экспериментальных данных, полученных в ходе выполнения лабораторных работ по всем темам из п. 6 настоящей рабочей программы. Проработка теоретического материала к защите лабораторных работ.

Руководствуясь положениями статьи 47 и статьи 48 Федерального закона от 29 декабря 2012 г. N 273-ФЗ «Об образовании в Российской Федерации» научно-педагогические работники и иные лица, привлекаемые университетом к реализации данной образовательной программы, пользуются предоставленными академическими правами и свободами в части свободы преподавания, свободы от вмешательства в профессиональную деятельность; свободы выбора и использования педагогически обоснованных форм, средств, методов обучения и воспитания; права на творческую инициативу, разработку и применение авторских программ и методов обучения и воспитания в пределах реализуемой образовательной программы и отдельной дисциплины.

Исходя из рамок, установленных учебным планом по трудоемкости и видам учебной работы по дисциплине, преподаватель самостоятельно выбирает тематику занятий по формам и количеству часов проведения контактной работы: лекции и иные учебные занятия, предусматривающие преимущественную передачу учебной информации преподавателем и (или) занятия семинарского типа (семинары, практические занятия, практикумы, лабораторные работы, коллоквиумы и иные аналогичные занятия), и (или) групповые консультации, и (или) индивидуальную работу обучающихся с преподавателем, в том числе индивидуальные консультации (по курсовым работам/проектам – при наличии курсовой работы/проекта по данной дисциплине в учебном плане).

Рекомендуемая тематика занятий максимально полно реализуется в контактной работе с обучающимися очной формы обучения. В случае реализации образовательной программы в заочной / очно-заочной форме трудоемкость дисциплины сохраняется, однако объем учебного материала в значительной части осваивается обучающимися в форме самостоятельной работы. При этом требования к ожидаемым образовательным результатам обучающихся по данной дисциплине не зависят от формы реализации образовательной программы.

7. Методические рекомендации по видам занятий

Лекционные занятия.

В ходе лекционных занятий обучающимся рекомендуется выполнять следующие действия. Вести конспектирование учебного материала. Обращать внимание на категории, формулировки, раскрывающие содержание тех или иных явлений и процессов, научные выводы и практические рекомендации по их применению. Задавать преподавателю уточняющие вопросы с целью уяснения теоретических положений, разрешения спорных ситуаций.

Желательно оставить в рабочих конспектах поля, на которых во внеаудиторное время можно сделать пометки из рекомендованной литературы, дополняющие материал прослушанной лекции, а также подчеркивающие особую важность тех или иных теоретических положений.

Лабораторные занятия.

На лабораторных занятиях в зависимости от темы занятия выполняется поиск информации по конкретной теме; подготовка теоретического материала к защите лабораторных работ на основе контрольных вопросов; обсуждение в круглых столах наиболее важных вопросов; разбор конкретных ошибок с группой студентов.

Самостоятельная работа.

Самостоятельная работа осуществляется в виде изучения литературы, эмпирических данных по публикациям и конкретных ситуаций из практики, подготовке индивидуальных работ, работа с лекционным материалом, самостоятельное изучение отдельных тем дисциплины; поиск и обзор литературы и электронных источников; чтение и изучение учебника и учебных пособий.

8. Фонд оценочных средств

8.1. Перечень компетенций с указанием этапов их формирования в процессе освоения образовательной программы в рамках учебной дисциплины

Основными этапами формирования указанных компетенций при изучении обучающимися дисциплины являются последовательное изучение содержательно связанных между собой тем учебных занятий. Изучение каждой темы предполагает овладение обучающимися необходимыми компетенциями. Результат аттестации обучающихся на различных этапах формирования компетенций показывает уровень освоения компетенций.

	Контролируемые разделы (темы) дисциплины	**Индекс контроли-руемой компетенции (или её части)**	**Оценочные средства по этапам формирования компетенций**
			текущий контроль по дисциплине
1	Концепция технической защиты информации.	ОПК-9	Опрос
2	Организационные основы технической защиты информации.	ОПК-9	Опрос
3	Теоретические основы технической защиты информации.	ОПК-9, ОПК-13	Выполнение и защита лабораторных работ
4	Физические основы утечки информации по техническим каналам.	ОПК-9, ОПК-13	Выполнение и защита лабораторных работ

5	Технические средства добывания информации.	ОПК-9, ОПК-13	Выполнение и защита лабораторных работ
6	Технические средства защиты информации.	ОПК-9, ОПК-13	Выполнение и защита лабораторных работ

8.2. Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений и навыков и (или) опыта деятельности процессе текущего контроля

Основные вопросы для защиты лабораторных работ и собеседования.

Тема 1. Концепция технической защиты информации.
Учебные вопросы:
1) Основные угрозы безопасности информации.
2) Активные и пассивные методы перехвата информации.
3) Активные и пассивные методы защиты информации.
4) Внутренние и внешние нарушители информационной безопасности.
5) Модели злоумышленников.

Тема 2. Организационные основы технической защиты информации.
Учебные вопросы:
1) Основные государственные нормативно-правовые акты по защите информации.
2) Требования к технической защите информации, содержащейся в государственных информационных системах.
3) Аттестация объектов информатизации.
4) Виды зон безопасности. Принципы оценки размеров зон RI и RII.

Тема 3. Теоретические основы технической защиты информации.
● Пассивные средства защиты информации от утечки по техническим каналам.
Учебные вопросы:
- Сетевые помехоподавляющие пассивные фильтры низких и высоких частот.
1) Какое значение имеют пассивные фильтры?
2) Назвать типы помехоподавляющих пассивных фильтров.
3) Привести определения полосы пропускания и полосы подавления фильтров низких и высоких частот.
4) На каких элементах реализуются пассивные фильтры?

- Сетевые пассивные полосно-заграждающие и полосно-пропускающие фильтры.
1) Привести определения полосы пропускания и полосы подавления полосно-пропускающего и полосно-заграждающего фильтров.
2) За счет каких свойств полосно-пропускающих и полосно-заграждающих фильтров обеспечивается полоса пропускания или подавления?
3) Как определяются полосы пропускания и подавления полосных фильтров?

● Влияние паразитных связей и наводок на утечку информации по проводным каналам.
Учебные вопросы:
- Изучение и расчет помех (наводок) в каналах связи при внешней параллельной паразитной связи.
1) Чем обусловлены помехи в каналах связи?
2) На какие виды подразделяются помехи?
3) Способы снижения помех.

- Изучение и расчет помех (наводок) в каналах связи при внешней паразитной связи последовательного вида.

1) Чем обусловлены помехи последовательного вида в каналах связи?
2) Могут ли появиться помехи в каналах при отсутствии гальванических связей?
3) Указать известные способы снижения помех.

Тема 4. Физические основы утечки информации по техническим каналам.

● Технические каналы утечки информации и распространение сигналов в них.

Учебные вопросы:

- Изучение анализатора проводных линий "Отклик-2" с целью обнаружения несанкционированных подключений к телефонным линиям. (На макете телефонной линии).

1) В чем сущность метода импульсной рефлектометрии?
2) Какие виды несанкционированного вмешательства в телефонную линию и нарушения линии позволяет определять анализатор "Отклик-2"?
3) В чем особенности и недостатки анализаторов подобного типа?

- Изучение принципа действия нелинейного локатора "Лорнет" на примере обнаружения макета электронного устройства перехвата информации.

1) Привести определение нелинейного элемента и назвать несколько видов нелинейных объектов.
2) В чем заключается принцип нелинейной локации?
3) Почему в отраженном сигнале от нелинейного элемента с *p-n*- переходом преобладает вторая гармоника?
4) Как зависит мощность сигнала, отраженного от объекта, от частоты локатора?

- Изучение портативного измерителя частоты и мощности радиосигналов MFP-8000, как средства мониторинга радиоэфира.

1) На чем основан принцип действия измерителя мощности СВЧ-колебаний MFP-8000?
2) Каков частотный диапазон обнаружения электромагнитного поля?
3) Каков радиус обнаружения и предельные мощности радиоизлучающих источников?

- Изучение универсального поискового прибора для обнаружения устройств скрытого съема информации СРМ-700.

1) Для обнаружения каких устройств скрытого съема информации предназначен прибор СРМ-700?
2) В чем сущность радиочастотного зондирования?
3) Как подразделяются по мощности (дальности вещания) нелегальные микропередатчики?
4) В чем отличие проверки телефонной линии при помощи прибора СРМ-700 от проверки анализатором "Отклик-2"?

- Изучение программно-аппаратного комплекса автоматического обнаружения подслушивающих устройств "Крона плюс".

1) Для обнаружения каких устройств скрытого съема информации предназначен комплекс "Крона плюс"?
2) Каков частотный диапазон обнаружения скрытых радиопередающих устройств?
3) Каков радиус обнаружения скрытых радиопередающих устройств?

Тема 5. Технические средства добывания информации.

● Технические средства разведки.
Учебные вопросы:
- Изучения принципа работы прибора ночного видения "Эдельвейс-ПМ"
1) Каковы особенности канала для сигналов ИК-излучений?
2) Каким образом можно передавать речевой сигнал с помощью ИК-излучения?
3) В какой области ИК-спектра преобладает отраженное и рассеянное ИК-излучение, а в какой собственное (тепловое)?

- Изучение широкополосного сканирующего приемника AR-8200.
1) Назначение и частотный диапазон приемника AR-8200.
2) Перечислить устройства, относящиеся к радиозакладкам и указать наиболее вероятные места их установки.
3) Что такое сканирование?
4) В чем проявляется уязвимость радиозакладок?
- Изучение анализатора спектра радиосигналов "Белан".
1) Какие параметры радиосигналов позволяет определять анализатор "Белан"?
2) Каков принцип действия и частотные характеристики анализатора "Белан"?
3) Какие параметры заносятся в списки обнаруженных излучений?
4) Какие сигналы считаются "известными" и "неизвестными"?

Тема 6. Технические средства защиты информации.
● Защита информации от утечки по техническим каналам.
Учебные вопросы:
- Изучение принципа работы блокиратора сотовых телефонов "Завеса".
1) Назвать частоты стандартов GSM, DAMPS, CDMA.
2) На чем основан принцип подавления сотовой связи?
3) Каков радиус подавления сотовых аппаратов при помощи блокиратора "Завеса"?

- Изучение принципа работы подавителя диктофонов "ЛГШ-104".
1) В чем состоит сложность обнаружения диктофонов?
2) Как подразделяются современные диктофоны по создаваемому электромагнитному полю?
3) В чем отличие принципов обнаружения и подавления кинематических и цифровых диктофонов?

- Изучение работы системы акустической и виброакустической защиты "Соната-АВ".
1) Чем отличается активная акустическая и виброакустическая защиты от пассивной?
2) Каковы принципы активной защиты?
3) В каких местах защищаемого помещения следует располагать генераторы шума активной акустической защиты?
4) На какие элементы конструкций следует устанавливать виброизлучатели?

- Изучение устройств защиты аналоговых и цифровых АТС "МП-1А" и "МП-1Ц".
1) В чем сущность метода частотно-временного скремблирования?
2) В чем заключается принцип кодирования цифрового потока информации, передаваемой по линиям связи?
3) Сущность стеганографического маскирования речевых сообщений.

- Изучение принципа работы генератора шума "ЛГШ-501", предназначенного для защиты информации от утечки по каналам ПЭМИН.
1) Назвать основные источники образования ПЭМИН.
2) В чем состоит принцип активной защиты по проводным каналам?

3) В чем состоит принцип активной защиты по радиоканалам?
4) Каков частотный диапазон устанавливаемой радиопомехи?

- Изучение принципа работы портативного металлодетектора "ВМ-311".
1) На чем основан принцип обнаружения металлических предметов?
2) Что такое вихревые токи?
3) На что влияет частота работы генератора металлодетектора?

8.3. Перечень вопросов и заданий для промежуточной аттестации по дисциплине

Вопросы для промежуточного контроля (экзамена)

1. Сущность системного подхода в вопросах защиты информации.
2. Основные концептуальные положения технической защиты информации.
3. Основные принципы технической защиты информации.
4. Экономическая обоснованность системы технической защиты информации.
5. Информация как предмет защиты.
6. Сущность энтропийного подхода к оценке количества информации.
7. Свойства информации, влияющие на ее безопасность.
8. Виды угроз безопасности информации, защищаемой техническими средствами.
9. Понятие модели злоумышленника.
10. Принципы добывания информации техническими средствами. Классификация средств технической разведки.
11. Различия параметров стационарных, возимых и носимых наземных средств добывания информации, особенности их применения.
12. Демаскирующие признаки объектов защиты информации, источники опасных сигналов.
13. Виды информации, защищаемой техническими средствами. Источники и носители информации, защищаемой техническими средствами.
14. Отличие источника информации от источника сигналов. В каких случаях они совпадают.
15. Понятия о техническом канале утечки информации, общая схема канала утечки.
16. Виды технических каналов утечки информации.
17. Понятие о контролируемой и опасной зонах, зоны R1, R'1, R2.
18. Физические основы утечки информации по акустическим каналам. Виды акустических каналов утечки информации.
19. Способы перехвата информации по прямому акустическому каналу.
20. Методы противодействия перехвату информации по прямому акустическому каналу.
21. Способы перехвата информации по акустовибрационному каналу.
22. Методы противодействия перехвату информации по акустовибрационному каналу.
23. Способы перехвата информации по акустооптическому каналу.
24. Методы противодействия перехвату информации по акустооптическому каналу.
25. Способы перехвата информации по акустоэлектрическому каналу.
26. Методы противодействия перехвату информации по акустоэлектрическому каналу.
27. Способы перехвата информации по акустоэлектромагнитному каналу.
28. Методы противодействия перехвату информации по акустоэлектромагнитному каналу.
30. Физические основы утечки информации по электрическим каналам. Виды электрических каналов утечки информации.

31. Перехват информации по линиям телефонной связи.
32. Методы противодействия перехвату информации по линиям телефонной связи.
33. Перехват информации по цепям электропитания.
34. Методы противодействия перехвату информации по цепям электропитания.
35. Физические основы утечки информации за счет побочного электромагнитного излучения.
36. Перехват информации за счет побочного электромагнитного излучения.
37. Методы противодействия перехвату информации за счет побочного электромагнитного излучения.
38. Физические основы утечки информации по цепям заземления.
39. Перехват информации по цепям заземления.
40. Методы противодействия перехвату информации по цепям заземления.
41. Физические основы утечки информации по оптическому каналу.
42. Перехват информации по оптическому каналу.
43. Методы противодействия перехвату информации по оптическому каналу.
44. Материально-вещественные каналы утечки информации и их особенности.
45. Организационные меры технической защиты информации в государственных и коммерческих структурах.
46. Показатели эффективности технической защиты информации.

8.4. Планируемые уровни сформированности компетенций обучающихся и критерии оценивания

Уровни	Содержательное описание уровня	Основные признаки выделения уровня (этапы формирования компетенции, критерии оценки сформированности)	Пятибалльная шкала (академическая) оценка	Двухбалльная шакала, зачет	БРС, % освоения (рейтинговая оценка)
Повышенный	Творческая деятельность	*Включает нижестоящий уровень.* Умение самостоятельно принимать решение, решать проблему/задачу теоретического и прикладного характера на основе изученных методов, приемов, технологий	отлично	зачтено	86-100
Базовый	Применение знаний и умений в более широких контекстах учебной и профессиональной деятельности, нежели по	*Включает нижестоящий уровень.* Способность собирать, систематизировать, анализировать и грамотно использовать информацию из самостоятельно найденных теоретических источников и	хорошо		71-85

	образцу с большей степени самостоятельности и инициативы	иллюстрировать ими теоретические положения или обосновывать практику применения			
Удовлетворительный (достаточный)	Репродуктивная деятельность	Изложение в пределах задач курса теоретически и практически контролируемого материала	удовлетворительно		55-70
Недостаточный	Отсутствие признаков удовлетворительного уровня		неудовлетворительно	не зачтено	Менее 55

9. Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины.

Основная литература

1. Технические средства и методы защиты информации: учеб. пособие для вузов/ А. П. Зайцев [и др.]; под ред. А. П. Зайцева, А. А. Шелупанова. - [4-е изд., испр. и доп.]. - М.: Горячая линия-Телеком, 2012. - 615 с.: ил. (15 экз)

Дополнительная литература

2.Основы информационной безопасности [Текст] : учеб. пособие / Е. Б. Белов [и др.], 2006. - 544 с. (16 экз)
3. Хорев П. Б. Методы и средства защиты информации в компьютерных системах [Текст] : учеб. пособие / П. Б. Хорев, 2006. - 255 с. (18 экз)

10. Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины (модуля).

- НЭБ Национальная электронная библиотека, диссертации и прочие издания
- eLIBRARY.RU Научная электронная библиотека, книги, статьи, тезисы докладов конференций
- Гребенников Электронная библиотека ИД журналы
- ЭБС Лань книги, журналы
- ЭБС Консультант студента
- ПРОСПЕКТ ЭБС
- ЭБС ZNANIUM.COM
- РГБ Информационное обслуживание по МБА
- БЕН РАН
- Электронно-библиотечная система (ЭБС) Кантитана (https://elib.kantiana.ru/)

11. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине.

Программное обеспечение обучения включает в себя:

- система электронного образовательного контента БФУ им. И. Канта – www.lms-3.kantiana.ru, обеспечивающую разработку и комплексное использование электронных образовательных ресурсов;
- серверное программное обеспечение, необходимое для функционирования сервера и связи с системой электронного обучения через Интернет;
- корпоративная платформа Microsoft Teams;
- установленное на рабочих местах обучающихся ПО: Microsoft Windows 7, Microsoft Office Standart 2010, антивирусное программное обеспечение Kaspersky Endpoint Security.
- система схемотехнического проектирования Multisim

12. Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине.

Для проведения занятий лекционного типа, практических и семинарских занятий используются специальные помещения (учебные аудитории), оборудованные техническими средствами обучения – мультимедийной проекционной техникой. Для проведения занятий лекционного типа используются наборы демонстрационного оборудования.

Для проведения лабораторных работ, (практических занятий – при необходимости) используются специальные помещения (учебные аудитории), оснащенные специализированным лабораторным оборудованием: персональными компьютерами с возможностью выхода в интернет и с установленным программным обеспечением, заявленным в п.11.

Для проведения групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации используются специальные помещения (учебные аудитории), оборудованные специализированной мебелью (для обучающихся), меловой / маркерной доской.

Для организации самостоятельной работы обучающимся предоставляются помещения, оснащенные компьютерной техникой с возможностью подключения к сети «Интернет» и обеспечением доступа в электронную информационно-образовательную среду университета.

Для обучения инвалидов и лиц с ограниченными возможностями здоровья университетом могут быть представлены специализированные средства обучения, в том числе технические средства коллективного и индивидуального пользования.

Для выполнения демонстрационных лабораторных работ используется следующее оборудование:

1. Анализатор спектра типа "СК-4 Белан - 32" – 1 шт.
2. Программно-аппаратный комплекс автоматического обнаружения, идентификации и нейтрализации подслушивающих устройств типа «Крона плюс». – 1 шт.
3. Нелинейный локатор типа «Лорнет». – 1 шт.
4. Анализатор проводных линий типа «Отклик». – 1 шт.
5. Антенна логопериодическая типа «ЕЛВ-26». – 1 шт.
6. Сканирующий приемник типа AR-8200 – 1 штука.
7. Портативный металлодетектор типа «ВМ311» - 1 штука.
8. Блокиратор сотовых телефонов типа «Завеса» - 1 штука.
9. Ручной измеритель частоты и мощности типа «РИЧ-8» - 1 штука.
10. Программное обеспечение к сканирующему приемнику AR-8200 МК типа «Филин» - 1 штука.
11. Прибор ночного видения типа «Эдельвейс - МП» - 1 – штука.

12. Универсальный поисковый прибор типа «СРМ-700 Advancer + BMP 1200». – 1 шт.
13. Аудиоизлучатель типа «Соната-АВ-АИ-65». – 1 шт.
14. Виброизлучатель типа «Соната-АВ-ВИ-45». – 1 шт.
15. Устройство защиты аналоговых АТС типа «МП-1А» – 1 шт.
16. Устройство защиты цифровых АТС типа «МП-1Ц» – 1 шт.
17. Универсальный генератор шума типа «Гром-ЗИ-4». – 1 шт.
18. Подавитель диктофонов типа «ЛГШ-104». 1 шт.
19. Генератор виброакустического шума ЛГШ-401. – 1 шт.
20. Генератор радиопомех типа «ЛГШ-501». – 1 шт.
21. Пьезоизлучатель типа «Соната-АВ-ПИ-45» – 1 шт.
22. Генератор виброакустического шума типа «Соната-АВ-1М». – 1 шт.
23. Комплекс на проведение исследований на ПЭМИН типа «НАВИГАТОР». – 1 шт.

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
федеральное государственное автономное образовательное учреждение высшего образования
«Балтийский федеральный университет имени Иммануила Канта»
Институт физико-математических наук и информационных технологий

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

«Теоретико-числовые методы в криптографии»

Шифр: 10.05.01
Специальность: «Компьютерная безопасность»
Специализация: «Математические методы защиты информации»
Квалификация (степень) выпускника: специалист по защите информации

Калининград
2022

Лист согласования

Составитель: Малыгина Екатерина Сергеевна, к.ф.-м.н., доцент

Рабочая программа утверждена на заседании учебно-методического совета института физико-математических наук и информационных технологий

Протокол № 01/22 от «01» февраля 2022 г.

Председатель учебно-методического
совета института физико-
математических наук и информационных
технологий

Первый заместитель директора Шпилевой А. А
ИФМНиИТ, к. ф.-м. н., доцент

Ведущий менеджер Е.П.Ставицкая

Содержание

1.Наименование дисциплины: «Теоретико-числовые методы в криптографии».

Цель дисциплины: целью освоения дисциплины «Теоретико-числовые методы в криптографии» является изложение основных понятий и методов теории чисел с ее приложениями в современной криптографии; ознакомление с методами оценки сложности применяемых на практике алгоритмов; построения эффективных алгоритмов решения некоторых прикладных задач в области компьютерной безопасности.

2. Перечень планируемых результатов обучения по дисциплине, соотнесенных с планируемыми результатами освоения образовательной программы

Код компетенции	Результаты освоения образовательной программы (ИДК)	Результаты обучения по дисциплине
ОПК-8. Способен применять методы научных исследований при проведении разработок в области обеспечения безопасности компьютерных систем и сетей.	ОПК-8.1. Знает принципы работы с научной литературой, методы поиска научно-технической информации. ОПК-8.2. Способен осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических документов. ОПК-8.3. Обладает навыками решения профессиональных задач с широким использованием актуальной научно-технической литературы.	- **знать** алгоритмы проверки чисел и многочленов на простоту; алгоритмы построения больших простых чисел; алгоритмы разложения чисел и многочленов на множители; алгоритмы дискретного логарифмирования в конечных циклических группах; - **уметь** применять типовые теоретико-числовые алгоритмы; проводить оценку сложности алгоритмов; разрабатывать эффективные алгоритмы и программы; - **владеть** навыками эффективного вычисления в кольцах вычетов и в кольцах многочленов; навыками разработки алгоритмов решения типовых профессиональных задач; методами построения быстрых вычислительных алгоритмов алгебры и теории чисел.
ОПК-10. Способен анализировать тенденции развития методов и средств криптографической защиты информации, использовать средства криптографической защиты информации при решении задач	ОПК-10.1. Понимает целесообразность использования криптографических алгоритмов в современных программных комплексах. ОПК-10.2. Способен применять методы криптоанализа к конкретным криптографическим примитивам. ОПК-10.3. Владеет навыками	- **знать** основные задачи/проблемы теории чисел в приложениях компьютерной безопасности; - **уметь** работать с литературой, в том числе зарубежной, касающейся задач и проблематики теории чисел в криптографических приложениях; - **владеть** практическими навыками применения стандартных алгоритмов в криптографических приложениях.

профессиональной деятельности.	реализации алгоритмов, в том числе криптографических, в современных программных комплексах.	

3. Место дисциплины в структуре образовательной программы

Дисциплина «Теоретико-числовые методы в криптографии» представляет собой дисциплину обязательной части блока дисциплин подготовки обучающихся.

4. Виды учебной работы по дисциплине.

Виды учебной работы по дисциплине зафиксированы учебным планом основной профессиональной образовательной программы по указанному направлению и профилю, выражаются в академических часах. Часы контактной работы и самостоятельной работы обучающегося и часы, отводимые на процедуры контроля, могут различаться в учебных планах ОПОП по формам обучения. Объем контактной работы включает часы контактной аудиторной работы (лекции/практические занятия/ лабораторные работы), контактной внеаудиторной работы (контроль самостоятельной работы), часы контактной работы в период аттестации. Контактная работа, в том числе может проводиться посредством электронной информационно-образовательной среды университета с использованием ресурсов сети Интернет и дистанционных технологий

5. Содержание дисциплины, структурированное по темам (разделам)

Исходя из рамок, установленных учебным планом по трудоемкости и видам учебной работы по дисциплине, преподаватель самостоятельно выбирает тематику занятий по формам и количеству часов проведения контактной работы: лекции и иные учебные занятия, предусматривающие преимущественную передачу учебной информации преподавателем и (или) занятия семинарского типа (семинары, практические занятия, практикумы, лабораторные работы, коллоквиумы и иные аналогичные занятия), и (или) групповые консультации, и (или) индивидуальную работу обучающихся с преподавателем, в том числе индивидуальные консультации (по курсовым работам/проектам – при наличии курсовой работы/проекта по данной дисциплине в учебном плане). Рекомендуемая тематика занятий максимально полно реализуется в контактной работе с обучающимися очной формы обучения. В случае реализации образовательной программы в заочной / очно-заочной форме трудоемкость дисциплины сохраняется, однако объем учебного материала в значительной части осваивается обучающимися в форме самостоятельной работы. При этом требования к ожидаемым образовательным результатам обучающихся по данной дисциплине не зависят от формы реализации образовательной программы.

№	Наименование раздела	Содержание раздела
1	Введение	Место теории чисел среди других математических дисциплин. Приложения теории чисел. Краткая история развития теории чисел. Литература по дисциплине.
2	Теория сложности вычислений	Моделирование и эффективность вычислений. Машина Тьюринга. Невычислимые функции. P-,

		NP-классы задач. Редукция и NP-полнота. Диагонализация и оракул. Односторонние функции. Криптографические приложения. Сложность операций с целыми числами. Сложность операций в кольце вычетов. Сложность алгоритма Евклида. Модульная арифметика и ее использование.
3	Элементы теории чисел	Квадратичные вычеты. Символы Лежандра и Якоби. Закон квадратичной взаимности Гаусса. Квадратные корни: метод Цассенхауза-Кантора. Классы вычетов, вычисления в кольцах вычетов. Строение мультипликативной группы кольца Z_m. Цепные дроби.
4	Быстрые вычисления	Быстрое возведение в квадрат. Быстрое возведение в степень. Алгоритм Баррета. Приведение по модулю. Вычисление НОД'а. Извлечение квадратного корня. Быстрое преобразование Фурье. Умножение многочленов с помощью БПФ. Метод Карацубы. Метод Тоома-Кука. Метод Монтгомери: редукция и умножение.
5	Основные теоретико-числовые задачи в криптографии	Факторизация целых чисел. Криптосистема RSA. Проблема квадратичных вычетов. Вычисление квадратных корней в Z_m. Задача дискретного логарифмирования. Задача Диффи-Хеллмана. Проблема составного модуля. Вычисление индивидуальных бит. Задача суммы подмножеств. Факторизация многочленов над конечным полем.
6	Криптография с открытым ключом	Вероятностные тесты на простоту. Еще тесты на простоту. Генерация простых чисел. Неприводимые многочлены над конечными полями. Образующие и элементы большого порядка.

6. Рекомендуемая тематика учебных занятий в форме контактной работы

Рекомендуемая тематика учебных занятий *лекционного* типа (предусматривающих преимущественную передачу учебной информации преподавателями):

№	Наименование раздела	Темы лекций
1	Введение	Лекция 1. Место теории чисел среди других математических дисциплин. Приложения теории чисел. Краткая история развития теории чисел. Литература по дисциплине.
2	Теория сложности вычислений	Лекция 2. Моделирование вычислений; Эффективность; Машина Тьюринга. Лекция 3. Невычислимые функции; P-класс; NP-класс; Редукция и NP-полнота. Лекция 4. Диагонализация; Оракул; Односторонние функции; Криптографические приложения. Лекция 5. Оценка сложности арифметических операций.

3	Элементы теории чисел	Лекция 6. Квадратичные вычеты. Символы Лежандра и Якоби. Закон квадратичной взаимности Гаусса. Лекция 7. Квадратные корни: метод Цассенхауза-Кантора. Лекция 8. Классы вычетов, вычисления в кольцах вычетов. Строение мультипликативной группы кольца Z_m.
4	Быстрые вычисления	Лекция 9. Быстрое возведение в квадрат; Быстрое возведение в степень; Алгоритм Баррета. Лекция 10. Приведение по модулю; Вычисление НОД'а; Извлечение квадратного корня. Лекция 11. Быстрое преобразование Фурье. Умножение многочленов с помощью БПФ. Лекция 12. Метод Карацубы. Метод Тоома-Кука. Лекция 13. Метод Монтгомери: редукция и умножение.
5	Основные теоретико-числовые задачи в криптографии	Лекция 14. Метод пробных делений. Ро-метод Полларда. p-1-метод Полларда. Лекция 15. Метод случайных квадратов. Метод квадратичного решета. Лекция 16. Вычисление квадратных корней в Z_m. Лекция 17. Задача дискретного логарифмирования: Шаг гиганта -- Шаг младенца. Ро-метод Полларда. Лекция 18. Задача дискретного логарифмирования: Метод исчисления индексов. Лекция 19. Задача Диффи-Хеллмана: Цифровая подпись; Классификация; Анализ безопасности; Приложения. Лекция 20-21. Хэш-функции. Приложения в задаче дискретного логарифмирования, RSA. Лекция 22-23. Задача суммы подмножеств. Решетки. Лекция 24. Факторизация многочленов над конечным полем: Свободная от квадратов факторизация; Алгоритм Берлекэмпа.
6	Криптография с открытым ключом	Лекция 25. Распределение простых чисел. Решето Эратосфена. Критерий Вильсона. Тест Ферма на простоту. Числа Капмайкла и их свойства. Лекция 26. Тесты Соловея-Штрассена и Миллера-Рабина. Лекция 27. Полиномиальный тест на простоту. Лекция 28. Числа Мерсенна и Ферма. Тест Люка-Лемера. Лекция 29. Построение простого числа с помощью теста Миллера-Рабина. Лекция 30. Надёжные простые и сильные простые числа. Циклическая атака на RSA. Лекция 31. Теорема Поклингтона. Метод Маурера. Лекция 32. Генерация простых чисел в цифровой подписи ГОСТ Р34.10-94. Лекция 33. Неприводимые многочлена над конечным полем. Тест на неприводимость.

		Генерация унитарного неприводимого многочлена. Лекция 34. Примитивные многочлены. Лекция 35. Элементы и образующие большого порядка.

Рекомендуемая тематика *практических* занятий:

1. Вычисление оценки сложности различных операций и алгоритмов.
2. Вычисления в кольцах вычетов, китайская теорема об остатках. В
3. Вычисление символов Лежандра и Якоби. Исследования разрешимости и решение квадратичных сравнений.
4. Приближение действительных чисел цепными дробями. Решение уравнений с помощью цепных дробей.
5. Реализация быстрого возведения в квадрат.
6. Реализация быстрого возведения в степень.
7. Реализация алгоритма Баррета.
8. Реализация приведения чисел по модулю.
9. Реализация вычисления НОД'а.
10. Реализация извлечения квадратного корня.
11. Реализация быстрого преобразования Фурье.
12. Реализация умножения многочленов с помощью БПФ.
13. Реализация метода Карацубы.
14. Реализация метода Тоома-Кука.
15. Реализация метода Монтгомери: редукция и умножение.
16. Реализация метода пробных делений.
17. Реализация ро-метод Полларда (для факторизации).
18. Реализация р-1-метода Полларда (для факторизации).
19. Реализация метода случайных квадратов (для факторизации).
20. Реализация метода квадратичного решета (для факторизации).
21. Реализация вычисления квадратных корней в Z_n.
22. Реализация метода “Шаг гиганта -- Шаг младенца” (дискретный логарифм).
23. Реализация ро-метода Полларда (дискретный логарифм).
24. Реализация метода исчисления индексов (дискретный логарифм).
25. Реализация “наивного” метод (сумма подмножеств).
26. Реализация LLL-редукции.
27. Реализация одного из методов факторизации многочленов.
28. Реализация теста Ферма.
29. Реализация теста Соловея-Штрассена.
30. Реализация теста Миллера-Рабина.
31. Реализация теста Люки-Лемера.
32. Реализация случайного поиска простого числа.
33. Реализация алгоритма Гордона.
34. Реализация построения простых чисел.
35. Реализация распознавания многочленов на неприводимость.
36. Реализация построения случайного унитарного неприводимого многочлена над конечным полем.
37. Реализация распознавания многочлена на примитивность.
38. Реализация построения случайного унитарного примитивного многочлена над конечным полем.
39. Вычисление порядка элемента группы.
40. Вычисление образующей циклической группы.

41. Вычисление элемента максимального порядка в мультипликативной группе кольца, поля.

На практических занятиях решаются задачи по теме занятия.

Требования к самостоятельной работе обучающихся

1. Работа с лекционным материалом, предусматривающая проработку конспекта лекций и учебной литературы, по всем темам из п. 6 настоящей рабочей программы.
2. Выполнение домашнего задания, предусматривающего решение задач, выполнение упражнений, выдаваемых на практических занятиях, по всем темам из п. 6 настоящей рабочей программы.

Руководствуясь положениями статьи 47 и статьи 48 Федерального закона от 29 декабря 2012 г. N 273-ФЗ «Об образовании в Российской Федерации» научно-педагогические работники и иные лица, привлекаемые университетом к реализации данной образовательной программы, пользуются предоставленными академическими правами и свободами в части свободы преподавания, свободы от вмешательства в профессиональную деятельность; свободы выбора и использования педагогически обоснованных форм, средств, методов обучения и воспитания; права на творческую инициативу, разработку и применение авторских программ и методов обучения и воспитания в пределах реализуемой образовательной программы и отдельной дисциплины.

Исходя из рамок, установленных учебным планом по трудоемкости и видам учебной работы по дисциплине, преподаватель самостоятельно выбирает тематику занятий по формам и количеству часов проведения контактной работы: лекции и иные учебные занятия, предусматривающие преимущественную передачу учебной информации преподавателем и (или) занятия семинарского типа (семинары, практические занятия, практикумы, лабораторные работы, коллоквиумы и иные аналогичные занятия), и (или) групповые консультации, и (или) индивидуальную работу обучающихся с преподавателем, в том числе индивидуальные консультации (по курсовым работам/проектам – при наличии курсовой работы/проекта по данной дисциплине в учебном плане).

Рекомендуемая тематика занятий максимально полно реализуется в контактной работе с обучающимися очной формы обучения. В случае реализации образовательной программы в заочной / очно-заочной форме трудоемкость дисциплины сохраняется, однако объем учебного материала в значительной части осваивается обучающимися в форме самостоятельной работы. При этом требования к ожидаемым образовательным результатам обучающихся по данной дисциплине не зависят от формы реализации образовательной программы.

7. Методические рекомендации по видам занятий

Лекционные занятия.

В ходе лекционных занятий обучающимся рекомендуется выполнять следующие действия. Вести конспектирование учебного материала. Обращать внимание на категории, формулировки, раскрывающие содержание тех или иных явлений и процессов, научные выводы и практические рекомендации по их применению. Задавать преподавателю уточняющие вопросы с целью уяснения теоретических положений, разрешения спорных ситуаций.

Желательно оставить в рабочих конспектах поля, на которых во внеаудиторное время можно сделать пометки из рекомендованной литературы, дополняющие материал прослушанной лекции, а также подчеркивающие особую важность тех или иных теоретических положений.

Практические и семинарские занятия.

На практических и семинарских занятиях в зависимости от темы занятия выполняется поиск информации по решению проблем, практические упражнения, контрольные работы, выработка индивидуальных или групповых решений, итоговое обсуждение с обменом знаниями, участие в круглых столах, разбор конкретных ситуаций, командная работа, представление портфолио и т.п.

Самостоятельная работа.

Самостоятельная работа осуществляется в виде изучения литературы, эмпирических данных по публикациям и конкретных ситуаций из практики, подготовке индивидуальных работ, работа с лекционным материалом, самостоятельное изучение отдельных тем дисциплины; поиск и обзор литературы и электронных источников; чтение и изучение учебника и учебных пособий.

8. Фонд оценочных средств

8.1. Перечень компетенций с указанием этапов их формирования в процессе освоения образовательной программы в рамках учебной дисциплины

Основными этапами формирования указанных компетенций при изучении обучающимися дисциплины являются последовательное изучение содержательно связанных между собой тем учебных занятий. Изучение каждой темы предполагает овладение обучающимися необходимыми компетенциями. Результат аттестации обучающихся на различных этапах формирования компетенций показывает уровень освоения компетенций.

Контролируемые разделы (темы) дисциплины	Индекс контроли-руемой компетенции (или её части)	Оценочные средства по этапам формирования компетенций
		текущий контроль по дисциплине
1. Введение	ОПК-8	Опрос, решение задач.
2. Теория сложности вычислений	ОПК-8 ОПК-10	Опрос, решение задач, контрольная работа
3. Элементы теории чисел	ОПК-8	Опрос, решение задач
4. Быстрые вычисления	ОПК-8 ОПК-10	Опрос, решение задач, программная реализация алгоритмов и ее защита
5. Основные теоретико-числовые задачи в криптографии	ОПК-8 ОПК-10	Опрос, решение задач, программная реализация алгоритмов и ее защита
6. Криптография с открытым ключом	ОПК-8 ОПК-10	Опрос, решение задач, программная реализация алгоритмов и ее защита, контрольная работа

8.2. Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений и навыков и (или) опыта деятельности процессе текущего контроля

Примеры вопросов для устного опроса:

По Теме 2. Теория сложности вычислений

1. Дать определение оценке сложности.
2. Вывести оценки сложности операций с целыми числами.
3. В чем заключается суть использования модульной арифметики?
4. Вывести оценки сложности операций в кольце классов вычетов.

По Теме 3. Элементы теории чисел

1. Дать определение: квадратичному вычету, символам Лежандра и Якоби.
2. Как осуществляются вычисления в кольцах классов вычетах?
3. Дать определение мультипликативной группе кольца классов вычетов.
4. Сформулировать закон квадратичной взаимности Гаусса.
5. В каких теоретико-числовых задачах используется китайская теорема об остатках?

По Теме 6. Криптография с открытым ключом

1. Дать определение псевдопростым числам и числам Кармайкла и перечислить их свойства.
2. Дать определение эйлеровым псевдопростым числам и перечислить их свойства.
3. Дать определение сильно псевдопростым числам и перечислить их свойства.
4. Дать определение числам Ферма и сформулировать их свойства.
5. Дать определение числам Мерсенна и сформулировать их свойства.

Типовые контрольные задания:

1. Определить, разрешимо ли сравнение $15x \equiv 24 \pmod{20}$?
2. Построить таблицы сложения и умножения для $Z/9Z$, найти обратимые элементы и делители нуля в данном кольце.
3. Вычислить функцию Эйлера $\phi(212)$.
4. Найти примитивные корни для $p = 23$.
5. Решить систему сравнений: $\begin{cases} x \equiv 3 \pmod{5}, \\ x \equiv 5 \pmod{7}, \\ x \equiv 8 \pmod{12}. \end{cases}$
6. Определить, являются ли простыми числа 371, 379.
7. Найти псевдопростое число по основанию 13.
8. Построит число Мерсенна M_7 и проверить его на простоту.
9. Используя число 17 построить 3-ех разрядное простое число.
10. Построить простое число для заданной границы $B = 100$.
11. Разложить на множители $n = 1017$ с помощью метода Полларда.
12. С помощью метода квадратичного решета разложить число 611.
13. Факторизовать число 2021 с помощью $(p - 1)$-метода Полларда.

8.3. Перечень вопросов и заданий для промежуточной аттестации по дисциплине

Вопросы для промежуточного контроля (зачета)

1. Моделирование и эффективность вычислений.
2. Машина Тьюринга.
3. Невычислимые функции. P-, NP-классы задач.

4. Редукция и NP-полнота. Диагонализация и оракул. Односторонние функции.
5. Криптографические приложения.
6. Вычисления в кольце целых чисел. Сложность операций с целыми числами.
7. Вычисления в кольцах вычетов. Сложность операций в кольце вычетов.
8. Алгоритм Евклида и его сложность.
9. Модульная арифметика и ее использование.
10. Квадратичные вычеты и невычеты.
11. Символы Лежандра и Якоби, их свойства.
12. Закон квадратичной взаимности Гаусса.
13. Квадратные корни: метод Цассенхауза-Кантора.
14. Строение мультипликативной группы кольца Z_m. Критерий цикличности. Первообразные корни.
15. Алгоритмы вычисления символа Лежандра.
16. Решение степенных и показательных сравнений.
17. Цепные дроби.

Вопросы для промежуточного контроля (экзамена)

1. Быстрое возведение в квадрат. Быстрое возведение в степень.
2. Алгоритм Баррета. Приведение по модулю.
3. Вычисление НОД'а. Извлечение квадратного корня.
4. Быстрое преобразование Фурье. Умножение многочленов с помощью БПФ.
5. Метод Карацубы. Метод Тоома-Кука.
6. Метод Монтгомери: редукция и умножение.
7. Частные виды простых чисел: простые числа Ферма и Мерсенна, их свойства.
8. Критерии простоты. Необходимые условия простоты.
9. Вопросы распределения простых чисел в натуральном ряду.
10. Теорема Чебышева и асимптотический закон распределения простых чисел.
11. Алгоритмы проверки чисел на простоту.
12. Тесты Соловея-Штрассена и Миллера-Рабина.
13. Методы построения больших простых чисел.
14. Алгоритмы экспоненциальной сложности.
15. Метод Ферма и его модификации.
16. Алгоритм Диксона.
17. Метод случайных квадратов.
18. Метод квадратичного решета.
19. Вероятностные алгоритмы факторизации Полларда.
20. Криптосистема RSA.
21. Задача дискретного логарифмирования в мультипликативной группе конечного поля.
22. Задача дискретного логарифмирования в произвольной мультипликативной группе.
23. Задача Диффи-Хеллмана.
24. Вычисление индивидуальных бит.
25. Задача суммы подмножеств.
26. Факторизация многочленов над конечным полем.
27. Генерация простых чисел.
28. Неприводимые многочлены над конечными полями.

8.4. Планируемые уровни сформированности компетенций обучающихся и критерии оценивания

Уровни	Содержательное описание уровня	Основные признаки выделения уровня (этапы формирования компетенции, критерии оценки сформированности)	Пятибалльная шкала (академическая) оценка	Двухбалльная шакала, зачет	БРС, % освоения (рейтинговая оценка)
Повышенный	Творческая деятельность	*Включает нижестоящий уровень.* Умение самостоятельно принимать решение, решать проблему/задачу теоретического и прикладного характера на основе изученных методов, приемов, технологий	отлично	зачтено	86-100
Базовый	Применение знаний и умений в более широких контекстах учебной и профессиональной деятельности, нежели по образцу с большей степени самостоятельности и инициативы	*Включает нижестоящий уровень.* Способность собирать, систематизировать, анализировать и грамотно использовать информацию из самостоятельно найденных теоретических источников и иллюстрировать ими теоретические положения или обосновывать практику применения	хорошо		71-85
Удовлетворительный (достаточный)	Репродуктивная деятельность	Изложение в пределах задач курса теоретически и практически контролируемого материала	удовлетворительно		55-70
Недостаточный	Отсутствие признаков удовлетворительного уровня		неудовлетворительно	не зачтено	Менее 55

9. Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины.

Основная литература

1. Кнауб, Л. В. *Теоретико-численные методы в криптографии* [Электронный ресурс] : Учеб. пособие / Л. В. Кнауб, Е. А. Новиков, Ю. А. Шитов. - Красноярск :

Сибирский федеральный университет, 2011. - 160 с. - ISBN 978-5-7638-2113-7. - Текст : электронный. - URL: https://znanium.com/catalog/product/441493.

Дополнительная литература

1. Романьков, В. А. Введение в криптографию : курс лекций / В.А. Романьков. — 2-е изд., испр. и доп. — Москва : ФОРУМ : ИНФРА-М, 2021. — 240 с. — (Высшее образование: Бакалавриат). - ISBN 978-5-00091-493-9. - Текст : электронный. - URL: https://znanium.com/catalog/product/1514566
2. Ященко, В. В. *Введение в криптографию*: Учебное пособие / Ященко В.В., - 4-е изд. - Москва :МЦНМО, 2014. - 352 с.: ISBN 978-5-4439-2162-4. - Текст : электронный. - URL: https://znanium.com/catalog/product/958585.

10. Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины (модуля).

- НЭБ Национальная электронная библиотека, диссертации и прочие издания
- eLIBRARY.RU Научная электронная библиотека, книги, статьи, тезисы докладов конференций
- Гребенников Электронная библиотека ИД журналы
- ЭБС Лань книги, журналы
- ЭБС Консультант студента
- ПРОСПЕКТ ЭБС
- ЭБС ZNANIUM.COM
- РГБ Информационное обслуживание по МБА
- БЕН РАН
- Электронно-библиотечная система (ЭБС) Кантитана (https://elib.kantiana.ru/)

11. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине.

Программное обеспечение обучения включает в себя:

- система электронного образовательного контента БФУ им. И. Канта – www.lms-3.kantiana.ru, обеспечивающую разработку и комплексное использование электронных образовательных ресурсов;
- серверное программное обеспечение, необходимое для функционирования сервера и связи с системой электронного обучения через Интернет;
- корпоративная платформа Microsoft Teams;
- установленное на рабочих местах обучающихся ПО: Microsoft Windows 7, Microsoft Office Standart 2010, антивирусное программное обеспечение Kaspersky Endpoint Security.
- специализированное ПО не требуется.

12. Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине.

Для проведения занятий лекционного типа, практических и семинарских занятий используются специальные помещения (учебные аудитории), оборудованные техническими

средствами обучения – мультимедийной проекционной техникой. Для проведения занятий лекционного типа используются наборы демонстрационного оборудования.

Для проведения лабораторных работ, (практических занятий – при необходимости) используются специальные помещения (учебные аудитории), оснащенные специализированным лабораторным оборудованием: персональными компьютерами с возможностью выхода в интернет и с установленным программным обеспечением, заявленным в п.11.

Для проведения групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации используются специальные помещения (учебные аудитории), оборудованные специализированной мебелью (для обучающихся), меловой / маркерной доской.

Для организации самостоятельной работы обучающимся предоставляются помещения, оснащенные компьютерной техникой с возможностью подключения к сети «Интернет» и обеспечением доступа в электронную информационно-образовательную среду университета.

Для обучения инвалидов и лиц с ограниченными возможностями здоровья университетом могут быть представлены специализированные средства обучения, в том числе технические средства коллективного и индивидуального пользования.

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ
федеральное государственное автономное образовательное учреждение
высшего образования
«Балтийский федеральный университет имени Иммануила Канта»
Институт физико-математических наук и информационных технологий

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

«Теория конечных полей и их приложения»

Шифр: 10.05.01
Специальность: «Компьютерная безопасность»
Специализация: «Математические методы защиты информации»
Квалификация (степень) выпускника: специалист по защите информации

Калининград
2022

Лист согласования

Составитель: Малыгина Екатерина Сергеевна, к.ф.-м.н., доцент

Рабочая программа утверждена на заседании учебно-методического совета института физико-математических наук и информационных технологий

Протокол № 01/22 от «01» февраля 2022 г.

Председатель учебно-методического
совета института физико-
математических наук и информационных
технологий

Первый заместитель директора Шпилевой А. А
ИФМНиИТ, к. ф.-м. н., доцент

Ведущий менеджер Е.П.Ставицкая

Содержание

1.Наименование дисциплины: «Теория конечных полей и их приложения».

Цель дисциплины: целью освоения дисциплины «Теория конечных полей и их приложения» является фундаментальная подготовка студентов в теории конечных полей, овладение быстрыми вычислениями в конечных полях, ознакомление с приложениями теории конечных полей в современной теории кодирования и криптографии.

2. Перечень планируемых результатов обучения по дисциплине, соотнесенных с планируемыми результатами освоения образовательной программы

Код компетенции	Результаты освоения образовательной программы (ИДК)	Результаты обучения по дисциплине
ОПК-2.2 Способен разрабатывать и анализировать математические модели механизмов защиты информации.	ОПК-2.2.1. Знает принципы построения средств криптографической защиты информации. ОПК-2.2.2. Умеет выявлять наиболее целесообразные подходы к обеспечению защиты информации компьютерной системы. ОПК-2.2.3. Владеет методами разработки математических моделей, реализуемых в средствах защиты информации.	- **знать** общие принципы экспериментального и теоретического исследования быстрых вычислений в конечных полях для приложений в теории кодирования и криптографии; оценки сложности алгоритмов; - **уметь** проводить анализ и формализацию задач, возникающих при реализации алгоритмов быстрых вычислений в конечных полях; - **владеть** методикой оценки эффективности алгоритма построения базисов конечного поля в целом и отдельных его компонент.

3. Место дисциплины в структуре образовательной программы

Дисциплина «Теория конечных полей и их приложения» представляет собой дисциплину обязательной части блока дисциплин подготовки обучающихся.

4. Виды учебной работы по дисциплине.

Виды учебной работы по дисциплине зафиксированы учебным планом основной профессиональной образовательной программы по указанному направлению и профилю, выражаются в академических часах. Часы контактной работы и самостоятельной работы обчающегося и часы, отводимые на процедуры контроля, могут различаться в учебных планах ОПОП по формам обучения. Объем контактной работы включает часы контактной аудиторной работы (лекции/практические занятия/ лабораторные работы), контактной внеаудиторной работы (контроль самостоятельной работы), часы контактной работы в период аттестации. Контактная работа, в том числе может проводиться посредством электронной информационно-образовательной среды университета с использованием ресурсов сети Интернет и дистанционных технологий

5. Содержание дисциплины, структурированное по темам (разделам)

Исходя из рамок, установленных учебным планом по трудоемкости и видам учебной работы по дисциплине, преподаватель самостоятельно выбирает тематику занятий по формам и количеству часов проведения контактной работы: лекции и иные учебные занятия, предусматривающие преимущественную передачу учебной информации преподавателем и (или) занятия семинарского типа (семинары, практические занятия, практикумы, лабораторные работы, коллоквиумы и иные аналогичные занятия), и (или) групповые консультации, и (или) индивидуальную работу обучающихся с преподавателем, в том числе индивидуальные консультации (по курсовым работам/проектам – при наличии курсовой работы/проекта по данной дисциплине в учебном плане). Рекомендуемая тематика занятий максимально полно реализуется в контактной работе с обучающимися очной формы обучения. В случае реализации образовательной программы в заочной / очно-заочной форме трудоемкость дисциплины сохраняется, однако объем учебного материала в значительной части осваивается обучающимися в форме самостоятельной работы. При этом требования к ожидаемым образовательным результатам обучающихся по данной дисциплине не зависят от формы реализации образовательной программы.

№	Наименование раздела	Содержание раздела
1	Евклидовы кольца	Алгоритм Евклида. Евклидовы кольца. Простые и неприводимые элементы. Единственность разложения на множители в евклидовых кольцах.
2	Построение конечных полей	Классы эквивалентности. Построение конечного поля на базе евклидова кольца.
3	Абстрактные свойства конечных полей	Характеристика поля. Порядок элемента и его свойства. Примитивные корни. Алгоритм Гаусса. Минимальные многочлены и их свойства. Сопряженные элементы.
4	Существование и единственность конечных полей	Функция Мёбиуса. Вычисление числа унитарных неприводимых многочленов. Подполя конечного поля.
5	Факторизация многочленов над конечными полями	Круговые многочлены и их свойства. Методы факторизации.
6	След, норма и битовое последовательное умножение	Отображение следа и его свойства. Отображение нормы и его свойства. Дуальные базисы. Умножение на примитивный корень поля. Умножение на произвольный скаляр. Умножение двух переменных.
7	Нормальные и дуальные базисы	Фундаментальные результаты. Арифметика в представлении нормальных базисов. Сложность нормальных базисов. Самодвойственные базисы. Число самодвойственных базисов.
8	Приложения	Криптография с открытым ключом. Криптосистема LUC. Криптосистема XTR. Криптосистемы на торах.

6. Рекомендуемая тематика учебных занятий в форме контактной работы

Рекомендуемая тематика учебных занятий *лекционного* типа (предусматривающих преимущественную передачу учебной информации преподавателями):

№	Наименование раздела	Темы лекций
1	Евклидовы кольца	Лекция 1. Алгоритм Евклида и НОД в Евклидовых кольцах. Лекция 2. Простые и неприводимые элементы. Единственность разложения на множители в евклидовых кольцах.
2	Построение конечных полей	Лекция 3. Отношение эквивалентности и классы эквивалентности в евклидовых кольцах. Построение конечных полей на базе евклидовых колец.
3	Абстрактные свойства конечных полей	Лекция 4. Характеристика поля. Порядок элемента и его свойства. Примитивные корни. Алгоритм Гаусса. Лекция 5. Минимальные многочлены и их свойства. Сопряженные элементы.
4	Существование и единственность конечных полей	Лекция 6-7. Функция Мёбиуса. Вычисление числа унитарных неприводимых многочленов. Подполя конечного поля.
5	Факторизация многочленов над конечными полями	Лекция 8. Круговые многочлены и их свойства. Лекция 9. Методы факторизации многочленов над конечными полями.
6	След, норма и битовое последовательное умножение	Лекция 10. Отображения следа и нормы, их свойства. Лекция 11. Даульные базисы. Лекция 12. Умножение на примитивный корень поля. Умножение на произвольный скаляр. Умножение двух переменных.
7	Нормальные и дуальные базисы	Лекция 13. Арифметика в представлении нормальных базисов. Сложность нормальных базисов. Лекция 14. Самодвойственные базисы. Число самодвойственных базисов. Лекция 15. След-ортогональные нормальные базисы.
8	Приложения	Лекция 16-17. Приложения конечных полей в криптографии с открытым ключом. Лекция 18. Криптосистема LUC. Лекция 19. Криптосистема XTR. Лекция 20. Криптосистемы на торах.

Рекомендуемая тематика *практических* занятий:

1. Реализация алгоритма Евклида в евклидовых кольца. Вычисление НОД'а элементов евклидова кольца.
2. Разложение на множители в евклидовых кольцах.
3. Построение конечного поля на базе евклидова кольца.
4. Вычисление примитивных корней поля. Вычисление порядка элемента. Реализация алгоритма Гаусса. Вычисление минимальных многочленов.
5. Вычисление числа унитарных неприводимых многочленов.

6. Построение подполей конечного поля.
7. Вычисление круговых многочленов.
8. Реализация некоторых методов факторизации.
9. Вычисление следа и нормы элементов конечного поля.
10. Реализация умножения на примитивный корень поля, умножения на произвольный скаляр, умножения двух переменных.
11. Построение нормального базиса. Умножение в нормальном базисе.
12. Построение ортогонального нормального базиса.
13. Построение самодвойственного нормального базиса.
14. Построение след-ортогонального нормального базиса.
15. Построение оптимального нормального базиса.
16. Реализация криптосистемы LUC.
17. Реализация криптосистемы XTR.
18. Реализация криптосистемы на торах.

На практических занятиях решаются задачи по теме занятия.

Требования к самостоятельной работе обучающихся

1. Работа с лекционным материалом, предусматривающая проработку конспекта лекций и учебной литературы, по всем темам из п. 6 настоящей рабочей программы.

2. Выполнение домашнего задания, предусматривающего решение задач, выполнение упражнений, выдаваемых на практических занятиях, по всем темам из п. 6 настоящей рабочей программы.

Руководствуясь положениями статьи 47 и статьи 48 Федерального закона от 29 декабря 2012 г. N 273-ФЗ «Об образовании в Российской Федерации» научно-педагогические работники и иные лица, привлекаемые университетом к реализации данной образовательной программы, пользуются предоставленными академическими правами и свободами в части свободы преподавания, свободы от вмешательства в профессиональную деятельность; свободы выбора и использования педагогически обоснованных форм, средств, методов обучения и воспитания; права на творческую инициативу, разработку и применение авторских программ и методов обучения и воспитания в пределах реализуемой образовательной программы и отдельной дисциплины.

Исходя из рамок, установленных учебным планом по трудоемкости и видам учебной работы по дисциплине, преподаватель самостоятельно выбирает тематику занятий по формам и количеству часов проведения контактной работы: лекции и иные учебные занятия, предусматривающие преимущественную передачу учебной информации преподавателем и (или) занятия семинарского типа (семинары, практические занятия, практикумы, лабораторные работы, коллоквиумы и иные аналогичные занятия), и (или) групповые консультации, и (или) индивидуальную работу обучающихся с преподавателем, в том числе индивидуальные консультации (по курсовым работам/проектам – при наличии курсовой работы/проекта по данной дисциплине в учебном плане).

Рекомендуемая тематика занятий максимально полно реализуется в контактной работе с обучающимися очной формы обучения. В случае реализации образовательной программы в заочной / очно-заочной форме трудоемкость дисциплины сохраняется, однако объем учебного материала в значительной части осваивается обучающимися в форме самостоятельной работы. При этом требования к ожидаемым образовательным результатам обучающихся по данной дисциплине не зависят от формы реализации образовательной программы.

7. Методические рекомендации по видам занятий

Лекционные занятия.

В ходе лекционных занятий обучающимся рекомендуется выполнять следующие действия. Вести конспектирование учебного материала. Обращать внимание на категории, формулировки, раскрывающие содержание тех или иных явлений и процессов, научные выводы и практические рекомендации по их применению. Задавать преподавателю уточняющие вопросы с целью уяснения теоретических положений, разрешения спорных ситуаций.

Желательно оставить в рабочих конспектах поля, на которых во внеаудиторное время можно сделать пометки из рекомендованной литературы, дополняющие материал прослушанной лекции, а также подчеркивающие особую важность тех или иных теоретических положений.

Практические и семинарские занятия.

На практических и семинарских занятиях в зависимости от темы занятия выполняется поиск информации по решению проблем, практические упражнения, контрольные работы, выработка индивидуальных или групповых решений, итоговое обсуждение с обменом знаниями, участие в круглых столах, разбор конкретных ситуаций, командная работа, представление портфолио и т.п.

Самостоятельная работа.

Самостоятельная работа осуществляется в виде изучения литературы, эмпирических данных по публикациям и конкретных ситуаций из практики, подготовке индивидуальных работ, работа с лекционным материалом, самостоятельное изучение отдельных тем дисциплины; поиск и обзор литературы и электронных источников; чтение и изучение учебника и учебных пособий.

8. Фонд оценочных средств

8.1. Перечень компетенций с указанием этапов их формирования в процессе освоения образовательной программы в рамках учебной дисциплины

Основными этапами формирования указанных компетенций при изучении обучающимися дисциплины являются последовательное изучение содержательно связанных между собой тем учебных занятий. Изучение каждой темы предполагает овладение обучающимися необходимыми компетенциями. Результат аттестации обучающихся на различных этапах формирования компетенций показывает уровень освоения компетенций.

Контролируемые разделы (темы) дисциплины	Индекс контроли-руемой компетенции (или её части)	Оценочные средства по этапам формирования компетенций
		текущий контроль по дисциплине
1. Евклидовы кольца	ОПК-2.2	Опрос, решение задач, программная реализация алгоритмов и ее защита
2. Построение конечных полей		
3. Абстрактные свойства конечных полей		
4. Существование и единственность конечных		

Контролируемые разделы (темы) дисциплины	Индекс контроли-руемой компетенции (или её части)	Оценочные средства по этапам формирования компетенций
		текущий контроль по дисциплине
полей		
5. Факторизация многочленов над конечными полями	ОПК-2.2	Опрос, решение задач, программная реализация алгоритмов и ее защита
6. След, норма и битовое последовательное умножение		
7. Нормальные и дуальные базисы		
8. Приложения		
Итоговая контрольная работа по всем темам дисциплины		Контрольная работа

8.2. Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений и навыков и (или) опыта деятельности процессе текущего контроля

Примеры вопросов для устного опроса:

1. Сформулировать основные свойства конечных полей.
2. Сформулировать основные свойства неприводимых над полем многочленов.
3. Привести примеры круговых многочленов над определенными конечными полями.
4. Дать определения нормы и следа элемента конечного поля.
5. Дать основные определения, касающиеся арифметики в конечных расширениях.
6. Дать определения нормального базиса, свободного элемента, минимального многочлена базиса.
7. Привести пример вычисления нормального базиса.
8. Дать определение дуального базиса.
9. Сформулировать основные свойства дуального базиса.
10. Показать взаимосвязь арифметических свойств нормальных и след-ортогональных базисов.

Типовые контрольные задания:

1. Рассмотрим $\mathbb{F}_{49} = \mathbb{F}_7[x]/(x^2 - 3)$ и $\alpha \in \mathbb{F}_{49}$.
   a) Найти порядок элемента α в $\mathbb{F}_{49}$.
   b) Найти примитивный корень поля и представить α как степень примитивного корня.
2. Изобразить с помощью диаграммы подполя поля $\mathbb{F}_{p^{16}}$.
3. Найти минимальный многочлен для элемента $\alpha^5 \in \mathbb{F}_{16}$ над $\mathbb{F}_2$.
4. Найти нормы и следы элементов поля $\mathbb{F}_{16} = \mathbb{F}_2[x]/(x^4 + x + 1)$.
5. Доказать, что кольцо циркулянтных матриц изоморфно кольцу многочленов с операциями по модулю $X^n - 1$.
6. Доказать, что если n – нечетное, то $\Phi_{2n}(x) = \Phi_n(-x)$.
7. Вычислить круговой многочлен $\Phi_{24}(x)$.
8. Разложить круговой многочлен $\Phi_{17}(x)$ на множители над $\mathbb{F}_2$.

9. Пусть F – поле характеристики 2. Вычислить $\Phi_{10}(x)$.
10. Найти нормальный базис поля $\mathbb{F}_8 = \mathbb{F}_2[X]/(X^3 + X^2 + 1)$. Представить многочлен $X^2 + X^4$ в стандартном базисе.
11. В поле $\mathbb{F}_{2^5}$ найти неприводимый трехчлен, порождающий нормальный базис.
12. В поле $\mathbb{F}_{2^4}$ найти нормальный базис, осуществить переход от нормального базиса к полиномиальному и наоборот.
13. Найти дуальный базис к базису $\{\alpha, \alpha^2, \alpha^3\}$ поля $\mathbb{F}_8$, где α - примитивный корень, удовлетворяющий условию $\alpha^3 = \alpha + 1$.
14. Пусть $\mathbb{F}_8 = \mathbb{F}_2[x]/(x^3 + x + 1)$. Построить дуальный базис к базису $\{1, \alpha, \alpha^2\}$.
15. Пусть $\mathbb{F}_{16} = \mathbb{F}_2[x]/(x^4 + x + 1)$. Построить дуальный базис к базису $\{1, \alpha, \alpha^2, \alpha^3\}$.
16. Найти оптимальные нормальные базисы поля $\mathbb{F}_{q^n}$, где q = 2, n = 10, 11.
17. Доказать, что для матрицы А нормального оптимального базиса в поле $\mathbb{F}_{2^n}$ второго или третьего типа $a_{i,j} = 1$ тогда и только тогда, когда выполняется одно из четырех соотношений:
$$2^i \pm 2^j = \pm 1 \pmod{2n+1}.$$
18. Осуществить переход от оптимального нормального базиса первого типа поля $\mathbb{F}_{2^4}$ к стандартному.
19. С помощью алгоритма быстрого умножения перемножить многочлены:
$P_1(X) = (1 + X^2)X^8 + (X^3 + 1)$ и $P_2(X) = (1 + X + X^7)X^{16} + X^6$.
20. Привести многочлен степени 22, заданный вектором коэффициентов
(00101000 10101000 10001010)
по модулю многочлена $1 + X^{11} + X^{15}$.
21. Пусть k = 5, $P(X) = 1 + X + X^4$, $f(X) = 1 + X^3$, $m_0 = 2$. Найти $f^{2^s}(X)$, выразив его в полиномиальном базисе.
22. Доказать, что умножение в поле $\mathbb{F}_q$, $q = 2^p - 1$ выполняется с битовой сложностью $M(p) + 11p$.

8.3. Перечень вопросов и заданий для промежуточной аттестации по дисциплине

Вопросы для промежуточного контроля (зачета)

1. Евклидовы кольца. Алгоритм Евклида.
2. Простые и неприводимые элементы. Единственность разложения на множители в евклидовых кольцах.
3. Фундаментальные свойства конечных полей.
4. Неприводимые многочлены над конечными полями.
5. Круговые многочлены.
6. Нормы и следы числового поля.
7. Расширения конечных полей степени p^k.
8. Расширения конечных полей степени, делящей $q - 1$.
9. Расширения конечных полей произвольной степени.
10. Построение примитивных элементов и примитивных многочленов.
11. Вычисление круговых многочленов.

12. Определение нормального базиса и арифметика в представлении нормальных базисов.
13. Сложность нормальных базисов.
14. Определение и построение дуального базиса.
15. Битовое последовательное умножение.
16. Самодвойственные базисы.
17. Число самодвойственных базисов.
18. Ортогональные нормальные базисы.
19. Существование самодвойственных нормальных базисов.
20. Число самодвойственных нормальных базисов.
21. След-ортогональные нормальные базисы.
22. Оптимальные нормальные базисы.
23. Быстрое умножение на примитивный корень поля.
24. Быстрое умножение на произвольный скаляр.
25. Быстрое умножение двух переменных.

8.4. Планируемые уровни сформированности компетенций обучающихся и критерии оценивания

Уровни	Содержательное описание уровня	Основные признаки выделения уровня (этапы формирования компетенции, критерии оценки сформированности)	Пятибалльная шкала (академическая) оценка	Двухбалльная шакала, зачет	БРС, % освоения (рейтинговая оценка)
Повышенный	Творческая деятельность	*Включает нижестоящий уровень.* Умение самостоятельно принимать решение, решать проблему/задачу теоретического и прикладного характера на основе изученных методов, приемов, технологий	отлично	зачтено	86-100
Базовый	Применение знаний и умений в более широких контекстах учебной и профессиональной деятельности, нежели по образцу с большей степени самостоятельности и	*Включает нижестоящий уровень.* Способность собирать, систематизировать, анализировать и грамотно использовать информацию из самостоятельно найденных теоретических источников и иллюстрировать ими теоретические положения или обосновывать практику применения	хорошо		71-85

	инициативы				
Удовлетворительный (достаточный)	Репродуктивная деятельность	Изложение в пределах задач курса теоретически и практически контролируемого материала	удовлетворительно		55-70
Недостаточный	Отсутствие признаков удовлетворительного уровня		неудовлетворительно	не зачтено	Менее 55

9. Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины.

Основная литература

1. *Быстрые мультипликаторы* : учеб.-метод. комплекс / сост. Е. С. Алексеенко. - Калининград : БФУ им. И. Канта, 2015. - 1 on-line, 95 с. ЭБС Кантиана.

Дополнительная литература

1. Романьков, В. А. Введение в криптографию : курс лекций / В.А. Романьков. — 2-е изд., испр. и доп. — Москва : ФОРУМ : ИНФРА-М, 2021. — 240 с. — (Высшее образование: Бакалавриат). - ISBN 978-5-00091-493-9. - Текст : электронный. - URL: https://znanium.com/catalog/product/1514566.

10. Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины (модуля).

- НЭБ Национальная электронная библиотека, диссертации и прочие издания
- eLIBRARY.RU Научная электронная библиотека, книги, статьи, тезисы докладов конференций
- Гребенников Электронная библиотека ИД журналы
- ЭБС Лань книги, журналы
- ЭБС Консультант студента
- ПРОСПЕКТ ЭБС
- ЭБС ZNANIUM.COM
- РГБ Информационное обслуживание по МБА
- БЕН РАН
- Электронно-библиотечная система (ЭБС) Кантитана (https://elib.kantiana.ru/)

11. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине.

Программное обеспечение обучения включает в себя:

- система электронного образовательного контента БФУ им. И. Канта – www.lms-3.kantiana.ru, обеспечивающую разработку и комплексное использование электронных образовательных ресурсов;
- серверное программное обеспечение, необходимое для функционирования сервера и связи с системой электронного обучения через Интернет;

- корпоративная платформа Microsoft Teams;
- установленное на рабочих местах обучающихся ПО: Microsoft Windows 7, Microsoft Office Standart 2010, антивирусное программное обеспечение Kaspersky Endpoint Security.
- специализированное ПО не требуется.

12. Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине.

Для проведения занятий лекционного типа, практических и семинарских занятий используются специальные помещения (учебные аудитории), оборудованные техническими средствами обучения – мультимедийной проекционной техникой. Для проведения занятий лекционного типа используются наборы демонстрационного оборудования.

Для проведения лабораторных работ, (практических занятий – при необходимости) используются специальные помещения (учебные аудитории), оснащенные специализированным лабораторным оборудованием: персональными компьютерами с возможностью выхода в интернет и с установленным программным обеспечением, заявленным в п.11.

Для проведения групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации используются специальные помещения (учебные аудитории), оборудованные специализированной мебелью (для обучающихся), меловой / маркерной доской.

Для организации самостоятельной работы обучающимся предоставляются помещения, оснащенные компьютерной техникой с возможностью подключения к сети «Интернет» и обеспечением доступа в электронную информационно-образовательную среду университета.

Для обучения инвалидов и лиц с ограниченными возможностями здоровья университетом могут быть представлены специализированные средства обучения, в том числе технические средства коллективного и индивидуального пользования.

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
федеральное государственное автономное образовательное учреждение высшего образования «Балтийский федеральный университет имени Иммануила Канта»
Институт физико-математических наук и информационных технологий

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

«Методы и средства криптографической защиты информации»

Шифр: 10.05.01
Специальность: «Компьютерная безопасность»
Специализация: «Математические методы защиты информации»
Квалификация (степень) выпускника: специалист по защите информации

Калининград
2022

Лист согласования

Составитель: Ставицкая Е.П., старший преподаватель, Дёмин С.А., старший преподаватель

Рабочая программа утверждена на заседании учебно-методического совета института физико-математических наук и информационных технологий

Протокол № 01/22 от «01» февраля 2022 г.

Председатель учебно-методического совета института физико-математических наук и информационных технологий

Первый заместитель директора ИФМНиИТ, к. ф.-м. н., доцент — Шпилевой А. А

Ведущий менеджер — Е.П.Ставицкая

Содержание

1.Наименование дисциплины: «Методы и средства криптографической защиты информации».

Цель дисциплины: целью освоения дисциплины «Методы и средства криптографической защиты информации» является получение студентами теоретических знаний о современных принципах и средствах защиты информации с помощью криптографических методов.

2. Перечень планируемых результатов обучения по дисциплине, соотнесенных с планируемыми результатами освоения образовательной программы

Код компетенции	Результаты освоения образовательной программы (ИДК)	Результаты обучения по дисциплине
ОПК-10. Способен анализировать тенденции развития методов и средств криптографической защиты информации, использовать средства криптографической защиты информации при решении задач профессиональной деятельности;	ОПК-10.1. Понимает целесообразность использования криптографических алгоритмов в современных программных комплексах. ОПК-10.2. Способен применять методы криптоанализа к конкретным криптографическим примитивам. ОПК-10.3. Владеет навыками реализации алгоритмов, в том числе криптографических, в современных программных комплексах.	Студент должен: • знать математические основы криптографических алгоритмов и современное программное обеспечение; • уметь формализовать и алгоритмизировать математические методы, моделировать криптографические алгоритмы в системах компьютерной алгебры и оценивать их эффективность. • владеть приемами реализации алгоритмов вычислений над конечными полями, кольцами; приемами работы с программными средствами прикладного, системного и специального назначения.

3. Место дисциплины в структуре образовательной программы

Дисциплин «Методы и средства криптографической защиты информации» входит в базовую часть (Б1.О.11.03) обязательной части блока дисциплин (модулей) подготовки специалистов по специальности 10.05.01«Компьютерная безопасность», специализация N 2 "Математические методы защиты информации"

4. Виды учебной работы по дисциплине.

Виды учебной работы по дисциплине зафиксированы учебным планом основной профессиональной образовательной программы по указанному направлению и профилю, выражаются в академических часах. Часы контактной работы и самостоятельной работы обучающегося и часы, отводимые на процедуры контроля, могут различаться в учебных

планах ОПОП по формам обучения. Объем контактной работы включает часы контактной аудиторной работы (лекции/практические занятия/ лабораторные работы), контактной внеаудиторной работы (контроль самостоятельной работы), часы контактной работы в период аттестации. Контактная работа, в том числе может проводиться посредством электронной информационно-образовательной среды университета с использованием ресурсов сети Интернет и дистанционных технологий

5. Содержание дисциплины, структурированное по темам (разделам)

Исходя из рамок, установленных учебным планом по трудоемкости и видам учебной работы по дисциплине, преподаватель самостоятельно выбирает тематику занятий по формам и количеству часов проведения контактной работы: лекции и иные учебные занятия, предусматривающие преимущественную передачу учебной информации преподавателем и (или) занятия семинарского типа (семинары, практические занятия, практикумы, лабораторные работы, коллоквиумы и иные аналогичные занятия), и (или) групповые консультации, и (или) индивидуальную работу обучающихся с преподавателем, в том числе индивидуальные консультации (по курсовым работам/проектам – при наличии курсовой работы/проекта по данной дисциплине в учебном плане). Рекомендуемая тематика занятий максимально полно реализуется в контактной работе с обучающимися очной формы обучения. В случае реализации образовательной программы в заочной / очно-заочной форме трудоемкость дисциплины сохраняется, однако объем учебного материала в значительной части осваивается обучающимися в форме самостоятельной работы. При этом требования к ожидаемым образовательным результатам обучающихся по данной дисциплине не зависят от формы реализации образовательной программы.

№ п/п	Наименование темы	Содержание темы
1	Основные исторические этапы развития криптографии.	История криптографии. Определение шифра. Примеры ручных шифров. Становление криптографии как науки.
2	Математические модели открытых сообщений.	Частотные характеристики открытых текстов. К – граммные модели открытых текстов. Избыточность языка. Критерии распознавания открытых текстов.
3	Основные задачи криптографии.	Шифрование. Контроль целостности сообщения. Аутентификация. Электронно-цифровая подпись. Проблема распределения ключей. Математическая модель шифра. Классификация шифров. Основные требования к шифрам.
4	Поточные шифры замены.	Шифры простой замены и их анализ. Лозунговые шифры. Использование частотных характеристик при анализе шифров простой замены и их усложнений. Многоалфавитные шифры замены. Шифры гаммирования. Использование неравновероятной гаммы. Повторное использование гаммы. Криптоанализ шифра Вижинера.
5	Шифры перестановки.	Разновидности шифров перестановки: шифры горизонтальной, перестановки, шифры вертикальной перестановки, маршрутные и геометрические перестановки. Элементы криптоанализа шифров перестановки.
6	Блочные шифры.	Блочные шифры простой замены Плейфера и Хилла. Принципы построения блочных шифрсистем. Архитектура современных блочных шифров: сеть Фейстеля, SP – сеть, XSL - сеть. Блочные

		криптосистемы: ГОСТ 28147-89 и его режим использования, IDEA, AES, ГОСТ 34.12-15 и ГОСТ 34.13-15. Режимы использования блочных шифров для шифрования данных и формирования кодов аутентичности. Комбинирование алгоритмов блочного шифрования. Методы анализа алгоритмов блочного шифрования. Рекомендации по использованию алгоритмов блочного шифрования.
7	Системы шифрования с открытым ключом.	Основной принцип асимметричного шифрования. Шифрсистема Шамира. Шифрсистема RSA и ее анализ. Шифрсистема Эль-Гамаля. Шифрсистема Мак-Элиаса. Шифрсистема на основе задачи об «укладке рюкзака». Практические аспекты использование криптосистем с открытыми ключами.
8	Криптографическая стойкость шифров.	Теоретическая и практическая стойкость шифров. Теоретико-информационный подход к определению криптографической стойкости шифров. Подходы к определению практической стойкости шифров. Криптоатаки.
9	Имитостойкость шифров.	Имитозащита. Характеристики имитостойкости шифров и их оценки. Примеры. Имитовставки. Коды аутентификации и имитозащита.
10	Помехоустойчивость шифров.	Шифры, не размножающие искажений типа замены знаков. Шифры, не распространяющие искажений типа вставка-пропуск знаков.
11	Принципы построения алгоритмов поточного шифрования.	Режимы использования поточных шифров. Строение поточных криптосистем. Примеры. Регистры сдвига: с линейной обратной связью и с обратной связью по переносу. Поточные шифрсистемы A5, RC4, схемы с нелинейной обратной связью.
12	Генераторы псевдослучайных последовательностей.	Конгруэнтные генераторы. Генераторы Фибоначчи. Генераторы, основанные на сложности решения задач теории чисел. Генераторы на основе линейных регистров сдвига. Линейные рекуррентные последовательности (ЛРП) над полем. Свойства ЛРП максимального периода. Линейная сложность псевдослучайной последовательности. Методы усложнения ЛРП: фильтрующие и и комбинирующие генераторы, и их свойства. Композиции линейных регистров сдвига. Алгоритм Берлекемпа – Месси.
13	Методы анализа криптографических алгоритмов.	Классификация методов анализа криптографических алгоритмов. Методы нахождения ключей криптографических алгоритмов: алгоритмические методы, алгебраические методы, статистические методы.
14	Конструкции хеш-функций.	Общие сведения о хеш-функциях. Криптографические хеш-функции. Ключевые и бесключевые хеш-функции. Итеративные способы построения хеш-функций. Понятие о стойкости хеш-функций. Современные криптографические хеш-функции.
15	Целостность данных и аутентификация источника данных.	Конструкции схем аутентификации на основе хеш-функций. Коды аутентичности сообщений: HMAC, UMAC. Системы CBC-MAC, EMAC, XOR-MAC, PCS-MAC.
16	Цифровые подписи.	Общие положения. Цифровые подписи на основе шифр систем с открытыми ключами. Цифровая подпись Фиата-Шамира. Цифровая подпись Эль-Гамаля. Стандарты цифровой подписи.

17	Алгоритмы идентификации.	Понятие криптографического протокола идентификации. Протоколы идентификации типа «запрос-ответ». Протоколы идентификации, использующие цифровую подпись. Протоколы с нулевым разглашением.
18	Алгоритмы распределения ключей.	Алгоритмы передачи ключей. Алгоритмы открытого распределения ключей. Алгоритмы предварительного распределения ключей.

6. Рекомендуемая тематика учебных занятий в форме контактной работы

Рекомендуемая тематика учебных занятий *лекционного* типа (предусматривающих преимущественную передачу учебной информации преподавателями):

№	Раздел	Тема лекции
1	Раздел 1. «Введение в криптографию»	Тема 1. Основные исторические этапы развития криптографии.
		Тема 2. Математические модели открытых сообщений.
		Тема 3. Основные задачи криптографии.
2	Раздел 2. «Основные классы шифров и их свойства»	Тема 4. Поточные шифры замены.
		Тема 5. Шифры перестановки.
		Тема 6. Блочные шифры.
		Тема 7. Системы шифрования с открытым ключом.
3	Раздел 3. «Надежность шифров»	Тема 8. Криптографическая стойкость шифров.
		Тема 9. Имитостойкость шифров.
		Тема 10. Помехоустойчивость шифра.
4	Раздел 4 «Методы синтеза и анализа симметричных криптосистем»	Тема 11. Принципы построения алгоритмов поточного шифрования.
		Тема 12. Генераторы псевдослучайных последовательностей.
		Тема 13. Методы анализа криптографических алгоритмов
5	Раздел 5. «Криптографические хеш-функции»	Тема 14. Конструкции хеш-функций.
		Тема 15. Целостность данных и аутентификация источника данных
6	Раздел 6. «Методы синтеза криптографических алгоритмов с открытым ключом»	Тема 16. Цифровые подписи.
		Тема 17. Алгоритмы идентификации.
		Тема 18. Алгоритмы распределения ключей.

Тематика практических занятий:

№ п/п	**Наименование темы**	**Тематика практического занятия.**
1	Основные исторические	Практическое занятие по данной теме не предусмотрено.

	этапы развития криптографии.	
2	Математические модели открытых сообщений.	1. Частотный анализ текста шифра простой однобуквенной замены. 2. Криптографический анализ аффинного шифра простой замены.
3	Основные задачи криптографии.	Практическое занятие по данной теме не предусмотрено.
4	Поточные шифры замены.	3. Криптографический анализ с помощью протяжки вероятного слова. 4. Криптографический анализ шифра Виженера (случай короткой длины ключа). 5. Вычисление вероятностного распределения знаков гаммы шифра модульного гаммирования.
5	Шифры перестановки.	6. Криптографический анализ шифра вертикальной перестановки.
6	Блочные шифры.	7. Построение шифра Хилла как блочного шифра простой замены над конечным полем и кольцом вычетов. 8. Реализация режимов блочного шифрования для шифра Хилла над кольцом вычетов: режим сцепления блоков. 9. Реализация режимов блочного шифрования для шифра Хилла над кольцом вычетов: режим обратной связи по шифртексту. 10. Построение шифра Хилла как шифра перестановки. 11. Построение и криптографический анализ аффинного шифра Хилла. 12. Линейный и дифференциальные методы анализа блочных криптосистем.
7	Системы шифрования с открытым ключом.	13. Криптографический анализ системы RSA при неправильном выборе параметров (при использовании одного модуля). 14. Криптографический анализ системы RSA при неправильном выборе параметров (при использовании малой экспоненты шифрования для шифрования близких сообщений). 15. Криптографический анализ системы Эль - Гамаля.
8	Криптографическая стойкость шифров.	16. Вычисление расстояния единственности шифра.
9	Имитостойкость шифров.	Практическое занятие по данной теме не предусмотрено.
10	Помехоустойчивость шифров.	Практическое занятие по данной теме не предусмотрено.
11	Принципы построения алгоритмов поточного шифрования.	17. Реализация линейных рекуррентных последовательностей на основе линейных регистров сдвига над полями GF(2), GF(5) и GF(7) и их анализ. 18. Алгоритм Берлекемпа – Месси. 19. Поточные шифр системы с элементами памяти. 20. Изучение характеристик регистров связи с обратной связью по переносу.
12	Генераторы псевдослучайных последовательностей.	21. Фильтрующие, комбинирующие генераторы и их свойства. 22. Композиции линейных регистров сдвига. 23. Методы тестирования генераторов псевдослучайных последовательностей используемых в криптографии. 24. Линейные регистры сдвига использующие нелинейное преобразование при обратной связи.

13	Методы анализа криптографических алгоритмов.	25. Криптографический анализ шифра модульного гаммирования с не равновероятной гаммой. 26. Корреляционный метод анализа поточной криптосистемы. 27. Разностный метод анализа блочной криптосистемы. 28. Дифференциальный метод анализа блочных криптосистем.
14	Конструкции хеш-функций.	29. Парадокс дней рождений. 30. Метод Хеллмана.
15	Целостность данных и аутентификация источника данных.	31. Конструкции хеш-функций MD5 и SHA. 32. Стандарт ГОСТ 34.11-12.
16	Цифровые подписи.	33. Цифровая подпись Эль-Гамаля.
17	Алгоритмы идентификации.	34. Криптографические протоколы идентификации.
18	Алгоритмы распределения ключей.	35. Криптографические протоколы открытого распределения ключей. 36. Криптографические протоколы предварительного распределения ключей.

Требования к самостоятельной работе обучающихся

1. Работа с лекционным материалом, предусматривающая проработку конспекта лекций и учебной литературы, по всем темам из п. 6 настоящей рабочей программы.

2. Выполнение домашнего задания, предусматривающего решение задач, выполнение упражнений, выдаваемых на практических занятиях, по всем темам из п. 6 настоящей рабочей программы.

Руководствуясь положениями статьи 47 и статьи 48 Федерального закона от 29 декабря 2012 г. N 273-ФЗ «Об образовании в Российской Федерации» научно-педагогические работники и иные лица, привлекаемые университетом к реализации данной образовательной программы, пользуются предоставленными академическими правами и свободами в части свободы преподавания, свободы от вмешательства в профессиональную деятельность; свободы выбора и использования педагогически обоснованных форм, средств, методов обучения и воспитания; права на творческую инициативу, разработку и применение авторских программ и методов обучения и воспитания в пределах реализуемой образовательной программы и отдельной дисциплины.

Исходя из рамок, установленных учебным планом по трудоемкости и видам учебной работы по дисциплине, преподаватель самостоятельно выбирает тематику занятий по формам и количеству часов проведения контактной работы: лекции и иные учебные занятия, предусматривающие преимущественную передачу учебной информации преподавателем и (или) занятия семинарского типа (семинары, практические занятия, практикумы, лабораторные работы, коллоквиумы и иные аналогичные занятия), и (или) групповые консультации, и (или) индивидуальную работу обучающихся с преподавателем, в том числе индивидуальные консультации (по курсовым работам/проектам – при наличии курсовой работы/проекта по данной дисциплине в учебном плане).

Рекомендуемая тематика занятий максимально полно реализуется в контактной работе с обучающимися очной формы обучения. В случае реализации образовательной программы в заочной / очно-заочной форме трудоемкость дисциплины сохраняется, однако объем учебного материала в значительной части осваивается обучающимися в форме

самостоятельной работы. При этом требования к ожидаемым образовательным результатам обучающихся по данной дисциплине не зависят от формы реализации образовательной программы.

№ п/п	**Наименование темы**	**Тематика самостоятельных работ.**
1	Основные исторические этапы развития криптографии.	Повторение теоретического материала к практическим занятиям. Ознакомление с литературой по курсу. Подготовка к контрольной работе.
2	Математические модели открытых сообщений.	Повторение теоретического материала к практическим занятиям. Ознакомление с литературой по курсу. Подготовка к контрольной работе.
3	Основные задачи криптографии.	Повторение теоретического материала к практическим занятиям. Ознакомление с литературой по курсу. Подготовка к контрольной работе.
4	Поточные шифры замены.	Повторение теоретического материала к практическим занятиям. Ознакомление с литературой по курсу. Подготовка к контрольной работе.
5	Шифры перестановки.	Повторение теоретического материала к практическим занятиям. Ознакомление с литературой по курсу. Подготовка к контрольной работе.
6	Блочные шифры.	Повторение теоретического материала к практическим занятиям. Ознакомление с литературой по курсу. Подготовка к контрольной работе.
7	Системы шифрования с открытым ключом.	Повторение теоретического материала к практическим занятиям. Ознакомление с литературой по курсу. Подготовка к контрольной работе.
8	Криптографическая стойкость шифров.	Повторение теоретического материала к практическим занятиям. Ознакомление с литературой по курсу. Подготовка к контрольной работе.
9	Имитостойкость шифров.	Повторение теоретического материала к практическим занятиям. Ознакомление с литературой по курсу. Подготовка к контрольной работе.
10	Помехоустойчивость шифров.	Повторение теоретического материала к практическим занятиям. Ознакомление с литературой по курсу. Подготовка к контрольной работе.
11	Принципы построения алгоритмов поточного шифрования.	Повторение теоретического материала к практическим занятиям. Ознакомление с литературой по курсу. Подготовка к контрольной работе.
12	Генераторы псевдослучайных последовательностей.	Повторение теоретического материала к практическим занятиям. Ознакомление с литературой по курсу. Подготовка к контрольной работе.
13	Методы анализа криптографических алгоритмов.	Повторение теоретического материала к практическим занятиям. Ознакомление с литературой по курсу. Подготовка к контрольной работе.

14	Конструкции хеш-функций.	Повторение теоретического материала к практическим занятиям. Ознакомление с литературой по курсу. Подготовка к контрольной работе.
15	Целостность данных и аутентификация источника данных.	Повторение теоретического материала к практическим занятиям. Ознакомление с литературой по курсу. Подготовка к контрольной работе.
16	Цифровые подписи.	Повторение теоретического материала к практическим занятиям. Ознакомление с литературой по курсу. Подготовка к контрольной работе.
17	Алгоритмы идентификации.	Повторение теоретического материала к практическим занятиям. Ознакомление с литературой по курсу. Подготовка к контрольной работе.
18	Алгоритмы распределения ключей.	Повторение теоретического материала к практическим занятиям. Ознакомление с литературой по курсу. Подготовка к контрольной работе.

7. Методические рекомендации по видам занятий

Лекционные занятия.

В ходе лекционных занятий обучающимся рекомендуется выполнять следующие действия. Вести конспектирование учебного материала. Обращать внимание на категории, формулировки, раскрывающие содержание тех или иных явлений и процессов, научные выводы и практические рекомендации по их применению. Задавать преподавателю уточняющие вопросы с целью уяснения теоретических положений, разрешения спорных ситуаций.

Желательно оставить в рабочих конспектах поля, на которых во внеаудиторное время можно сделать пометки из рекомендованной литературы, дополняющие материал прослушанной лекции, а также подчеркивающие особую важность тех или иных теоретических положений.

Практические и семинарские занятия.

На практических и семинарских занятиях в зависимости от темы занятия выполняется поиск информации по решению проблем, практические упражнения, контрольные работы, выработка индивидуальных или групповых решений, итоговое обсуждение с обменом знаниями, участие в круглых столах, разбор конкретных ситуаций, командная работа, представление портфолио и т.п.

Самостоятельная работа.

Самостоятельная работа осуществляется в виде изучения литературы, эмпирических данных по публикациям и конкретных ситуаций из практики, подготовке индивидуальных работ, работа с лекционным материалом, самостоятельное изучение отдельных тем дисциплины; поиск и обзор литературы и электронных источников; чтение и изучение учебника и учебных пособий.

8. Фонд оценочных средств

8.1. Перечень компетенций с указанием этапов их формирования в процессе освоения образовательной программы в рамках учебной дисциплины

Основными этапами формирования указанных компетенций при изучении обучающимися дисциплины являются последовательное изучение содержательно связанных между собой тем учебных занятий. Изучение каждой темы предполагает овладение обучающимися необходимыми компетенциями. Результат аттестации обучающихся на различных этапах формирования компетенций показывает уровень освоения компетенций.

Контролируемые модули, разделы (темы) дисциплины	Индекс контролируемой компетенции (или её части)	Оценочные средства по этапам формирования компетенций
		текущий контроль по дисциплине
Тема 1. Основные исторические этапы развития криптографии.	ОПК-10	Устный опрос, решение задач.
Тема 2. Математические модели открытых сообщений.	ОПК-10	Устный опрос, решение задач.
Тема 3. Основные задачи криптографии.	ОПК-10	Устный опрос, решение задач.
Тема 4. Поточные шифры замены.	ОПК-10	Устный опрос, решение задач.
Тема 5. Шифры перестановки.	ОПК-10	Устный опрос, решение задач.
Тема 6. Блочные шифры.	ОПК-10	Устный опрос, контрольная работа.
Тема 7. Системы шифрования с открытым ключом.	ОПК-10	Устный опрос, решение задач.
Тема 8. Криптографическая стойкость шифров.	ОПК-10	Устный опрос, решение задач.
Тема 9. Имитостойкость шифров.	ОПК-10	Устный опрос, решение задач.
Тема 10. Помехоустойчивость шифра.	ОПК-10	Устный опрос, решение задач.
Тема 11. Принципы построения алгоритмов поточного шифрования.	ОПК-10	Устный опрос, решение задач.
Тема 12. Генераторы псевдослучайных последовательностей.	ОПК-10	Устный опрос, решение задач.
Тема 13. Методы анализа криптографических алгоритмов	ОПК-10	Устный опрос, решение задач.
Тема 14. Принципы построения алгоритмов поточного шифрования.	ОПК-10	Устный опрос, решение задач.
Тема 15. Генераторы псевдослучайных последовательностей.	ОПК-10	Устный опрос, решение задач.

Тема 16. Цифровые подписи.	ОПК-10	Устный опрос, решение задач.
Тема 17. Алгоритмы идентификации.	ОПК-10	Устный опрос, решение задач.
Тема 18. Алгоритмы распределения ключей.	ОПК-10	Устный опрос, контрольная работа.

8.2. Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений и навыков и (или) опыта деятельности процессе текущего контроля

Типовые контрольные задания

Контрольная работа № 1 «Блочные криптосистемы»
Вариант 1

Задание 1.
Дан шифрованный текст:
СК_МЗТЗЗЯЕИЕНЫГРХЧТБЯШГУЯТНЫЦКЗДПЬФЮЬННЦЗЗЮНКДКДБНБШУЕДТЖ
ВАЗИ_ОГЧЩЦТЦФЕДКБЫУЛЯЮОЛШШЮОРЫРДАЦВИ

Известно, что он получен с использованием блочного шифра Хилла в режиме «сцепления блоков» (CBC). Ключевыми параметрами являются:

- инициализирующий вектор $IV = \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix}$

- ключевая матрица $A = \begin{pmatrix} 22 & 3 & 25 \\ 24 & 24 & 1 \\ 18 & 19 & 14 \end{pmatrix}$

Примечание: недостающие символы в последнем блоке при шифровании дополняются пробелами в виде знака подчеркивание: «_»

Стандартная кодировка символов алфавита

А	Б	В	Г	Д	Е	Ж	З	И	К	Л	М	Н	О	П	Р
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15

С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ы	Ь	Э	Ю	Я	_
16	17	18	19	20	21	22	23	24	25	26	27	28	29	30

А) Определить ключи расшифрования.
Б) Расшифровать текст.

Задание 2.
Режимы работы блочных шифров.

Задание 3.
Раскройте понятие SP-сети.

Количество вариантов соответствует количеству студентов в группе. Рассматриваемые режимы в задании 1 – сцепление блоков и режим обратной связи по шифротексту.

Контрольная работа № 2 «Криптографические протоколы распределения ключей»

Вариант 1

1. Дать определение пороговой схемы разделения секрета между n пользователями.

2. В рамках схемы открытого распределения ключей Диффи - Хеллмана участники A и B обменялись сообщениями

$$A \to B: r_A = 3^x = 5 \pmod 7, \quad B \to A: r_B = 3^y = 4.$$

Определить выработанный общий ключ k_{AB}.

3. В рамках протокола выработки ключа конференц-связи участники A,B,C выработали индивидуальные секретные ключи x,y,z и обменялись сообщениями (в поле GF(q), α - примитивный элемент поля):

$A \to B: X = \alpha^x$, $B \to C: Y = \alpha^y$, $C \to A: Z = \alpha^z$, $A \to B: Z_1 = Z^x$, $B \to C: X_1 = X^y$, $C \to A: Y_1 = Y^z$.

Запишите формулу по которой будет вычислен ключ конференц-связи k_{ABC}.

4. Схема Блома предварительного распределения ключей между n абонентами (номера абонентов равны 1,2,…,n), использующая многочлен степени 2m от двух переменных $f(x,y)=\sum_{i=0}^{m}\sum_{j=0}^{m} a_{ij}x^i y^j$, $1 \le m < n$, является стойкой к компрометации

а) m абонентов; б) (n-m) абонентов; в) 2m абонентов; г) (m+1) абонентов.

Укажите правильный ответ, а затем его обоснуйте.

5. Рассмотрим протокол Шамира передачи сообщения «k» от участника «A» к участнику «B» на основе коммутирующего шифрпреобразования $E_t(k)$, (t – разовый ключ). Пусть в рамках данного протокола участники обменялись следующими данными:

$A \to B: y_1 = E_{t(1)}(k)$, $B \to A: y_2 = E_{t(2)}(y_1)$, $A \to B: y_3 = E^{-1}_{t(1)}(y_2)$.

Запишите формулу по которой участник B вычисляет сообщение k.

6. Рассмотрим протокол ЭЦП в системе RSA, в которой открытым ключом является пара (n,e)=(15,3). Вычислите цифровую подпись s для сообщения m=2.

Устные опросы

Раздел 1. «Введение в криптографию».

1.Приведите классификацию классических шифров по преобразованию.
2. В чем заключаются преобразования в шифрах замены?
3. В чем заключаются преобразования в шифрах перестановки?
4. Приведите примеры шифров простой замены и сложной замены.
5. В чем принципиальное различие шифров простой замены и многоалфавитной замены?
6. Почему омофонический шифр не является многоалфавитным шифром?
7. Сколько ключей имеет шифр Цезаря над алфавитом мощности N?
8. Сколько ключей имеет шифр аффинный шифр простой замены над алфавитом мощности N?

9. Сколько различных вариантов ключа имеет шифр столбцовой перестановки, если таблица имеет размер 6 на 5?
10. Может ли быть блочный шифр шифром разнозначной замены?
11. Приведите пример шифра, перестановки который может рассматриваться и как блочный шифр.
12. Какие свойства открытого текста используют при вскрытии шифра вертикальной перестановки?
13. Каково максимальное число ключей в шифре простой замены?
14. Что такое эквивалентные ключи? Имеет ли шифр Плейфера эквивалентные ключи?
15. На каких принципах строится криптоанализ шифра простой замены?

Раздел 2. «Основные классы шифров и их свойства».

1. На каких принципах строится криптоанализ шифра Виженера?
2. Каковы основные этапы криптоанализа шифра Виженера?
3. Какие шифры называют шифрами гаммирования?
4. Какие разновидности шифров гаммирования существуют?
5. Какие ограничения накладываются на ключи шифра гаммирования, чтобы он был «совершенным»?
6. Какие проблемы существуют при реализации, безусловно стойкого шифра гаммирования?
7. Приведите описание вероятностной модели криптосистемы.
8. Почему в качестве гаммы нецелесообразно использовать текст художественного произведения?
9. Почему возникает проблема синхронизации поточных шифров?
10. Для каких целей применяют усложнения линейных рекуррентных последовательностей?
11. Какой метод шифрования аналоговых сигналов обеспечивает гарантированную стойкость?
12. В каких случаях можно использовать блочный шифр в режиме простой замены?
13. Перечислите известные режимы блочных шифров?
14. Слабости и достоинства блочного и поточного шифрования.
15. Каковы основные недостатки шифров Шамира и Эль-Гамаля?
16. Безопасность, каких криптосистем базируется на вычислительной задаче факторицации больших чисел?
17. Каковы требования к параметрам криптосистемы RSA?
18. В каком случае для криптоанализа RSA применим метод Ферма?

Раздел 3. «Надежность шифров».

1. Что понимается под энтропией криптосистемы?
2. Какова связь между надежностью криптосистемы и величиной ее энтропии?
3. Как связаны значения избыточности и расстояние единственности?
4. Какие шифры называются совершенными? Приведите пример совершенного шифра.
5. Какие условия накладываются на ключ совершенного шифра?
6. Какие атаки используют в криптоанализе?
7. Чем отличаются понятия теоритической и практической стойкости шифра?
8. Каким образом априорные вероятностные распределения на множествах открытых текстов и ключей индуцируют вероятностное распределение на множестве шифрованных текстов?
9. Что такое имитостойкость шифра?
10. Является ли шифр гаммирования шифром, не размножающим искажения типа

«пропуск знаков»?
11. Перечислите методы имитозащиты данных?

Раздел 4 «Методы синтеза и анализа симметричных криптосистем».

1. В чем заключаются достоинства и недостатки систем поточного шифрования по сравнению с блочными шифрами?
2. Что с точки зрения криптографического алгоритма определяет управляющий блок?
3. Чем различаются генерации истинно случайных и псевдослучайных последовательностей чисел?
4. Какие алгоритмы генерации псевдослучайных чисел используют в криптографии?
5. Какие причины обусловили широкое использование линейных регистров сдвига в качестве управляющих блоков поточных шифрсистем?
6. Что такое комбинирующие генераторы?
7. Какова длина отрезка, необходимого для восстановления минимального многочлена заданной линейной рекуррентной последовательности с помощью алгоритма Берлекемпа-Мэсси?
8. Какие существуют типы генераторов Макларена-Марсальи?
9. Преимущества и недостатки РСЛОС и РСОСП.

Раздел 5. «Криптографические хеш-функции».

1. Что называется хеш-функцией?
2. Какими свойствами должны обладать хеш-функции?
3. Назовите наиболее распространенные алгоритмы бесключевых хеш-функций?
4. Как формируются ключевые хеш-функции?
5. Для каких целей применяются хеш-функции?
6. Почему нельзя использовать в качестве хеш-функций линейные отображения?
7. Какие задачи решает код HMAC?

Раздел 6. «Методы синтеза криптографических алгоритмов с открытым ключом».

1. Какими свойствами обладает цифровая подпись?
2. Какие алгоритмы асимметричной криптографии могут использоваться в схеме цифровой подписи?
3. Можно ли реализовать цифровую подпись методами симметричной криптографии?
4. Каково назначение цифрового сертификата?
5. Что понимают под инфраструктурой открытых ключей?
6. Почему в криптографических системах, основанных на открытых ключах, нельзя использовать одинаковые ключи для шифрования и цифровой подписи?
7. Что понимается под криптографическим протоколом?
8. Приведите классификацию криптографических протоколов.
9. Приведите примеры парольных протоколов идентификации.
10. Приведите пример протокола привязки к биту.
11. Какая идея лежит в основе протоколов с нулевым разглашением?
12. Как можно использовать цифровую подпись для защиты протоколов передачи ключей?
13. Каковы назначения и структура сертификата открытого ключа?
14. Приведите классификацию протоколов распределения ключей.
15. Что такое схема разделения секрета?

1.3 Вопросы для промежуточного контроля

Вопросы для промежуточного контроля (зачета)

1. Алгебраическая модель шифра.
2. Модели открытых сообщений.
3. Классификация шифров.
4. Блочные шифры: режимы шифрования, сеть Фейстеля.
5. Сформулируйте необходимое и достаточное условие обратимости матрицы в криптосистеме Хилла, когда арифметические операции выполняются по модулю составного числа. Приведите примеры.
6. Матричный шифр Хилла используется для зашифрования открытого текста, представленного в виде двоичной последовательности. Сколько ключей имеет такой шифр?
7. Постойте матричную криптосистему Хилла для режима сцепления блоков.
8. Шифр модульного гаммирования. Почему недопустимо использовать дважды одну и ту же гамму для зашифрования разных открытых текстов?
9. Шифр модульного гаммирования. Решение систем сравнений. Почему в качестве гаммы нецелесообразно использовать текст художественного произведения? Предложите метод вскрытия такого шифра.
10. Почему неопределенность шифра по открытому тексту (или ключу) можно рассматривать как меру теоретической стойкости шифра?
11. Каким образом априорное вероятностное распределение на множествах открытых текстов и ключей индуцирует вероятностное распределение на множестве шифрованных текстов?
12. Какой шифр называется совершенным?
13. Чем отличается понятие теоретической и практической стойкости шифра?
14. Каковы с точки зрения криптографии преимущества и недостатки перехода к шифрованию сообщений в алфавитах большей мощности?
15. В каких случаях можно рекомендовать использовать блочный шифр в режиме простой замены?
16. От каких потенциальных слабостей позволяет избавиться использование блочных шифров в режимах шифрования с обратной связью?
17. В чем заключаются достоинства и недостатки систем поточного шифрования по сравнению с блочными шифрами?
18. Что с точки зрения криптографического алгоритма определяет управляющий блок?
19. За счет чего можно обеспечить стойкость алгоритма шифрования при повторном использовании ключей?

Типовые практические задания для промежуточного контроля (зачета)

1. Рассмотрим аффинный шифр с уравнением зашифрования $y = (a \cdot x + b) \bmod N$, где N – мощность алфавита. Определите размер ключевого пространства, для N=296.

2. Дан аффинный шифр с уравнением зашифрования $y = (17 \cdot x + 11) \bmod N$, где N – мощность алфавита. Определите ключ расшифрования, для N=26.

3. Дана криптограмма : ЭКЕНЛДЦОИИПЯ. Определите, ключ шифра и расшифруйте сообщение, если известно, что был использован шифр табличной перестановки.

4. Криптосистема Хилла представлена ключом К – квадратная матрица размера 3 на 3 над кольцом Z_8

$$K = \begin{pmatrix} 1 & 0 & 2 \\ 0 & 3 & 0 \\ 1 & 1 & 3 \end{pmatrix}$$

Открытое сообщение представлено двумя блоками (3, 2, 1) и (0, 1, 1). Открытое сообщение было зашифровано методом сцепления блоков с блоком инициализации (1, 1, 0). Чему равен шифрованный текст?

5. Криптосистема Хилла представлена ключом К – квадратная матрица размера 3 на 3 над кольцом Z_8

$$K = \begin{pmatrix} 1 & 0 & 2 \\ 0 & 3 & 0 \\ 1 & 1 & 3 \end{pmatrix}$$

Открытое сообщение представлено двумя блоками (5, 1, 2) и (2, 1, 3). Открытое сообщение было зашифровано в режиме обратной связи по шифртексту с блоком инициализации (2, 1, 1). Чему равен шифрованный текст?

6. Для зашифрования блока открытого текста (1, 7, 4) использовали аффинный шифр Хилла с ключом

$k = \left(K, b^{\downarrow}\right)$, где $K = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 2 \\ 1 & 0 & 1 \end{pmatrix}$, $b^{\downarrow} = \begin{pmatrix} 2 \\ 1 \\ 2 \end{pmatrix}$ над Z_8

Вычислите блок шифрованного текста.

7. Даны параметры криптосистемы RSA: P=47, Q=139, N=PQ=6533 и E=13 – открытый ключ. Сколько ключей расшифрования данная криптосистема имеет?

8. Даны параметры криптосистемы RSA: P=11, Q=19, N=PQ=209 и E=91. Сколько различных незашифрованных блоков в шифртексте дает данная криптосистема?

9. В криптосистеме Уильямса заданы следующие параметры: P=19, Q=31, N=PQ=589, (N, 2) – открытый ключ. Вычислите закрытый ключ d.

10. Пусть $X = \{x_0, x_1\}$ - множество открытых текстов, $Y = \{y_0, y_1, y_2\}$ - множество шифртекстов, $K = \{k_0, k_1, k_2\}$ - множество ключей, $p(k_i) = \frac{1}{3}, i = 0,...,2$. Правило зашифрования: $E_{k_i}(x_j) = y_m, m = (i + j) \bmod 3, i = 0,...,2,\ j = 0,1$. Докажите, что данный шифр является совершенным

11. Пусть $X = \{x_0, x_1\}$ - множество открытых текстов, $Y = \{y_0, y_1, y_2\}$ - множество шифртекстов, $K = \{k_0, k_1, k_2\}$ - множество ключей, $p(k_i) = \frac{1}{3}, i = 0,...,2$. Правило зашифрования: $E_{k_i}(x_j) = y_m, m = (i + j) \bmod 3, i = 0,...,2,\ j = 0,1$.
Будет ли выполнятся для данного шифра равенство H(X/Y)=H(X)?

8.4. Планируемые уровни сформированности компетенций обучающихся и критерии оценивания

Уровни	Содержательное описание уровня	Основные признаки выделения уровня (этапы формирования компетенции, критерии оценки сформированности)	Пятибалльная шкала (академическая) оценка	Двухбалльная шакала, зачет	БРС, % освоения (рейтинговая оценка)
Повышенный	Творческая деятельность	*Включает нижестоящий уровень.* Умение самостоятельно принимать решение, решать проблему/задачу теоретического и прикладного характера на основе изученных методов, приемов, технологий	отлично	зачтено	86-100
Базовый	Применение знаний и умений в более широких контекстах учебной и профессиональной деятельности, нежели по образцу с большей степени самостоятельности и инициативы	*Включает нижестоящий уровень.* Способность собирать, систематизировать, анализировать и грамотно использовать информацию из самостоятельно найденных теоретических источников и иллюстрировать ими теоретические положения или обосновывать практику применения	хорошо		71-85
Удовлетворительный (достаточный)	Репродуктивная деятельность	Изложение в пределах задач курса теоретически и практически контролируемого материала	удовлетворительно		55-70
Недостаточный	Отсутствие признаков удовлетворительного уровня		неудовлетворительно	не зачтено	Менее 55

9. Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины.

Основная литература

1. Аверченков, В. И. Криптографические методы защиты информации : учебное пособие / В. И. Аверченков, М. Ю. Рытов, С. А. Шпичак. — 2-е изд., стер. - Москва : ФЛИНТА, 2017. - 215 с. - ISBN 978-5-9765-2947-2. - Текст : электронный. - URL: https://znanium.com/catalog/product/1090754 (дата обращения: 27.04.2022). – Режим доступа: по подписке.

Дополнительная литература

1. Ищукова, Е. А. Криптографические протоколы и стандарты: Учебное пособие / Ищукова Е.А., Лобова Е.А. - Таганрог:Южный федеральный университет, 2016. - 80 с.: ISBN 978-5-9275-2066-4. - Текст : электронный. - URL: https://znanium.com/catalog/product/991903 (дата обращения: 27.04.2022). – Режим доступа: по подписке.

2. Голиков, А. М. Кодирование и шифрование информации в системах связи Часть 2. Шифрование : курс лекций, компьютерный практикум, задание на самостоятельную работу : учебное пособие для специалитета: 210601.65 Радиоэлектронные системы и комплексы / А. М. Голиков. - Томск : Томский государственный университет систем управления и радиоэлектроники, 2016. - 490 с. - Текст : электронный. - URL: https://znanium.com/catalog/product/1845870 (дата обращения: 27.04.2022). – Режим доступа: по подписке.

10. Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины (модуля).

- НЭБ Национальная электронная библиотека, диссертации и прочие издания
- eLIBRARY.RU Научная электронная библиотека, книги, статьи, тезисы докладов конференций
- Гребенников Электронная библиотека ИД журналы
- ЭБС Лань книги, журналы
- ЭБС Консультант студента
- ПРОСПЕКТ ЭБС
- ЭБС ZNANIUM.COM
- РГБ Информационное обслуживание по МБА
- БЕН РАН
- Электронно-библиотечная система (ЭБС) Кантитана (https://elib.kantiana.ru/)

11. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине.

Программное обеспечение обучения включает в себя:

- система электронного образовательного контента БФУ им. И. Канта – www.lms-3.kantiana.ru, обеспечивающую разработку и комплексное использование электронных образовательных ресурсов;
- серверное программное обеспечение, необходимое для функционирования сервера и связи с системой электронного обучения через Интернет;
- корпоративная платформа Microsoft Teams;
- установленное на рабочих местах обучающихся ПО: Microsoft Windows 7, Microsoft Office Standart 2010, антивирусное программное обеспечение Kaspersky Endpoint Security.
- Среда программирования Microsoft Visual Studio (любая версия);

– Система компьютерной алгебры Maple.

12. Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине.

Для проведения занятий лекционного типа, практических и семинарских занятий используются специальные помещения (учебные аудитории), оборудованные техническими средствами обучения – мультимедийной проекционной техникой. Для проведения занятий лекционного типа используются наборы демонстрационного оборудования.

Для проведения лабораторных работ, (практических занятий – при необходимости) используются специальные помещения (учебные аудитории), оснащенные специализированным лабораторным оборудованием: персональными компьютерами с возможностью выхода в интернет и с установленным программным обеспечением, заявленным в п.11.

Для проведения групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации используются специальные помещения (учебные аудитории), оборудованные специализированной мебелью (для обучающихся), меловой / маркерной доской.

Для организации самостоятельной работы обучающимся предоставляются помещения, оснащенные компьютерной техникой с возможностью подключения к сети «Интернет» и обеспечением доступа в электронную информационно-образовательную среду университета.

Для обучения инвалидов и лиц с ограниченными возможностями здоровья университетом могут быть представлены специализированные средства обучения, в том числе технические средства коллективного и индивидуального пользования.

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
федеральное государственное автономное образовательное учреждение высшего образования «Балтийский федеральный университет имени Иммануила Канта»
Институт физико-математических наук и информационных технологий

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

«Методы алгебраической геометрии в криптографии»

Шифр: 10.05.01
Специальность: «Компьютерная безопасность»
Специализация: «Математические методы защиты информации»
Квалификация (степень) выпускника: специалист по защите информации

Калининград
2022

Лист согласования

Составитель: Мельничук Евгений Михайлович, ассистент Института физико-математических наук и информационных технологий

Рабочая программа утверждена на заседании учебно-методического совета института физико-математических наук и информационных технологий
Протокол № 01/22 от «01» февраля 2022 г.

Председатель учебно-методического совета института физико-математических наук и информационных технологий
Первый заместитель директора ИФМНиИТ, к. ф.-м. н., доцент — Шпилевой А. А

Ведущий менеджер — Е.П.Ставицкая

Содержание

1.Наименование дисциплины: «Методы алгебраической геометрии в криптографии».

Цель дисциплины: целями освоения дисциплины «Методы алгебраической геометрии в криптографии» являются ознакомление студентов с основными понятиями алгебраической геометрии; ознакомление студентов с основными алгебро-геометрическими методами, применяемыми в криптографии

2. Перечень планируемых результатов обучения по дисциплине, соотнесенных с планируемыми результатами освоения образовательной программы

Код компетенции	Результаты освоения образовательной программы (ИДК)	Результаты обучения по дисциплине
ОПК-2.2 Способен разрабатывать и анализировать математические модели механизмов защиты информации;	ОПК-2.2.1. Знает принципы построения средств криптографической защиты информации. ОПК-2.2.2. Умеет выявлять наиболее целесообразные подходы к обеспечению защиты информации компьютерной системы. ОПК-2.2.3. Владеет методами разработки математических моделей, реализуемых в средствах защиты информации.	• ***знать*** основные понятия и методы алгебраической геометрии, применяемые в криптографии • ***уметь*** грамотно применять изученные математические методы, математические пакеты для обработки, детального анализа и систематизации криптографической информации; • ***владеть*** навыками решения задач алгебраической геометрии.

3. Место дисциплины в структуре образовательной программы

Дисциплина «Методы алгебраической геометрии в криптографии» представляет собой дисциплину обязательной части блока дисциплин подготовки обучающихся.

4. Виды учебной работы по дисциплине.

Виды учебной работы по дисциплине зафиксированы учебным планом основной профессиональной образовательной программы по указанному направлению и профилю, выражаются в академических часах. Часы контактной работы и самостоятельной работы обучающегося и часы, отводимые на процедуры контроля, могут различаться в учебных планах ОПОП по формам обучения. Объем контактной работы включает часы контактной аудиторной работы (лекции/практические занятия/ лабораторные работы), контактной внеаудиторной работы (контроль самостоятельной работы), часы контактной работы в период аттестации. Контактная работа, в том числе может проводиться посредством электронной информационно-образовательной среды университета с использованием ресурсов сети Интернет и дистанционных технологий

5. Содержание дисциплины, структурированное по темам (разделам)

Исходя из рамок, установленных учебным планом по трудоемкости и видам учебной работы по дисциплине, преподаватель самостоятельно выбирает тематику занятий по формам и количеству часов проведения контактной работы: лекции и иные учебные занятия, предусматривающие преимущественную передачу учебной информации преподавателем и (или) занятия семинарского типа (семинары, практические занятия, практикумы, лабораторные работы, коллоквиумы и иные аналогичные занятия), и (или) групповые консультации, и (или) индивидуальную работу обучающихся с преподавателем, в том числе индивидуальные консультации (по курсовым работам/проектам – при наличии курсовой работы/проекта по данной дисциплине в учебном плане). Рекомендуемая тематика занятий максимально полно реализуется в контактной работе с обучающимися очной формы обучения. В случае реализации образовательной программы в заочной / очно-заочной форме трудоемкость дисциплины сохраняется, однако объем учебного материала в значительной части осваивается обучающимися в форме самостоятельной работы. При этом требования к ожидаемым образовательным результатам обучающихся по данной дисциплине не зависят от формы реализации образовательной программы.

№	Наименование раздела	Содержание раздела
1	Введение в алгебраическую геометрию	Задачи и программа курса. Место теории алгебраической геометрии в ряду других математических и прикладных дисциплин. Источники её развития и области приложения. Роль теории алгебраической геомететрии в задачах защиты информации. Формы самостоятельной работы студентов по изучению курса. Основная литература к курсу. Повторение основных понятий прикладной алгебры. Кольца, идеалы, поля, расширения полей.
2	Теория категорий	Определение категории, объекты и морфизмы. Изоморфизм объектов категории. Примеры категорий. Двойственная категория. Ковариантные и контравариантные функторы. Эквивалентность категорий.
3	Многообразия	Теорема Гильберта о нулях. Аффинные многообразия, регулярныефункции на аффинном многообразии, морфизмы. Квазипроективные многообразия. Проективные многообразия.
4	Локальные свойства	Локальное кольцо точки. Локализация кольца и локальные кольца. Касательное пространство и его инвариантность. Простые и особые точки на алгебраическом многообразии.
5	Пучки	Спектр кольца. Точки спектра. Примеры. Свойства точекс пектра, поле вычетов в точке. Локальное кольцо точки спектра. Определение предпучка. Примеры. Структурный предпучок на аффинной схеме. Определение пучка. Примеры. Пучок, ассоциированный с предпучком. Слои пучка

6	Схема	Определение схемы. Морфизм схем. Аффинные схемы и их морфизмы.

6. Рекомендуемая тематика учебных занятий в форме контактной работы

Рекомендуемая тематика учебных занятий *лекционного* типа (предусматривающих преимущественную передачу учебной информации преподавателями):

№	Наименование раздела	Темы лекций
1	Введение в алгебраическую геометрию	Лекция 1. Повторение основных понятий прикладной алгебры. Кольца, идеалы, поля, расширения полей.
2	Теория категорий	Лекция 2-3. Определение категории, объекты и морфизмы. Изоморфизм объектов категории. Примеры категорий. Двойственная категория. Ковариантные и контравариантные функторы. Эквивалентность категорий.
3	Многообразия	Лекция 4-5. Теорема Гильберта о нулях. Аффинные многообразия, регулярныефункции на аффинном многообразии, морфизмы. Лекция 6. Квазипроективные многообразия. Проективные многообразия.
4	Локальные свойства	Лекция 7-8. Локальное кольцо точки. Локализация кольца и локальные кольца. Касательное пространство и его инвариантность.
5	Пучки	Лекция 9-10. Спектр кольца. Лекция 11-12 Пучки.
6	Схема	Лекция 13-14. Определение схемы. Лекция 15. Морфизм схем. Лекция 16. Аффинные схемы и их морфизмы.

Рекомендуемая тематика *практических* занятий:

1. Кольца, идеалы, поля, алгебраической расширение полей.
2. Свойства и примеры категорий.
3. Свойства и примеры аффинных и проективных многообразий.
4. Локальное кольцо точки. Локализация кольца и локальные кольца.
5. Примеры и свойства спектра кольца и пучков.
6. Свойства и простейшие примеры схем.

На практических занятиях решаются задачи по теме занятия.

Требования к самостоятельной работе обучающихся

1. Работа с лекционным материалом, предусматривающая проработку конспекта лекций и учебной литературы, по всем темам из п. 6 настоящей рабочей программы.

2. Выполнение домашнего задания, предусматривающего решение задач, выполнение упражнений, выдаваемых на практических занятиях, по всем темам из п. 6 настоящей рабочей программы.

Руководствуясь положениями статьи 47 и статьи 48 Федерального закона от 29 декабря 2012 г. N 273-ФЗ «Об образовании в Российской Федерации» научно-педагогические работники и иные лица, привлекаемые университетом к реализации данной образовательной программы, пользуются предоставленными академическими правами и свободами в части свободы преподавания, свободы от вмешательства в профессиональную деятельность; свободы выбора и использования педагогически обоснованных форм, средств, методов обучения и воспитания; права на творческую инициативу, разработку и применение авторских программ и методов обучения и воспитания в пределах реализуемой образовательной программы и отдельной дисциплины.

Исходя из рамок, установленных учебным планом по трудоемкости и видам учебной работы по дисциплине, преподаватель самостоятельно выбирает тематику занятий по формам и количеству часов проведения контактной работы: лекции и иные учебные занятия, предусматривающие преимущественную передачу учебной информации преподавателем и (или) занятия семинарского типа (семинары, практические занятия, практикумы, лабораторные работы, коллоквиумы и иные аналогичные занятия), и (или) групповые консультации, и (или) индивидуальную работу обучающихся с преподавателем, в том числе индивидуальные консультации (по курсовым работам/проектам – при наличии курсовой работы/проекта по данной дисциплине в учебном плане).

Рекомендуемая тематика занятий максимально полно реализуется в контактной работе с обучающимися очной формы обучения. В случае реализации образовательной программы в заочной / очно-заочной форме трудоемкость дисциплины сохраняется, однако объем учебного материала в значительной части осваивается обучающимися в форме самостоятельной работы. При этом требования к ожидаемым образовательным результатам обучающихся по данной дисциплине не зависят от формы реализации образовательной программы.

7. Методические рекомендации по видам занятий

Лекционные занятия.

В ходе лекционных занятий обучающимся рекомендуется выполнять следующие действия. Вести конспектирование учебного материала. Обращать внимание на категории, формулировки, раскрывающие содержание тех или иных явлений и процессов, научные выводы и практические рекомендации по их применению. Задавать преподавателю уточняющие вопросы с целью уяснения теоретических положений, разрешения спорных ситуаций.

Желательно оставить в рабочих конспектах поля, на которых во внеаудиторное время можно сделать пометки из рекомендованной литературы, дополняющие материал прослушанной лекции, а также подчеркивающие особую важность тех или иных теоретических положений.

Практические и семинарские занятия.

На практических и семинарских занятиях в зависимости от темы занятия выполняется поиск информации по решению проблем, практические упражнения, контрольные работы, выработка индивидуальных или групповых решений, итоговое обсуждение с обменом знаниями, участие в круглых столах, разбор конкретных ситуаций, командная работа, представление портфолио и т.п.

Самостоятельная работа.

Самостоятельная работа осуществляется в виде изучения литературы, эмпирических данных по публикациям и конкретных ситуаций из практики, подготовке индивидуальных работ, работа с лекционным материалом, самостоятельное изучение отдельных тем дисциплины; поиск и обзор литературы и электронных источников; чтение и изучение учебника и учебных пособий.

8. Фонд оценочных средств

8.1. Перечень компетенций с указанием этапов их формирования в процессе освоения образовательной программы в рамках учебной дисциплины

Основными этапами формирования указанных компетенций при изучении обучающимися дисциплины являются последовательное изучение содержательно связанных между собой тем учебных занятий. Изучение каждой темы предполагает овладение обучающимися необходимыми компетенциями. Результат аттестации обучающихся на различных этапах формирования компетенций показывает уровень освоения компетенций.

Контролируемые разделы (темы) дисциплины	Индекс контроли-руемой компетенции (или её части)	Оценочные средства по этапам формирования компетенций
		текущий контроль по дисциплине
1. Введение в алгебраическую геометрию	ОПК-2.2	Опрос, решение задач.
2. Теория категорий	ОПК-2.2	Опрос, решение задач
3. Многообразия	ОПК-2.2	Опрос, решение задач
4. Локальные свойства	ОПК-2.2	Опрос, решение задач
5. Пучки	ОПК-2.2	Опрос, решение задач
6. Схема	ОПК-2.2	Опрос, решение задач, контрольная работа

8.2. Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений и навыков и (или) опыта деятельности процессе текущего контроля

Примеры вопросов для устного опроса:

По Теме 5. Пучки

1. Что такое спектр кольца?
2. Что такое точки спектра?
3. Свойства точекс пектра, поле вычетов в точке.
4. Что такое локальное кольцо точки спектра?
5. Что такое предпучок?
6. Что такое структурный предпучок на аффинной схеме?
7. Что такое пучок?.
8. Что такое пучок, ассоциированный с предпучком?
9. Что такое слой пучка?

Типовые контрольные задания:

Тема: Дифференциальные уравнения первого порядка

1. Пусть A – кольцо, S – мультипликативное подмножество в A. Доказать, что для всякого идеала $\mathfrak{a} \subset A$, дизъюнктного с S, существует простой идеал, содержащий $\mathfrak{a}$ и дизъюнктный с S

2. Пусть V – собственное аффинное алгебраическое подмножество в $\mathbb{A}^n$, $f \in K[X_1,\ldots, X_n]$. Доказать, что если f обращается в нуль на $\mathbb{A}^n - V$, то $f = 0$

3. Пусть $C = Z(Y^2 - X^3) \subset \mathbb{A}^2$. Доказать, что

a. $f : \mathbb{A}^1 \to C$, $t \mapsto (t^2, t^3)$ – параметризация C;

b. f имеет рациональное обратное отображение $g : C \dashrightarrow \mathbb{A}^1$, определяемое формулой $(x, y) \mapsto y/x$, если $(x, y) \neq (0, 0)$, и $g(0, 0) = 0$.

c. $D(g) = C \setminus \{(0, 0)\}$;

d. f и g задают взаимно обратные изоморфизмы $\mathbb{A}^1 \setminus \{0\} \cong C \setminus \{(0, 0)\}$.

8.3. Перечень вопросов и заданий для промежуточной аттестации по дисциплине

Вопросы для промежуточного контроля (экзамена)

1. Кольца и идеалы. Подкольц. Примеры колец.
2. Поле. Подполе. Примеры полей. Алгебраическое расширение поля.
3. Определение категории, объекты и морфизмы. Изоморфизм объектов категории. Примеры категорий.
4. Дуальная категория.
5. Функтор. Ковариантные и контравариантные функторы. Примеры.
6. Естественное преобразование (морфизм) функтора.
7. Теорема Гильберта о нулях.
8. Аффинные многообразия. Примеры аффинных многообразий.
9. Морфизмы.
10. Проективные многообразия. Примеры проективных многообразий

11. Локальное кольцо точки. Локализация кольца и локальные кольца
12. Касательное пространство и его инвариантность.
13. Простые и особые точки на алгебраическом многообразии.
14. Касательное расслоение.
15. Локальные параметры в точке и их свойства
16. Спектр кольца. Примеры.
17. Точки спектра. Свойства точек спектра, поле вычетов в точке.
18. Локальное кольцо точки спектра
19. Структурный предпучок на аффинной схеме.
20. Определение пучка. Примеры.
21. Пучок, ассоциированный с предпучком. Слои пучка.
22. Определение схемы. Морфизм схем. Примеры.
23. Аффинные схемы и их морфизмы.
24. Склеивание схем.

8.4. Планируемые уровни сформированности компетенций обучающихся и критерии оценивания

Уровни	Содержательное описание уровня	Основные признаки выделения уровня (этапы формирования компетенции, критерии оценки сформированности)	Пятибалльная шкала (академическая) оценка	Двухбалльная шакала, зачет	БРС, % освоения (рейтинговая оценка)
Повышенный	Творческая деятельность	*Включает нижестоящий уровень.* Умение самостоятельно принимать решение, решать проблему/задачу теоретического и прикладного характера на основе изученных методов, приемов, технологий	отлично	зачтено	86-100
Базовый	Применение знаний и умений в более широких	*Включает нижестоящий уровень.* Способность собирать, систематизировать, анализировать и	хорошо		71-85

	контекстах учебной и профессиональной деятельности, нежели по образцу с большей степени самостоятельности и инициативы	грамотно использовать информацию из самостоятельно найденных теоретических источников и иллюстрировать ими теоретические положения или обосновывать практику применения			
Удовлетворительный (достаточный)	Репродуктивная деятельность	Изложение в пределах задач курса теоретически и практически контролируемого материала	удовлетворительно		55-70
Недостаточный	Отсутствие признаков удовлетворительного уровня		неудовлетворительно	не зачтено	Менее 55

9. Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины.

Основная литература

1. Алешников С.И., Болтнев Ю.Ф. Математические методы защиты информации. Часть 5. Методы алгебраических кривых: Учебное пособие. – Калининград: БФУ им. И. Канта, 2015. – 166 с. on-line. ЭБС Кантиана

Дополнительная литература

1. Кнауб, Л. В. *Теоретико-численные методы в криптографии* [Электронный ресурс] : Учеб. пособие / Л. В. Кнауб, Е. А. Новиков, Ю. А. Шитов. - Красноярск : Сибирский федеральный университет, 2011. - 160 с. - ISBN 978-5-7638-2113-7. - Текст : электронный. - URL: https://znanium.com/catalog/product/441493
2. Романьков, В. А. Введение в криптографию : курс лекций / В.А. Романьков. — 2-е изд., испр. и доп. — Москва : ФОРУМ : ИНФРА-М, 2021. — 240 с. — (Высшее образование: Бакалавриат). - ISBN 978-5-00091-493-9. - Текст : электронный. - URL: https://znanium.com/catalog/product/1514566
3. Ященко, В. В. *Введение в криптографию*: Учебное пособие / Ященко В.В., - 4-е изд. - Москва :МЦНМО, 2014. - 352 с.: ISBN 978-5-4439-2162-4. - Текст : электронный. - URL: https://znanium.com/catalog/product/958585

10. Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины (модуля).

- НЭБ Национальная электронная библиотека, диссертации и прочие издания
- eLIBRARY.RU Научная электронная библиотека, книги, статьи, тезисы докладов конференций
- ЭБС ZNANIUM.COM
- Электронно-библиотечная система (ЭБС) Кантитана (https://elib.kantiana.ru/)

11. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине.

Программное обеспечение обучения включает в себя:

- система электронного образовательного контента БФУ им. И. Канта – www.lms-3.kantiana.ru, обеспечивающую разработку и комплексное использование электронных образовательных ресурсов;
- серверное программное обеспечение, необходимое для функционирования сервера и связи с системой электронного обучения через Интернет;
- корпоративная платформа Microsoft Teams;
- установленное на рабочих местах обучающихся ПО: Microsoft Windows 7, Microsoft Office Standart 2010, антивирусное программное обеспечение Kaspersky Endpoint Security.
- специализированное ПО не требуется.

12. Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине.

Для проведения занятий лекционного типа, практических и семинарских занятий используются специальные помещения (учебные аудитории), оборудованные техническими средствами обучения – мультимедийной проекционной техникой. Для проведения занятий лекционного типа используются наборы демонстрационного оборудования.

Для проведения лабораторных работ, (практических занятий – при необходимости) используются специальные помещения (учебные аудитории), оснащенные специализированным лабораторным оборудованием: персональными компьютерами с возможностью выхода в интернет и с установленным программным обеспечением, заявленным в п.11.

Для проведения групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации используются специальные помещения (учебные аудитории), оборудованные специализированной мебелью (для обучающихся), меловой / маркерной доской.

Для организации самостоятельной работы обучающимся предоставляются помещения, оснащенные компьютерной техникой с возможностью подключения к сети «Интернет» и обеспечением доступа в электронную информационно-образовательную среду университета.

Для обучения инвалидов и лиц с ограниченными возможностями здоровья университетом могут быть представлены специализированные средства обучения, в том числе технические средства коллективного и индивидуального пользования.

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
федеральное государственное автономное образовательное учреждение высшего образования «Балтийский федеральный университет имени Иммануила Канта»
Институт физико-математических наук и информационных технологий

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

«Криптографические протоколы»

Шифр: 10.05.01
Специальность: «Компьютерная безопасность»
Специализация: «Математические методы защиты информации»
Квалификация (степень) выпускника: специалист по защите информации

Калининград
2022

Лист согласования

Составитель: Ставицкая Е.П., старший преподаватель, Дёмин С.А., старший преподаватель

Рабочая программа утверждена на заседании учебно-методического совета института физико-математических наук и информационных технологий

Протокол № 01/22 от «01» февраля 2022 г.

Председатель учебно-методического совета института физико-математических наук и информационных технологий

Первый заместитель директора ИФМНиИТ, к. ф.-м. н., доцент — Шпилевой А. А

Ведущий менеджер — Е.П.Ставицкая

Содержание

1.Наименование дисциплины: «Криптографические протоколы».

Цель дисциплины: целью освоения дисциплины «Криптографические протоколы» является ознакомление студентов с существующими подходами к анализу и синтезу криптографических протоколов, изучение отечественных и международных стандартов в этой области.

2. Перечень планируемых результатов обучения по дисциплине, соотнесенных с планируемыми результатами освоения образовательной программы

Код компетенции	Результаты освоения образовательной программы (ИДК)	Результаты обучения по дисциплине
ОПК-10. Способен анализировать тенденции развития методов и средств криптографической защиты информации, использовать средства криптографической защиты информации при решении задач профессиональной деятельности;	ОПК-10.1. Понимает целесообразность использования криптографических алгоритмов в современных программных комплексах. ОПК-10.2. Способен применять методы криптоанализа к конкретным криптографическим примитивам. ОПК-10.3. Владеет навыками реализации алгоритмов, в том числе криптографических, в современных программных комплексах.	Студент должен знать: • типовые протоколы, используемые в сетях связи; • основные типы криптографических протоколов и принципов их построения с использованием различных классов криптосистем; • основные уязвимости и свойства криптографических протоколов, характеризующие их безопасность. Студент должен уметь: • использовать симметричные и асимметричные криптосистемы для построения криптографических протоколов; • проводить анализ криптографических протоколов. Студент должен владеть: • криптографической терминологией данной дисциплины; • подходами к разработке и анализу безопасности криптографических протоколов.

3. Место дисциплины в структуре образовательной программы

Дисциплин «Криптографические протоколы» входит в базовую часть (Б1.О.11.05) обязательной части блока дисциплин (модулей) подготовки специалистов по специальности 10.05.01«Компьютерная безопасность», специализация N 2 "Математические методы защиты информации"

4. Виды учебной работы по дисциплине.

Виды учебной работы по дисциплине зафиксированы учебным планом основной профессиональной образовательной программы по указанному направлению и профилю,

выражаются в академических часах. Часы контактной работы и самостоятельной работы обчающегося и часы, отводимые на процедуры контроля, могут различаться в учебных планах ОПОП по формам обучения. Объем контактной работы включает часы контактной аудиторной работы (лекции/практические занятия/ лабораторные работы), контактной внеаудиторной работы (контроль самостоятельной работы), часы контактной работы в период аттестации. Контактная работа, в том числе может проводиться посредством электронной информационно-образовательной среды университета с использованием ресурсов сети Интернет и дистанционных технологий

5. Содержание дисциплины, структурированное по темам (разделам)

Исходя из рамок, установленных учебным планом по трудоемкости и видам учебной работы по дисциплине, преподаватель самостоятельно выбирает тематику занятий по формам и количеству часов проведения контактной работы: лекции и иные учебные занятия, предусматривающие преимущественную передачу учебной информации преподавателем и (или) занятия семинарского типа (семинары, практические занятия, практикумы, лабораторные работы, коллоквиумы и иные аналогичные занятия), и (или) групповые консультации, и (или) индивидуальную работу обучающихся с преподавателем, в том числе индивидуальные консультации (по курсовым работам/проектам – при наличии курсовой работы/проекта по данной дисциплине в учебном плане). Рекомендуемая тематика занятий максимально полно реализуется в контактной работе с обучающимися очной формы обучения. В случае реализации образовательной программы в заочной / очно-заочной форме трудоемкость дисциплины сохраняется, однако объем учебного материала в значительной части осваивается обучающимися в форме самостоятельной работы. При этом требования к ожидаемым образовательным результатам обучающихся по данной дисциплине не зависят от формы реализации образовательной программы.

№ п/п	**Наименование темы**	**Содержание темы**
1	Введение в дисциплину.	Понятие криптографического протокола. Роль криптографических протоколов в системах защиты информации. Свойства протоколов, характеризующие их безопасность. Основные виды уязвимостей. Виды атак на криптографические протоколы. Основные виды криптографических протоколов. Примеры. Подходы к классификации криптографических протоколов.
2	Схемы цифровой подписи.	Определение схемы цифровой подписи. Схемы цифровой подписи на основе симметричных и асимметричных шифрсистем. Примеры. Схемы Эль-Гамаля, Фиата – Фейга – Шамира и Шнора, их свойства. Семейство схем типа Эль-Гамаля. Протоколы цифровой подписи на эллиптических кривых: обобщенная схема Эль-Гамаля, схема Нюберга-Рюппеля. Стандарты США и России электронной подписи. Виды электронной подписи. Одноразовые подписи. Схема цифровой подписи вслепую. Схема конфиденциальной цифровой подписи. Подписи с обнаружением подделки.
3	Криптографические протоколы идентификации.	Протоколы идентификации на основе паролей, протоколы «рукопожатия» и типа «запрос-ответ». Идентификация с использованием систем открытого шифрования. Понятие протоколов интерактивного доказательства и доказательства знания. Протоколы с нулевым разглашением. Протоколы Фиата-Шамира, Шаума, Окамото и Шнорра. Связь между

		протоколами электронной цифровой подписи и идентификации. Протоколы идентификации с самосертифицируемыми ключами.
4	Криптографические протоколы передачи ключей.	Протоколы генерации и передачи ключей. Примеры протоколов передачи ключей на основе симметричных и асимметричных шифрсистем. Двух- и трехсторонние протоколы передачи ключей. Функции доверенной третьей стороны и выполняемые ею роли. Инфраструктура открытых ключей. Управление открытыми ключами. Стандарт X.509. Проверка и отзыв сертификата открытого ключа.
5	Криптографические протоколы открытого распределения ключей.	Протоколы открытого распределения ключей. Протокол Диффи-Хэллмана и его модификации и способы защиты от атаки «противник в середине». Протоколы аутентификации и передачи ключей NS, Kerberos. Понятие аутентифицированного протокола распределения ключей. Примеры.
6	Криптографические протоколы предварительного распределения ключей.	Схемы предварительного распределения ключей. Схемы Блома и на основе пересечений множеств. Групповые протоколы. Протоколы разделения секрета и распределения ключей для телеконференции.
7	Прикладные криптографические протоколы.	Протоколы битовых обязательств и их свойства. Протокол подписания контракта и сертифицированной электронной почты. Протоколы электронного голосования. Особенности построения семейства протоколов IPsec. Обзор стандартов в области криптографических протоколов.

6. Рекомендуемая тематика учебных занятий в форме контактной работы

Рекомендуемая тематика учебных занятий *лекционного* типа (предусматривающих преимущественную передачу учебной информации преподавателями):

Темы лекций
Тема 1. Введение в дисциплину.
Тема 2. Схемы цифровой подписи.
Тема 3. Криптографические протоколы идентификации.
Тема 4. Криптографические протоколы передачи ключей.
Тема 5. Криптографические протоколы открытого распределения ключей.
Тема 6. Криптографические протоколы предварительного распределения ключей.
Тема 7. Прикладные криптографические протоколы.

Тематика практических занятий:

№ п/п	Наименование темы	Тематика практического занятия.
1	Введение в дисциплину.	1. Понятие криптографического протокола.
2	Схемы цифровой подписи.	2. Цифровые подписи на основе систем шифрования с открытыми ключами. 3. Цифровые подписи на основе специально разработанных алгоритмов. 4. Российский стандарт электронной подписи.
3	Криптографические протоколы идентификации.	5. Протоколы идентификации, использующие технику доказательства знаний. 6. Протоколы решения математических задач. 7. Аргумент с нулевым разглашением.
4	Криптографические протоколы передачи ключей.	8. Протоколы распределения сеансовых ключей. 9. Протокол Нидхема - Шрёдера. 10. Базовый протокол Kerberos.
5	Криптографические протоколы открытого распределения ключей.	11. Протокол Диффи – Хеллмана и его усиление. 12. Аутентифицированные протоколы.
6	Криптографические протоколы предварительного распределения ключей.	13. Модулярные схемы разделения секрета. 14. Групповой протокол разделения секрета. 15. Криптографические протоколы скрытой передачи секрета.
7	Прикладные криптографические протоколы.	16. Особенности построения протоколов IPsec.

Требования к самостоятельной работе обучающихся

1. Работа с лекционным материалом, предусматривающая проработку конспекта лекций и учебной литературы, по всем темам из п. 6 настоящей рабочей программы.

2. Выполнение домашнего задания, предусматривающего решение задач, выполнение упражнений, выдаваемых на практических занятиях, по всем темам из п. 6 настоящей рабочей программы.

Руководствуясь положениями статьи 47 и статьи 48 Федерального закона от 29 декабря 2012 г. N 273-ФЗ «Об образовании в Российской Федерации» научно-педагогические работники и иные лица, привлекаемые университетом к реализации данной образовательной программы, пользуются предоставленными академическими правами и свободами в части свободы преподавания, свободы от вмешательства в профессиональную деятельность; свободы выбора и использования педагогически обоснованных форм, средств, методов обучения и воспитания; права на творческую инициативу, разработку и применение авторских программ и методов обучения и воспитания в пределах реализуемой образовательной программы и отдельной дисциплины.

Исходя из рамок, установленных учебным планом по трудоемкости и видам учебной работы по дисциплине, преподаватель самостоятельно выбирает тематику занятий по формам и количеству часов проведения контактной работы: лекции и иные учебные занятия, предусматривающие преимущественную передачу учебной информации преподавателем и (или) занятия семинарского типа (семинары, практические занятия, практикумы, лабораторные работы, коллоквиумы и иные аналогичные занятия), и (или) групповые консультации, и (или) индивидуальную работу обучающихся с преподавателем, в том числе индивидуальные консультации (по курсовым работам/проектам – при наличии курсовой работы/проекта по данной дисциплине в учебном плане).

Рекомендуемая тематика занятий максимально полно реализуется в контактной работе с обучающимися очной формы обучения. В случае реализации образовательной программы в заочной / очно-заочной форме трудоемкость дисциплины сохраняется, однако объем учебного материала в значительной части осваивается обучающимися в форме самостоятельной работы. При этом требования к ожидаемым образовательным результатам обучающихся по данной дисциплине не зависят от формы реализации образовательной программы.

№ п/п	**Наименование темы**	**Тематика самостоятельных работ.**
1	Введение в дисциплину.	Формальные методы анализа протоколов обеспечения безопасности.
2	Схемы цифровой подписи.	Стандарты цифровой подписи США и России. Стираемые подписи.
3	Криптографические протоколы идентификации.	Протокол аутентификации на основе криптосистемы RSA.
4	Криптографические протоколы передачи ключей.	Протокол Kerberos. Смешанные протоколы.
5	Криптографические протоколы открытого распределения ключей.	Протоколы совместной выработки общего ключа: протокол Асмута-Блюма, схема Якоби.
6	Криптографические протоколы предварительного распределения ключей.	Индивидуально-групповой протокол разделения секрета. Теоретико-числовой протокол скрытой передачи секретов.
7	Прикладные криптографические протоколы.	Структура протоколов IPsec. Управление ключами протоколов IPsec. Атаки на протоколы IPsec.

7. Методические рекомендации по видам занятий

Лекционные занятия.

В ходе лекционных занятий обучающимся рекомендуется выполнять следующие действия. Вести конспектирование учебного материала. Обращать внимание на категории, формулировки, раскрывающие содержание тех или иных явлений и процессов, научные выводы и практические рекомендации по их применению. Задавать преподавателю

уточняющие вопросы с целью уяснения теоретических положений, разрешения спорных ситуаций.

Желательно оставить в рабочих конспектах поля, на которых во внеаудиторное время можно сделать пометки из рекомендованной литературы, дополняющие материал прослушанной лекции, а также подчеркивающие особую важность тех или иных теоретических положений.

Практические и семинарские занятия.

На практических и семинарских занятиях в зависимости от темы занятия выполняется поиск информации по решению проблем, практические упражнения, контрольные работы, выработка индивидуальных или групповых решений, итоговое обсуждение с обменом знаниями, участие в круглых столах, разбор конкретных ситуаций, командная работа, представление портфолио и т.п.

Самостоятельная работа.

Самостоятельная работа осуществляется в виде изучения литературы, эмпирических данных по публикациям и конкретных ситуаций из практики, подготовке индивидуальных работ, работа с лекционным материалом, самостоятельное изучение отдельных тем дисциплины; поиск и обзор литературы и электронных источников; чтение и изучение учебника и учебных пособий.

8. Фонд оценочных средств

8.1. Перечень компетенций с указанием этапов их формирования в процессе освоения образовательной программы в рамках учебной дисциплины

Основными этапами формирования указанных компетенций при изучении обучающимися дисциплины являются последовательное изучение содержательно связанных между собой тем учебных занятий. Изучение каждой темы предполагает овладение обучающимися необходимыми компетенциями. Результат аттестации обучающихся на различных этапах формирования компетенций показывает уровень освоения компетенций.

Контролируемые модули, разделы (темы) дисциплины	Индекс контролируемой компетенции (или её части)	Оценочные средства по этапам формирования компетенций
		текущий контроль по дисциплине
Тема 1. Введение в дисциплину.	ОПК-10	Устный опрос, решение задач.
Тема 2. Схемы цифровой подписи.	ОПК-10	Устный опрос, решение задач.
Тема 3. Криптографические протоколы идентификации.	ОПК-10	Устный опрос, решение задач.
Тема 4. Криптографические протоколы передачи ключей.	ОПК-10	Устный опрос, решение задач.
Тема 5. Криптографические протоколы открытого распределения ключей.	ОПК-10	Устный опрос, решение задач.
Тема 6. Криптографические протоколы	ОПК-10	Устный опрос, контрольная работа.

предварительного распределения ключей.		
Тема 7. Прикладные криптографические протоколы.	ОПК-10	Устный опрос, решение задач.

8.2. Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений и навыков и (или) опыта деятельности процессе текущего контроля

Типовые контрольные задания

Контрольная работа «Криптографические протоколы распределения ключей»

Вариант 1 (*примерный типовой вариант*)

Задание 1. Рассмотрим протокол Шамира передачи ключа «***k***» от участника ***A*** к участнику ***B*** на основе коммутирующего шифрпреобразования $E_t(k)$, (t – разовый ключ одного из участников). Пусть в рамках данного протокола участники обменялись следующими сообщениями:

$$A \rightarrow B: y_1 = E_{tA}(k),$$
$$B \rightarrow A: y_2 = E_{tB}(y_1),$$
$$A \rightarrow B: y_3 = E^{-1}{}_{tA}(y_2).$$

(E_t^{-1} – правило расшифрования на ключе t).
Тогда ключ ***k*** участник В вычисляет по формуле:

а) $k = E^{-1}{}_{tA}(y_1)$; б) $k = E^{-1}{}_{tB}(y_1)$; в) $k = E^{-1}{}_{tB}(y_3)$; г) $k = E^{-1}{}_{tA}(y_2)$.

Укажите правильный ответ.

Задание 2. В рамках протокола MTI открытого распределения ключей участники ***A*** и ***B*** обменялись данными:

$$A \rightarrow B: r_A = 5,$$
$$B \rightarrow A: r_B = 2.$$

Найти общий ключ связи участников при условии, что $\alpha=3$, $Z_p=Z_7$, открытые ключи участников А и В равны соответственно $z_A=3$, $z_B=6$.

Задание 3. В рамках протокола выработки ключа конференцсвязи участники ***A,B,C*** выработали индивидуальные секретные ключи x,y,z и обменялись сообщениями (в поле GF(q), α - примитивный элемент поля):

$$A \rightarrow B: X = \alpha^x,$$
$$B \rightarrow C: Y = \alpha^y,$$
$$C \rightarrow A: Z = \alpha^z,$$
$$A \rightarrow B: Z_1 = Z^x,$$
$$B \rightarrow C: X_1 = X^y,$$
$$C \rightarrow A: Y_1 = Y^z.$$

Тогда ключ конференц -связи k_{ABC} вычисляется по формуле:

а) $k_{ABC} = Z_1 \cdot X_1 \cdot Y_1$; б) $k_{ABC} = xyz$; в) $k_{ABC} = x+y+z$; г) $k_{ABC} = \alpha^{xyz}$.

Укажите правильный ответ.

Задание 4. Каково назначение и структура сертификата открытого ключа?

Количество вариантов соответствует количеству студентов в группе.

Устные опросы

Тема 1. Введение в дисциплину.

1.Приведите классификацию криптографических протоколов.
2. Охарактеризуйте понятие «протокол обеспечение безопасности».
3. Дайте определение понятие «интерактивное доказательство».
4. Перечислите наиболее распространённые атаки на криптографические протоколы.
5. Приведите примеры способов защиты от атак на криптографические протоколы.
6. Приведите примеры защищенных протоколов, в которых не требуется обеспечение свойства конфиденциальности.
7. Перечислите основные методы анализа криптографических протоколов.

Тема 2. Схемы цифровой подписи.

1. Какие задачи позволяет решать цифровая подпись?
2. В чем принципиальная сложность практического применения систем цифровой подписи?
3. Почему в криптографических системах, основанных на открытых ключах, нельзя использовать одинаковые ключи для шифрования сообщения и цифровой подписи?
4. Что такое удостоверяющий центр?
5. Перечислите основные подходы к построению схем цифровой подписи.
6. Приведите примеры цифровых подписей семейства Эль-Гамаля.
7. Что означает термин «схема конфиденциальной цифровой подписи»?
8. Что означает термин «нотаризация цифровых подписей»?

Тема 3. Криптографические протоколы идентификации.

1. Приведите классификацию алгоритмов идентификации?
2. В чем заключаются недостатки парольной аутентификации?
3. Перечислите возможные уязвимости схемы одноразовых паролей.
4. Чем определяется повышенная надежность идентификации при использовании пластиковых карт?
5. В каких целях в протоколах используют временную метку?
6. В каких целях в протоколах используют «случайные числа»?
7. Какие идеи лежат в основе построения протоколов с нулевым разглашением?
8. Какие атаки существуют для протоколов идентификации?
9. Приведите примеры с описанием знакомых Вам криптографических протоколов идентификации?
10. Что означает термин «схема привязки к биту»?
11. Что означают свойства связывания и сокрытия для протоколов привязки к биту?

Тема 4. Криптографические протоколы передачи ключей.

1. Перечислите достоинства и недостатки централизованного распределения ключей.
2. Приведите примеры криптографических протоколов передачи ключей с использованием симметричных систем шифрования.
3. Приведите примеры криптографических протоколов передачи ключей с

использованием асимметричных систем шифрования.
4. Какие системы шифрования нельзя использовать в криптографическом протоколе Шамира?
5. Перечислите недостатки протокола NS?
6. С какой целью вводится второй сервер в протоколе Kerberos?
7. Как используют цифровую подпись для защиты протоколов передачи ключей?
8. Каково назначение сертификата открытого ключа?
9. Какова структура сертификата открытого ключа?
10. Перечислите основные атаки на протоколы передачи ключей?

Тема 5. Криптографические протоколы открытого распределения ключей.

1. Для чего нужно открытое распределение ключей?
2. Перечислите виды протоколов открытого распределения ключей и их свойства.
3. Каков основной недостаток протокола распределения ключей Диффи-Хеллмана и каковы пути его устранения?
4. Покажите устойчивость к атаке «противник в середине» для всех вариантов протокола MTI.
5. Перечислите протоколы, не обеспечивающие свойства аутентичности ключа.
6. Приведите примеры протоколов обеспечивающих свойство взаимного подтверждения правильности получения ключа.
7. Покажите, что протокол STS можно аутентифицировать, если провести аутентификацию сообщений и аутентификацию идентификаторов сторон.

Тема 6. Криптографические протоколы предварительного распределения ключей.

1. Какими свойствами должны обладать криптографические протоколы предварительного распределения ключей?
2. Докажите оптимальность схемы Блома.
3. Что такое схема разделения секрета?
4. Каково назначение схемы разделения секрета?
5. Предложите схему разделения секрета для двух групп из трех участников каждая, если составы групп не пересекаются.
6. Предложите схему разделения секрета для двух групп из трех участников каждая, если имеется один участник, входящий в обе группы.
7. В чем общность схемы разделения секрета и способа распределения ключей для конференцсвязи?
8. В чем отличия схемы разделения секрета и способа распределения ключей для конференцсвязи?

Тема 7. Прикладные криптографические протоколы.

1. Какими свойствами должны обладать криптографический протокол подписания контракта?
2. Какие протоколы относят к протоколам сертифицированной электронной почты?
3. Какими свойствами должны обладать криптографический протокол подписания контракта?
4. Предложите способ, позволяющий модифицировать протокол сертифицированной электронной почты так, чтобы для него выполнялось свойство конфиденциальности.
5. Перечислите требуемые свойства для протокола электронного голосования.
6. Сколько нечестных комиссий может участвовать в протоколе электронного голосования, не нарушая его основных свойств?

1.3 Вопросы для промежуточного контроля

Вопросы для промежуточного контроля (зачета)

1. Определение протокола. Основные характеристики протоколов. Типы протоколов. Криптографический протокол. Классификация криптографических протоколов.
2. Электронная цифровая подпись: определение, свойства, на сложности решения каких задач основана надежность схемы ЭЦП, структура сертификатов открытых ключей
3. Подходы к построению ЭЦП: на основе шифрсистем с открытым ключом.
4. Цифровая подпись Фиата-Шамира.
5. Схема ЭЦП Эль-Гамаля.
6. Алгоритм DSA.
7. Цифровая подпись Шнорра.
8. Схема цифровой подписи вслепую.
9. Протоколы идентификации: определение, цели, классификация; слабая аутентификация; защита от компрометации базы данных; одноразовые пароли.
10. Протоколы идентификации: сильная аутентификация, случайные последовательности и метки времени, примеры протоколов с использованием симметричных алгоритмов шифрования.
11. Протоколы идентификации: сильная аутентификация, случайные последовательности и метки времени, примеры протоколов с использованием асимметричных алгоритмов шифрования.
12. Протокол привязки к биту. Схема Голдвассера-Микали.
13. Игровые протоколы. Протокол подписания контракта.
14. Протоколы передачи ключей с использованием симметричного шифрования, примеры.
15. Протоколы передачи ключей с использованием односторонней функции, примеры.
16. Протоколы передачи ключей: протокол Шамира.
17. Трехсторонние протоколы передачи ключей, примеры.
18. Протоколы передачи ключей с использованием асимметричного шифрования без использования цифровой подписи, примеры.
19. Протоколы передачи ключей с использованием асимметричного шифрования с использованием цифровой подписи, примеры, сертификаты.
20. Международный стандарт X.509 (варианты протокола).
21. Открытое распределение ключей. Протокол Диффи - Хеллмана и его усиление.
22. Открытое распределение ключей. Протокол MTI.
23. Предварительное распределение ключей: проблема предварительного распределения ключей в сети связи, свойство схем предварительного распределения ключей.
24. Схемы разделения секрета.
25. Управление ключами. Жизненный цикл ключей.

Типовые практические задания для промежуточного контроля (зачета)

1.Рассмотрим протокол Шамира передачи ключа «***k***» от участника ***A*** к участнику ***B*** на основе коммутирующего шифрпреобразования $E_t(k)$, (t – разовый ключ одного из участников). Пусть в рамках данного протокола участники обменялись следующими сообщениями:

$$A \rightarrow B: y_1 = E_{tA}(k),$$
$$B \rightarrow A: y_2 = E_{tB}(y_1),$$
$$A \rightarrow B: y_3 = E^{-1}{}_{tA}(y_2).$$

(E_t^{-1} – правило расшифрования на ключе t).
Запишите формулу вычисление ключа ***k*** участником В.

2. В рамках протокола MTI открытого распределения ключей участники ***A*** и ***B*** обменялись данными:

$$A \rightarrow B: r_A = 5,$$
$$B \rightarrow A: r_B = 2.$$

Найти общий ключ связи участников при условии, что $\alpha=3$, $Z_p=Z_7$, открытые ключи участников А и В равны соответственно $z_A=3$, $z_B=6$.

3. В рамках протокола выработки ключа конференцсвязи участники ***A,B,C*** выработали индивидуальные секретные ключи x,y,z и обменялись сообщениями (в поле GF(q), α - примитивный элемент поля):

$$A \rightarrow B: X = \alpha^x,$$
$$B \rightarrow C: Y = \alpha^y,$$
$$C \rightarrow A: Z = \alpha^z,$$
$$A \rightarrow B: Z_1 = Z^x,$$
$$B \rightarrow C: X_1 = X^y,$$
$$C \rightarrow A: Y_1 = Y^z.$$

Запишите формулу вычисления ключа конференцсвязи k_{ABC}.

8.4. Планируемые уровни сформированности компетенций обучающихся и критерии оценивания

Уровни	Содержательное описание уровня	Основные признаки выделения уровня (этапы формирования компетенции, критерии оценки сформированности)	Пятибалльная шкала (академическая) оценка	Двухбалльная шакала, зачет	БРС, % освоения (рейтинговая оценка)
Повышенный	Творческая деятельность	*Включает нижестоящий уровень.* Умение самостоятельно принимать решение, решать проблему/задачу теоретического и прикладного характера на основе изученных методов, приемов, технологий	отлично	зачтено	86-100
Базовый	Применение знаний и умений в более	*Включает нижестоящий уровень.* Способность собирать, систематизировать,	хорошо		71-85

	широких контекстах учебной и профессиональной деятельности, нежели по образцу с большей степени самостоятельности и инициативы	анализировать и грамотно использовать информацию из самостоятельно найденных теоретических источников и иллюстрировать ими теоретические положения или обосновывать практику применения			
Удовлетворительный (достаточный)	Репродуктивная деятельность	Изложение в пределах задач курса теоретически и практически контролируемого материала	удовлетворительно		55-70
Недостаточный	Отсутствие признаков удовлетворительного уровня		неудовлетворительно	не зачтено	Менее 55

9. Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины.

Основная литература

1. Ищукова, Е. А. Криптографические протоколы и стандарты: Учебное пособие / Ищукова Е.А., Лобова Е.А. - Таганрог:Южный федеральный университет, 2016. - 80 с.: ISBN 978-5-9275-2066-4. - Текст : электронный. - URL: https://znanium.com/catalog/product/991903 (дата обращения: 27.04.2022). – Режим доступа: по подписке.

Дополнительная литература

1. Аверченков, В. И. Криптографические методы защиты информации : учебное пособие / В. И. Аверченков, М. Ю. Рытов, С. А. Шпичак. — 2-е изд., стер. - Москва : ФЛИНТА, 2017. - 215 с. - ISBN 978-5-9765-2947-2. - Текст : электронный. - URL: https://znanium.com/catalog/product/1090754 (дата обращения: 27.04.2022). – Режим доступа: по подписке.
2. Голиков, А. М. Кодирование и шифрование информации в системах связи Часть 2. Шифрование : курс лекций, компьютерный практикум, задание на самостоятельную работу : учебное пособие для специалитета: 210601.65 Радиоэлектронные системы и комплексы / А. М. Голиков. - Томск : Томский государственный университет систем управления и радиоэлектроники, 2016. - 490 с. - Текст : электронный. - URL: https://znanium.com/catalog/product/1845870 (дата обращения: 27.04.2022). – Режим доступа: по подписке.

10. Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины (модуля).

- НЭБ Национальная электронная библиотека, диссертации и прочие издания

- eLIBRARY.RU Научная электронная библиотека, книги, статьи, тезисы докладов конференций
- Гребенников Электронная библиотека ИД журналы
- ЭБС Лань книги, журналы
- ЭБС Консультант студента
- ПРОСПЕКТ ЭБС
- ЭБС ZNANIUM.COM
- РГБ Информационное обслуживание по МБА
- БЕН РАН
- Электронно-библиотечная система (ЭБС) Кантитана (https://elib.kantiana.ru/)

11. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине.

Программное обеспечение обучения включает в себя:

- система электронного образовательного контента БФУ им. И. Канта – www.lms-3.kantiana.ru, обеспечивающую разработку и комплексное использование электронных образовательных ресурсов;
- серверное программное обеспечение, необходимое для функционирования сервера и связи с системой электронного обучения через Интернет;
- корпоративная платформа Microsoft Teams;
- установленное на рабочих местах обучающихся ПО: Microsoft Windows 7, Microsoft Office Standart 2010, антивирусное программное обеспечение Kaspersky Endpoint Security.
- Среда программирования Microsoft Visual Studio (любая версия);
- Система компьютерной алгебры Maple.

12. Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине.

Для проведения занятий лекционного типа, практических и семинарских занятий используются специальные помещения (учебные аудитории), оборудованные техническими средствами обучения – мультимедийной проекционной техникой. Для проведения занятий лекционного типа используются наборы демонстрационного оборудования.

Для проведения лабораторных работ, (практических занятий – при необходимости) используются специальные помещения (учебные аудитории), оснащенные специализированным лабораторным оборудованием: персональными компьютерами с возможностью выхода в интернет и с установленным программным обеспечением, заявленным в п.11.

Для проведения групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации используются специальные помещения (учебные аудитории), оборудованные специализированной мебелью (для обучающихся), меловой / маркерной доской.

Для организации самостоятельной работы обучающимся предоставляются помещения, оснащенные компьютерной техникой с возможностью подключения к сети «Интернет» и обеспечением доступа в электронную информационно-образовательную среду университета.

Для обучения инвалидов и лиц с ограниченными возможностями здоровья университетом могут быть представлены специализированные средства обучения, в том числе технические средства коллективного и индивидуального пользования.

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
федеральное государственное автономное образовательное учреждение высшего образования «Балтийский федеральный университет имени Иммануила Канта»
Институт физико-математических наук и информационных технологий

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

«Компьютерный практикум по криптографии на эллиптических кривых»

Шифр: 10.05.01
Специальность: «Компьютерная безопасность»
Специализация: «Математические методы защиты информации»
Квалификация (степень) выпускника: специалист по защите информации

Калининград
2022

Лист согласования

Составитель: Болтнев Ю.Ф, старший преподаватель

Рабочая программа утверждена на заседании учебно-методического совета института физико-математических наук и информационных технологий
Протокол № 01/22 от «01» февраля 2022 г.
Председатель учебно-методического
совета института физико-
математических наук и информационных
технологий
Первый заместитель директора Шпилевой А. А
ИФМНиИТ, к. ф.-м. н., доцент

Ведущий менеджер Е.П.Ставицкая

Содержание

1.Наименование дисциплины: «Компьютерный практикум по криптографии на эллиптических кривых».

Цель дисциплины: формирование у обучаемых способности применять современные методы и средства исследования для обеспечения информационной безопасности компьютерных систем; формирование способности ориентироваться в современных и перспективных математических методах защиты информации, оценивать возможность и эффективность их применения в конкретных задачах защиты информации; овладение методами современной алгебры, применяемыми в криптографии, теории кодирования и общих моделях безопасности компьютерных систем.

2. Перечень планируемых результатов обучения по дисциплине, соотнесенных с планируемыми результатами освоения образовательной программы

Код компетенции	Результаты освоения образовательной программы (ИДК)	Результаты обучения по дисциплине
ОПК-2.1 Способен разрабатывать алгоритмы, реализующие современные математические методы защиты информации.	ОПК-2.1.1. Знает алгоритмы, реализующие современные математические методы защиты информации. ОПК-2.1.2. Разрабатывает рекомендации и предложения по совершенствованию и повышению эффективности защиты информации. ОПК-2.1.3. Владеет методами отладки создаваемых средств защиты.	**Знать** уравнения и основные свойства эллиптических кривых над конечными полями различной характеристики; групповой закон на множестве рациональных точек и структуру группы рациональных точек; методы подсчёта числа рациональных точек эллиптических кривых над конечными полями; **Уметь** определять структуру группы рациональных точек эллиптической кривой над конечным полем; моделировать алгоритмы в системах компьютерной алгебры, оценивать их работоспособность и эффективность **Владеть** навыками эффективных вычислений в группе точек эллиптической кривой; методами расчета параметров криптосистем на эллиптических кривых, обеспечивающих их надежность и эффективность

3. Место дисциплины в структуре образовательной программы

Дисциплина «Компьютерный практикум по криптографии на эллиптических кривых» представляет собой дисциплину обязательной части блока дисциплин подготовки студентов.

4. Виды учебной работы по дисциплине.

Виды учебной работы по дисциплине зафиксированы учебным планом основной профессиональной образовательной программы по указанному направлению и профилю, выражаются в академических часах. Часы контактной работы и самостоятельной работы студента и часы, отводимые на процедуры контроля, могут различаться в учебных планах ОПОП по формам обучения. Объем контактной работы включает часы контактной аудиторной работы (лекции/практические занятия/ лабораторные работы), контактной внеаудиторной работы (контроль самостоятельной работы), часы контактной работы в период аттестации. Контактная работа, в том числе может проводиться посредством электронной информационно-образовательной среды университета с использованием ресурсов сети Интернет и дистанционных технологий

5. Содержание дисциплины, структурированное по темам (разделам)

Исходя из рамок, установленных учебным планом по трудоемкости и видам учебной работы по дисциплине, преподаватель самостоятельно выбирает тематику занятий по формам и количеству часов проведения контактной работы: лекции и иные учебные занятия, предусматривающие преимущественную передачу учебной информации преподавателем и (или) занятия семинарского типа (семинары, практические занятия, практикумы, лабораторные работы, коллоквиумы и иные аналогичные занятия), и (или) групповые консультации, и (или) индивидуальную работу обучающихся с преподавателем, в том числе индивидуальные консультации (по курсовым работам/проектам – при наличии курсовой работы/проекта по данной дисциплине в учебном плане). Рекомендуемая тематика занятий максимально полно реализуется в контактной работе со студентами очной формы обучения. В случае реализации образовательной программы в заочной / очно-заочной форме трудоемкость дисциплины сохраняется, однако объем учебного материала в значительной части осваивается студентами в форме самостоятельной работы. При этом требования к ожидаемым образовательным результатам студентов по данной дисциплине не зависят от формы реализации образовательной программы.

№ п/п	Наименование темы	Содержание темы
1	Изоморфизм кривых. Групповой закон композиции	Основные определения. Уравнение Вейерштрасса. Дискриминант и j-инвариант. Изоморфизм кривых. Сложение точек эллиптической кривой. Структура группы.
2	Эллиптические кривые над полем рациональных чисел и над полями различных характеристик	Кривые над K , char(K) ≠ 2, 3. Кривые над K , char(K) = 2. Классы изоморфизмов. Подгруппа кручения. Теорема Лутц-Нагеля. Теорема Мазура. Теорема Морделла.
3	Эллиптические кривые над	Квадратичный характер и подсчёт числа точек. Дзета-функция эллиптической кривой над конечным

	конечными полями. Подсчет числа точек на кривой.	полем. Теорема Хассе. Теорема Вейля. *L*-многочлен. Суперсингулярные эллиптические кривые. Многочлены деления. Группа *m*-кручения. Идея алгоритма Шуфа.
4	Криптография на эллиптических кривых	Маркировка единичных сообщений в случае характеристики, не равной 2 и в случае характеристики, равной 2. Протокол Диффи–Хеллмана, протокол Месси–Омуры, протокол Эль-Гамаля.

6. Рекомендуемая тематика учебных занятий в форме контактной работы

Рекомендуемая тематика учебных занятий *лекционного* типа (предусматривающих преимущественную передачу учебной информации преподавателями):

№	Наименование раздела	Содержание раздела
1	Тема 1. Изоморфизм кривых. Групповой закон композиции.	Лекция №1. Изоморфизм кривых. Лекция №2. Групповой закон композиции.
2	Тема 2. Эллиптические кривые над полем рациональных чисел и над полями различных характеристик.	Лекция № 3. Эллиптические кривые над полем рациональных чисел Лекция №4. Эллиптические кривые над полями различных характеристик.
3	Тема 3. Эллиптические кривые над конечными полями. Подсчет числа точек на кривой.	Лекция № 5. Эллиптические кривые над конечными полями. Лекция № 6. Подсчет числа точек на кривой.
4	Тема 4. Криптография на эллиптических кривых	Лекция № 7. Криптография на эллиптических кривых

Рекомендуемая тематика *лабораторных* занятий:

№ п/п	Наименование темы
1	Изоморфизмы, инварианты и классификация эллиптических кривых.
2	Групповой закон на эллиптической кривой.
3	Исследование структуры группы рациональных точек
4	L-многочлен эллиптической кривой. Подсчѐт числа рациональных точек кривой
5	Определение структуры группы точек эллиптической кривой над конечным полем
6	Алгоритмы маркировки, демаркировки, шифровки и дешифровки для эллиптических кривых

Требования к самостоятельной работе студентов

1. Работа с лекционным материалом, предусматривающая проработку конспекта лекций и учебной литературы, по всем лабораторным работам, описанным выше. Каждая лабораторная работа снабжена списком статей и выполняется индивидуально или в группе из не более 2х человек.

Руководствуясь положениями статьи 47 и статьи 48 Федерального закона от 29 декабря 2012 г. N 273-ФЗ «Об образовании в Российской Федерации» научно-педагогические работники и иные лица, привлекаемые университетом к реализации данной образовательной программы, пользуются предоставленными академическими правами и свободами в части свободы преподавания, свободы от вмешательства в профессиональную деятельность; свободы выбора и использования педагогически обоснованных форм, средств, методов обучения и воспитания; права на творческую инициативу, разработку и применение авторских программ и методов обучения и воспитания в пределах реализуемой образовательной программы и отдельной дисциплины.

Исходя из рамок, установленных учебным планом по трудоемкости и видам учебной работы по дисциплине, преподаватель самостоятельно выбирает тематику занятий по формам и количеству часов проведения контактной работы: лекции и иные учебные занятия, предусматривающие преимущественную передачу учебной информации преподавателем и (или) занятия семинарского типа (семинары, практические занятия, практикумы, лабораторные работы, коллоквиумы и иные аналогичные занятия), и (или) групповые консультации, и (или) индивидуальную работу обучающихся с преподавателем, в том числе индивидуальные консультации (по курсовым работам/проектам – при наличии курсовой работы/проекта по данной дисциплине в учебном плане).

Рекомендуемая тематика занятий максимально полно реализуется в контактной работе со студентами очной формы обучения. В случае реализации образовательной программы в заочной / очно-заочной форме трудоемкость дисциплины сохраняется, однако объем учебного материала в значительной части осваивается студентами в форме самостоятельной работы. При этом требования к ожидаемым образовательным результатам студентов по данной дисциплине не зависят от формы реализации образовательной программы.

7. Методические рекомендации по видам занятий

Лекционные занятия.

В ходе лекционных занятий обучающимся рекомендуется выполнять следующие действия. Вести конспектирование учебного материала. Обращать внимание на категории, формулировки, раскрывающие содержание тех или иных явлений и процессов, научные выводы и практические рекомендации по их применению. Задавать преподавателю уточняющие вопросы с целью уяснения теоретических положений, разрешения спорных ситуаций.

Желательно оставить в рабочих конспектах поля, на которых во внеаудиторное время можно сделать пометки из рекомендованной литературы, дополняющие материал прослушанной лекции, а также подчеркивающие особую важность тех или иных теоретических положений.

Практические и семинарские занятия.

На практических и семинарских занятиях в зависимости от темы занятия выполняется поиск информации по решению проблем, практические упражнения, контрольные работы, выработка индивидуальных или групповых решений, итоговое

обсуждение с обменом знаниями, участие в круглых столах, разбор конкретных ситуаций, командная работа, представление портфолио и т.п.

Самостоятельная работа.

Самостоятельная работа осуществляется в виде изучения литературы, эмпирических данных по публикациям и конкретных ситуаций из практики, подготовке индивидуальных работ, работа с лекционным материалом, самостоятельное изучение отдельных тем дисциплины; поиск и обзор литературы и электронных источников; чтение и изучение учебника и учебных пособий.

8. Фонд оценочных средств

8.1. Перечень компетенций с указанием этапов их формирования в процессе освоения образовательной программы в рамках учебной дисциплины

Основными этапами формирования указанных компетенций при изучении обучающимися дисциплины являются последовательное изучение содержательно связанных между собой тем учебных занятий. Изучение каждой темы предполагает овладение обучающимися необходимыми компетенциями. Результат аттестации обучающихся на различных этапах формирования компетенций показывает уровень освоения компетенций.

Контролируемые разделы (темы) дисциплины	Индекс контролируемой компетенции (или её части)	Оценочные средства по этапам формирования компетенций
		текущий контроль по дисциплине
1. Изоморфизм кривых. Групповой закон композиции	ОПК-2.1	Защита лабораторных работ
2. Эллиптические кривые над полем рациональных чисел и над полями различных характеристик	ОПК-2.1	Защита лабораторных работ
3. Эллиптические кривые над конечными полями. Подсчет числа точек на кривой.	ОПК-2.1	Защита лабораторных работ
4. Криптография на эллиптических кривых	ОПК-2.1	Защита лабораторных работ

8.2. Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений и навыков и (или) опыта деятельности процессе текущего контроля

Типовые задачи

Тема 1. Изоморфизм кривых. Групповой закон композиции

	Задача
Оценка «удовлетворительно» или низкой уровень освоения компетенции	Пусть E – эллиптическая кривая над $\square$ с уравнением $Y^2 = X^3 + 3$, $P = (1, 2)$ – её точка. Вычислить координаты точки $3P$.

Оценка «хорошо» или повышенный уровень освоения компетенции	Вычислить дискриминант и j-инвариант кривой $C / \square$: $Y^2 = X^3 - 2$.
Оценка «отлично» или высокий уровень освоения компетенции	Определить, изоморфны ли над $\square$ эллиптические кривые E_1 и E_2 E_1: $Y^2 = X^3 - X$, E_2: $Y^2 = X^3 + 4X$;

Тема 2. Эллиптические кривые над полем рациональных чисел и над полями различных характеристик

	Задача
Оценка «удовлетворительно» или низкой уровень освоения компетенции	Пусть E – эллиптическая кривая над $\square_3$ с уравнением $Y^2 = X^3 + X + 2$, $P = (2, 0)$, $Q = (1, 1)$ – её точки. Вычислить координаты точки $P - Q$.
Оценка «хорошо» или повышенный уровень освоения компетенции	Для заданной кривой определить все точки конечного порядка. $C / \square$: $Y^2 = X^3 - 2$.
Оценка «отлично» или высокий уровень освоения компетенции	Для заданной кривой определить все точки конечного порядка. Определить также структуру группы, образованной этими точками. $C / \square$: $Y^2 = X^3 + 8$.

Тема 3. Эллиптические кривые над конечными полями. Подсчет числа точек на кривой.

	Задача
Оценка «удовлетворительно» или низкой уровень освоения компетенции	Пусть E – эллиптическая кривая над $\square_7$ с уравнением $Y^2 = X^3 + 5X + 4$. Подсчитать число точек $E(\square_7)$, используя квадратичный характер.
Оценка «хорошо» или повышенный уровень освоения компетенции	Пусть E – эллиптическая кривая над $\square_4$, имеющая уравнение $Y^2 = X^3 + 1$. Найти $E(\square_4)$.
Оценка «отлично» или высокий уровень освоения компетенции	Для эллиптической кривой E: $y^2 = x^3 + x + 7$ определенной над конечным полем $\square_{17}$ определить структуру группы $E(\square_{17})$

Типовые контрольные работы

Проверочная работа по теме

«Эллиптические кривые над конечными полями. Подсчет числа точек на кривой»

Вариант 1.

Задача 1. Для эллиптической кривой $E/\square$ с уравнением $y^2 = x^3 - 36x$ определить все точки конечного порядка. Определить также структуру группы, образованной этими точками.

Задача 2. Для эллиптической кривой E: $y^2 = x^3 + x + 7$ определенной над конечным полем $\square_{17}$ определить структуру группы $E(\square_{17})$

Задача 3. Для заданной эллиптической кривой над конечным полем $E/\square_3$ с уравнением $y^2 = = x^3 - x$ по методу Вейля вычислить число N_r рациональных точек

8.3. Перечень вопросов и заданий для промежуточной аттестации по дисциплине

1. Плоские аффинные алгебраические кривые.
2. Проективная плоскость. Плоские проективные алгебраические кривые.
3. Неособые алгебраические кривые. Касательные. Точки перегиба.
4. Эллиптические кривые над полем действительных чисел. Закон сложение точек.
5. Эллиптически кривые над полем рациональных чисел. Теорема Морделла.
6. Нормальная форма неособой кубической кривой. Эллиптические кривые над произвольным полем. Дискриминант и j-инвариант.
7. Изоморфизмы эллиптических кривых.
8. Классы изоморфизмов.
9. Групповой закон на множестве рациональных точек. Порядок точек.
10. Различные виды уравнений эллиптической кривой над конечным полем. Изоморфизмы эллиптических кривых.
11. Точки конечного порядка. Подгруппа кручения. Ранг группы точек.
12. Дзета-функция эллиптической кривой над конечным полем. Теорема Хассе-Вейля.
13. L-многочлен. Методы подсчёта числа рациональных точек эллиптической кривой.
14. Суперсингулярные эллиптические кривые.
15. Структура группы рациональных точек над конечным полем.
16. Тест на простоту, основанный на свойствах эллиптических кривых.
17. Алгоритм Ленстры разложения целых чисел на множители.
18. Криптосистемы с открытым ключом на эллиптических кривых. Вложение исходного текста в группу рациональных точек.
19. RSA-криптосистемы на эллиптических кривых. Шифрующая и дешифрующая функции.
20. Дискретный логарифм на эллиптической кривой.
21. Криптосистемы Massey-Omura и ElGamal на эллиптических кривых.
22. Методы генерации пары (E, B).
23. Эндоморфизм Фробениуса эллиптической кривой.
24. Многочлены деления
25. Группа n-кручения $E[n]$
26. Алгоритм Шуфа

8.4. Планируемые уровни сформированности компетенций обучающихся и критерии оценивания

Уровни	Содержательное описание уровня	Основные признаки выделения уровня (этапы формирования компетенции, критерии оценки сформированности)	Пятибалльная шкала (академическая) оценка	Двухбалльная шакала, зачет	БРС, % освоения (рейтинговая оценка)

Повышенный	Творческая деятельность	*Включает нижестоящий уровень.* Умение самостоятельно принимать решение, решать проблему/задачу теоретического и прикладного характера на основе изученных методов, приемов, технологий	отлично	зачтено	86-100
Базовый	Применение знаний и умений в более широких контекстах учебной и профессиональной деятельности, нежели по образцу с большей степени самостоятельности и инициативы	*Включает нижестоящий уровень.* Способность собирать, систематизировать, анализировать и грамотно использовать информацию из самостоятельно найденных теоретических источников и иллюстрировать ими теоретические положения или обосновывать практику применения	хорошо		71-85
Удовлетворительный (достаточный)	Репродуктивная деятельность	Изложение в пределах задач курса теоретически и практически контролируемого материала	удовлетворительно		55-70
Недостаточный	Отсутствие признаков удовлетворительного уровня		неудовлетворительно	не зачтено	Менее 55

9. Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины.

Основная литература

1. Алешников, С. И. Математические методы защиты информации [Электронный ресурс]: учеб. пособие/ С. И. Алешников, Ю. Ф. Болтнев ; Балт. федер. ун-т им. И. Канта. - Калининград: БФУ им. И. Канта, 2015 - 2015. - Ч. 4: Вычислительный практикум по эллиптическим кривым и криптографии на эллиптических кривых on-line, 60 с.. - Библиогр.: с. 58-59. - ISBN 978-5-9971-0389-7: Б.ц. Имеются экземпляры в отделах /There are copies in departments: ЭБС Кантиана(1)

Дополнительная литература

1. Болотов, А. А. Элементарное введение в эллиптическую криптографию. Протоколы криптографии на эллиптических кривых/ А. А. Болотов, С. Б. Гашков, А. Б. Фролов. - 2-е изд.. - М.: КомКнига, 2012. - 303 с. - (Защита информации). - Вариант загл.: Протоколы криптографии на эллиптических кривых. - Библиогр.: с. 264-268 (97 назв.). - Предм. указ.: с. 269-274. - ISBN 978-5-484-01291-6: 401.00, 401.00, 367.00, р. Имеются экземпляры в отделах /There are copies in departments: всего /all 27: УБ(26), ч.з.N3(1)

10. Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины (модуля).

- НЭБ Национальная электронная библиотека, диссертации и прочие издания
- eLIBRARY.RU Научная электронная библиотека, книги, статьи, тезисы докладов конференций
- Гребенников Электронная библиотека ИД журналы
- ЭБС Лань книги, журналы
- ЭБС Консультант студента
- ПРОСПЕКТ ЭБС
- ЭБС ZNANIUM.COM
- РГБ Информационное обслуживание по МБА
- БЕН РАН
- Электронно-библиотечная система (ЭБС) Кантитана (https://elib.kantiana.ru/)

11. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине.

Программное обеспечение обучения включает в себя:

- система электронного образовательного контента БФУ им. И. Канта – www.lms-3.kantiana.ru, обеспечивающую разработку и комплексное использование электронных образовательных ресурсов;
- серверное программное обеспечение, необходимое для функционирования сервера и связи с системой электронного обучения через Интернет;
- корпоративная платформа Microsoft Teams;
- установленное на рабочих местах студентов ПО: Microsoft Windows 7, Microsoft Office Standart 2010, антивирусное программное обеспечение Kaspersky Endpoint Security.
- специализированное ПО (при наличии): система компьютерной алгебры Sage, fpylll

12. Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине.

Для проведения занятий лекционного типа, практических и семинарских занятий используются специальные помещения (учебные аудитории), оборудованные техническими средствами обучения – мультимедийной проекционной техникой. Для проведения занятий лекционного типа используются наборы демонстрационного оборудования.

Для проведения лабораторных работ, (практических занятий – при необходимости) используются специальные помещения (учебные аудитории), оснащенные

специализированным лабораторным оборудованием: персональными компьютерами с возможностью выхода в интернет и с установленным программным обеспечением, заявленным в п.11.

Для проведения групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации используются специальные помещения (учебные аудитории), оборудованные специализированной мебелью (для обучающихся), меловой / маркерной доской.

Для организации самостоятельной работы обучающимся предоставляются помещения, оснащенные компьютерной техникой с возможностью подключения к сети «Интернет» и обеспечением доступа в электронную информационно-образовательную среду университета.

Для обучения инвалидов и лиц с ограниченными возможностями здоровья университетом могут быть представлены специализированные средства обучения, в том числе технические средства коллективного и индивидуального пользования.

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
федеральное государственное автономное образовательное учреждение высшего образования «Балтийский федеральный университет имени Иммануила Канта»
Институт физико-математических наук и информационных технологий

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

«Криптография на решётках»

Шифр: 10.05.01
Специальность: «Компьютерная безопасность»
Специализация: «Математические методы защиты информации»
Квалификация (степень) выпускника: специалист по защите информации

Калининград
2022

Лист согласования

Составитель: Киршанова Е.А., PhD., доцент.

Рабочая программа утверждена на заседании учебно-методического совета института физико-математических наук и информационных технологий

Протокол № 01/22 от «01» февраля 2022 г.

Председатель учебно-методического
совета института физико-
математических наук и информационных
технологий

Первый заместитель директора Шпилевой А. А
ИФМНиИТ, к. ф.-м. н., доцент

Ведущий менеджер Е.П.Ставицкая

Содержание

1.Наименование дисциплины: «Криптография на решётках».

Цель дисциплины: изучение новых парадигм конструкций пост-квантовых асимметрических механизмов (цифровой подписи, шифрования, обмена ключами); теоретические и практические навыки криптоанализа этих механизмов, в основе которых используются евклидовы решетки

2. Перечень планируемых результатов обучения по дисциплине, соотнесенных с планируемыми результатами освоения образовательной программы

Код компетенции	Результаты освоения образовательной программы (ИДК)	Результаты обучения по дисциплине
ОПК-8 Способность применять методы научных исследований при проведении разработок в области обеспечения безопасности компьютерных систем и сетей.	ОПК-8.1. Знает принципы работы с научной литературой, методы поиска научно-технической информации. ОПК-8.2. Способен осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических документов. ОПК-8.3. Обладает навыками решения профессиональных задач с широким использованием актуальной научно-технической литературы.	**Знать** базовый синтаксис языка Python для выполнения лабораторных работ по курсу. **Уметь** строить схему цифровой подписи на решетке и оценивать её криптографическую стойкость, строить схему шифрования на решетке и оценивать её криптографическую стойкость. **Владеть** навыками криптоанализа асимметричных протоколов, основанных на евклидовых решетках.
ОПК-10 Способность анализировать тенденции развития методов и средств криптографической защиты информации, использовать средства криптографической защиты информации при решении задач профессиональной деятельности	ОПК-10.1. Понимает целесообразность использования криптографических алгоритмов в современных программных комплексах. ОПК-10.2. Способен применять методы криптоанализа к конкретным криптографическим примитивам. ОПК-10.3. Владеет навыками реализации алгоритмов, в том числе криптографических, в современных программных комплексах.	**Знать** основные понятия дисциплины (решётка, минимумы решетки, задача нахождения короткого вектора, алгоритмы нахождения короткого вектора, алгоритмы редукции базиса, дуальная решетка, задачи «в среднем» (SIS, LWE), дискретное Гауссово распределение) и алгоритмы на решетках. **Уметь** находить короткий вектор решетки и, в общем, моделировать задачи на решетках используя готовые библиотеки (fpylll, Sage).

		Владеть методами криптоанализа, основанного на алгоритмах редукции базиса решетки.
ОПК-2.1 Способен разрабатывать алгоритмы, реализующие современные математические методы защиты информации.	ОПК-2.1.1. Знает алгоритмы, реализующие современные математические методы защиты информации. ОПК-2.1.2. Разрабатывает рекомендации и предложения по совершенствованию и повышению эффективности защиты информации. ОПК-2.1.3. Владеет методами отладки создаваемых средств защиты.	**Знать** принципы работы алгоритма редукции базиса, его асимптотический анализ, а также принципы построения схемы цифровой подписи и схемы шифрования на решетке, методы доказательства безопасности этих примитивов. **Уметь** строить основные ассиметричные криптографические примитивы, сложность которых основана на “задачах в среднем” на решетках **Владеть** навыками реализации алгоритмов, связанных с криптографией на решетках (генерация выборки, декодирование относительно решетки, редукция базиса), и их использования.

3. Место дисциплины в структуре образовательной программы

Дисциплина «Криптография на решётках» представляет собой дисциплину обязательной части блока дисциплин подготовки студентов.

4. Виды учебной работы по дисциплине.

Виды учебной работы по дисциплине зафиксированы учебным планом основной профессиональной образовательной программы по указанному направлению и профилю, выражаются в академических часах. Часы контактной работы и самостоятельной работы студента и часы, отводимые на процедуры контроля, могут различаться в учебных планах ОПОП по формам обучения. Объем контактной работы включает часы контактной аудиторной работы (лекции/практические занятия/ лабораторные работы), контактной внеаудиторной работы (контроль самостоятельной работы), часы контактной работы в период аттестации. Контактная работа, в том числе может проводиться посредством электронной информационно-образовательной среды университета с использованием ресурсов сети Интернет и дистанционных технологий

5. Содержание дисциплины, структурированное по темам (разделам)

Исходя из рамок, установленных учебным планом по трудоемкости и видам учебной работы по дисциплине, преподаватель самостоятельно выбирает тематику занятий по формам и количеству часов проведения контактной работы: лекции и иные учебные занятия, предусматривающие преимущественную передачу учебной информации преподавателем и (или) занятия семинарского типа (семинары, практические занятия, практикумы, лабораторные работы, коллоквиумы и иные аналогичные занятия), и (или) групповые консультации, и (или) индивидуальную работу обучающихся с преподавателем, в том числе индивидуальные консультации (по курсовым работам/проектам – при наличии курсовой работы/проекта по данной дисциплине в учебном плане). Рекомендуемая тематика занятий максимально полно реализуется в контактной работе со студентами очной формы обучения. В случае реализации образовательной программы в заочной / очно-заочной форме трудоемкость дисциплины сохраняется, однако объем учебного материала в значительной части осваивается студентами в форме самостоятельной работы. При этом требования к ожидаемым образовательным результатам студентов по данной дисциплине не зависят от формы реализации образовательной программы.

№	Наименование раздела	Содержание раздела
1	Введение.	Основные определения: евклидова решетка, определитель, минимумы решетки, построение решетки из кодов.
2	Теорема Минковского.	Формулировка теоремы, её доказательство и следствия. Вычисление минимума q-арной решетки. Теорема Минковского-Хлавки.
3	LLL алгоритм	QR-декомпозиция, HNF форма матрицы, редукция по размеру. Алгоритм LLL редукции, его анализ.
4	Алгоритмы для задачи SVP. BKZ алгоритм.	Алгоритм перечисления SVP. Блочная редукция Коркина-Золотарева. Алгоритм просеивания.
5	Задачи CVP и SVP	Определение “задач в худшем”. Определение задачи ближайшего вектора (CVP), кратчайшего вектора (SVP). Редукция от SVP к CVP.
6	Задачи BDD, approxSVP, uSVP.	Определение “задач в среднем”. Задача декодирования с ограниченным расстоянием (BDD), задача аппроксимации короткого вектора (approxSVP), задача уникального короткого вектора (uSVP). Их эквивалентность.
7	Гауссово распределение на решётке.	Дуальные решетки и преобразование Фурье. Определение Гауссового распределения на решетке. Формула сложения Пуассона. Алгоритм выборки в

		соответствии с Гауссовым распределением над целыми числами. Алгоритм Кляйна для Гауссовой выборки над решеткой. Анализ алгоритма.
8	Задача SIS, алгоритм цифровой подписи на решетках.	Определение задачи нахождения короткого целого решения (SIS). Редукция от approxSVP к SIS. Построение подписи GPV на решетке. Доказательство безопасности конструкции.
9	Задача LWE, метод шифрования.	Определения задачи обучения с ошибками (LWE). HNF форма LWE. Построение шифрования на LWE, анализ безопасности примитива. Квантовая редукция от задачи LWE к SIS.

6. Рекомендуемая тематика учебных занятий в форме контактной работы

Рекомендуемая тематика учебных занятий *лекционного* типа (предусматривающих преимущественную передачу учебной информации преподавателями):

№	Наименование раздела	Содержание раздела
1	Введение.	Лекция №1. Основные определения
2	Теорема Минковского.	Лекция № 2. Последовательные минимумы решетки
3	LLL алгоритм	Лекция № 3. QR-декомпозиция, HNF форма матрицы, редукция по размеру. Лекция № 4. Алгоритм LLL редукции.
4	Алгоритмы для задачи SVP. BKZ алгоритм.	Лекция № 5. Алгоритм перечисления SVP. BKZ редукция Лекция № 6. Алгоритм просеивания.
5	Задачи CVP и SVP	Лекция № 7. Определение “задач в худшем”. Определение задачи ближайшего вектора (CVP), кратчайшего вектора (SVP). Редукция от SVP к CVP. Лекция № 8. Сложность CVP
6	Задачи BDD, approxSVP, uSVP.	Лекция № 9. Редукции между “задачами в среднем”.
7	Гауссово распределение на решётке.	Лекция № 10. Дуальные решетки и преобразование Фурье. Определение Гауссового распределения на решетке. Формула сложения Пуассона. Лекция №11. Алгоритм выборки в соответствии с Гауссовым распределением над целыми числами. Лекция № 12. Алгоритм Кляйна для

		Гауссовой выборки над решеткой.
8	Задача SIS, алгоритм цифровой подписи на решетках.	Лекция № 13. SIS Редукция от approxSVP к SIS. Лекция №14. Построение подписи GPV на решетке.
9	Задача LWE, метод шифрования.	Лекция № 15. LWE. Построение шифрования на LWE, анализ безопасности примитива.

Рекомендуемая тематика *практических* занятий:

№ п/п	**Наименование Темы**	**Содержание темы**
1	Введение.	Примеры и контрпримеры решеток. Доказательство неоднозначности базиса решетки.
2	Теорема Минковского.	Доказательство теоремы Минковского-Хлавки
3	LLL алгоритм	Доказательство свойств QR-факторизации
4	Гауссово распределение на решётке.	Доказательства свойств Гауссовой функции. Гауссова функция на дуальной решетке. Доказательство формулы сложения Пуассона.
5	Задача SIS, алгоритм цифровой подписи на решетках.	Доказательство Leftover Hash Lemma.
6	Задача LWE, метод шифрования.	Доказательство сложности HNF формы LWE.

Рекомендуемый перечень тем *лабораторных* работ *(при наличии)*

№ п/п	Наименование раздела дисциплины	Тема лабораторной работы
1	Введение	Установка и использование библиотеки FPyLLL.
2	LLL алгоритм	Алгоритм Копперсмита нахождения малых корней многочлена. Реализация алгоритма в Sage.
3	Задачи CVP и SVP	Алгоритм факторизации Шнорра. Реализация алгоритма с помощью библиотек FPyLLL, G6K.
4	Задачи BDD, approxSVP, uSVP.	Алгоритм для задачи спрятанного числа (the hidden number problem)
5	Задача SIS, алгоритм цифровой подписи на решетках.	Атака на подписи GGH/NTRU

Требования к самостоятельной работе студентов

1. Работа с лекционным материалом, предусматривающая проработку конспекта лекций и учебной литературы, по всем лабораторным работам, описанным выше. Каждая лабораторная работа снабжена списком статей и выполняется индивидуально или в группе из не более 2х человек.

Руководствуясь положениями статьи 47 и статьи 48 Федерального закона от 29 декабря 2012 г. N 273-ФЗ «Об образовании в Российской Федерации» научно-педагогические работники и иные лица, привлекаемые университетом к реализации данной образовательной программы, пользуются предоставленными академическими правами и свободами в части свободы преподавания, свободы от вмешательства в профессиональную деятельность; свободы выбора и использования педагогически обоснованных форм, средств, методов обучения и воспитания; права на творческую инициативу, разработку и применение авторских программ и методов обучения и воспитания в пределах реализуемой образовательной программы и отдельной дисциплины.

Исходя из рамок, установленных учебным планом по трудоемкости и видам учебной работы по дисциплине, преподаватель самостоятельно выбирает тематику занятий по формам и количеству часов проведения контактной работы: лекции и иные учебные занятия, предусматривающие преимущественную передачу учебной информации преподавателем и (или) занятия семинарского типа (семинары, практические занятия, практикумы, лабораторные работы, коллоквиумы и иные аналогичные занятия), и (или) групповые консультации, и (или) индивидуальную работу обучающихся с преподавателем, в том числе индивидуальные консультации (по курсовым работам/проектам – при наличии курсовой работы/проекта по данной дисциплине в учебном плане).

Рекомендуемая тематика занятий максимально полно реализуется в контактной работе со студентами очной формы обучения. В случае реализации образовательной программы в заочной / очно-заочной форме трудоемкость дисциплины сохраняется, однако объем учебного материала в значительной части осваивается студентами в форме самостоятельной работы. При этом требования к ожидаемым образовательным результатам студентов по данной дисциплине не зависят от формы реализации образовательной программы.

7. Методические рекомендации по видам занятий

Лекционные занятия.

В ходе лекционных занятий обучающимся рекомендуется выполнять следующие действия. Вести конспектирование учебного материала. Обращать внимание на категории, формулировки, раскрывающие содержание тех или иных явлений и процессов, научные выводы и практические рекомендации по их применению. Задавать преподавателю уточняющие вопросы с целью уяснения теоретических положений, разрешения спорных ситуаций.

Желательно оставить в рабочих конспектах поля, на которых во внеаудиторное время можно сделать пометки из рекомендованной литературы, дополняющие материал прослушанной лекции, а также подчеркивающие особую важность тех или иных теоретических положений.

Практические и семинарские занятия.

На практических и семинарских занятиях в зависимости от темы занятия выполняется поиск информации по решению проблем, практические упражнения, контрольные работы, выработка индивидуальных или групповых решений, итоговое обсуждение с обменом знаниями, участие в круглых столах, разбор конкретных ситуаций, командная работа, представление портфолио и т.п.

Самостоятельная работа.

Самостоятельная работа осуществляется в виде изучения литературы, эмпирических данных по публикациям и конкретных ситуаций из практики, подготовке индивидуальных работ, работа с лекционным материалом, самостоятельное изучение

отдельных тем дисциплины; поиск и обзор литературы и электронных источников; чтение и изучение учебника и учебных пособий.

8. Фонд оценочных средств

8.1. Перечень компетенций с указанием этапов их формирования в процессе освоения образовательной программы в рамках учебной дисциплины

Основными этапами формирования указанных компетенций при изучении обучающимися дисциплины являются последовательное изучение содержательно связанных между собой тем учебных занятий. Изучение каждой темы предполагает овладение обучающимися необходимыми компетенциями. Результат аттестации обучающихся на различных этапах формирования компетенций показывает уровень освоения компетенций.

Контролируемые разделы (темы) дисциплины	Индекс контролируемой компетенции (или её части)	Оценочные средства по этапам формирования компетенций
		текущий контроль по дисциплине
Тема 1. Введение.	ОПК-2.1 ОПК-8	Решение задач
Тема 2. Теорема Минковского.	ОПК-2.1 ОПК-8	Решение задач
Тема 3. LLL алгоритм.	ОПК-8 ОПК-10 ОПК-2.1	Индивидуальная или групповая работа
Тема 4. Алгоритмы для задачи SVP. BKZ алгоритм.	ОПК-8 ОПК-10 ОПК-2.1	Индивидуальная или групповая работа
Тема 5. Задачи CVP и SVP	ОПК-8 ОПК-10 ОПК-2.1	Индивидуальная или групповая работа
Тема 6. Задачи BDD, approxSVP, uSVP	ОПК-8 ОПК-10 ОПК-2.1	Индивидуальная или групповая работа
Тема 7. Гауссово распределение на решётке.	ОПК-2.1 ОПК-8	Решение задач
Тема 8. Задача SIS, алгоритм цифровой подписи на решетках.	ОПК-8 ОПК-10 ОПК-2.1	Индивидуальная или групповая работа
Тема 9. Задача LWE, метод шифрования.	ОПК-8 ОПК-10 ОПК-2.1	Решение задач

8.2. Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений и навыков и (или) опыта деятельности процессе текущего контроля

Тема 1. Введение

Пример задачи:

Пример и контрпример решёток.

1. Покажите, что aZ + bZ – решётка для любых a, b ∈ Q
2. Покажите, что Z + 2Z не является решёткой

Тема 2. Теорема Минковского.

Задание. Теорема Минковского-Хлавки

Докажите, что с вероятностью $\geq 1 - 2^{-m}$ для $G \in \mathbb{Z}_q^{m \times n}$ выполняется

$$\lambda_1^\infty(L(G)) \geq \frac{1}{4} q^{1-n/m}.$$

Для этого

1. Зафиксируйте $B = \frac{1}{4} q^{1-n/m}$ и рассмотрите $\Pr_G[\lambda_1^\infty(L(G)) < B]$,
2. Покажите, что

$$\Pr_G[\lambda_1^\infty(L(G)) < B] \leq \sum_{s \in \mathbb{Z}_q^n} \sum_{\substack{y \in \mathbb{Z}^m \\ |y|_\infty < B}} \Pr[y = Gs \bmod q]$$

,

3. Покажите, что

$$\sum_{s \in \mathbb{Z}_q^n} \sum_{\substack{y \in \mathbb{Z}^m \\ |y|_\infty < B}} \Pr[y = Gs \bmod q] \begin{cases} = 0, & s = 0, \\ < 2^{-m}, & s \neq 0. \end{cases}$$

Тема 7. Гауссово распределение на решётке.

Задание. Гауссова функция.

Докажите, что $\rho = \hat{\rho}$ для $\rho(x) = e^{-\pi \|x\|}$. Подсказка: $\int_{-\infty}^{\infty} e^{-ax^2} dx = \sqrt{\frac{\pi}{a}}$ для $a > 0$.

Тема 8. Задача SIS, алгоритм цифровой подписи на решетках.

Задание. Leftover Hash Lemma для решеток.

Докажите, что $\Delta[(A, r^t A), (A, u)] \leq 2^{-\Omega(n)}$ для $A \leftarrow \mathcal{U}(\mathbb{Z}_q^{m \times n})$, $u \leftarrow \mathcal{U}(\mathbb{Z}_q^n)$, $r \leftarrow D_{\mathbb{Z}^m, \sigma}$, $m \geq n \log q$, $q-$простое.

1. Постройте изоморфизм $\mathbb{Z}_q^n \cong \mathbb{Z}^m / A^\perp$.

   Вывод: $D_{\mathbb{Z}^m, \sigma} \cdot A$ следует случайному равномерному распределению $\iff$ $D^t_{\mathbb{Z}^m, \sigma} \bmod A^\perp$ случайно равномерно в $\mathbb{Z}^m / A^\perp$.

2. Докажите, что $\Pr_{b \leftarrow D_{\mathbb{Z}^m, \sigma}}[b - \text{класс смежности в } A^\perp] \approx \frac{\rho_\sigma(A^\perp)}{\rho_\sigma(\mathbb{Z})}$ и, что эта величина независима от b. Для этого можете использовать зависимость $\eta_\varepsilon(A^\perp)$ от λ_1 дуальной решетки, а для λ_1 неравенство Минковского-Хлавки (см. Лекцию №2).

8.3. Перечень вопросов и заданий для промежуточной аттестации по дисциплине

1. Определение евклидовой решетки. Размерность, ранг решетки. Базис решетки.
2. Минимумы решетки. Минимум q-арной решетки.
3. Граница Минковского. Граница Минковского-Хлавки для q-арной решетки.
4. QR-факторизация. HNF-форма базиса.
5. LLL-редуцированный базис. Определение. Свойства.
6. Алгоритм LLL редукции.
7. Формулировка задачи SVP. Сложность задачи.
8. Алгоритм перечисления для задачи SVP. Сложность алгоритма.
9. Алгоритм блочной редукции Коркина-Золоторева. Зависимость фактора аппроксимации от времени работы.
10. Алгоритм просеивания для задачи SVP. Сложность алгоритма.
11. Задача нахождения ближайшего вектора (CVP). Редукция SVP к CVP.
12. Задача декодирования с ограниченным расстоянием (BDD). Редукция задачи аппроксимации короткого вектора к BDD.
13. Задача уникального короткого вектора (uSVP). Редукция от BDD к uSVP.
14. Понятие дуальной решетки. Редукция задачи uSVP к задачи аппроксимации короткого вектора.
15. Преобразование Фурье. Гауссова функция
16. Сглаживающий параметр. Гауссова выборка над Z. Алгоритм. Сложность.
17. Алгоритм Кляйна для Гауссовой выборки над произвольной решеткой.
18. Формулировка задачи SIS.
19. Сложность задачи SIS. Редукция от SIS к задаче аппроксимации короткого вектора.
20. Цифровая подпись на решетках. Конструкция. Парадигма доказательства.
21. Задача LWE. Связь LWE с решетками.
22. Схема шифрования на задаче LWE. Доказательство стойкости схемы.

8.4. Планируемые уровни сформированности компетенций обучающихся и критерии оценивания

Уровни	Содержательное описание уровня	Основные признаки выделения уровня (этапы формирования компетенции, критерии оценки сформированности)	Пятибалльная шкала (академическая) оценка	Двухбалльная шакала, зачет	БРС, % освоения (рейтинговая оценка)
Повышенный	Творческая деятельность	*Включает нижестоящий уровень.* Умение самостоятельно принимать решение, решать	отлично	зачтено	86-100

		проблему/задачу теоретического и прикладного характера на основе изученных методов, приемов, технологий			
Базовый	Применение знаний и умений в более широких контекстах учебной и профессиональной деятельности, нежели по образцу с большей степени самостоятельности и инициативы	*Включает нижестоящий уровень.* Способность собирать, систематизировать, анализировать и грамотно использовать информацию из самостоятельно найденных теоретических источников и иллюстрировать ими теоретические положения или обосновывать практику применения	хорошо		71-85
Удовлетворительный (достаточный)	Репродуктивная деятельность	Изложение в пределах задач курса теоретически и практически контролируемого материала	удовлетворительно		55-70
Недостаточный	Отсутствие признаков удовлетворительного уровня		неудовлетворительно	не зачтено	Менее 55

9. Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины.

Основная литература

1. Кнауб, Л. В. *Теоретико-численные методы в криптографии* [Электронный ресурс] : Учеб. пособие / Л. В. Кнауб, Е. А. Новиков, Ю. А. Шитов. - Красноярск : Сибирский федеральный университет, 2011. - 160 с. - ISBN 978-5-7638-2113-7. - Текст : электронный. - URL: https://znanium.com/catalog/product/441493

Дополнительная литература

1. Романьков, В. А. Введение в криптографию : курс лекций / В.А. Романьков. — 2-е изд., испр. и доп. — Москва : ФОРУМ : ИНФРА-М, 2021. — 240 с. — (Высшее образование: Бакалавриат). - ISBN 978-5-00091-493-9. - Текст : электронный. - URL: https://znanium.com/catalog/product/1514566
2. Ященко, В. В. *Введение в криптографию*: Учебное пособие / Ященко В.В., - 4-е изд. - Москва :МЦНМО, 2014. - 352 с.: ISBN 978-5-4439-2162-4. - Текст : электронный. - URL: https://znanium.com/catalog/product/958585

Интернет-ресурсы:

1. Лекции Проф. Др. Дамиена Штеле. ENS Lyon. Находятся в открытом доступе по адресу http://perso.ens-lyon.fr/damien.stehle/LBCF_course.html|

2. Лекции Проф. Др. Одеда Регева. NUY. Находятся в открытом доступе по адресу https://cims.nyu.edu/~regev/teaching/lattices_fall_2009/index.html

3. Лекции Проф. Др. Даниеле Мичанчио. Находятся в открытом доступе по адресу https://cseweb.ucsd.edu/classes/wi04/cse206a/

10. Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины (модуля).

- НЭБ Национальная электронная библиотека, диссертации и прочие издания
- eLIBRARY.RU Научная электронная библиотека, книги, статьи, тезисы докладов конференций
- Гребенников Электронная библиотека ИД журналы
- ЭБС Лань книги, журналы
- ЭБС Консультант студента
- ПРОСПЕКТ ЭБС
- ЭБС ZNANIUM.COM
- РГБ Информационное обслуживание по МБА
- БЕН РАН
- Электронно-библиотечная система (ЭБС) Кантитана (https://elib.kantiana.ru/)

11. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине.

Программное обеспечение обучения включает в себя:
- система электронного образовательного контента БФУ им. И. Канта – www.lms-3.kantiana.ru, обеспечивающую разработку и комплексное использование электронных образовательных ресурсов;
- серверное программное обеспечение, необходимое для функционирования сервера и связи с системой электронного обучения через Интернет;
- корпоративная платформа Microsoft Teams;
- установленное на рабочих местах студентов ПО: Microsoft Windows 7, Microsoft Office Standart 2010, антивирусное программное обеспечение Kaspersky Endpoint Security.
- специализированное ПО (при наличии): система компьютерной алгебры Sage, fpylll

12. Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине.

Для проведения занятий лекционного типа, практических и семинарских занятий используются специальные помещения (учебные аудитории), оборудованные техническими средствами обучения – мультимедийной проекционной техникой. Для проведения занятий лекционного типа используются наборы демонстрационного оборудования.

Для проведения лабораторных работ, (практических занятий – при необходимости) используются специальные помещения (учебные аудитории), оснащенные специализированным лабораторным оборудованием: персональными компьютерами с возможностью выхода в интернет и с установленным программным обеспечением, заявленным в п.11.

Для проведения групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации используются специальные помещения (учебные аудитории), оборудованные специализированной мебелью (для обучающихся), меловой / маркерной доской.

Для организации самостоятельной работы обучающимся предоставляются помещения, оснащенные компьютерной техникой с возможностью подключения к сети «Интернет» и обеспечением доступа в электронную информационно-образовательную среду университета.

Для обучения инвалидов и лиц с ограниченными возможностями здоровья университетом могут быть представлены специализированные средства обучения, в том числе технические средства коллективного и индивидуального пользования.

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
федеральное государственное автономное образовательное учреждение высшего образования «Балтийский федеральный университет имени Иммануила Канта»
Институт физико-математических наук и информационных технологий

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

«Основы построения защищенных компьютерных сетей»

Шифр: 10.05.01
Специальность: «Компьютерная безопасность»
Специализация: «Математические методы защиты информации»
Квалификация (степень) выпускника: Специалист по защите информации

Калининград
2022

Лист согласования

Составитель: Новоселов Семен Александрович, старший преподаватель.

Рабочая программа утверждена на заседании учебно-методического совета института физико-математических наук и информационных технологий

Протокол № 01/22 от «01» февраля 2022 г.

Председатель учебно-методического совета института физико-математических наук и информационных технологий

Первый заместитель директора ИФМНиИТ, к. ф.-м. н., доцент — Шпилевой А. А

Ведущий менеджер — Е.П.Ставицкая

Содержание

1.Наименование дисциплины: «Основы построения защищенных компьютерных сетей».

Целью освоения дисциплины является теоретическая и практическая подготовка специалистов к деятельности, связанной с построением защищенных сетевых автоматизированных систем, а также обучение принципам и методам защиты информации в компьютерных сетях.

Необходимость изучения дисциплины заключается в подготовке студентов для научной и практической деятельности в области обеспечения защиты компьютерных сетей от постоянно растущего числа угроз безопасности и хакерских атак.

Основные **задачи** изучения дисциплины:

- изучение типовых угроз безопасности в компьютерных сетях;
- изучение криптографических и программно-аппаратных методов обеспечения информационной безопасности в компьютерных сетях;
- приобретение навыков настройки и эксплуатации средств обеспечения безопасности в компьютерных сетях;
- овладение средствами и методами проектирования и построения защищенных сетевых автоматизированных систем;
- овладение средствами и методами выявления и нейтрализации попыток нарушения безопасности в компьютерных сетях.

2. Перечень планируемых результатов обучения по дисциплине, соотнесенных с планируемыми результатами освоения образовательной программы

Код компетенции	Результаты освоения образовательной программы (ИДК)	Результаты обучения по дисциплине
ОПК-9. Способен решать задачи профессиональной деятельности с учетом текущего состояния и тенденций развития методов защиты информации в операционных системах, компьютерных сетях и системах управления базами данных, а также методов и средств защиты информации от утечки по техническим каналам, сетей и систем передачи информации;	ОПК-9.1. Знает методы защиты информации в операционных системах, компьютерных сетях и системах управления базами данных, а также методы и средства защиты информации от утечки по техническим каналам, сетей и систем передачи информации. ОПК-9.2. Умеет решать задачи профессиональной деятельности с учетом текущего состояния и тенденций развития методов защиты информации в операционных системах, компьютерных сетях и системах управления базами данных, а также методов и средств защиты информации от утечки по техническим	**Знать** теоретические основы дисциплин защиты информации, основные угрозы безопасности сетей, средства и методы хранения и передачи аутентификационной информации, основные протоколы идентификации и аутентификации абонентов сети, защитные механизмы и средства обеспечения сетевой безопасности, средства и методы предотвращения и обнаружения вторжений. **Уметь** использовать полученные теоретические знания для решения конкретных прикладных задач, формулировать политику безопасности компьютерных сетей, уметь применять защищенные протоколы, межсетевые экраны и средства обнаружения вторжений для защиты информации в сетях, осуществлять меры противодействия нарушениям

	каналам, сетей и систем передачи информации. ОПК-9.3. Владеет навыками решения задач профессиональной деятельности с учетом текущего состояния и тенденций развития методов защиты информации в операционных системах, компьютерных сетях и системах управления базами данных, а также методов и средств защиты информации от утечки по техническим каналам, сетей и систем передачи информации.	сетевой безопасности с использованием различных программных и аппаратных средств защиты **Владеть** практическими навыками настройки политики безопасности основных операционных систем, а также локальных компьютерных сетей, построенных на их основе; навыками настройки межсетевых экранов, методиками анализа сетевого трафика, методиками анализа результатов работы средств обнаружения вторжений.
ОПК-16. Способен проводить мониторинг работоспособности и анализ эффективности средств защиты информации в компьютерных системах и сетях;	ОПК-16.1. Знает устройство, принципы функционирования, порядок настройки, мониторинга работоспособности и анализа эффективности средств защиты информации в компьютерных системах и сетях. ОПК-16.2. Умеет осуществлять мониторинг работоспособности и анализ эффективности средств защиты информации в компьютерных системах и сетях. ОПК-16.3. Владеет навыками мониторинга работоспособности и анализа эффективности средств защиты информации в компьютерных системах и сетях.	**Знать** механизмы реализации атак в сетях TCP/IP, современные методы выявления уязвимостей компьютерных сетей, основные современные отечественные и зарубежные стандарты в области компьютерной безопасности; знать средства и методы хранения и передачи аутентификационной информации, основные протоколы идентификации и аутентификации абонентов сети, защитные механизмы и средства обеспечения сетевой безопасности, средства и методы предотвращения и обнаружения вторжений **Уметь** проводить аудит безопасности компьютерных сетей, грамотно проводить анализ безопасности систем на соответствие стандартам, уметь выявлять уязвимости компьютерных систем и проводить их классификацию. **Владеть** практическими навыками и методиками, по оценке безопасности компьютерных сетей.

3. Место дисциплины в структуре образовательной программы

Дисциплина «Основы построения защищенных компьютерных сетей» представляет собой дисциплину базовой части Блока 1 Дисциплины (модули) подготовки студентов.

4. Виды учебной работы по дисциплине.

Виды учебной работы по дисциплине зафиксированы учебным планом основной профессиональной образовательной программы по указанному направлению и профилю, выражаются в академических часах. Часы контактной работы и самостоятельной работы студента и часы, отводимые на процедуры контроля, могут различаться в учебных планах ОПОП по формам обучения. Объем контактной работы включает часы контактной аудиторной работы (лекции/практические занятия/ лабораторные работы), контактной внеаудиторной работы (контроль самостоятельной работы), часы контактной работы в период аттестации. Контактная работа, в том числе может проводиться посредством электронной информационно-образовательной среды университета с использованием ресурсов сети Интернет и дистанционных технологий

5. Содержание дисциплины, структурированное по темам (разделам)

Исходя из рамок, установленных учебным планом по трудоемкости и видам учебной работы по дисциплине, преподаватель самостоятельно выбирает тематику занятий по формам и количеству часов проведения контактной работы: лекции и иные учебные занятия, предусматривающие преимущественную передачу учебной информации преподавателем и (или) занятия семинарского типа (семинары, практические занятия, практикумы, лабораторные работы, коллоквиумы и иные аналогичные занятия), и (или) групповые консультации, и (или) индивидуальную работу обучающихся с преподавателем, в том числе индивидуальные консультации (по курсовым работам/проектам – при наличии курсовой работы/проекта по данной дисциплине в учебном плане). Рекомендуемая тематика занятий максимально полно реализуется в контактной работе со студентами очной формы обучения. В случае реализации образовательной программы в заочной / очно-заочной форме трудоемкость дисциплины сохраняется, однако объем учебного материала в значительной части осваивается студентами в форме самостоятельной работы. При этом требования к ожидаемым образовательным результатам студентов по данной дисциплине не зависят от формы реализации образовательной программы.

№	Наименование раздела	Содержание раздела
1.1	Сетевые атаки	Стадии проведения сетевой атаки – сбор информации, определение топологии сети, идентификация узлов, сканирование портов, реализация атаки, завершение. Классификации сетевых угроз, уязвимостей и атак. Удаленные и локальные атаки. Эскалация привилегий. Атаки на реализации сетевых протоколов, отдельные узлы и службы. Основные механизмы проведения сетевых атак на различных уровнях модели ISO/OSI.
1.2	Механизмы реализации атак в сетях TCP/IP	Удаленное определение версии ОС с использованием особенностей реализации стека протоколов TCP/IP. Использование баннеров для определения версии ОС. Методы сбора информации с

		использованием протокола ICMP. Сетевой сканер nmap. Методы сканирования портов - TCP ACK, NULL, FIN и Xmas сканирования. Пассивное прослушивание. Фрагментация данных. Подделка IP адреса. Подмена доменных имен
1.3	Примеры сетевых атак в сетях TCP/IP. Технические меры защиты от сетевых атак	Принуждение к ускоренной передаче. Атаки, направленные на отказ в обслуживании. Перехват сессии TCP/IP. Уязвимость в библиотеке OpenSSL при обработке пакетов расширения Heartbeat (Heartbleed – CVE-2014-0160). Уязвимость в Bash при обработке переменных окружения (Shellshock – CVE-2014-6271). Изменение конфигурации и состояния хостов. Недостатки протоколов семейства TCP/IP с точки зрения обеспечения безопасности информации. Технические меры защиты от сетевых атак.
1.4	Выявление сетевых атак путем анализа трафика	Сетевой сниффер WireShark. Пользовательский интерфейс программы. Фильтр отображения пакетов. Поиск кадров. Выделение ключевых кадров. Сохранение данных захвата. Анализ протоколов Ethernet и ARP. Анализ протоколов ICMP и IP. Анализ протокола TCP. Исследование сетевой топологии. Обнаружение доступных сетевых служб. Выявление уязвимых мест атакуемой системы. Выявление атаки на протокол SMB.
2.1	Криптографические протоколы обеспечения безопасности	Протоколы аутентификации на прикладном уровне. Протокол Kerberos. Протоколы аутентификации на транспортном уровне. Протокол SSL/TLS. Достоинства и недостатки аутентификации на различных уровнях модели ISO/OSI.
2.2	Защита виртуальных частных сетей (VPN)	Назначение, основные возможности, принципы функционирования и варианты реализации VPN. Организация туннелирования на различных

		уровнях модели ISO/OSI. Достоинства и недостатки применения VPN. Протокол IPSEC. Протоколы AH и ESP. Особенности работы протокола IPSEC в туннельном и транспортном режимах. Протокол управления ключами ISAKMP/Oakley. Использование протокола L2TP для организации виртуальных частных сетей.
3.1	Средства и методы обеспечения целостности и конфиденциальности	Средства защиты от несанкционированного доступа. Мандатное управление доступом. Избирательное управление доступом. Управление доступом на основе ролей. Журнализация. Системы резервного копирования. Система проверки целостности TripWire. Электронная цифровая подпись. Удостоверяющие центры.
3.2	Средства защиты локальных сетей при подключении к Интернет.	Межсетевые экраны (МЭ). Место и роль МЭ в обеспечении сетевой безопасности. Классификация МЭ. Требования к МЭ. Основные возможности и схемы развертывания МЭ. Достоинства и недостатки МЭ. Построение правил фильтрации. Методы сетевой трансляции адресов (NAT). Шлюзы уровня приложений. Реализация сетевой политики безопасности с использованием МЭ. Методы обхода межсетевых экранов.
3.3	Защита серверов и рабочих станций. Средства и методы предотвращения и обнаружения вторжений.	Системы обнаружения вторжений (СОВ). Назначение и возможности средств обнаружения вторжений на хосты, протоколы и сетевые службы. Место и роль средств обнаружения вторжений в общей системе обеспечения сетевой безопасности. Классификация СОВ. Выявление атак на основе сигнатур атак и выявления аномалий. Система обнаружения вторжений Snort.

		Аудит прикладных служб. Средства обнаружения уязвимостей сетевых служб. Сетевые сканеры XSpider и Nessus/OpenVAS.

6. Рекомендуемая тематика учебных занятий в форме контактной работы

Рекомендуемая тематика учебных занятий *лекционного* типа (предусматривающих преимущественную передачу учебной информации преподавателями):

№	Наименование раздела	Темы лекций
1.1	Сетевые атаки	Лекция 1. Введение. Стадии проведения сетевой атаки. Классификации сетевых угроз, уязвимостей и атак. Удаленные и локальные атаки. Эскалация привилегий. Лекция 2. Атаки на реализации сетевых протоколов, отдельные узлы и службы. Основные механизмы проведения сетевых атак на различных уровнях модели ISO/OSI. Лекция 3. Базовые сетевые протоколы и их безопасность: TCP/IP, HTTP(S)
1.2	Механизмы реализации атак в сетях TCP/IP	Лекция 4. Сетевое сканирование. Сканер nmap. Пассивное прослушивание. Фрагментация данных. Подделка IP адреса. Подмена доменных имен
1.3	Примеры сетевых атак в сетях TCP/IP. Технические меры защиты от сетевых атак	Лекция 5. Принуждение к ускоренной передаче. Атаки, направленные на отказ в обслуживании. Перехват сессии TCP/IP. Лекция 6. Уязвимость в библиотеке OpenSSL при обработке пакетов расширения Heartbeat (Heartbleed – CVE-2014-0160). Лекция 7. Уязвимость в Bash при обработке переменных окружения (Shellshock – CVE-2014-6271). Лекция 8. Недостатки протоколов семейства TCP/IP с точки зрения обеспечения безопасности информации. Технические меры защиты от сетевых атак.
1.4	Выявление сетевых атак путем анализа трафика	Лекция 9. Сетевой сниффер WireShark. Лекция 10. Анализ протоколов Ethernet и ARP. Анализ протоколов ICMP и IP. Анализ протокола TCP. Лекция 11. Выявление сетевых атак.
2.1	Криптографические протоколы обеспечения безопасности	Лекция 12. Достоинства и недостатки аутентификации на различных уровнях модели ISO/OSI. Лекция 13. Протоколы аутентификации на прикладном уровне. Протокол Kerberos. Лекция 14. Протоколы аутентификации на транспортном уровне. Протокол SSL/TLS.

2.2	Защита виртуальных частных сетей (VPN)	Лекция 15. Назначение, основные возможности, принципы функционирования и варианты реализации VPN. Организация туннелирования на различных уровнях модели ISO/OSI. Достоинства и недостатки применения VPN. Лекция 16. Протокол IPSEC. Протоколы AH и ESP. Особенности работы протокола IPSEC в туннельном и транспортном режимах. Лекция 17. Протокол управления ключами ISAKMP/Oakley. Лекция 18. Использование протокола L2TP для организации виртуальных частных сетей.
3.1	Средства и методы обеспечения целостности и конфиденциальности	Лекция 19. Средства защиты от несанкционированного доступа. Мандатное управление доступом. Избирательное управление доступом. Управление доступом на основе ролей. Лекция 20. Журнализация. Системы резервного копирования. Лекция 21. Система проверки целостности TripWire. Лекция 22. Электронная цифровая подпись.
3.2	Средства защиты локальных сетей при подключении к Интернет.	Лекция 23. Межсетевые экраны (МЭ). Построение правил фильтрации. Лекция 24. Методы сетевой трансляции адресов (NAT). Шлюзы уровня приложений. Лекция 25. Методы обхода межсетевых экранов.
3.3	Защита серверов и рабочих станций. Средства и методы предотвращения и обнаружения вторжений.	Лекция 26. Системы обнаружения вторжений (СОВ). Выявление атак на основе сигнатур атак и выявления аномалий. Система обнаружения вторжений Snort. Лекция 27. Аудит прикладных служб. Сетевые сканеры XSpider и Nessus/OpenVAS.

Рекомендуемая тематика *практических* занятий:

1. Механизмы реализации атак в сетях TCP/IP.
2. Примеры сетевых атак в сетях TCP/IP. Технические меры защиты от сетевых атак.
3. Выявление сетевых атак путем анализа трафика.
4. Защита виртуальных частных сетей (VPN). Развертывание VPN на основе OpenVPN.
5. Организация туннелей с использованием ssh.
6. Настройка и использование прокси-сервера SQUID.
7. Средства и методы обеспечения целостности и конфиденциальности
8. Межсетевые экраны. Настройка и использование встроенного пакетного фильтра ОС Linux iptables.
9. Использование и настройка средства обнаружения вторжений Snort.

Требования к самостоятельной работе студентов

1. Работа с лекционным материалом, предусматривающая проработку конспекта лекций и учебной литературы, по всем темам из п. 6 настоящей рабочей программы.

2. Выполнение домашнего задания, предусматривающего решение задач, выполнение упражнений, выдаваемых на практических занятиях, по всем темам из п. 6 настоящей рабочей программы.

Руководствуясь положениями статьи 47 и статьи 48 Федерального закона от 29 декабря 2012 г. N 273-ФЗ «Об образовании в Российской Федерации» научно-педагогические работники и иные лица, привлекаемые университетом к реализации данной образовательной программы, пользуются предоставленными академическими правами и свободами в части свободы преподавания, свободы от вмешательства в профессиональную деятельность; свободы выбора и использования педагогически обоснованных форм, средств, методов обучения и воспитания; права на творческую инициативу, разработку и применение авторских программ и методов обучения и воспитания в пределах реализуемой образовательной программы и отдельной дисциплины.

Исходя из рамок, установленных учебным планом по трудоемкости и видам учебной работы по дисциплине, преподаватель самостоятельно выбирает тематику занятий по формам и количеству часов проведения контактной работы: лекции и иные учебные занятия, предусматривающие преимущественную передачу учебной информации преподавателем и (или) занятия семинарского типа (семинары, практические занятия, практикумы, лабораторные работы, коллоквиумы и иные аналогичные занятия), и (или) групповые консультации, и (или) индивидуальную работу обучающихся с преподавателем, в том числе индивидуальные консультации (по курсовым работам/проектам – при наличии курсовой работы/проекта по данной дисциплине в учебном плане).

Рекомендуемая тематика занятий максимально полно реализуется в контактной работе со студентами очной формы обучения. В случае реализации образовательной программы в заочной / очно-заочной форме трудоемкость дисциплины сохраняется, однако объем учебного материала в значительной части осваивается студентами в форме самостоятельной работы. При этом требования к ожидаемым образовательным результатам студентов по данной дисциплине не зависят от формы реализации образовательной программы.

7. Методические рекомендации по видам занятий

Лекционные занятия.

В ходе лекционных занятий обучающимся рекомендуется выполнять следующие действия. Вести конспектирование учебного материала. Обращать внимание на категории, формулировки, раскрывающие содержание тех или иных явлений и процессов, научные выводы и практические рекомендации по их применению. Задавать преподавателю уточняющие вопросы с целью уяснения теоретических положений, разрешения спорных ситуаций.

Желательно оставить в рабочих конспектах поля, на которых во внеаудиторное время можно сделать пометки из рекомендованной литературы, дополняющие материал прослушанной лекции, а также подчеркивающие особую важность тех или иных теоретических положений.

Практические и семинарские занятия.

На практических и семинарских занятиях в зависимости от темы занятия выполняется поиск информации по решению проблем, практические упражнения, контрольные работы, выработка индивидуальных или групповых решений, итоговое обсуждение с обменом знаниями, участие в круглых столах, разбор конкретных ситуаций, командная работа, представление портфолио и т.п.

Самостоятельная работа.

Самостоятельная работа осуществляется в виде изучения литературы, эмпирических данных по публикациям и конкретных ситуаций из практики, подготовке индивидуальных работ, работа с лекционным материалом, самостоятельное изучение отдельных тем дисциплины; поиск и обзор литературы и электронных источников; чтение и изучение учебника и учебных пособий.

8. Фонд оценочных средств

8.1. Перечень компетенций с указанием этапов их формирования в процессе освоения образовательной программы в рамках учебной дисциплины

Основными этапами формирования указанных компетенций при изучении обучающимися дисциплины являются последовательное изучение содержательно связанных между собой тем учебных занятий. Изучение каждой темы предполагает овладение обучающимися необходимыми компетенциями. Результат аттестации обучающихся на различных этапах формирования компетенций показывает уровень освоения компетенций.

Контролируемые разделы (темы) дисциплины	Индекс контроли-руемой компетенции (или её части)	Оценочные средства по этапам формирования компетенций
		текущий контроль по дисциплине
1.1. Сетевые атаки	ОПК-9 ОПК-16	Решение задач
1.2 Механизмы реализации атак в сетях TCP/IP	ОПК-9 ОПК-16	Решение задач
1.3. Примеры сетевых атак в сетях TCP/IP. Технические меры защиты от сетевых атак	ОПК-9 ОПК-16	Решение задач. Реферат или групповое задание
1.4. Выявление сетевых атак путем анализа трафика	ОПК-9 ОПК-16	Решение задач. Контрольная работа
2.1. Криптографические протоколы обеспечения безопасности	ОПК-9	Решение задач
2.2. Защита виртуальных частных сетей (VPN)	ОПК-9	Решение задач
3.1. Средства и методы обеспечения целостности и конфиденциальности	ОПК-9 ОПК-16	Решение задач
3.2. Средства защиты локальных сетей при подключении к Интернет.	ОПК-9 ОПК-16	Решение задач
3.3. Защита серверов и рабочих станций. Средства и методы предотвращения и обнаружения вторжений.	ОПК-9 ОПК-16	Решение задач. Контрольная работа

8.2. Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений и навыков и (или) опыта деятельности процессе текущего контроля

Типовые контрольные задания:

По теме «Выявление сетевых атак путем анализа трафика»:

Вариант 1

Собрать сетевой трафик в сети kantiana в течение 10 минут.

1. Отфильтровать трафик по протоколам TCP/IP, ARP, SMTP, HTTP, DNS
2. Составить список активных хостов по данным ARP-протокола
3. Определить какие хосты являются рабочими станциями, а какие серверами
4. Определить наличие DNS и HTTP серверов в локальной сети
5. По данным SSDP-протокола определить наличие и тип устройств в сети (принтеров, сканеров и т.п.)

По теме «Защита серверов и рабочих станций. Средства и методы предотвращения и обнаружения вторжений»:

Вариант 1

1. Запустите на учебной машине с Linux один из web-серверов (nginx, apache и т.п.)
2. Просканируйте защищаемую систему с помощью одного из web-сканеров, например, nikto.
3. Детектирует ли Snort использование таких сканеров?
4. Можно ли подобрать такие настройки сканера, что Snort не детектирует его?

Типовые задания практических работ:

1. Составить правила к iptables для блокировки доступа к сайту www.example.com
2. Составьте правило к Snort для детектирования доступа к сайту www.example.com
3. Составьте правило к Snort для детектирования атаки Shellshock (CVE-2014-6271).
4. С помощью сниффера выявить наличие сетевого сканера nmap при проведении сканирования методами TCP SYN и TCP Xmas.

Образцы выполнения некоторых типов заданий

Задача № 1. Написать сниффер для перехвата и вывода на консоль cookies, относящихся к сайту example.com.

Решение

```
require 'pcaprub' # используем библиотеку pcaprub

# запускаем прослушивание mon0

capture = PCAPRUB::Pcap.open_live('mon0', 65535, true, 0)
#capture.setfilter('tcp')



cookies = []
```

```
while true
  #puts(capture.stats())
  pkt = capture.next() # считываем пакет
  if pkt && pkt =~ /Host:.*example\.com\r\n/
    puts pkt
    m = pkt.match /Cookie:(.*)\r\n/
    if m && !cookies.include?(m[1])
      p m[1]
      cookies.push m[1]
    end
  end
end
```

Задача № 2. Настроить iptables для реализации следующей политики безопасности хоста:

1. Всем разрешен доступ к веб-серверу.
2. Доступ к ssh разрешен только с адреса 192.168.1.6
3. Все остальные входящие соединения запрещены.

Решение

```
iptables -A INPUT -p tcp -s 192.168.1.6 --dport=22 -j ACCEPT
iptables -A INPUT -p tcp --dport=80 -j ACCEPT
iptables -A INPUT -j DROP
```

Задача № 3. Составить правило Snort для детектирования попытки доступа к директори «/dir» веб-сервера.

Решение

```
alert tcp $EXTERNAL_NET any -> $HTTP_SERVERS $HTTP_PORTS (
   msg:"WEB-MISC /dir";
   flow:to_server,established;
   uricontent:"/dir";
   nocase;
   classtype:attempted-recon;
```

)

Типовые задания для проектов и рефератов:

1. Методы определения сетевых снифферов в локальной сети
2. Программное обеспечение для анализа защищенности веб серверов
3. Возможности сканера безопасности Nessus
4. Создание единого пространства безопасности на основе ActiveDirectory
5. Принцип внедрения и методы борьбы с руткитами
6. Методики проведения аудита информационной безопасности
7. Использование DNS для обнаружения сетевых узлов
8. Исследование криптографической стойкости паролей
9. Модели информационной безопасности
10. Анализ выбранных уязвимостей из базы CVE/NVD.
11. Уязвимости сайтов, ведущие к раскрытию исходного кода.
12. Исследование раскрытия данных процесса в браузере Firefox (CVE-2014-1580).
13. Исследование некорректной обработки BMP-изображений в браузере Firefox (CVE-2014-8637).
14. Исследование уязвимости в веб-сервере Nginx 1.3.9-1.4.0 (CVE-2013-2028).
15. Исследование сети Интернет с помощью сканера Nmap. Настройка Nmap для массового сканирования целей.
16. Определение версии веб-сервера по особенностям реализации HTTP-протокола.

8.3. Перечень вопросов и заданий для промежуточной аттестации по дисциплине

Вопросы для промежуточного контроля (зачета)

1. Стадии проведения сетевой атаки
2. Классификация сетевых угроз и уязвимостей
3. Основные механизмы проведения сетевых атак
4. Способы удаленного определения версии ОС
5. Методы сбора информации с использованием протокола ICMP
6. Методы сканирования портов
7. Перечислить возможности сетевых снифферов
8. Протоколы аутентификации на прикладном уровне
9. Протоколы аутентификации на транспортном уровне
10. Достоинства и недостатки аутентификации на различных уровнях модели ISO/OSI
11. Назначение, основные возможности, принципы функционирования и варианты реализации VPN
12. Организация туннелирования на различных уровнях модели ISO/OSI
13. Достоинства и недостатки применения VPN
14. Особенности работы протокола IPSEC в туннельном и транспортном режимах
15. Протокол управления ключами ISAKMP/Oakley
16. Использование протокола L2TP для организации виртуальных частных сетей.
17. Средства защиты от несанкционированного доступа
18. Назначение и основные возможности систем резервного копирования
19. Назначение и принцип работы электронной цифровой подписи
20. Принцип работы систем проверки целостности данных

21. Роль межсетевых экранов в обеспечении сетевой безопасности
22. Классификация межсетевых экранов
23. Назначение метода сетевой трансляции адресов
24. Возможности и назначение шлюзов уровня приложений
25. Реализация сетевой политики безопасности с использованием межсетевых экранов
26. Назначение и возможности систем обнаружения вторжений
27. Классификация систем обнаружения вторжений
28. Назначение и возможности сетевых сканеров безопасности

8.4. Планируемые уровни сформированности компетенций обучающихся и критерии оценивания

Уровни	Содержательное описание уровня	Основные признаки выделения уровня (этапы формирования компетенции, критерии оценки сформированности)	Пятибалльная шкала (академическая) оценка	Двухбалльная шакала, зачет	БРС, % освоения (рейтинговая оценка)
Повышенный	Творческая деятельность	*Включает нижестоящий уровень.* Умение самостоятельно принимать решение, решать проблему/задачу теоретического и прикладного характера на основе изученных методов, приемов, технологий	отлично	зачтено	86-100
Базовый	Применение знаний и умений в более широких контекстах учебной и профессиональной деятельности, нежели по образцу с большей степени самостоятельности и инициативы	*Включает нижестоящий уровень.* Способность собирать, систематизировать, анализировать и грамотно использовать информацию из самостоятельно найденных теоретических источников и иллюстрировать ими теоретические положения или обосновывать практику применения	хорошо		71-85
Удовлетворительный (достаточный)	Репродуктивная деятельность	Изложение в пределах задач курса теоретически и практически	удовлетворительно		55-70

		контролируемого материала			
Недостаточный	Отсутствие признаков удовлетворительного уровня		неудовлетворительно	не зачтено	Менее 55

9. Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины.

Основная литература

1. Шаньгин, В. Ф. Комплексная защита информации в корпоративных системах : учебное пособие / В. Ф. Шаньгин. — Москва : ФОРУМ : ИНФРА-М, 2020. — 592 с. - ISBN 978-5-8199-0730-6. - Текст : электронный. - URL: https://znanium.com/catalog/product/1093695 **(online)**
2. Шаньгин, В. Ф. Информационная безопасность компьютерных систем и сетей : учебное пособие / В.Ф. Шаньгин. — Москва : ФОРУМ : ИНФРА-М, 2020. — 416 с. - ISBN 978-5-8199-0754-2. - Текст : электронный. - URL: https://znanium.com/catalog/product/1093657 **(online)**

Дополнительная литература

1. Бирюков, А. А. Информационная безопасность: защита и нападение / А.А. Бирюков. - 2-е изд., перераб. и доп. - Москва : ДМК Пресс, 2017. - 434 с. - ISBN 978-5-97060-435-9. - Текст : электронный. - URL: https://znanium.com/catalog/product/1028060 **(online)**
2. Шелухин, О. И. Обнаружение вторжений в компьютерные сети (сетевые аномалии): Учебное пособие для вузов / О.И. Шелухин, Д.Ж. Сакалема, А.С. Филинова. - Москва : Гор. линия-Телеком, 2013. - 220 с.: ил.; . ISBN 978-5-9912-0323-4, 500 экз. - Текст : электронный. - URL: https://znanium.com/catalog/product/421968 **(online)**
3. Платонов, В.В. Программно-аппаратные средства обеспечения информационной безопасности вычислительных сетей/В.В. Платонов. 2-е изд. – М: Издательский центр «Академия», 2014. – 336 с. **(10 экз.)**

10. Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины (модуля).

- НЭБ Национальная электронная библиотека, диссертации и прочие издания
- eLIBRARY.RU Научная электронная библиотека, книги, статьи, тезисы докладов конференций
- Гребенников Электронная библиотека ИД журналы
- ЭБС Лань книги, журналы
- ЭБС Консультант студента
- ПРОСПЕКТ ЭБС
- ЭБС ZNANIUM.COM
- РГБ Информационное обслуживание по МБА
- БЕН РАН
- Электронно-библиотечная система (ЭБС) Кантитана (https://elib.kantiana.ru/)
- База уязвимостей CVE (https://cve.mitre.org).
- База уязвимостей NVD (https://nvd.nist.gov).
- База уязвимостей и эксплойтов (www.exploit-db.com).

– Курс по системе Metasploit от Offensive Security (https://www.offensive-security.com/metasploit-unleashed/)

11. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине.

Программное обеспечение обучения включает в себя:

- система электронного образовательного контента БФУ им. И. Канта – www.lms-3.kantiana.ru, обеспечивающую разработку и комплексное использование электронных образовательных ресурсов;
- серверное программное обеспечение, необходимое для функционирования сервера и связи с системой электронного обучения через Интернет;
- корпоративная платформа Microsoft Teams;
- установленное на рабочих местах студентов ПО: Microsoft Windows 7-11.
- специализированное ПО:
    - Kali Linux (Свободное ПО, лицензия GPL).
    - Nmap (Свободное ПО, лицензия GPL).
    - VirtualBox (Свободное ПО, лицензия GPL).
    - Wireshark (Свободное ПО, лицензия GPL).
    - OpenVAS (Свободное ПО, лицензия GPL)
    - Metasploit Framework (Свободное ПО, лицензия BSD).

12. Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине.

Для проведения занятий лекционного типа, практических и семинарских занятий используются специальные помещения (учебные аудитории), оборудованные техническими средствами обучения – мультимедийной проекционной техникой. Для проведения занятий лекционного типа используются наборы демонстрационного оборудования.

Для проведения лабораторных работ, (практических занятий – при необходимости) используются специальные помещения (учебные аудитории), оснащенные специализированным лабораторным оборудованием: персональными компьютерами с возможностью выхода в интернет и с установленным программным обеспечением, заявленным в п.11.

Для проведения групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации используются специальные помещения (учебные аудитории), оборудованные специализированной мебелью (для обучающихся), меловой / маркерной доской.

Для организации самостоятельной работы обучающимся предоставляются помещения, оснащенные компьютерной техникой с возможностью подключения к сети «Интернет» и обеспечением доступа в электронную информационно-образовательную среду университета.

Для обучения инвалидов и лиц с ограниченными возможностями здоровья университетом могут быть представлены специализированные средства обучения, в том числе технические средства коллективного и индивидуального пользования.

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ
федеральное государственное автономное образовательное учреждение высшего образования «Балтийский федеральный университет имени Иммануила Канта»

Институт физико-математических наук и информационных технологий

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

«Защита программ и данных»

Шифр: 10.05.01
Специальность: «Компьютерная безопасность»
Специализация: «Математические методы защиты информации»
Квалификация (степень) выпускника: специалист по защите информации

Калининград
2022 г.

ЛИСТ СОГЛАСОВАНИЯ

Составитель: Олефиренко Денис Олегович, ассистент Института физико-математических наук и информационных технологий.

Рабочая программа утверждена на заседании учебно-методического совета института физико-математических наук и информационных технологий
Протокол № 01/22 от «01» февраля 2022 г.

Председатель учебно-методического
совета института физико-
математических наук и информационных
технологий
Первый заместитель директора Шпилевой А. А
ИФМНиИТ, к. ф.-м. н., доцент

Ведущий менеджер Е.П.Ставицкая

СОДЕРЖАНИЕ

1. Наименование дисциплины: «Защита программ и данных»

Целью изучения дисциплины *«Защита программ и данных»* является получение обучающимися глубоких теоретических и практических знаний об угрозах со стороны современного программного обеспечения и способах защиты от них, формирование навыков по использованию различных программно-аппаратных средств для противодействия этим угрозам, а также развитие умения анализировать исполняемый код программы на предмет наличия в ней недекларированных возможностей.

Необходимость изучения дисциплины объясняется большой востребованностью на современном рынке труда специалистов по защите прикладного программного обеспечения и автоматизированных систем обработки данных от угроз информационной безопасности.

Основные **задачи** изучения дисциплины:

- формирование глубоких теоретических знаний об угрозах безопасности со стороны программного обеспечения и методах противодействия им;
- развитие практических навыков по анализу внутренней структуры программного продукта при отсутствии исходного кода, а также по защите программного продукта от подобного анализа.

2. Перечень планируемых результатов обучения по дисциплине, соотнесенных с планируемыми результатами освоения образовательной программы

В результате освоения ООП обучающийся должен овладеть следующими результатами обучения по дисциплине.

Код компетенции	Результаты освоения образовательной программы (ИДК)	Результаты обучения по дисциплине
ОПК-13. Способен разрабатывать компоненты программных и программно-аппаратных средств защиты информации в компьютерных системах и проводить анализ их безопасности;	ОПК-13.1. Знает принципы функционирования программных и программно-аппаратных средств защиты информации в компьютерных системах, принципы и методы разработки их компонент, методики анализа их безопасности. ОПК-13.2. Способен разрабатывать компоненты программных и программно-аппаратных средств защиты информации в компьютерных системах. ОПК-13.3. Способен проводить анализ безопасности компонент программных и программно-аппаратных средств защиты	Студент, изучивший курс *«Защита программ и данных»*, должен: **З Н А Т Ь :** • базовые принципы, лежащие в основе наиболее распространённых формальных моделей политик безопасности, политик управления доступом и информационными потоками в компьютерных системах; • инструменты в операционных системах, посредством которых в данной системе можно реализовать ту или иную политику безопасности; **У М Е Т Ь :** • строить теоретические модели политик безопасности, политик управления доступом и информационными потоками в компьютерных системах с учётом различных факторов; **В Л А Д Е Т Ь :**

	информации в компьютерных системах.	• навыками по реализации формальных моделей безопасности на практике.

3. Место дисциплины в структуре ООП ВО

Курс «Защита программ и данных» относится к обязательной части блока «Дисциплины (модули)» и входит в модуль №8: «Программно-аппаратные средства обеспечения информационной безопасности».

4. Виды учебной работы по дисциплине

Виды учебной работы по дисциплине зафиксированы учебным планом основной профессиональной образовательной программы по указанному направлению и профилю, выражаются в академических часах. Часы контактной работы и самостоятельной работы студента и часы, отводимые на процедуры контроля, могут различаться в учебных планах ОПОП по формам обучения. Объем контактной работы включает часы контактной аудиторной работы (лекции/практические занятия/ лабораторные работы), контактной внеаудиторной работы (контроль самостоятельной работы), часы контактной работы в период аттестации. Контактная работа, в том числе может проводиться посредством электронной информационно-образовательной среды университета с использованием ресурсов сети Интернет и дистанционных технологий

5. Содержание дисциплины, структурированное по темам (разделам)

Тема 1. Анализ программных реализаций

Задача анализа программных реализаций. Метод экспериментов, статический метод, динамический метод. Принципы функционирования отладчиков. Факторы, ограничивающие возможности отладчиков. Методы поиска функций защиты в машинном коде: метод маяков, метод Step-Trace. Анализ потоков данных. Особенности анализа оверлейного кода, параллельного кода. Особенности анализа машинного кода в среде, управляемой сообщениями.

Тема 2. Защита программ от анализа

Защита от дизассемблирования. Защита от отладки. Методы встраивания защиты в программное обеспечение.

Тема 3. Программные закладки

Понятие программной закладки. Классификация программных закладок. Модель «наблюдатель»: модульная структура закладки, организация информационного взаимодействия между клиентской и серверной частями. Модель «перехват»: перехватчики паролей первого, второго и третьего рода, защита от перехватчиков паролей первого рода в Windows, средства и методы перехвата сетевого трафика, перехват обращений пользователя к документам, электронной почте и веб-страницам. Модель «искажение»: применение программных закладок для несанкционированного повышения полномочий пользователя.

Тема 4. Внедрение программных закладок

Предпосылки к внедрению программных закладок: уязвимости программного обеспечения, уязвимости политики безопасности, человеческий фактор. Методы внедрения программных за-

кладок: маскировка под «безобидное» программное обеспечение, подмена, прямое и косвенное ассоциирование.

Тема 5. Противодействие программным закладкам

Методы выявления программных закладок: сигнатурное и эвристическое сканирование, контроль целостности, мониторинг информационных потоков, изолированная программная среда, программные ловушки. Принципы построения политики безопасности, обеспечивающей высокую защищённость от программных закладок.

Тема 6. Компьютерные вирусы

Бинарные вирусы Windows и Linux: структура, порядок инициализации, алгоритмы поиска и заражения жертвы. Сетевые вирусы: онлайн-вирусы, почтовые вирусы, IM-вирусы. Скриптовые вирусы: макровирусы, shell-вирусы, HTML-вирусы. Комбинированные вирусы. Средства и методы маскировки вирусов и противодействия антивирусному программному обеспечению: стелс-технологии, полиморфные преобразования кода.

6. Рекомендуемая тематика учебных занятий в форме контактной работы

Рекомендуемая тематика учебных занятий *лекционного* типа (предусматривающих преимущественную передачу учебной информации преподавателями):

№ п/п	Наименование раздела	Содержание раздела
1	Анализ программных реализаций	Лекции 1-3. Задача анализа программных реализаций. Метод экспериментов, статический метод, динамический метод. Принципы функционирования отладчиков. Факторы, ограничивающие возможности отладчиков. Методы поиска функций защиты в машинном коде: метод маяков, метод Step-Trace. Анализ потоков данных. Особенности анализа оверлейного кода, параллельного кода. Особенности анализа машинного кода в среде, управляемой сообщениями
2	Защита программ от анализа	Лекции 4-5. Защита от дизассемблирования. Защита от отладки. Методы встраивания защиты в программное обеспечение.
3	Программные закладки	Лекции 6-8. Понятие программной закладки. Классификация программных закладок. Модель «наблюдатель»: модульная структура закладки, организация информационного взаимодействия между клиентской и серверной частями. Модель «перехват»: перехватчики паролей первого, второго и третьего рода, защита от перехватчиков паролей первого рода в Windows, средства и методы перехвата сетевого трафика, перехват обращений пользователя к документам, электронной почте и веб-страницам. Модель «искажение»: применение программных закладок для несанкционированного повышения полномочий пользователя.

4	Внедрение программных закладок	Лекции 9-11. Предпосылки к внедрению программных закладок: уязвимости программного обеспечения, уязвимости политики безопасности, человеческий фактор. Методы внедрения программных закладок: маскировка под «безобидное» программное обеспечение, подмена, прямое и косвенное ассоциирование.
5	Противодействие программным закладкам	Лекции 12-15. Методы выявления программных закладок: сигнатурное и эвристическое сканирование, контроль целостности, мониторинг информационных потоков, изолированная программная среда, программные ловушки. Принципы построения политики безопасности, обеспечивающей высокую защищённость от программных закладок.
6	Компьютерные вирусы	Лекции 16-19. Бинарные вирусы Windows и Linux: структура, порядок инициализации, алгоритмы поиска и заражения жертвы. Сетевые вирусы: онлайн-вирусы, почтовые вирусы, IM-вирусы. Скриптовые вирусы: макровирусы, shell-вирусы, HTML-вирусы. Комбинированные вирусы. Средства и методы маскировки вирусов и противодействия антивирусному программному обеспечению: стелс-технологии, полиморфные преобразования кода.

Рекомендуемый перечень тем *лабораторных* работ:

1. Анализ программной реализации методом экспериментов.
2. Анализ программной реализации статическим методом.
3. Анализ программной реализации динамическим методом.
4. Защита от дизассемблирования.
5. Защита от отладчика.
6. Программные закладки: модель «наблюдатель».
7. Программные закладки: модель «перехват».
8. Программные закладки: модель «искажение».
9. Методы внедрения программных закладок.
10. Методы выявления программных закладок.
11. Настройка антивирусного программного обеспечения.
12. Методы обхода антивирусной защиты.

Требования к самостоятельной работе обучающихся

1. Работа с лекционным материалом, предусматривающая проработку конспекта лекций и учебной литературы, по всем темам из п. 6 настоящей рабочей программы.

2. Выполнение домашнего задания, предусматривающего решение задач, выполнение упражнений, выдаваемых на практических занятиях, по всем темам из п. 6 настоящей рабочей программы.

Руководствуясь положениями статьи 47 и статьи 48 Федерального закона от 29 декабря 2012 г. N 273-ФЗ «Об образовании в Российской Федерации» научно-педагогические работники и иные лица, привлекаемые университетом к реализации данной образовательной программы,

пользуются предоставленными академическими правами и свободами в части свободы преподавания, свободы от вмешательства в профессиональную деятельность; свободы выбора и использования педагогически обоснованных форм, средств, методов обучения и воспитания; права на творческую инициативу, разработку и применение авторских программ и методов обучения и воспитания в пределах реализуемой образовательной программы и отдельной дисциплины.

Исходя из рамок, установленных учебным планом по трудоемкости и видам учебной работы по дисциплине, преподаватель самостоятельно выбирает тематику занятий по формам и количеству часов проведения контактной работы: лекции и иные учебные занятия, предусматривающие преимущественную передачу учебной информации преподавателем и (или) занятия семинарского типа (семинары, практические занятия, практикумы, лабораторные работы, коллоквиумы и иные аналогичные занятия), и (или) групповые консультации, и (или) индивидуальную работу обучающихся с преподавателем, в том числе индивидуальные консультации (по курсовым работам/проектам – при наличии курсовой работы/проекта по данной дисциплине в учебном плане).

Рекомендуемая тематика занятий максимально полно реализуется в контактной работе с обучающимися очной формы обучения. В случае реализации образовательной программы в заочной / очно-заочной форме трудоемкость дисциплины сохраняется, однако объем учебного материала в значительной части осваивается обучающимися в форме самостоятельной работы. При этом требования к ожидаемым образовательным результатам обучающихся по данной дисциплине не зависят от формы реализации образовательной программы.

7. Методические рекомендации по видам занятий

Лекционные занятия.

В ходе лекционных занятий обучающимся рекомендуется выполнять следующие действия. Вести конспектирование учебного материала. Обращать внимание на категории, формулировки, раскрывающие содержание тех или иных явлений и процессов, научные выводы и практические рекомендации по их применению. Задавать преподавателю уточняющие вопросы с целью уяснения теоретических положений, разрешения спорных ситуаций.

Желательно оставить в рабочих конспектах поля, на которых во внеаудиторное время можно сделать пометки из рекомендованной литературы, дополняющие материал прослушанной лекции, а также подчеркивающие особую важность тех или иных теоретических положений.

Практические и семинарские занятия.

На практических и семинарских занятиях в зависимости от темы занятия выполняется поиск информации по решению проблем, практические упражнения, контрольные работы, выработка индивидуальных или групповых решений, итоговое обсуждение с обменом знаниями, участие в круглых столах, разбор конкретных ситуаций, командная работа, представление портфолио и т.п.

Самостоятельная работа.

Самостоятельная работа осуществляется в виде изучения литературы, эмпирических данных по публикациям и конкретных ситуаций из практики, подготовке индивидуальных работ, работа с лекционным материалом, самостоятельное изучение отдельных тем дисциплины; поиск и обзор литературы и электронных источников; чтение и изучение учебника и учебных пособий.

8. Фонд оценочных средств

8.1. Перечень компетенций с указанием этапов их формирования в процессе освоения образовательной программы в рамках учебной дисциплины

Основными этапами формирования указанных компетенций при изучении обучающимися дисциплины являются последовательное изучение содержательно связанных между собой тем учебных занятий. Изучение каждой темы предполагает овладение обучающимися необходимыми компетенциями. Результат аттестации обучающихся на различных этапах формирования компетенций показывает уровень освоения компетенций.

Контролируемые модули, разделы (темы) дисциплины	Индекс контролируемой компетенции	Оценочные средства по этапам формирования компетенций
		Текущий контроль
Тема 1. Анализ программных реализаций	**ОПК-13**	Устный опрос, лабораторная работа, контрольная работа
Тема 2. Защита программ от анализа	**ОПК-13**	Устный опрос, лабораторная работа
Тема 3. Программные закладки	**ОПК-13**	Устный опрос, лабораторная работа
Тема 4. Внедрение программных закладок	**ОПК-13**	Устный опрос, лабораторная работа, контрольная работа
Тема 5. Противодействие программным закладкам	**ОПК-13**	Устный опрос, лабораторная работа, контрольная работа
Тема 6. Компьютерные вирусы	**ОПК-13**	Устный опрос, лабораторная работа, реферат, групповое задание

8.2. Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений и навыков и (или) опыта деятельности процессе текущего контроля

Типовые контрольные работы

Тема 1. Анализ программных реализаций

Задания контрольной работы

Вариант 1	**Вариант 2**
1. Выявить суть работы программы путём изменения входных данных в файлах и реестре и анализа результатов на выходе. **2.** Исследовать особенности реализации программы с помощью дизассемблирования.	**1.** Выявить суть работы программы путём изменения входных данных в файлах и реестре и анализа результатов на выходе. **2.** Исследовать особенности реализации программы путём её запуска под отладчиком.

Тема 4. Внедрение программных закладок

Проверяемые компетенции

ОПК-13	*Способен разрабатывать компоненты программных и программно-аппаратных средств защиты информации в компьютерных системах и проводить анализ их безопасности.*

Задания контрольной работы

Вариант 1	Вариант 2
Используя переполнение буфера в стеке, внедрить в исходную программу следующий эксплойт: push 1000 push 200 call Beep push 0 call ExitThread	Используя целочисленное переполнение, внедрить в исходную программу следующий эксплойт: push 1000 push 200 call Beep push 0 call ExitThread

Тема 5. Противодействие программным закладкам

Проверяемые компетенции

ОПК-13	*Способен разрабатывать компоненты программных и программно-аппаратных средств защиты информации в компьютерных системах и проводить анализ их безопасности.*

Задания контрольной работы

Вариант 1	Вариант 2
Доработать программу из предыдущей контрольной работы таким образом, чтобы она не была подвержена атаке на переполнение буфера.	Доработать программу из предыдущей контрольной работы таким образом, чтобы она не была подвержена атаке на целочисленное переполнение.

Примеры вопросов для устного опроса

Вопросы

1	Что представляет собой анализ программной реализации?
2	Почему задача анализа программных реализаций является актуальной?
3	На какие этапы разбивается анализ программной реализации?
4	Какие методы применяются в ходе анализа программной реализации?
5	Почему метод экспериментов с «чёрным ящиком» так называется?
6	В чём состоит суть метода экспериментов с «чёрным ящиком»?
7	В чём заключаются достоинства и недостатки метода экспериментов с «чёрным ящиком»?
8	Какие приёмы используются при анализе программы методом экспериментов с «чёрным ящиком»?
9	Как определить наличие марканта («соли») в схеме шифрования архиватора ARJ?
10	Как восстановить схему шифрования, реализованную в архиваторе ARJ?
11	В чём заключается статический метод анализа программ?
12	Каковы достоинства и недостатки статического метода?
13	Какие проблемы возникают при дизассемблировании программных файлов?
14	Каковы типичные свойства «глупых» дизассемблеров?
15	Каковы типичные свойства «умных» дизассемблеров?

16	Какие проблемы возникают при изучении листинга дизассемблера?
17	Каким образом в программах, написанных на языке C/C++, осуществляется передача параметров в функцию?
18	Каким образом в программах, написанных на языке C/C++, функции возвращают результат в родительскую процедуру?
19	Что обозначается чёрным, тёмно-синим, светло-синим, зелёным и малиновым цветами в окне IDA View-A дизассемблера IDA?
20	Что такое «режим отображения кода в виде графа» дизассемблера IDA?
21	Что такое Hex-Rays?
22	В чём заключается главное достоинство Hex-Rays по сравнению с другими дизассемблерами?
23	В чём заключается основной недостаток Hex-Rays?
24	Как загрузить в дизассемблер IDA отладочную информацию в формате PDB?
25	Может ли пользователь отредактировать листинг, выдаваемый дизассемблером IDA? Если да, то как?
26	В каких случаях статический метод анализа программных реализаций является самым эффективным?
27	Какие средства для отладки программ вы знаете?
28	Что такое флаг трассировки?
29	Что такое программные и аппаратные точки останова?
30	Каковы основные функции отладчиков?
31	В чём заключаются достоинства и недостатки динамического метода программных реализаций?
32	Какие факторы ограничивают возможности отладчиков?
33	На какие этапы разделяется анализ программы динамическим методом?
34	Что такое метод маяков?
35	Какие фрагменты программы обычно используются в методе маяков?
36	Назовите два способа, с помощью которых можно установить точки останова на маяки. В чём состоят достоинства и недостатки этих способов?
37	В чём суть метода Step-Trace?
38	Почему при использовании метода Step-Trace точки останова нужно применять с осторожностью?
39	Что делает аналитик на втором этапе анализа программы динамическим методом?
40	В чём заключается метод аппаратной точки останова?
41	Каковы отличия в применении метода Step-Trace на втором этапе анализа программы динамическим методом от его использования на первом этапе?
42	Что происходит на третьем этапе анализа программы динамическим методом?
43	Как открыть исполняемый бинарный файл отладчиком, встроенным в Visual Studio?
44	Назовите основные комбинации клавиш, которые используются при отслеживании работы программы в отладчике, встроенном в Visual Studio.
45	Какие окна отладчика, встроенного в Visual Studio, целесообразно выводить на экран при анализе программы, исходный код которой неизвестен?
46	Как в отладчике, встроенном в Visual Studio, можно установить аппаратную точку останова на обращение к заданной области памяти?

47	Что происходит в отладчике, встроенном в Visual Studio, при срабатывании аппаратной точки останова?
48	Что отображается в окне Call Stack у отладчика, встроенного в Visual Studio?
49	Как повысить удобочитаемость информации, отображаемой в окне Call Stack у отладчика, встроенного в Visual Studio?
50	Почему метод аппаратной точки останова не всегда эффективен?
51	Что означают знаки вопроса, отображаемые в окне дампа памяти у отладчика, встроенного в Visual Studio?
52	Почему при разных запусках одной и той же программы некоторые буферы могут располагаться по разным адресам оперативной памяти?
53	Что обычно находится в оперативной памяти по адресу [ebp + 8]?
54	Что делает команда lea у процессоров семейства Intel x86?
55	Каким образом утилита ipconfig отличает включённые сетевые адаптеры от выключенных?
56	Почему при анализе оверлейных программ могут теряться точки останова?
57	Как предотвратить «уход» оверлейной программы из-под отладчика?
58	Сколько точек входа обычно имеет графическая программа Windows?
59	Почему классическая схема применения метода Step-Trace не годится для анализа графических программ Windows?
60	Каким образом можно узнать адрес оконной функции для заданного окна графической программы Windows?
61	В какое место оконной функции следует ставить точку останова?
62	Каким образом можно узнать адрес диалоговой функции для заданного диалогового окна графической программы Windows?
63	Как открыть исполняемый файл в редакторе ресурсов Visual Studio?
64	Чем отличается модальное диалоговое окно от немодального?
65	Какие системные функции Windows применяются для создания диалогового окна?
66	Почему точку останова удобнее ставить не в самое начало анализируемой функции, а после команды mov ebp, esp?
67	Что обычно делает диалоговая функция, получив сообщение WM_INITDIALOG?
68	Как отличить в скомпилированной программе глобальные переменные от локальных?
69	Каким образом можно с помощью отладчика, встроенного в Visual Studio, изменить значения некоторых ячеек в памяти отлаживаемого процесса?
70	Как проще всего узнать, к каким разделам и ключам реестра обращается анализируемая программа?
71	Какие проблемы возникают при анализе параллельного кода динамическим методом?
72	Что такое системный отладчик?
73	Почему анализ ядра операционной системы рекомендуется выполнять на виртуальных машинах?
74	Почему не следует без веских причин загружать системный отладчик автоматически при старте операционной системы?
75	Как с помощью системного отладчика можно проанализировать точку входа драйвера?

76	Как проще всего узнать, к каким файлам, папкам и прочим именованным каналам обращается анализируемая программа?
77	Расскажите про основные возможности программы FileMon.
78	Расскажите про основные возможности программы RegMon.
79	Расскажите про основные возможности программы Process Explorer.
80	Как проще всего узнать, в адресное пространство каких процессов загружена некоторая библиотека в данный момент времени?
81	Как проще всего узнать, каким алгоритмом упакован исполняемый файл?
82	Каким образом можно использовать для анализа программ антивирусные мониторы?

Тема 2. Защита программ от анализа

В о п р о с ы

1	Для чего применяется защита кода от анализа?
2	Почему в большинстве современных программ защита кода от анализа не применяется?
3	Какие «побочные эффекты» возникают при использовании средств защиты программного кода от анализа?
4	В чём заключаются преимущества и недостатки встроенной защиты кода от анализа?
5	В чём заключаются преимущества и недостатки пристыковочной защиты кода от анализа?
6	Каким образом динамическое изменение кода программы затрудняет её анализ?
7	Каким образом полиморфные преобразования кода программы затрудняют её анализ?
8	Каковы побочные эффекты от использования полиморфных преобразований кода?
9	Каким образом косвенные вызовы функций в программе затрудняют её анализ?
10	Каким образом вызовы функций через обработчики исключительных ситуаций затрудняют анализ кода программы?
11	Каким образом вызовы функций в отдельных потоках затрудняют анализ кода программы?
12	Каким образом вызовы функций по таймеру затрудняют анализ кода программы?
13	Каким образом нестандартные способы сравнения данных затрудняют анализ кода программы?
14	Каким образом динамический импорт системных функций затрудняет анализ кода программы?
15	Как можно напрямую передать управление в ядро Windows, не пользуясь стандартными системными библиотеками?
16	Каким образом можно незаметно для программ-мониторов вызывать функции ядра Windows посредством драйвера?
17	Как можно затруднить анализ программы, модифицируя содержимое таблицы адресов импортируемых модулей?
18	Каков самый простой (и ненадёжный) способ определить, что данный процесс Windows выполняется под отладчиком?
19	Каким образом контроль целостности кода программы затрудняет её анализ под от-

	ладчиком?
20	Каким образом генерирование в программе нефатальных исключительных ситуаций затрудняет её анализ под отладчиком?

Тема 3. Программные закладки

В о п р о с ы

1	Что такое программная закладка?
2	Какие программные закладки вы знаете?
3	В чём заключается опасность программных закладок?
4	Что такое информационный поток?
5	Как в рамках субъектно-ориентированной модели описывается операция порождения нового субъекта доступа?
6	Каковы две основные причины возникновения НСД в рамках субъектно-ориентированной модели?
7	Какие модели взаимодействия программной закладки с атакуемой системой вы знаете?
8	Дайте формальное описание модели «наблюдатель».
9	Для каких целей чаще всего применяются программные закладки, действующие по модели «наблюдатель»?
10	Каковы типичные недостатки программных закладок, действующих по модели «наблюдатель»?
11	Каким образом программные закладки, действующие по модели «наблюдатель», обычно обеспечивают свою повторную активизацию после перезагрузки атакованной операционной системы?
12	Как выглядит общая схема взаимодействия клиентской и серверной частей у программной закладки, действующей по схеме «наблюдатель»?
13	Какие преимущества даёт программной закладке, действующей по схеме «наблюдатель», модульная архитектура?
14	Дайте формальное описание модели «перехват».
15	Как устроены перехватчики паролей первого рода?
16	Как устроены перехватчики паролей второго рода?
17	Как устроены перехватчики паролей третьего рода?
18	Как устроены мониторы файловых систем?
19	Как устроены мониторы сети?
20	Дайте формальное описание модели «уборка мусора».
21	Дайте формальное описание модели «искажение».
22	Какие средства динамического изменения полномочий поддерживаются операционными системами семейства Unix?
23	Какие средства динамического изменения полномочий поддерживаются операционными системами семейства Windows?
24	Каким образом несанкционированное порождение дочернего процесса системным процессом позволяет повысить полномочия пользователя?
25	Каким образом несанкционированная модификация машинного кода у монитора безопасности объектов позволяет повысить полномочия пользователя?

26	Какие сетевые атаки можно реализовать в рамках модели «искажение»?
27	Что такое стелс-технология?
28	Каковы основные функции стелс-драйвера?

Тема 4. Внедрение программных закладок

В о п р о с ы

1	Можно ли внедрить программную закладку в адекватно защищённую компьютерную систему?
2	Какие типичные уязвимости компьютерных систем вы знаете?
3	Что такое переполнение буфера?
4	Как переполнение буфера в стеке программы позволяет нарушителю передать управление на произвольный адрес в текущем адресном пространстве?
5	Как отлаживать в Visual Studio консольную программу, запущенную в режиме перенаправления стандартного ввода?
6	Как устроен механизм DEP?
7	В чём заключалась уязвимость GetAdmin в Windows NT?
8	Как проверить, присутствуют ли в ядре операционной системы уязвимости, подобные GetAdmin?
9	В чём заключалась уязвимость %00 в Internet Explorer 5?
10	В чём заключалась уязвимость AdminTrap в Windows NT?
11	Чем опасно наличие на рабочем столе пользователя окон, обслуживаемых системными процессами?
12	В чём заключалась уязвимость сервера NetDDE в Windows 2000?
13	В чём заключалась уязвимость графического формата WMF в Windows, исправленная в январе 2006 г.?
14	В чём заключается уязвимость program.exe?
15	Как можно проверить, есть ли в операционной системе программы, подверженные уязвимости program.exe?
16	Как в рамках субъектно-ориентированной модели формально описывается внедрение программной закладки в атакованную систему?
17	По каким признакам классифицируются методы внедрения программных закладок?
18	В чём заключается метод маскировки программной закладки под прикладное программное обеспечение?
19	В чём состоит основной недостаток метода маскировки программной закладки под прикладное программное обеспечение?
20	В чём заключается метод маскировки программной закладки под системное программное обеспечение?
21	Какими преимуществами обладает метод маскировки программной закладки под системное программное обеспечение?
22	Как в Windows можно установить новую службу?
23	Что нужно добавить в прикладную программу Windows, чтобы она могла запускаться в режиме службы?
24	Как сделать самоинсталлирующуюся службу для Windows?
25	В чём заключается метод внедрения программной закладки путём подмены

	системного программного обеспечения?
26	Почему в Windows 2000 и более поздних версиях внедрение программной закладки путём подмены системного программного обеспечения практически невозможно?
27	В чём состоит суть прямого ассоциирования?
28	В чём состоит суть косвенного ассоциирования?

Тема 5. Противодействие программным закладкам

В о п р о с ы

1	На какие две группы делятся методы защиты от программных закладок?
2	Что такое принцип минимизации программного обеспечения?
3	Что такое принцип минимизации полномочий?
4	Что такое изолированная программная среда?
5	Какие требования предъявляются к программно-аппаратным средствам антивирусной защиты?
6	Что такое сигнатурное сканирование?
7	В чём заключаются достоинства и недостатки сигнатурного сканирования?
8	Что такое эвристическое сканирование?
9	В чём заключаются достоинства и недостатки эвристического сканирования?
10	Как программные закладки могут защищаться от эвристического сканирования?
11	Как часто нужно выполнять антивирусное сканирование?
12	Какие достоинства и недостатки имеет антивирусное сканирование «на лету»?
13	Что такое контроль целостности программного обеспечения?
14	Какие достоинства и недостатки имеет контроль целостности программного обеспечения?
15	Что такое контроль целостности конфигурации системы?
16	Какие ключи реестра Windows наиболее важны с точки зрения защиты от программных закладок?
17	Какие достоинства и недостатки имеет контроль целостности конфигурации системы?
18	Что такое антивирусный мониторинг?
19	Что такое программные ловушки?
20	Можно ли обеспечить эффективную антивирусную защиту одними лишь программно-аппаратными средствами?
21	Что относится к мероприятиям по организационному сопровождению антивирусной защиты?
22	О чём нужно проинструктировать пользователей сети, оснащённой комплексной системой антивирусной защиты?
23	Как проверяется адекватность поведения лиц, ответственных за обеспечение антивирусной защиты сети, в случае успешных вирусных атак?
24	Как организуется защита от программных закладок ранее неизвестных типов?
25	В чём заключается инспекция состояния антивирусной защиты?
26	Как и почему можно преодолеть антивирусную защиту?
27	Какие мероприятия проводятся в случае обнаружения факта успешного внедрения программной закладки в защищаемую систему?

28	В каких случаях осуществляется выявление программных закладок в ручном режиме?
29	Каковы типичные признаки поражения системы программной закладкой?
30	Как просмотреть список процессов, выполняющихся в операционной системе в данный момент?
31	Как можно отличить вредоносный процесс от нормального?
32	Как с помощью утилиты Process Explorer быстро определить, какие процессы пользуются функциями заданной библиотеки?
33	Как с помощью утилиты Process Explorer быстро определить, какие процессы работают с заданным объектом операционной системы?
34	Почему при ручном обнаружении программных закладок не следует сразу же останавливать обнаруженные вредоносные процессы?
35	Как проще всего найти exe-файл, которым был порождён заданный процесс?
36	Какие свойства процесса позволяет получить утилита Process Explorer?
37	Какие свойства библиотеки позволяет получить утилита Process Explorer?
38	Какими способами можно запретить доступ к обнаруженному вредоносному файлу?
39	Как можно изменить права доступа к файлу, если он не отображается в проводнике Windows?
40	Как просмотреть список всех служб Windows?
41	Какие ключи реестра Windows чаще всего используются программными закладками для организации автозапуска после перезагрузки операционной системы?
42	Каковы типичные признаки вредоносного exe-файла?
43	Как определить, все ли найденные вредоносные программы корректно удалены из системы?
44	Как можно выявить файл, скрытый с помощью стелс-технологии?

Тема 6. Компьютерные вирусы

В о п р о с ы

1	Что такое компьютерный вирус?
2	Является ли задача выявления компьютерного вируса алгоритмически разрешимой в общем случае?
3	Когда появились первые компьютерные вирусы?
4	Какой компьютерный вирус причинил наибольший ущерб за всю историю вычислительной техники?
5	Какой компьютерный вирус вызвал самую масштабную эпидемию за всю историю вычислительной техники?
6	Почему написать вирус для Windows сложнее, чем для MS-DOS?
7	Почему первые макровирусы распространились так широко?
8	Существуют ли психотропные компьютерные вирусы, способные убить человека?
9	Каким требованиям должен удовлетворять эффективно размножающийся компьютерный вирус?
10	Что означает требование универсальности, предъявляемое к компьютерным вирусам?
11	Почему компьютерный вирус не должен повторно заражать одни и те же объекты?
12	Каким требованиям должен удовлетворять компьютерный вирус, эффективно раз-

	множающийся в защищённых компьютерных системах?
13	Каким требованиям должен удовлетворять эффективно размножающийся сетевой вирус?
14	Что такое стелс-механизм компьютерного вируса?
15	Чем пассивное размножение компьютерного вируса отличается от активного?
16	К какому классу компьютерных вирусов относится вирус Морриса?
17	Сколько времени обычно требуется для заражения незащищённого компьютера, подключенного к Интернету?
18	Почему прогнозы аналитиков о грядущем «вирусном апокалипсисе» не оправдались?
19	Расскажите о вирусе MSBlast.
20	Чем отличаются онлайн-вирусы от почтовых вирусов?
21	Каковы основные этапы жизненного цикла онлайн-вируса?
22	В чём состоят достоинства и недостатки онлайн-вирусов по сравнению с почтовыми?
23	Какие методы применяются онлайн-вирусами для получения доступа к ресурсам компьютеров-жертв? Какой из этих методов используется чаще всего?
24	Почему большинство онлайн-вирусов функционируют под управлением операционной системы Windows?
25	Каковы основные этапы жизненного цикла почтового вируса?
26	Каким образом почтовые вирусы формируют тему и тело заражённого письма?
27	Как чаще всего почтовые вирусы прикрепляют своё телу к заражённому письму?
28	В чём заключается метод прикрепления почтового вируса к телу заражённого письма посредством встроенных кодов HTML?
29	Как почтовые вирусы используют в ходе распространения уязвимости программного обеспечения атакуемых систем?
30	В чём заключается метод прикрепления почтового вируса к телу заражённого письма, основанный на ссылках, встроенных в письмо?

8.3. Перечень вопросов и заданий для промежуточной аттестации по дисциплине

Перечень вопросов для промежуточного контроля (зачёта)

1	Задача анализа программной реализации.
2	Метод экспериментов, статический метод, динамический метод.
3	Принципы функционирования отладчиков. Факторы, ограничивающие возможности отладчиков.
4	Методы поиска функций защиты в машинном коде: метод маяков, метод Step-Trace.
5	Анализ потоков данных.
6	Особенности анализа оверлейного кода, параллельного кода.
7	Особенности анализа машинного кода в среде, управляемой сообщениями.
8	Защита от дизассемблирования.
9	Защита от отладки.
10	Методы встраивания защиты в программное обеспечение.
11	Понятие программной закладки. Классификация программных закладок.

12	Модель «наблюдатель»: модульная структура закладки, организация информационного взаимодействия между клиентской и серверной частями.
13	Модель «перехват»: перехватчики паролей первого, второго и третьего рода, защита от перехватчиков паролей.
14	Модель «искажение»: применение программных закладок для несанкционированного повышения полномочий пользователя.
15	Предпосылки к внедрению программных закладок.
16	Методы внедрения программных закладок.
17	Методы выявления программных закладок.
18	Принципы построения политики безопасности, обеспечивающей высокую защищённость от программных закладок.
19	Бинарные вирусы Windows и Linux: структура, порядок инициализации, алгоритмы поиска и заражения жертвы.
20	Сетевые вирусы: онлайн-вирусы, почтовые вирусы, IM-вирусы.
21	Скриптовые вирусы: макровирусы, shell-вирусы, HTML-вирусы.
22	Комбинированные вирусы.
23	Средства и методы маскировки вирусов и противодействия антивирусному программному обеспечению.

8.4. Планируемые уровни сформированности компетенций обучающихся и критерии оценивания

Уровни	Содержательное описание уровня	Основные признаки выделения уровня (этапы формирования компетенции, критерии оценки сформированности)	Пятибалльная шкала (академическая) оценка	Двухбалльная шакала, зачет	БРС, % освоения (рейтинговая оценка)
Повышенный	Творческая деятельность	*Включает нижестоящий уровень.* Умение самостоятельно принимать решение, решать проблему/задачу теоретического и прикладного характера на основе изученных методов, приемов, технологий	отлично	зачтено	86-100
Базовый	Применение знаний и умений в более широких контекстах учебной и профессиональной	*Включает нижестоящий уровень.* Способность собирать, систематизировать, анализировать и грамотно использовать информацию из самостоятельно найденных	хорошо		71-85

	деятельности, нежели по образцу с большей степени самостоятельности и инициативы	теоретических источников и иллюстрировать ими теоретические положения или обосновывать практику применения			
Удовлетворительный (достаточный)	Репродуктивная деятельность	Изложение в пределах задач курса теоретически и практически контролируемого материала	удовлетворительно		55-70
Недостаточный	Отсутствие признаков удовлетворительного уровня		неудовлетворительно	не зачтено	Менее 55

9. Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины.

Основная литература

1. Проскурин, В. Г. Защита программ и данных: учеб. пособие для вузов/ В. Г. Проскурин. - 2-е изд., стер.. - М.: Академия, 2012. - 198, [1] с.: ил. - (Высшее профессиональное образование. Информационная безопасность). - (Бакалавриат). - Библиогр.: с. 195-196 (31 назв.). - ISBN 978-5-7695-9288-1: 540.10, 540.10, р. Имеются экземпляры в отделах /There are copies in departments: всего /all 15: УБ(14), ч.з.N3(1)

Дополнительная литература

1. Платонов, В. В. Программно-аппаратные средства защиты информации: учеб. для вузов/ В. В. Платонов. - 2-е изд., стер.. - Москва: Академия, 2014. - 330, [1] с.: табл.. - (Высшее образование. Информационная безопасность). - (Бакалавриат). - Библиогр.: с. 326-327. - ISBN 978-5-4468-1302-5: 880.03, 888.03, р. Имеются экземпляры в отделах /There are copies in departments: всего /all 10: УБ(9), ч.з.N3(1)

10. Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины (модуля).

- НЭБ Национальная электронная библиотека, диссертации и прочие издания
- eLIBRARY.RU Научная электронная библиотека, книги, статьи, тезисы докладов конференций
- Гребенников Электронная библиотека ИД журналы
- ЭБС Лань книги, журналы
- ЭБС Консультант студента
- ПРОСПЕКТ ЭБС
- ЭБС ZNANIUM.COM

- РГБ Информационное обслуживание по МБА
- БЕН РАН
- Электронно-библиотечная система (ЭБС) Кантитана (https://elib.kantiana.ru/)

11. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине.

Программное обеспечение обучения включает в себя:

- система электронного образовательного контента БФУ им. И. Канта – www.lms-3.kantiana.ru, обеспечивающую разработку и комплексное использование электронных образовательных ресурсов;
- серверное программное обеспечение, необходимое для функционирования сервера и связи с системой электронного обучения через Интернет;
- корпоративная платформа Microsoft Teams;
- установленное на рабочих местах обучающихся ПО: Microsoft Windows 7, Microsoft Office Standart 2010, антивирусное программное обеспечение Kaspersky Endpoint Security.
- специализированное ПО не требуется.

12. Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине.

Для проведения занятий лекционного типа, практических и семинарских занятий используются специальные помещения (учебные аудитории), оборудованные техническими средствами обучения – мультимедийной проекционной техникой. Для проведения занятий лекционного типа используются наборы демонстрационного оборудования.

Для проведения лабораторных работ, (практических занятий – при необходимости) используются специальные помещения (учебные аудитории), оснащенные специализированным лабораторным оборудованием: персональными компьютерами с возможностью выхода в интернет и с установленным программным обеспечением, заявленным в п.11.

Для проведения групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации используются специальные помещения (учебные аудитории), оборудованные специализированной мебелью (для обучающихся), меловой / маркерной доской.

Для организации самостоятельной работы обучающимся предоставляются помещения, оснащенные компьютерной техникой с возможностью подключения к сети «Интернет» и обеспечением доступа в электронную информационно-образовательную среду университета.

Для обучения инвалидов и лиц с ограниченными возможностями здоровья университетом могут быть представлены специализированные средства обучения, в том числе технические средства коллективного и индивидуального пользования.

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
федеральное государственное автономное образовательное учреждение высшего образования «Балтийский федеральный университет имени Иммануила Канта»
Институт физико-математических наук и информационных технологий

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

«Защита в операционных системах»

Шифр: 10.05.01
Специальность: «Компьютерная безопасность»
Специализация: «Математические методы защиты информации»
Квалификация (степень) выпускника: специалист по защите информации

Калининград
2022

Лист согласования

Составитель: Мельничук Евгений Михайлович, ассистент Института физико-математических наук и информационных технологий

Рабочая программа утверждена на заседании учебно-методического совета института физико-математических наук и информационных технологий
Протокол № 01/22 от «01» февраля 2022 г.

Председатель учебно-методического
совета института физико-
математических наук и
информационных технологий
Первый заместитель директора Шпилевой А. А
ИФМНиИТ, к. ф.-м. н., доцент

Ведущий менеджер Е.П.Ставицкая

Содержание

1.Наименование дисциплины: «Защита в операционных системах».

Цель дисциплины: целями освоения дисциплины «Защита в операционных системах» являются обучить студентов принципам построения и обслуживания защищенных операционных систем, анализа безопасности защищенных операционных систем; формированию научного мировоззрения и развитию системного мышления.

2. Перечень планируемых результатов обучения по дисциплине, соотнесенных с планируемыми результатами освоения образовательной программы

Код компетенции	Результаты освоения образовательной программы (ИДК)	Результаты обучения по дисциплине
ОПК-11. Способен разрабатывать политики безопасности, политики управления доступом и информационным и потоками в компьютерных системах с учетом угроз безопасности информации и требований по защите информации;	ОПК-11.1. Знает меры по обеспечению информационной безопасности и методы управления процессом их реализации на объекте защиты. ОПК-11.2. Способен формировать политику информационной безопасности, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности. ОПК-11.3. Владеет навыками управления процессом реализации политики информационной безопасности, организации и поддержки выполнения комплекса мер по обеспечению информационной безопасности на объекте защиты.	***знать*** защитные механизмы и внутренние средства обеспечения безопасности в различных операционных системах; принципы хранения и передачи используемой при аутентификации информации; ***уметь*** применять специализированные средства для поиска и устранения проблем безопасности в различных операционных системах; ● ***владеть*** навыками администрирования основных операционных систем.
ОПК-13. Способен разрабатывать компоненты программных и программно-аппаратных	ОПК-13.1. Знает принципы функционирования программных и программно-аппаратных средств защиты информации в компьютерных системах, принципы и методы разработки их компонент, методики анализа их	● ***знать*** требования к подсистеме аудита и политике аудита; ● ***уметь*** настраивать политику безопасности и аудита для основных операционных систем, а также локальных вычислительных сетей, построенных на их основе;

средств защиты информации в компьютерных системах и проводить анализ их безопасности;	безопасности. ОПК-13.2. Способен разрабатывать компоненты программных и программно-аппаратных средств защиты информации в компьютерных системах ОПК-13.3. Способен проводить анализ безопасности компонент программных и программно-аппаратных средств защиты информации в компьютерных системах	• ***владеть*** навыками по использованию сторонних программных и программно-аппаратных средств защиты информации от несанкционированного доступа для усиления процедуры аутентификации.

3. Место дисциплины в структуре образовательной программы

Дисциплина «Защита в операционных системах» представляет собой дисциплину обязательной части блока 1 Дисциплины (модули) подготовки обучающихся, входит в Модуль 8. Программно-аппаратные средства обеспечения информационной безопасности.

4. Виды учебной работы по дисциплине.

Виды учебной работы по дисциплине зафиксированы учебным планом основной профессиональной образовательной программы по указанному направлению и профилю, выражаются в академических часах. Часы контактной работы и самостоятельной работы обчающегося и часы, отводимые на процедуры контроля, могут различаться в учебных планах ОПОП по формам обучения. Объем контактной работы включает часы контактной аудиторной работы (лекции/практические занятия/ лабораторные работы), контактной внеаудиторной работы (контроль самостоятельной работы), часы контактной работы в период аттестации. Контактная работа, в том числе может проводиться посредством электронной информационно-образовательной среды университета с использованием ресурсов сети Интернет и дистанционных технологий

5. Содержание дисциплины, структурированное по темам (разделам)

Исходя из рамок, установленных учебным планом по трудоемкости и видам учебной работы по дисциплине, преподаватель самостоятельно выбирает тематику занятий по формам и количеству часов проведения контактной работы: лекции и иные учебные занятия, предусматривающие преимущественную передачу учебной информации преподавателем и (или) занятия семинарского типа (семинары, практические занятия, практикумы, лабораторные работы, коллоквиумы и иные аналогичные занятия), и (или) групповые консультации, и (или) индивидуальную работу обучающихся с преподавателем, в том числе индивидуальные консультации (по курсовым работам/проектам – при наличии курсовой работы/проекта по данной дисциплине в учебном плане). Рекомендуемая тематика занятий максимально полно реализуется в контактной работе с обучающимися очной формы обучения. В случае реализации образовательной программы в заочной / очно-заочной форме трудоемкость дисциплины сохраняется, однако объем учебного материала в значительной части

осваивается обучающимися в форме самостоятельной работы. При этом требования к ожидаемым образовательным результатам обучающихся по данной дисциплине не зависят от формы реализации образовательной программы.

№	Наименование раздела	Содержание раздела
1	Введение и основные понятия	Цели и задачи курса. Место дисциплины в учебном процессе. Методические рекомендации по изучению курса. Обзор литературы.
2	Базовые механизмы защиты операционных систем	Угрозы безопасности операционной системы; классификация угроз; наиболее распространённые угрозы. Понятие защищённой операционной системы. Подходы к организации защиты. Этапы построения защиты. Административные меры защиты.
3	Управление доступом	Субъекты, объекты, методы и права доступа. Привилегии субъекта доступа. Требования к правилам разграничения доступа. Дискреционное управление доступом; матрица доступа. Изолированная программная среда. Мандатное управление доступом; метки доступа. Контроль информационных потоков. Проблемы реализации мандатного управления доступом в операционных системах. Управление доступом в операционных системах семейства UNIX. Субъекты, объекты, методы и права доступа. UID, EUID, GID, EGID. Атрибуты защиты объектов доступа. Средства динамического изменения полномочий субъектов: SUID/SGID. Расширения стандартной системы управления доступом в SCO UNIX, Solaris, Linux. Управление доступом в операционных системах семейства Windows. Субъекты, объекты, методы и права доступа, привилегии субъекта. Маркеры доступа субъектов, дескрипторы защиты объектов. Порядок проверки прав доступа, порядок назначения дескрипторов защиты создаваемым объектам. Средства динамического изменения полномочий субъектов; олицетворение субъектов доступа. Расширение дискреционной системы управления доступом: автоматическое наследование атрибутов защиты объектов, ограниченные маркеры доступа, мандатный контроль целостности, контроль учётных записей, элементы изолированной программной среды.
4	Идентификация, аутентификация и авторизация	Понятие идентификации, аутентификации и авторизации пользователей. Средства и методы хранения эталонных копий аутентификационной информации. Протоколы передачи аутентификационной информации по каналам вычислительной сети. Криптографическое обеспечение аутентификации. Аутентификация на основе пароля. Средства и методы защиты от компрометации и подбора паролей. Парольная аутентификация в UNIX, библиотеки PAM. Парольная

		аутентификация в Windows; средства управления параметрами аутентификации. Аутентификация на основе внешних носителей ключа. Особенности проверки аутентификационной информации для различных типов носителей. Проблемы генерации, рассылки и смены ключей. Биометрическая аутентификация: общая схема, преимущества, проблемы. Достоинства и недостатки различных схем биометрической аутентификации.
5	Аудит	Необходимость аудита в защищённой системе. Требования к подсистеме аудита. Реализация аудита в UNIX и Windows.
6	Домены Windows	Понятие домена. Преимущества доменной организации информационной инфраструктуры предприятия. Важнейшие понятия доменной структуры Windows: контроллер домена, организационное подразделение (OU), сайт, глобальный каталог. Назначение и принципы функционирования доменных служб Active Directory (AD DS). Сквозная аутентификация, возникающие проблемы и способы их решения. Наделение пользователей домена полномочиями на отдельных компьютерах. Централизованное управление политикой безопасности в домене; локальная и групповая политика; административные шаблоны. Доменный лес Windows Server 2000/2003; преимущества разветвлённой структуры по сравнению с «плоской» доменной архитектурой Windows NT 4.0 Server. Идентификация компьютеров в сети. Двусторонние транзитивные отношения доверия. Средства и методы синхронизации баз данных на контроллерах разных доменов одного леса. Аутентификация по протоколу Kerberos. Делегирование полномочий.

6. Рекомендуемая тематика учебных занятий в форме контактной работы

Рекомендуемая тематика учебных занятий *лекционного* типа (предусматривающих преимущественную передачу учебной информации преподавателями):

№	Наименование раздела	Темы лекций
1	Введение и основные понятия	Лекция 1. Цели и задачи курса. Место дисциплины в учебном процессе. Методические рекомендации по изучению курса.
2	Базовые механизмы защиты операционных систем	Лекция 2. Угрозы безопасности операционной системы; классификация угроз; наиболее распространённые угрозы. Лекция 3. Понятие защищённой операционной системы. Подходы к организации защиты. Этапы построения защиты. Административные меры защиты.

3	Управление доступом	Лекция 4. Требования к правилам разграничения доступа. Дискреционное управление доступом; матрица доступа. Изолированная программная среда. Мандатное управление доступом; метки доступа. Лекция 5. Управление доступом в операционных системах семейства UNIX. Лекция 6. Управление доступом в операционных системах семейства Windows.
4	Идентификация, аутентификация и авторизация	Лекция 7. Идентификации, аутентификации и авторизации пользователей. Лекция 8. Аутентификация на основе пароля. Лекция 9. Аутентификация на основе внешних носителей ключа. Лекция 10. Биометрическая аутентификация
5	Аудит	Лекция 11. Необходимость аудита в защищённой системе. Требования к подсистеме аудита. Лекция 12. Реализация аудита в UNIX Лекция 13. Реализация аудита в Windows.
6	Домены Windows	Лекция 14. Понятие домена. Централизованное управление политикой безопасности в домене; локальная и групповая политика; административные шаблоны. Лекция 15. Доменный лес Windows Server 2000/2003. Kerberos.

Рекомендуемая тематика *практических* занятий:

1. Сканеры безопасности: использование специализированных средств для поиска и устранения уязвимостей в подсистеме безопасности у различных операционных систем.
2. Управление доступом в операционных системах семейства UNIX.
3. Управление доступом в ОС Windows: базовые средства. Управление доступом в ОС Windows: средства для минимизации полномочий. Управление доступом в ОС Windows: элементы изолированной программной среды. Управление доступом в ОС Windows: средства для контроля целостности.
4. Аутентификация в UNIX.
5. Аутентификация в Windows.
6. Аудит в UNIX.
7. Аудит в Windows.
8. Создание доменного леса для различных версий Windows Server и присоединение к нему рабочих станций, на которых установлены клиентские версии Windows и другие операционные системы. Управление структурными единицами в домене Windows Server: пользователи домена, группы пользователей, организационные подразделения, сайты. Групповые политики в домене Windows.Основы централизованного планирования политики безопасности в доменном лесу Windows Server.

На практических занятиях решаются задачи по теме занятия.

Требования к самостоятельной работе обучающихся

1. Работа с лекционным материалом, предусматривающая проработку конспекта лекций и учебной литературы, по всем темам из п. 6 настоящей рабочей программы.

2. Выполнение домашнего задания, предусматривающего решение задач, выполнение упражнений, выдаваемых на практических занятиях, по всем темам из п. 6 настоящей рабочей программы.

Руководствуясь положениями статьи 47 и статьи 48 Федерального закона от 29 декабря 2012 г. N 273-ФЗ «Об образовании в Российской Федерации» научно-педагогические работники и иные лица, привлекаемые университетом к реализации данной образовательной программы, пользуются предоставленными академическими правами и свободами в части свободы преподавания, свободы от вмешательства в профессиональную деятельность; свободы выбора и использования педагогически обоснованных форм, средств, методов обучения и воспитания; права на творческую инициативу, разработку и применение авторских программ и методов обучения и воспитания в пределах реализуемой образовательной программы и отдельной дисциплины.

Исходя из рамок, установленных учебным планом по трудоемкости и видам учебной работы по дисциплине, преподаватель самостоятельно выбирает тематику занятий по формам и количеству часов проведения контактной работы: лекции и иные учебные занятия, предусматривающие преимущественную передачу учебной информации преподавателем и (или) занятия семинарского типа (семинары, практические занятия, практикумы, лабораторные работы, коллоквиумы и иные аналогичные занятия), и (или) групповые консультации, и (или) индивидуальную работу обучающихся с преподавателем, в том числе индивидуальные консультации (по курсовым работам/проектам – при наличии курсовой работы/проекта по данной дисциплине в учебном плане).

Рекомендуемая тематика занятий максимально полно реализуется в контактной работе с обучающимися очной формы обучения. В случае реализации образовательной программы в заочной / очно-заочной форме трудоемкость дисциплины сохраняется, однако объем учебного материала в значительной части осваивается обучающимися в форме самостоятельной работы. При этом требования к ожидаемым образовательным результатам обучающихся по данной дисциплине не зависят от формы реализации образовательной программы.

7. Методические рекомендации по видам занятий

Лекционные занятия.

В ходе лекционных занятий обучающимся рекомендуется выполнять следующие действия. Вести конспектирование учебного материала. Обращать внимание на категории, формулировки, раскрывающие содержание тех или иных явлений и процессов, научные выводы и практические рекомендации по их применению. Задавать преподавателю уточняющие вопросы с целью уяснения теоретических положений, разрешения спорных ситуаций.

Желательно оставить в рабочих конспектах поля, на которых во внеаудиторное время можно сделать пометки из рекомендованной литературы, дополняющие материал прослушанной лекции, а также подчеркивающие особую важность тех или иных теоретических положений.

Практические и семинарские занятия.

На практических и семинарских занятиях в зависимости от темы занятия выполняется поиск информации по решению проблем, практические упражнения, контрольные работы, выработка индивидуальных или групповых решений, итоговое обсуждение с обменом знаниями, участие в круглых столах, разбор конкретных ситуаций, командная работа, представление портфолио и т.п.

Самостоятельная работа.

Самостоятельная работа осуществляется в виде изучения литературы, эмпирических данных по публикациям и конкретных ситуаций из практики, подготовке индивидуальных работ, работа с лекционным материалом, самостоятельное изучение отдельных тем дисциплины; поиск и обзор литературы и электронных источников; чтение и изучение учебника и учебных пособий.

8. Фонд оценочных средств

8.1. Перечень компетенций с указанием этапов их формирования в процессе освоения образовательной программы в рамках учебной дисциплины

Основными этапами формирования указанных компетенций при изучении обучающимися дисциплины являются последовательное изучение содержательно связанных между собой тем учебных занятий. Изучение каждой темы предполагает овладение обучающимися необходимыми компетенциями. Результат аттестации обучающихся на различных этапах формирования компетенций показывает уровень освоения компетенций.

Контролируемые разделы (темы) дисциплины	Индекс контроли-руемой компетенции (или её части)	Оценочные средства по этапам формирования компетенций
		текущий контроль по дисциплине
1. Введение и основные понятия	ОПК-11 ОПК-13	Опрос
2. Базовые механизмы защиты операционных 3. систем	ОПК-11 ОПК-13	Опрос, выполнение лабораторных работ
4. Управление доступом	ОПК-11 ОПК-13	Опрос, выполнение лабораторных работ
5. Идентификация, аутентификация и авторизация	ОПК-11 ОПК-13	Опрос, выполнение лабораторных работ
6. Аудит	ОПК-11 ОПК-13	Опрос, выполнение лабораторных работ
7. Домены Windows	ОПК-11 ОПК-13	Опрос, выполнение лабораторных работ

8.2. Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений и навыков и (или) опыта деятельности процессе текущего контроля

Примеры лабораторных работа:

1. Предоставление существующим пользователям и пользовательским группам нужных прав доступа на требуемые файлы и каталоги в ОС Windows.
2. Предоставление существующим пользователям и пользовательским группам нужных прав доступа на требуемые файлы и каталоги в ОС Linux.
3. Создание в ОС Windows новых пользователей и пользовательских групп и удаление существующих. Задание, изменение и сброс пароля учётной записи.
4. Создание в ОС Linux новых пользователей и пользовательских групп и удаление существующих. Задание, изменение и сброс пароля учётной записи.
5. Настройка и проведение аудита в системах Linux.
6. Настройка и проведение аудита в системах Windows.
7. Создание домена на базе Windows Server, присоединение к нему клиентских машин. Создание структуры доменных пользователей и настройка их полномочий средствами Active Directory.

8.3. Перечень вопросов и заданий для промежуточной аттестации по дисциплине

Вопросы для итогового контроля (зачёта)

1. Угрозы безопасности операционной системы. Классификация угроз. Наиболее распространенные угрозы.
2. Понятие защищенной операционной системы. Подходы к организации защиты.
3. Этапы построения защиты. Административные меры защиты.
4. Субъекты, объекты, методы и права доступа. Привилегии субъекта доступа.
5. Требования к правилам разграничения доступа.
6. Дискреционное управление доступом. Матрица доступа.
7. Изолированная программная среда.
8. Мандатное управление доступом. Метки доступа.
9. Контроль информационных потоков.
10. Управление доступом в операционных системах семейства UNIX. Атрибуты защиты объектов доступа.
11. Средства динамического изменения полномочий субъектов в операционных системах семейства UNIX. Расширение стандартной системы управления доступом в Linux.

12. Управление доступом в операционных системах семейства Windows. Субъекты, объекты, методы и права доступа. Привилегии субъекта. Маркеры доступа субъектов, дескрипторы защиты объектов.
13. Порядок проверки прав доступа, порядок назначения дескрипторов защиты создаваемым объектам.
14. Средства динамического изменения полномочий субъектов в операционных системах семейства Windows.
15. Расширение дискреционной системы управления доступом.
16. Понятие идентификации, аутентификации и авторизации пользователей.
17. Средства и методы хранения эталонных копий аутентификационной информации.
18. Протоколы передачи аутентификационной информации по каналам вычислительной сети.
19. Криптографическое обеспечение аутентификации пользователей.
20. Аутентификация на основе пароля. Средства и методы защиты от компрометации и подбора паролей.
21. Парольная аутентификация в UNIX. Библиотеки PAM.
22. Парольная аутентификация в Windows. Средства управления параметрами аутентификации.
23. Аутентификация на основе внешних носителей ключа. Особенности проверки аутентификационной информации для различных типов носителей.
24. Проблемы генерации, рассылки и смены ключей.
25. Биометрическая аутентификация: общая схема, преимущества, проблемы. Достоинства и недостатки различных схем биометрической аутентификации.
26. Необходимость аудита в защищенной системе. Требования к подсистеме аудита.
27. Реализация аудита в UNIX и Windows.
28. Преимущества доменной организации информационной инфраструктуры предприятия. Важнейшие понятия доменной структуры Windows: контроллер домена, организационное подразделение (OU), сайт, глобальный каталог. Назначение и принципы функционирования доменных служб Active Directory (AD DS).
29. Сквозная аутентификация: суть, возникающие проблемы и пути их решения.
30. Наделение пользователей домена полномочиями на отдельных компьютерах.
31. Централизованное управление политикой безопасности в домене. Локальная и групповая политика. Административные шаблоны.
32. Доменный лес Windows Server 2000/2003. Преимущества разветвленной структуры по сравнению с «плоской» доменной архитектурой Windows NT 4.0 Server.
33. Идентификация компьютеров в сети. Двусторонние транзитивные отношения доверия.
34. Средства и методы синхронизации баз данных на контроллерах разных доменов одного леса.
35. Аутентификация Kerberos. Групповая политика. Делегирование полномочий.

8.4. Планируемые уровни сформированности компетенций обучающихся и критерии оценивания

Уровни	Содержательное описание уровня	Основные признаки выделения уровня (этапы формирования компетенции, критерии оценки сформированности)	Пятибалльная шкала (академическая) оценка	Двухбалльная шакала, зачет	БРС, % освоения (рейтинговая оценка)
Повышенный	Творческая деятельность	*Включает нижестоящий уровень.* Умение самостоятельно принимать решение, решать проблему/задачу теоретического и прикладного характера на основе изученных методов, приемов, технологий	отлично	зачтено	86-100
Базовый	Применение знаний и умений в более широких контекстах учебной и профессиональной деятельности, нежели по образцу с большей степени самостоятельности и инициативы	*Включает нижестоящий уровень.* Способность собирать, систематизировать, анализировать и грамотно использовать информацию из самостоятельно найденных теоретических источников и иллюстрировать ими теоретические положения или обосновывать практику применения	хорошо		71-85
Удовлетворительный	Репродуктивная	Изложение в пределах задач курса	удовлетворительно		55-70

(достаточный)	деятельность	теоретически и практически контролируемого материала			
Недостаточный	Отсутствие признаков удовлетворительного уровня		неудовлетворительно	не зачтено	Менее 55

9. Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины.

Основная литература

1. Проскурин, В. Г. Защита в операционных системах: Учебное пособие для вузов / В.Г. Проскурин. - Москва : Гор. линия-Телеком, 2014. - 192 с.: ил.; . - (Специальность). ISBN 978-5-9912-0379-1, 500 экз. - Текст : электронный. - URL: https://znanium.com/catalog/product/461004 ЭБС Znanium(1)

Дополнительная литература

1. Широков, А. И. Операционные системы и среды: основные понятия теории : учебник / А. И. Широков, Ф. Г. Кирдяшов, С. Э. Мурадханов ; под ред. Е. А. Калашникова, Л. П. Рябова. - Москва : Изд. Дом НИТУ «МИСиС», 2018. - 192 с. - ISBN 978-5-906953-49-0. - Текст : электронный. - URL: https://znanium.com/catalog/product/1232238 ЭБС Znanium(1)

10. Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины (модуля).

- https://technet.microsoft.com/ru-ru/windowsserver/windows-server-security.aspx – официальный портал «Безопасность Windows Server».
- http://www.securitylab.ru/software/ – каталог средств для обнаружения и защиты от вредоносного ПО.
- http://forum.antichat.ru/ – большой русскоязычный форум на тему хакерства.
- http://xaker. ru/ – сайт журнала «Хакер».
- Электронная библиотечная система «Znanium» (https://znanium.com/)

11. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине.

Программное обеспечение обучения включает в себя:

- система электронного образовательного контента БФУ им. И. Канта – www.lms-3.kantiana.ru, обеспечивающую разработку и комплексное использование электронных образовательных ресурсов;

- серверное программное обеспечение, необходимое для функционирования сервера и связи с системой электронного обучения через Интернет;
- корпоративная платформа Microsoft Teams;
- установленное на рабочих местах обучающихся ПО: Microsoft Windows 7, Microsoft Office Standart 2010, антивирусное программное обеспечение Kaspersky Endpoint Security.
- специализированное ПО не требуется.
- Virtual Box - программный продукт виртуализации для различных операционных систем
- Образ системы Linux

12. Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине.

Для проведения занятий лекционного типа, практических и семинарских занятий используются специальные помещения (учебные аудитории), оборудованные техническими средствами обучения – мультимедийной проекционной техникой. Для проведения занятий лекционного типа используются наборы демонстрационного оборудования.

Для проведения лабораторных работ, (практических занятий – при необходимости) используются специальные помещения (учебные аудитории), оснащенные специализированным лабораторным оборудованием: персональными компьютерами с возможностью выхода в интернет и с установленным программным обеспечением, заявленным в п.11.

Для проведения групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации используются специальные помещения (учебные аудитории), оборудованные специализированной мебелью (для обучающихся), меловой / маркерной доской.

Для организации самостоятельной работы обучающимся предоставляются помещения, оснащенные компьютерной техникой с возможностью подключения к сети «Интернет» и обеспечением доступа в электронную информационно-образовательную среду университета.

Для обучения инвалидов и лиц с ограниченными возможностями здоровья университетом могут быть представлены специализированные средства обучения, в том числе технические средства коллективного и индивидуального пользования.

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
федеральное государственное автономное образовательное учреждение высшего образования «Балтийский федеральный университет имени Иммануила Канта»
Институт физико-математических наук и информационных технологий

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

«Основы построения защищенных баз данных»

Шифр: 10.05.01
Специальность: «Компьютерная безопасность»
Специализация: «Математические методы защиты информации»
Квалификация (степень) выпускника: Специалист по защите информации

Калининград
2022

Лист согласования

Составитель: старший преподаватель Института физико-математических наук и информационных технологий ***Козьминых Е.В***.

Рабочая программа утверждена на заседании учебно-методического совета института физико-математических наук и информационных технологий

Протокол № 01/22 от «01» февраля 2022 г.

Председатель учебно-методического совета института физико-математических наук и информационных технологий

Первый заместитель директора ИФМНиИТ, к. ф.-м. н., доцент — Шпилевой А. А

Ведущий менеджер — Е.П.Ставицкая

Содержание

1.Наименование дисциплины: «Основы построения защищенных баз данных».

Целью освоения дисциплины является формирование навыков и умений по обеспечению безопасности информации в автоматизированных системах, основу которых составляют базы данных, дать навыки работы со встроенными в Системы управления базами данных (далее – СУБД) средствами защиты, а также показать возможные пути построения собственных механизмов защиты информации в АИС с СУБД.

Необходимость изучения дисциплины продиктована тем, что значительная часть современных информационных систем накапливает большие объемы данных. Для их обработки используются системы управления базами данных. Существует множество угроз безопасности баз данных, связанных с уязвимостями как самой СУБД, так и языка обработки данных (например, различного рода SQL-инъекции и т.п.). При создании и эксплуатации информационных систем, в составе которых есть базы данных, необходимо обеспечить безопасность хранения и обработки данных.

Основные **задачи** изучения дисциплины:

- формирование у обучаемых навыков по выявлению угроз безопасности информационных систем, в которых накапливаются большие объемы данных, и их обработка связана с использованием систем управления базами данных;
- овладение методами обеспечения безопасности баз данных, получение навыков конфигурирования встроенных механизмов обеспечения безопасности СУБД;
- получение опыта разработки и использования собственных элементов, используемых для защиты информации СУБД, в том числе в части аудита работы пользователей информационной системы, разграничения доступа к данным, резервированию и восстановлению баз данных.

2. Перечень планируемых результатов обучения по дисциплине, соотнесенных с планируемыми результатами освоения образовательной программы

Код компетенции	Результаты освоения образовательной программы (ИДК)	Результаты обучения по дисциплине
ОПК-14. Способен проектировать базы данных, администрировать системы управления базами данных в соответствии с требованиями по защите информации;	ОПК-14.1. Знает методы, алгоритмы и инструменты для проектирования баз данных, администрирования систем управления базами данных в соответствии с требованиями по защите информации. ОПК-14.2. Умеет проектировать базы данных, администрировать системы управления базами данных в соответствии с требованиями по защите информации. ОПК-14.3. Владеет навыками проектирования баз данных, администрирования систем управления базами данных в соответствии с требованиями по защите информации.	**Знать** требования отечественных и зарубежных стандартов в области безопасности баз данных, методы защиты, принципы защиты баз данных, принципы работы механизмов защиты СУБД. **Уметь** использовать встроенные механизмы СУБД, в части разграничения доступа и управления пользователями, аудита, резервирования информации, а также проектировать собственные элементы механизмов безопасности, администрировать СУБД в соответствии с требованиями по защите информации. **Владеть** методами проектирования баз данных и механизмов защиты баз данных

ОПК-2.2 Способен разрабатывать и анализировать математические модели механизмов защиты информации;	ОПК-2.2.1. Знает принципы построения средств криптографической защиты информации. ОПК-2.2.2. Умеет выявлять наиболее целесообразные подходы к обеспечению защиты информации компьютерной системы. ОПК-2.2.3. Владеет методами разработки математических моделей, реализуемых в средствах защиты информации.	Студент, изучивший курс, должен: **Знать** методы разработки и анализа математических моделей механизмов защиты информации в СУБД. **Уметь** провести анализ механизмов защиты СУБД на основе построения математической модели механизмов защиты СУБД, как встроенных, так и разработанных самостоятельно **Владеть** методами и средствами оценки защищенности информационной системы, содержащей СУБД

3. Место дисциплины в структуре образовательной программы

Дисциплина «Основы построения защищенных баз данных» представляет собой дисциплину базовой части Блока 1 Дисциплины (модули) подготовки студентов.

4. Виды учебной работы по дисциплине.

Виды учебной работы по дисциплине зафиксированы учебным планом основной профессиональной образовательной программы по указанному направлению и профилю, выражаются в академических часах. Часы контактной работы и самостоятельной работы студента и часы, отводимые на процедуры контроля, могут различаться в учебных планах ОПОП по формам обучения. Объем контактной работы включает часы контактной аудиторной работы (лекции/практические занятия/ лабораторные работы), контактной внеаудиторной работы (контроль самостоятельной работы), часы контактной работы в период аттестации. Контактная работа, в том числе может проводиться посредством электронной информационно-образовательной среды университета с использованием ресурсов сети Интернет и дистанционных технологий

5. Содержание дисциплины, структурированное по темам (разделам)

Исходя из рамок, установленных учебным планом по трудоемкости и видам учебной работы по дисциплине, преподаватель самостоятельно выбирает тематику занятий по формам и количеству часов проведения контактной работы: лекции и иные учебные занятия, предусматривающие преимущественную передачу учебной информации преподавателем и (или) занятия семинарского типа (семинары, практические занятия, практикумы, лабораторные работы, коллоквиумы и иные аналогичные занятия), и (или) групповые консультации, и (или) индивидуальную работу обучающихся с преподавателем, в том числе индивидуальные консультации (по курсовым работам/проектам – при наличии курсовой работы/проекта по данной дисциплине в учебном плане). Рекомендуемая тематика занятий максимально полно реализуется в контактной работе со студентами очной формы обучения. В случае реализации образовательной программы в заочной / очно-заочной форме трудоемкость дисциплины сохраняется, однако объем учебного материала в значительной части осваивается студентами в форме самостоятельной работы. При этом требования к ожидаемым образовательным результатам студентов по данной дисциплине не зависят от формы реализации образовательной программы.

№ п/п	Наименование темы	Содержание темы
1	Теоретические основы обеспечения безопасности в СУБД.	Понятие безопасности БД. Угрозы безопасности БД: общие и специфические. Требования безопасности БД. Общее описание средств обеспечения защиты информации в СУБД. Политики безопасности СУБД и модели безопасности в СУБД. Дискреционные и мандатные модели разграничения доступа. Классификация моделей. Особенности реализации моделей разграничения доступа в СУБД.
2	Обеспечение целостности баз данных.	Угрозы целостности СУБД. Основные виды и причины возникновения угроз целостности. Способы противодействия. Транзакции как средство изолированности пользователей. Блокировки. Режимы блокирования. Правила согласования блокировок. Применение стратегий блокирования. Декларативный и процедурный контроль целостности. Способы поддержания ссылочной целостности. Триггеры. Цели использования триггеров для обеспечения защиты данных.
3	Механизмы обеспечения конфиденциальности в СУБД.	Классификация угроз конфиденциальности баз данных. Получение несанкционированного доступа к конфиденциальной информации путем логических выводов и атак вида «SQL-инъекция». Методы противодействия основным угрозам нарушения конфиденциальности баз данных. Средства идентификации и аутентификации. Методы аутентификации пользователей СУБД. Совместное применение средств идентификации и аутентификации, встроенных в СУБД и в ОС. Преимущества и недостатки встроенных средств аутентификации. Внешняя и сквозная аутентификация. Технология Single-Sign-On (SSO). Средства управления доступом. Основные понятия: субъекты и объекты, группы пользователей, привилегии, роли и представления. Виды привилегий. Использование ролей и привилегий пользователей. Соотношение прав доступа, определяемых ОС и СУБД. Использование представлений для обеспечения конфиденциальности информации в СУБД. Механизмы тщательного контроля доступа. Аудит и подотчетность. Подотчетность действий пользователя и аудит связанных с безопасностью событий. Регистрация действий пользователя. Управление набором регистрируемых событий. Анализ регистрационной информации. Криптографические методы защиты баз данных. Особенности применения криптографических методов. Прозрачное шифрование и шифрование по требованию.
4	Обеспечение высокой доступности баз данных.	Средства, поддерживающие высокую доступность баз данных. Задачи и средства администрирования: мониторинг производительности серверов СУБД. Оптимизация доступа к данным в БД: индексирование, кластеризация данных, профилирование и оптимизация запросов. Кластерная организация серверов баз данных. Виды сбоев БД и СУБД. Резервирование и восстановление БД. Избыточность данных. Программное и аппаратное зеркалирование. Тиражирование данных.

6. Рекомендуемая тематика учебных занятий в форме контактной работы

Рекомендуемая тематика учебных занятий *лекционного* типа (предусматривающих преимущественную передачу учебной информации преподавателями):

№	Тема лекции
1	Тема 1. Теоретические основы обеспечения безопасности в СУБД
2	Тема 2. Обеспечение целостности баз данных
3	Тема 3. Механизмы обеспечения конфиденциальности в СУБД
4	Тема 4. Обеспечение высокой доступности баз данных

Рекомендуемая тематика *лабораторных* занятий:

№ п/п	Наименование темы	Содержание темы
1	Теоретические основы обеспечения безопасности в СУБД.	Развертывание тестовой СУБД. Основы работы с ПО Oracle Developer, Enterprise manager, SQLPlus. и языком SQL. Управление экземпляром базы данных. Управление структурами хранения базы данных.
2	Обеспечение целостности баз данных.	Мониторинг и разрешение конфликтов блокировок. Мультиплексирование управляющих файлов, журнальных групп, обеспечение создания избыточных копий архивных журналов.
3	Механизмы обеспечения конфиденциальности в СУБД.	Контроль использования ресурсов пользователями, стандартные возможности парольной безопасности . Администрирование пользователей, предоставление привилегий, использование ролей. Разграничение доступа на уровне строк: VIRTUAL PRIVATE DATABASE. Настройка различных видов аудита баз данных, создание и использование триггеров для целей аудита. Настройка встроенных механизмов шифрования.
4	Обеспечение высокой доступности баз данных.	Конфигурирование сетевой среды Oracle. Резервирование и восстановление. Перемещение данных (экспорт и импорт).

Руководствуясь положениями статьи 47 и статьи 48 Федерального закона от 29 декабря 2012 г. N 273-ФЗ «Об образовании в Российской Федерации» научно-педагогические работники и иные лица, привлекаемые университетом к реализации данной образовательной программы, пользуются предоставленными академическими правами и свободами в части свободы преподавания, свободы от вмешательства в профессиональную деятельность; свободы выбора и использования педагогически обоснованных форм, средств, методов обучения и воспитания; права на творческую инициативу, разработку и применение авторских программ и методов обучения и воспитания в пределах реализуемой образовательной программы и отдельной дисциплины.

Исходя из рамок, установленных учебным планом по трудоемкости и видам учебной работы по дисциплине, преподаватель самостоятельно выбирает тематику занятий по формам и количеству часов проведения контактной работы: лекции и иные учебные занятия, предусматривающие преимущественную передачу учебной информации преподавателем и (или) занятия семинарского типа (семинары, практические занятия, практикумы, лабораторные работы, коллоквиумы и иные аналогичные занятия), и (или) групповые консультации, и (или) индивидуальную работу обучающихся с преподавателем, в том числе индивидуальные консультации (по курсовым работам/проектам – при наличии курсовой работы/проекта по данной дисциплине в учебном плане).

Рекомендуемая тематика занятий максимально полно реализуется в контактной работе со студентами очной формы обучения. В случае реализации образовательной программы в заочной / очно-заочной форме трудоемкость дисциплины сохраняется, однако объем учебного материала в значительной части осваивается студентами в форме самостоятельной работы. При этом требования к ожидаемым образовательным результатам студентов по данной дисциплине не зависят от формы реализации образовательной программы.

7. Методические рекомендации по видам занятий

Лекционные занятия.

В ходе лекционных занятий обучающимся рекомендуется выполнять следующие действия. Вести конспектирование учебного материала. Обращать внимание на категории, формулировки, раскрывающие содержание тех или иных явлений и процессов, научные выводы и практические рекомендации по их применению. Задавать преподавателю уточняющие вопросы с целью уяснения теоретических положений, разрешения спорных ситуаций.

Желательно оставить в рабочих конспектах поля, на которых во внеаудиторное время можно сделать пометки из рекомендованной литературы, дополняющие материал прослушанной лекции, а также подчеркивающие особую важность тех или иных теоретических положений.

Практические и семинарские занятия.

На практических и семинарских занятиях в зависимости от темы занятия выполняется поиск информации по решению проблем, практические упражнения, контрольные работы, выработка индивидуальных или групповых решений, итоговое обсуждение с обменом знаниями, участие в круглых столах, разбор конкретных ситуаций, командная работа, представление портфолио и т.п.

Самостоятельная работа.

Самостоятельная работа осуществляется в виде изучения литературы, эмпирических данных по публикациям и конкретных ситуаций из практики, подготовке индивидуальных работ, работа с лекционным материалом, самостоятельное изучение отдельных тем дисциплины; поиск и обзор литературы и электронных источников; чтение и изучение учебника и учебных пособий.

8. Фонд оценочных средств

8.1. Перечень компетенций с указанием этапов их формирования в процессе освоения образовательной программы в рамках учебной дисциплины

Основными этапами формирования указанных компетенций при изучении обучающимися дисциплины являются последовательное изучение содержательно связанных между собой тем учебных занятий. Изучение каждой темы предполагает овладение обучающимися необходимыми компетенциями. Результат аттестации

обучающихся на различных этапах формирования компетенций показывает уровень освоения компетенций.

Контролируемые разделы (темы) дисциплины	Индекс контроли-руемой компетенции (или её части)	Оценочные средства по этапам формирования компетенций
		текущий контроль по дисциплине
Тема 1. Теоретические основы обеспечения безопасности в СУБД.	ОПК-14	Устный опрос, Тестирование, выполнение лабораторных работ
Тема 2. Обеспечение целостности баз данных.	ОПК-14 ОПК-2.2	выполнение лабораторных работ
Тема 3. Механизмы обеспечения конфиденциальности в СУБД.	ОПК-14 ОПК-2.2	Тестирование, выполнение лабораторных работ
Тема 4. Обеспечение высокой доступности баз данных.	ОПК-14	Тестирование, выполнение лабораторных работ

8.2. Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений и навыков и (или) опыта деятельности процессе текущего контроля

Типовые вопросы для устного опроса:

Тема 1. Теоретические основы обеспечения безопасности в СУБД.

	Вопрос
Оценка «удовлетворительно» - низкий уровень освоения компетенции	Объяснить сущность понятия безопасности баз данных. Перечислить основные методы построения защищенных информационных систем, основные понятия, связанные с архитектурой систем управления базами данных.
Оценка «хорошо» - повышенный уровень освоения компетенции	Объяснить сущность понятия безопасности баз данных. Перечислить этапы научного формирования проблемы обеспечения информационной безопасности баз данных и критерии качества баз данных, основные подходы к методам построения защищенных информационных систем. Перечислить основные понятия, связанные с архитектурой систем управления базами данных.
Оценка «отлично» - высокий уровень освоения компетенции	Объяснить сущность понятия безопасности баз данных, привести примеры и сравнить с другими информационными системами. Перечислить этапы научного формирования проблемы обеспечения информационной безопасности баз данных и критерии качества баз данных, основные подходы к методам построения защищенных информационных систем, привести примеры и сравнить с другими информационными системами. Показать структуру свойства информационной безопасности баз данных.

Тема 3. Механизмы обеспечения конфиденциальности в СУБД.

	Вопрос
Оценка «удовлетворительно» - низкой уровень освоения компетенции	Перечислить основные механизмы обеспечения конфиденциальности информации СУБД.
Оценка «хорошо» - повышенный уровень освоения компетенции	Перечислить основные механизмы обеспечения конфиденциальности информации СУБД и объяснить принципы их функционирования и настройки.
Оценка «отлично» - высокий уровень освоения компетенции	Перечислить основные механизмы обеспечения конфиденциальности информации СУБД и объяснить принципы их функционирования и настройки, построить примерную математическую модель механизма.

Примеры тестовых вопросов

Тема 1. Постановка задачи обеспечения информационной безопасности баз данных

Вопрос теста	**Варианты ответов**
1. Основной структурой хранения данных в БД является	Таблица Файл Ссылка
2. Наличие индекса (INDEX) в таблице	Увеличивает скорость чтения данных таблицы Не влияет на скорости чтения и записи в таблицу Уменьшает скорость записи данных в таблицу
3. Выберите верные утверждения, относящиеся к понятию «Табличное пространство» (TABLESPACE)	Служит для хранения объ□ктов, например, таблиц и индексов Не может содержать таблицы разных пользователей Может быть переведено в автономный (OFFLINE) режим (недоступно для пользователей) Может быть переведено в режим «только для чтения» (READ ONLY) Может принадлежать нескольк□м базам данных

Тема 3. Механизмы обеспечения конфиденциальности в СУБД.

Вопрос теста	**Варианты ответов**	
1. Выберите команды для назначения и отмены привилегий	ALTER и REVOKE GRANT и REVKE CREATE и DELETE GRANT и DROP	
2. Сопоставьте понятие и его описание	Привилегия	Поименованный набор ограничений на использование ресурсов
	Профиль	Поименованная группа привилег□й и других ролей
	Роль	Право выполнять конкретный тип предложений SQL или право доступа к объекту другого пользователя
3. Выберите объектные привилегии	CREATE ANY INDEX	

	ALTER PROCEURE	
	CREATE VIEW	
	CREATE TALE	
	DELETE ANY TABLE	
	UPDATE TABLE	
	RESTRITED SESSION	
	SELECT TABLE	
	EXECUTE POCEDURE	
	ALTER TABLESPASE	
4. Пароль может быть назначен:	Пользователю	
	Таблице	
	Роли	
5. Выберите механизмы, обеспечивающие согласованность чтения и изменения данных при одновременном доступе к общим ресурсам	блокировки	
	аудит	
	транзакции	
6. Сопоставьте понятие и его описание из области транзакций	COMMIT	Откат транзакции до указанной точки сохранения, не отменяя все сделанные до нее изменения
	SAVEPOINT	Завершение транзакции, выполненные изменения становятся постоянными, освобождаются блокировки.
	ROLLBACK	Определение точки сохранения внутри транзакции
	ROLLBACK TO SAVEPOINT	Завершение транзакции, выполненные изменения отменяются, освобождаются блокировки.

Тема 4. Обеспечение высокой доступности баз данных.

Вопрос теста	**Варианты ответов**	
Выберите основные методы защиты службы прослушивателя Listener	Защита Listener от сканирования	Ведение и анализ журнала подключений (log-файла)
	Защита от атак типа «отказ в обслуживани□»	Включение парольной защиты Listener
	Защита от атак перехвата пароля	Установка атрибутов средствами ОС
	Защита от перебора паролей к Listener	Включение SSL-шифрования между клиентом и Listener
	Защита от неправомерного доступа к конфигурационным файлам	Смена стандартного порта Listener
Сопоставьте название дополнительного пакета обеспечения безопасности Oracle и его краткого описания	Orale Database Vault	Система контроля SQL-запросов к БД
	Oracle Audit Vault	Прозрачное шифрование данных
	Oracle Enterprise User Security	Реализация мандатной модели разграничения доступа
	Transparent Data Encryption	Расширенн□й аудит

	Oracle Database Firewal	Единая система управления учетными записями и правами пользователей множества БД	
Расставьте по порядку этапы реализации атаки на СУБД	Сбор информации о системе, атаки на службу Listener	3	
	Получение SID	5	
	Получение аутентификационных данных (user\password)	1	
	Повышение привилегий внутри БД	2	
	Получение доступа к ОС средствами СУБД	4	

Выполнение лабораторных работ

Тема 1. Теоретические основы обеспечения безопасности в СУБД.

Тематика лабораторных работ

- Развертывание тестовой СУБД (4)
- Основы работы с ПО Oracle Developer, Enterprise manager, SQLPlus. и языком SQL
- Управление экземпляром базы данных.
- Управление структурами хранения базы данных.

Тема 2. Обеспечение целостности баз данных.

Тематика лабораторных работ

- Мониторинг и разрешение конфликтов блокировок.
- Мультиплексирование управляющих файлов, журнальных групп, обеспечение создания избыточных копий архивных журналов.

Тема 3. Механизмы обеспечения конфиденциальности в СУБД.

Тематика лабораторных работ

- Контроль использования ресурсов пользователями, стандартные возможности парольной безопасности.
- Администрирование пользователей, предоставление привилегий, использование ролей.
- Разграничение доступа на уровне строк: VIRTUAL PRIVATE DATABASE.
- Настройка различных видов аудита баз данных, создание и использование триггеров для целей аудита.
- Настройка встроенных механизмов шифрования.

Тема 4. Обеспечение высокой доступности баз данных.

Тематика лабораторных работ:

- Конфигурирование сетевой среды Oracle.
- Резервирование и восстановление.
- Перемещение данных (экспорт и импорт).

8.3. Перечень вопросов и заданий для промежуточной аттестации по дисциплине

Вопросы для промежуточного контроля (зачета)

1. Понятие безопасности БД. Угрозы безопасности БД: общие и специфические.
2. Требования безопасности БД. Общее описание средств обеспечения защиты информации в СУБД.
3. Политики безопасности СУБД и модели безопасности в СУБД.
4. Дискреционные и мандатные модели разграничения доступа. Классификация моделей.
5. Особенности реализации моделей разграничения доступа в СУБД.
6. Мандатные модели разграничения доступа.
7. Угрозы целостности СУБД. Основные виды и причины возникновения угроз целостности. Способы противодействия.
8. Транзакции как средство изолированности пользователей. Блокировки. Режимы блокирования. Правила согласования блокировок. Применение стратегий блокирования.
9. Декларативный и процедурный контроль целостности. Способы поддержания ссылочной целостности.
10. Триггеры. Цели использования триггеров для обеспечения защиты данных.
11. Классификация угроз конфиденциальности баз данных.
12. Получение несанкционированного доступа к конфиденциальной информации путем логических выводов и атак вида «SQL-инъекция».
13. Методы противодействия основным угрозам нарушения конфиденциальности баз данных.
14. Средства идентификации и аутентификации. Методы аутентификации пользователей СУБД.
15. Совместное применение средств идентификации и аутентификации, встроенных в СУБД и в ОС. Преимущества и недостатки встроенных средств аутентификации.
16. Внешняя и сквозная аутентификация. Технология Single-Sign-On (SSO).
17. Средства управления доступом. Основные понятия: субъекты и объекты, группы пользователей, привилегии, роли и представления.
18. Виды привилегий. Использование ролей и привилегий пользователей. Соотношение прав доступа, определяемых ОС и СУБД.
19. Использование представлений для обеспечения конфиденциальности информации в СУБД.
20. Механизмы тщательного контроля доступа. Аудит и подотчетность.
21. Подотчетность действий пользователя и аудит связанных с безопасностью событий.
22. Регистрация действий пользователя. Управление набором регистрируемых событий. Анализ регистрационной информации.
23. Криптографические методы защиты баз данных. Особенности применения криптографических методов. Прозрачное шифрование и шифрование по требованию.
24. Средства, поддерживающие высокую доступность баз данных.
25. Задачи и средства администрирования: мониторинг производительности серверов СУБД.

26. Оптимизация доступа к данным в БД: индексирование, кластеризация данных, профилирование и оптимизация запросов.
27. Кластерная организация серверов баз данных.
28. Виды сбоев БД и СУБД.
29. Резервирование и восстановление БД. Избыточность данных. Программное и аппаратное зеркалирование.
30. Тиражирование данных.

8.4. Планируемые уровни сформированности компетенций обучающихся и критерии оценивания

Уровни	Содержательное описание уровня	Основные признаки выделения уровня (этапы формирования компетенции, критерии оценки сформированности)	Пятибалльная шкала (академическая) оценка	Двухбалльная шакала, зачет	БРС, % освоения (рейтинговая оценка)
Повышенный	Творческая деятельность	*Включает нижестоящий уровень.* Умение самостоятельно принимать решение, решать проблему/задачу теоретического и прикладного характера на основе изученных методов, приемов, технологий	отлично	зачтено	86-100
Базовый	Применение знаний и умений в более широких контекстах учебной и профессиональной деятельности, нежели по образцу с большей степени самостоятельности и инициативы	*Включает нижестоящий уровень.* Способность собирать, систематизировать, анализировать и грамотно использовать информацию из самостоятельно найденных теоретических источников и иллюстрировать ими теоретические положения или обосновывать практику применения	хорошо		71-85
Удовлетворительный (достаточный)	Репродуктивная деятельность	Изложение в пределах задач курса теоретически и практически контролируемого материала	удовлетворительно		55-70

Недостаточный	Отсутствие признаков удовлетворительного уровня	неудовлетворительно	не зачтено	Менее 55

9. Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины.

Основная литература

1. Голицына, О. Л. Базы данных : учебное пособие / О. Л. Голицына, Н. В. Максимов, И. И. Попов. — 4-е изд., перераб. и доп. — Москва : ФОРУМ : ИНФРА-М, 2020. — 400 с. — (Высшее образование: Бакалавриат). - ISBN 978-5-00091-516-5. - Текст : электронный. - URL: https://znanium.com/catalog/product/1053934 (дата обращения: 11.01.2022). – Режим доступа: по подписке.
2. Шаньгин, В. Ф. Комплексная защита информации в корпоративных системах : учебное пособие / В. Ф. Шаньгин. — Москва : ФОРУМ : ИНФРА-М, 2020. — 592 с. - ISBN 978-5-8199-0730-6. - Текст : электронный. - URL: https://znanium.com/catalog/product/1093695 **(online)**

Дополнительная литература

1. Агальцов, В. П. Базы данных : в 2 книгах. Книга 2. Распределенные и удаленные базы данных : учебник / В.П. Агальцов. — Москва : ФОРУМ : ИНФРА-М, 2021. — 271 с. — (Высшее образование: Бакалавриат). - ISBN 978-5-8199-0713-9. - Текст : электронный. - URL: https://znanium.com/catalog/product/1514118 (дата обращения: 11.01.2022). – Режим доступа: по подписке.
2. Шаньгин, В. Ф. Информационная безопасность компьютерных систем и сетей : учебное пособие / В.Ф. Шаньгин. — Москва : ФОРУМ : ИНФРА-М, 2020. — 416 с. - ISBN 978-5-8199-0754-2. - Текст : электронный. - URL: https://znanium.com/catalog/product/1093657 **(online)**
3. Бирюков, А. А. Информационная безопасность: защита и нападение / А.А. Бирюков. - 2-е изд., перераб. и доп. - Москва : ДМК Пресс, 2017. - 434 с. - ISBN 978-5-97060-435-9. - Текст : электронный. - URL: https://znanium.com/catalog/product/1028060 **(online)**

10. Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины (модуля).

- НЭБ Национальная электронная библиотека, диссертации и прочие издания
- eLIBRARY.RU Научная электронная библиотека, книги, статьи, тезисы докладов конференций
- Гребенников Электронная библиотека ИД журналы
- ЭБС Лань книги, журналы
- ЭБС Консультант студента
- ПРОСПЕКТ ЭБС
- ЭБС ZNANIUM.COM
- РГБ Информационное обслуживание по МБА
- БЕН РАН
- Электронно-библиотечная система (ЭБС) Кантитана (https://elib.kantiana.ru/)
- База уязвимостей CVE (https://cve.mitre.org).
- База уязвимостей NVD (https://nvd.nist.gov).
- База уязвимостей и эксплойтов (www.exploit-db.com).

– Курс по системе Metasploit от Offensive Security (https://www.offensive-security.com/metasploit-unleashed/)

11. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине.

Программное обеспечение обучения включает в себя:

– система электронного образовательного контента БФУ им. И. Канта – www.lms-3.kantiana.ru, обеспечивающую разработку и комплексное использование электронных образовательных ресурсов;
– серверное программное обеспечение, необходимое для функционирования сервера и связи с системой электронного обучения через Интернет;
– корпоративная платформа Microsoft Teams;
– установленное на рабочих местах студентов ПО: Microsoft Windows 7-11.
– специализированное ПО:
– Свободно распространяемая версия проигрывателя виртуальных машин (актуальная версия Oracle Virtual Box или VMware Workstation Player).
– Свободно распространяемая версия СУБД «Oracle XE» версии 11 или выше.
– Свободно распространяемая версия Oracle SQL Developer.

12. Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине.

Для проведения занятий лекционного типа, практических и семинарских занятий используются специальные помещения (учебные аудитории), оборудованные техническими средствами обучения – мультимедийной проекционной техникой. Для проведения занятий лекционного типа используются наборы демонстрационного оборудования.

Для проведения лабораторных работ, (практических занятий – при необходимости) используются специальные помещения (учебные аудитории), оснащенные специализированным лабораторным оборудованием: персональными компьютерами с возможностью выхода в интернет и с установленным программным обеспечением, заявленным в п.11.

Для проведения групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации используются специальные помещения (учебные аудитории), оборудованные специализированной мебелью (для обучающихся), меловой / маркерной доской.

Для организации самостоятельной работы обучающимся предоставляются помещения, оснащенные компьютерной техникой с возможностью подключения к сети «Интернет» и обеспечением доступа в электронную информационно-образовательную среду университета.

Для обучения инвалидов и лиц с ограниченными возможностями здоровья университетом могут быть представлены специализированные средства обучения, в том числе технические средства коллективного и индивидуального пользования.

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
федеральное государственное автономное образовательное учреждение высшего образования «Балтийский федеральный университет имени Иммануила Канта»
Институт физико-математических наук и информационных технологий

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

«Защита данных в государственных информационных системах»

Шифр: 10.05.01
Специальность: «Компьютерная безопасность»
Специализация: «Математические методы защиты информации»
Квалификация (степень) выпускника: Специалист по защите информации

Калининград
2022

Лист согласования

Составитель: старший преподаватель Института физико-математических наук и информационных технологий ***Козьминых Е.В***.

Рабочая программа утверждена на заседании учебно-методического совета института физико-математических наук и информационных технологий
Протокол № 01/22 от «01» февраля 2022 г.

Председатель учебно-методического совета института физико-математических наук и информационных технологий
Первый заместитель директора ИФМНиИТ, к. ф.-м. н., доцент — Шпилевой А. А

Ведущий менеджер — Е.П.Ставицкая

Содержание

1.Наименование дисциплины: «Защита данных в государственных информационных системах».

Целью изучения дисциплины «Защита данных в государственных информационных системах» является теоретическая и практическая подготовка специалистов к деятельности, связанной с комплексным анализом возможных угроз и созданием адекватной модели нарушителя, постановкой конкретных задач заданной степени сложности в рамках модели для обеспечения информационной безопасности автоматизированных систем, относящихся к категории государственных информационных систем, а также содействие фундаментализации образования и развитию системного мышления.

Необходимость изучения дисциплины следует из необходимости формирования у обучающихся базы для практического применения полученных знаний исходя из необходимости подготовки специалистов для работы в государственных и муниципальных органах, формированию мотивации к профессиональной деятельности, основ профессиональной этики.

Основные **задачи** изучения дисциплины:

-формирование у обучаемых понимания терминологии в области защиты информации государственных информационных систем;

-овладение методами классификации информационных систем, оценки угроз информационной безопасности, выбора средств защиты информации, на основе соотнесения обязательных требований по защите с учетом актуальных угроз;

-формирование понимания социальной значимости своей профессии в части защиты интересов личности, общества и государства, мотивации к выполнению профессиональной деятельности.

2. Перечень планируемых результатов обучения по дисциплине, соотнесенных с планируемыми результатами освоения образовательной программы

Код компетенции	Результаты освоения образовательной программы (ИДК)	Результаты обучения по дисциплине
ОПК-1. Способен оценивать роль информации, информационных технологий и информационной безопасности в современном обществе, их значение для обеспечения объективных потребностей личности, общества и государства;	ОПК.1.1. Демонстрирует знания понятия информации, информационной безопасности, место и роль информационной безопасности в системе национальной безопасности Российской Федерации, основы государственной информационной политики; ОПК.1.2. Демонстрирует знание основных средств и способов обеспечения информационной безопасности, принципов	**Знать**: место и роль информационной безопасности в системе национальной безопасности Российской Федерации, основы государственной информационной политики, стратегию развития информационного общества в России **Уметь**: классифицировать защищаемую информацию по видам тайны и степеням конфиденциальности **Владеть**: профессиональной терминологией в области информационной безопасности

	построения систем защиты информации; ОПК.1.3. Классифицирует защищаемую информацию по видам тайны и степеням конфиденциальности; классифицирует и оценивает угрозы информационной безопасности для объекта информатизации;	
ОПК-5. Способен применять нормативные правовые акты, нормативные и методические документы, регламентирующие деятельность по защите информации;	ОПК-5.1. Демонстрирует знание нормативных правовых актов, нормативных и методических документов, регламентирующих деятельность по защите информации в организации; классифицирует и оценивает угрозы информационной безопасности для объекта информатизации. ОПК-5.2. Формулирует основные требования по защите конфиденциальной информации, персональных данных и охране результатов интеллектуальной деятельности в организации ОПК-5.3. Анализирует и разрабатывает проекты локальных правовых актов, инструкций, регламентов и организационно-распорядительных документов, регламентирующих работу по обеспечению информационной безопасности в организации.	**Знать:** законодательство Российской Федерации, государственные стандарты и нормативные документы по защите информации, основные общеметодологические принципы теории информационной безопасности применительно к защите государственных информационных систем **Уметь**: систематизировать информацию, формулировать требования к защищаемым системам на основе требований нормативных и правовых документов **Владеть**: средствами поиска, методами обобщения нормативных и методических материалов в сфере своей профессиональной деятельности
ОПК-6. Способен при решении профессиональных задач организовывать защиту информации ограниченного доступа в компьютерных системах и сетях в соответствии с нормативными	ОПК-6.1. Понимает угрозы безопасности информации и возможные пути их реализации, нормативные правовые акты, нормативные и методические документы Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю. ОПК-6.2. Способен организовать защиту информации ограниченного	**Знать**: стандарты и нормативные документы по защите информации, в том числе нормативные правовые акты и нормативные методические документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю применительно к организации защиты государственных информационных систем

правовыми актами и нормативными методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю;	доступа в соответствии с нормативными правовыми актами, нормативными и методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю. ОПК-6.3. Обладает навыками организации защиты информации ограниченного доступа в соответствии с нормативными правовыми актами, нормативными и методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю.	**Уметь**: систематизировать информацию, формулировать требования к защищаемым государственным информационным системам на основе требований нормативных и правовых документов, организовать выбор, внедрение и эксплуатацию средств защиты информации, аттестацию по требованиям безопасности **Владеть**: средствами поиска, обобщения научно-технической информации, нормативных и методических материалов, опыта в сфере своей профессиональной деятельности, разработки инструкций администраторам и пользователям государственных информационных систем
ОПК-2.3 Способен проводить сравнительный анализ и осуществлять обоснованный выбор программных и программно-аппаратных средств защиты информации с учетом реализованных в них математических методов;	ОПК-2.3.1. Знает теоретико-числовые методы и алгоритмы, применяемые в средствах защиты информации. ОПК-2.3.2. Осуществляет обоснованный выбор программных и программно-аппаратных средств защиты информации с учетом реализованных в них математических методов. ОПК-2.3.3. Владеет методами анализа существующих методов и средств, применяемых для контроля и защиты информации.	**Знать**: классификацию средств защиты информации, условия сертификации средств защиты информации, требования по выбору средств защиты информации в соответствии с установленным классом государственной информационной системы **Уметь**: разрабатывать модели угроз и нарушителя информационных систем, оценивать эффективность средств и методов защиты информации, определять причины, виды, источники и каналы утечки, искажения информации, оценить степень надежности системы защиты, проводить обоснование и выбор рационального решения по выбору программных и программно-аппаратных средств защиты информации с учетом реализованных в них математических методов **Владеть**: практическими умениями разработки и ведения технической документации информационных систем, настройки средств защиты информации применительно в установленному классу системы

3. Место дисциплины в структуре образовательной программы

Дисциплина «Защита данных в государственных информационных системах» представляет собой дисциплину базовой части Блока 1 Дисциплины (модули) подготовки студентов.

4. Виды учебной работы по дисциплине.

Виды учебной работы по дисциплине зафиксированы учебным планом основной профессиональной образовательной программы по указанному направлению и профилю, выражаются в академических часах. Часы контактной работы и самостоятельной работы студента и часы, отводимые на процедуры контроля, могут различаться в учебных планах ОПОП по формам обучения. Объем контактной работы включает часы контактной аудиторной работы (лекции/практические занятия/ лабораторные работы), контактной внеаудиторной работы (контроль самостоятельной работы), часы контактной работы в период аттестации. Контактная работа, в том числе может проводиться посредством электронной информационно-образовательной среды университета с использованием ресурсов сети Интернет и дистанционных технологий

5. Содержание дисциплины, структурированное по темам (разделам)

Исходя из рамок, установленных учебным планом по трудоемкости и видам учебной работы по дисциплине, преподаватель самостоятельно выбирает тематику занятий по формам и количеству часов проведения контактной работы: лекции и иные учебные занятия, предусматривающие преимущественную передачу учебной информации преподавателем и (или) занятия семинарского типа (семинары, практические занятия, практикумы, лабораторные работы, коллоквиумы и иные аналогичные занятия), и (или) групповые консультации, и (или) индивидуальную работу обучающихся с преподавателем, в том числе индивидуальные консультации (по курсовым работам/проектам – при наличии курсовой работы/проекта по данной дисциплине в учебном плане). Рекомендуемая тематика занятий максимально полно реализуется в контактной работе со студентами очной формы обучения. В случае реализации образовательной программы в заочной / очно-заочной форме трудоемкость дисциплины сохраняется, однако объем учебного материала в значительной части осваивается студентами в форме самостоятельной работы. При этом требования к ожидаемым образовательным результатам студентов по данной дисциплине не зависят от формы реализации образовательной программы.

№ п/п	Наименование темы	Содержание темы
1	Информационная безопасность в системе национальной безопасности Российской Федерации. Стандарты в области защиты информации государственных информационных систем	Основные положения Доктрины информационной безопасности РФ. Национальные интересы РФ. Угрозы информационной безопасности РФ. Источники угроз информационной безопасности РФ. Государственная система защиты информации. Стратегия национальной безопасности Российской Федерации до 2030 года. Стратегия развития информационного общества в РФ. Виды информации, подлежащей защите. Классификация факторов, воздействующих на защищаемую информацию (ГОСТ Р 51275-2006). Практические правила управления информационной безопасностью (ГОСТ Р ИСО/МЭК 17799-2005). Задачи и функции подразделений по защите информации государственного органа.

№ п/п	Наименование темы	Содержание темы
2	Классификация государственных информационных систем. Угрозы безопасности информационных систем. Модели угроз и нарушителя.	Федеральный закон от 27.07.2006 N 149-ФЗ "Об информации, информационных технологиях и о защите информации". Постановлением от 06 июля 2015г. №676 утверждены «Требования к порядку создания, развития, ввода в эксплуатацию, эксплуатации и вывода из эксплуатации государственных информационных систем и дальнейшего хранения содержащейся в их базах данных информации. Классификация государственных информационных систем. Угрозы безопасности информационных систем. Классификация угроз. Модели нарушителя и типичные атаки. Анализ рисков. Модель действий вероятного нарушителя и модель угроз. Классификация основных видов атак. Сетевая (компьютерная) разведка. Примеры сетевых атак.
3	Защита информации в государственных информационных системах от утечки по техническим каналам.	Технические каналы утечки информации. Характеристика канала утечки информации за счет ПЭМИН. Классификация электронных устройств перехвата информации, а том числе внедряемых в средства вычислительной техники. Средства и методы защиты от утечки по техническим каналам.
4	Методы и средства защиты информации в государственных информационных системах. Сертификация средств защиты информации. Выбор средств защиты информации, настройка механизмов защиты информации в соответствии с классом информационной системы.	Основные принципы создания комплексных систем защиты информации. Обзор средств и методов информационной/компьютерной безопасности. Модели управления доступом. Контроль прав доступа. Классификация и требования к настройке механизмов средств защиты информации, применяемым в государственных информационных системах: - программных и программно-технических средств защиты информации от несанкционированного доступа; - антивирусных средств защиты информации; - межсетевых экранов; - средств криптографической защиты информации; - средств создания и проверки электронной подписи; - средств обнаружения атак (вторжений); - средств защиты среды виртуализации; - средств контроля за действиями пользователей; - средств анализа защищенности.
5	Порядок аттестации государственных информационных систем по требованиям безопасности информации. Ведение технической документации.	Порядок аттестации государственных информационных систем по требованиям безопасности информации. Ведение технической документации.

6. Рекомендуемая тематика учебных занятий в форме контактной работы

Рекомендуемая тематика учебных занятий *лекционного* типа (предусматривающих преимущественную передачу учебной информации преподавателями):

№	Тема лекции
1	**Тема 1.** Информационная безопасность в системе национальной безопасности Российской Федерации. Стандарты в области защиты информации государственных информационных систем
2	**Тема 2.** Классификация государственных информационных систем. Угрозы безопасности информационных систем. Модели угроз и нарушителя.
3	**Тема 3.** Защита информации в государственных информационных системах от утечки по техническим каналам.
4	**Тема 4.** Методы и средства защиты информации в государственных информационных системах. Сертификация средств защиты информации. Выбор средств защиты информации, настройка механизмов защиты информации в соответствии с классом информационной системы.
5	**Тема 5.** Порядок аттестации государственных информационных систем по требованиям безопасности информации. Ведение технической документации.

Рекомендуемая тематика *практических* занятий:

№ п/п	Наименование Темы	Содержание темы
1	Информационная безопасность в системе национальной безопасности Российской Федерации. Стандарты в области защиты информации государственных информационных систем	Получение актуальной информации с официального сайта ФСТЭК России (перечень органов по аттестации, реестр аккредитованных ФСТЭК России органов по сертификации и испытательных лабораторий и государственный реестр сертифицированных средств защиты информации). Перечень средств защиты информации, сертифицированных ФСБ России (сайт ФСБ России). Разработка Политики информационной безопасности организации.
2	Классификация государственных информационных систем. Угрозы безопасности информационных систем. Модели угроз и нарушителя.	Определение класса государственной информационной системы по ее описанию. Разработка модели угроз. Определение актуальных угроз. Разработка модели нарушителя.
3	Защита информации в государственных информационных системах от утечки по техническим каналам.	Работа с банком данных угроз безопасности информации (сайт ФСТЭК России).
4	Методы и средства защиты информации в государственных информационных системах. Сертификация средств	Настройка средств и систем защиты информации в соответствии с требованиями к государственным информационным системам соответствующего класса: - программных и программно-технических средств защиты информации от несанкционированного доступа; - антивирусных средств защиты информации;

№ п/п	Наименование Темы	Содержание темы
	защиты информации. Выбор средств защиты информации, настройка механизмов защиты информации в соответствии с классом информационной системы.	- межсетевых экранов; - средств криптографической защиты информации; - средств создания и проверки электронной подписи; - средств обнаружения атак (вторжений); - средств защиты среды виртуализации; - средств контроля за действиями пользователей; - средств анализа защищенности.
5	Порядок аттестации государственных информационных систем по требованиям безопасности информации. Ведение технической документации.	Ведение технической документации государственной информационной системы: журналов, перечней и т.п., разработка инструкций пользователей и администраторов.

Руководствуясь положениями статьи 47 и статьи 48 Федерального закона от 29 декабря 2012 г. N 273-ФЗ «Об образовании в Российской Федерации» научно-педагогические работники и иные лица, привлекаемые университетом к реализации данной образовательной программы, пользуются предоставленными академическими правами и свободами в части свободы преподавания, свободы от вмешательства в профессиональную деятельность; свободы выбора и использования педагогически обоснованных форм, средств, методов обучения и воспитания; права на творческую инициативу, разработку и применение авторских программ и методов обучения и воспитания в пределах реализуемой образовательной программы и отдельной дисциплины.

Исходя из рамок, установленных учебным планом по трудоемкости и видам учебной работы по дисциплине, преподаватель самостоятельно выбирает тематику занятий по формам и количеству часов проведения контактной работы: лекции и иные учебные занятия, предусматривающие преимущественную передачу учебной информации преподавателем и (или) занятия семинарского типа (семинары, практические занятия, практикумы, лабораторные работы, коллоквиумы и иные аналогичные занятия), и (или) групповые консультации, и (или) индивидуальную работу обучающихся с преподавателем, в том числе индивидуальные консультации (по курсовым работам/проектам – при наличии курсовой работы/проекта по данной дисциплине в учебном плане).

Рекомендуемая тематика занятий максимально полно реализуется в контактной работе со студентами очной формы обучения. В случае реализации образовательной программы в заочной / очно-заочной форме трудоемкость дисциплины сохраняется, однако объем учебного материала в значительной части осваивается студентами в форме самостоятельной работы. При этом требования к ожидаемым образовательным результатам студентов по данной дисциплине не зависят от формы реализации образовательной программы.

7. Методические рекомендации по видам занятий

Лекционные занятия.

В ходе лекционных занятий обучающимся рекомендуется выполнять следующие действия. Вести конспектирование учебного материала. Обращать внимание на категории, формулировки, раскрывающие содержание тех или иных явлений и процессов, научные

выводы и практические рекомендации по их применению. Задавать преподавателю уточняющие вопросы с целью уяснения теоретических положений, разрешения спорных ситуаций.

Желательно оставить в рабочих конспектах поля, на которых во внеаудиторное время можно сделать пометки из рекомендованной литературы, дополняющие материал прослушанной лекции, а также подчеркивающие особую важность тех или иных теоретических положений.

Практические и семинарские занятия.

На практических и семинарских занятиях в зависимости от темы занятия выполняется поиск информации по решению проблем, практические упражнения, контрольные работы, выработка индивидуальных или групповых решений, итоговое обсуждение с обменом знаниями, участие в круглых столах, разбор конкретных ситуаций, командная работа, представление портфолио и т.п.

Самостоятельная работа.

Самостоятельная работа осуществляется в виде изучения литературы, эмпирических данных по публикациям и конкретных ситуаций из практики, подготовке индивидуальных работ, работа с лекционным материалом, самостоятельное изучение отдельных тем дисциплины; поиск и обзор литературы и электронных источников; чтение и изучение учебника и учебных пособий.

8. Фонд оценочных средств

8.1. Перечень компетенций с указанием этапов их формирования в процессе освоения образовательной программы в рамках учебной дисциплины

Основными этапами формирования указанных компетенций при изучении обучающимися дисциплины являются последовательное изучение содержательно связанных между собой тем учебных занятий. Изучение каждой темы предполагает овладение обучающимися необходимыми компетенциями. Результат аттестации обучающихся на различных этапах формирования компетенций показывает уровень освоения компетенций.

Контролируемые разделы (темы) дисциплины	Индекс контроли-руемой компетенции (или её части)	Оценочные средства по этапам формирования компетенций
		текущий контроль по дисциплине
Тема 1. Информационная безопасность в системе национальной безопасности Российской Федерации. Стандарты в области защиты информации государственных информационных систем	***ОПК-1***	Устный опрос, выполнение практических заданий
Тема 2. Классификация государственных информационных систем. Угрозы безопасности информационных систем. Модели угроз и нарушителя.	***ОПК-5*** ***ОПК-6***	Устный опрос, выполнение практических заданий
Тема 3. Защита информации в государственных	***ОПК-6*** ***ОПК-2.3***	Устный опрос, выполнение практических заданий

Контролируемые разделы (темы) дисциплины	Индекс контроли-руемой компетенции (или её части)	Оценочные средства по этапам формирования компетенций
		текущий контроль по дисциплине
информационных системах от утечки по техническим каналам.		
Тема 4. Методы и средства защиты информации в государственных информационных системах. Сертификация средств защиты информации. Выбор средств защиты информации, настройка механизмов защиты информации в соответствии с классом информационной системы.	***ОПК-5*** ***ОПК-6*** ***ОПК-2.3***	Устный опрос, выполнение практических заданий
Тема 5. Порядок аттестации государственных информационных систем по требованиям безопасности информации. Ведение технической документации.	***ОПК-5*** ***ОПК-6***	

8.2. Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений и навыков и (или) опыта деятельности процессе текущего контроля

Типовые вопросы для устного опроса:

Тема 1. Информационная безопасность в системе национальной безопасности Российской Федерации. Стандарты в области защиты информации государственных информационных систем.

	Вопрос
Оценка «зачтено» - пороговый уровень освоения компетенции	Перечислить основные законодательные акты и ведомства, регулирующие сферу информационной безопасности Российской Федерации.
Оценка «зачтено» - достаточный уровень освоения компетенции	Перечислить основные законодательные акты и примерные разделы документов. Описать построение государственной системы защиты информации. Перечислить основные функции подразделений информационной безопасности государственных органов.
Оценка «зачтено» - высокий уровень освоения компетенции	Перечислить основные законодательные акты и разделы документов, стандарты по обеспечению информационной безопасности. Описать построение государственной системы защиты информации. Перечислить функции подразделений информационной безопасности государственных органов.

Тема 2. **Классификация государственных информационных систем. Угрозы безопасности информационных систем. Модели угроз и нарушителя.**

	Вопрос
Оценка «зачтено» - пороговый уровень освоения компетенции	Перечислить критерии классификации государственных информационных систем, угроз безопасности.
Оценка «зачтено» - достаточный уровень освоения компетенции	Перечислить критерии классификации государственных информационных систем, угроз безопасности. Описать принципы построения модели угроз и модели нарушителя.
Оценка «зачтено» - высокий уровень освоения компетенции	Перечислить критерии классификации государственных информационных систем, угроз безопасности. Описать принципы построения модели угроз и модели нарушителя, понятия актуальности угрозы, типов нарушителей.

Тема 4. Методы и средства защиты информации в государственных информационных системах. Сертификация средств защиты информации. Выбор средств защиты информации, настройка механизмов защиты информации в соответствии с классом информационной системы.

	Вопрос
Оценка «зачтено» - пороговый уровень освоения компетенции	Перечислить Методы и средства защиты информации в государственных информационных системах, порядок сертификация средств защиты информации.
Оценка «зачтено» - достаточный уровень освоения компетенции	Перечислить Методы и средства защиты информации в государственных информационных системах, порядок сертификация средств защиты информации, сопоставление классов средств защиты информации и класса информационной системы.
Оценка «зачтено» - высокий уровень освоения компетенции	Перечислить Методы и средства защиты информации в государственных информационных системах, порядок сертификация средств защиты информации, сопоставление классов средств защиты информации и класса информационной системы. Описать практическую настройку выбранного типа средства защиты информации.

Тема 4. Методы и средства защиты информации в государственных информационных системах. Сертификация средств защиты информации. Выбор средств защиты информации, настройка механизмов защиты информации в соответствии с классом информационной системы.

	Вопрос
Оценка «зачтено» - пороговый уровень освоения компетенции	Привести классификацию средств защиты информации, принципы их выбора для применения в государственной информационной системы.
Оценка «зачтено» - достаточный уровень освоения компетенции	Привести классификацию средств защиты информации, математические модели работы, принципы их функционирования, выбора для применения в государственной информационной системы.
Оценка «зачтено» - высокий уровень освоения компетенции	Привести классификацию средств защиты информации, математические модели работы, принципы их функционирования, выбора для применения в государственной информационной системы. Описать практическую настройку выбранного типа средства защиты информации.

8.3. Перечень вопросов и заданий для промежуточной аттестации по дисциплине

1. Основные положения Доктрины информационной безопасности РФ. Национальные интересы РФ. Угрозы информационной безопасности РФ.
2. Источники угроз информационной безопасности РФ. Государственная система защиты информации.
3. Стратегия национальной безопасности Российской Федерации до 2030 года.
4. Стратегия развития информационного общества в РФ.
5. Виды информации, подлежащей защите.
6. Классификация факторов, воздействующих на защищаемую информацию (ГОСТ Р 51275-2006).
7. Практические правила управления информационной безопасностью (ГОСТ Р ИСО/МЭК 17799-2005).
8. Задачи и функции подразделений по защите информации государственного органа.
9. Федеральный закон от 27.07.2006 N 149-ФЗ "Об информации, информационных технологиях и о защите информации".
10. Постановление правительства от 6 июля 2015г. №676 «Об утверждении требований к порядку создания, развития, ввода в эксплуатацию, эксплуатации и вывода из эксплуатации государственных информационных систем и дальнейшего хранения содержащейся в их базах данных информации.
11. Классификация государственных информационных систем.
12. Угрозы безопасности информационных систем. Классификация угроз.
13. Модели нарушителя и типичные атаки.
14. Анализ рисков.
15. Модель действий вероятного нарушителя и модель угроз.
16. Классификация основных видов атак.
17. Сетевая (компьютерная) разведка. Примеры сетевых атак.
18. Технические каналы утечки информации. Характеристика канала утечки информации за счет ПЭМИН.
19. Классификация электронных устройств перехвата информации, а том числе внедряемых в средства вычислительной техники.
20. Средства и методы защиты от утечки по техническим каналам.
21. Основные принципы создания комплексных систем защиты информации. Обзор средств и методов информационной/компьютерной безопасности. Модели управления доступом. Контроль прав доступа.
22. - 30. Классификация и требования к настройке механизмов средств защиты информации, применяемым в государственных информационных системах:

- программных и программно-технических средств защиты информации от несанкционированного доступа;

- антивирусных средств защиты информации;

- межсетевых экранов;

- средств криптографической защиты информации;

- средств создания и проверки электронной подписи;

- средств обнаружения атак (вторжений);

- средств защиты среды виртуализации;

- средств контроля за действиями пользователей;

- средств анализа защищенности.

31. Порядок аттестации государственных информационных систем по требованиям безопасности информации.

32. Ведение технической документации.

8.4. Планируемые уровни сформированности компетенций обучающихся и критерии оценивания

Уровни	Содержательное описание уровня	Основные признаки выделения уровня (этапы формирования компетенции, критерии оценки сформированности)	Пятибалльная шкала (академическая) оценка	Двухбалльная шакала, зачет	БРС, % освоения (рейтинговая оценка)
Повышенный	Творческая деятельность	*Включает нижестоящий уровень.* Умение самостоятельно принимать решение, решать проблему/задачу теоретического и прикладного характера на основе изученных методов, приемов, технологий	отлично	зачтено	86-100
Базовый	Применение знаний и умений в более широких контекстах учебной и профессиональной деятельности, нежели по образцу с большей степени самостоятельности и инициативы	*Включает нижестоящий уровень.* Способность собирать, систематизировать, анализировать и грамотно использовать информацию из самостоятельно найденных теоретических источников и иллюстрировать ими теоретические положения или обосновывать практику применения	хорошо		71-85

Удовлетворительный (достаточный)	Репродуктивная деятельность	Изложение в пределах задач курса теоретически и практически контролируемого материала	удовлетворительно		55-70
Недостаточный	Отсутствие признаков удовлетворительного уровня		неудовлетворительно	не зачтено	Менее 55

9. Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины.

Основная литература

1. Организационное и правовое обеспечение информационной безопасности [Электронный ресурс] : учеб. и практикум для бакалавриата и магистратуры / [Т. А. Полякова [и др.] ; под ред.: Т. А. Поляковой, А. А. Стрельцова, 2019. - 1 on-line, 325 с. ЭБС Кантиана
2. Шаньгин, В. Ф. Комплексная защита информации в корпоративных системах : учебное пособие / В. Ф. Шаньгин. — Москва : ФОРУМ : ИНФРА-М, 2020. — 592 с. - ISBN 978-5-8199-0730-6. - Текст : электронный. - URL: https://znanium.com/catalog/product/1093695 **(online)**

Дополнительная литература

1. Проскурин, В. Г. Защита в операционных системах: Учебное пособие для вузов / В.Г. Проскурин. - Москва : Гор. линия-Телеком, 2014. - 192 с.: ил.; . - (Специальность). ISBN 978-5-9912-0379-1, 500 экз. - Текст : электронный. - URL: https://znanium.com/catalog/product/461004 ЭБС Znanium(1)
2. Шаньгин, В. Ф. Информационная безопасность компьютерных систем и сетей : учебное пособие / В.Ф. Шаньгин. — Москва : ФОРУМ : ИНФРА-М, 2020. — 416 с. - ISBN 978-5-8199-0754-2. - Текст : электронный. - URL: https://znanium.com/catalog/product/1093657 **(online)**
3. Бирюков, А. А. Информационная безопасность: защита и нападение / А.А. Бирюков. - 2-е изд., перераб. и доп. - Москва : ДМК Пресс, 2017. - 434 с. - ISBN 978-5-97060-435-9. - Текст : электронный. - URL: https://znanium.com/catalog/product/1028060 **(online)**

10. Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины (модуля).

- НЭБ Национальная электронная библиотека, диссертации и прочие издания
- eLIBRARY.RU Научная электронная библиотека, книги, статьи, тезисы докладов конференций
- Гребенников Электронная библиотека ИД журналы
- ЭБС Лань книги, журналы
- ЭБС Консультант студента
- ПРОСПЕКТ ЭБС
- ЭБС ZNANIUM.COM
- РГБ Информационное обслуживание по МБА
- БЕН РАН

- Электронно-библиотечная система (ЭБС) Кантитана (https://elib.kantiana.ru/)
- База уязвимостей CVE (https://cve.mitre.org).
- База уязвимостей NVD (https://nvd.nist.gov).
- База уязвимостей и эксплойтов (www.exploit-db.com).
- Курс по системе Metasploit от Offensive Security (https://www.offensive-security.com/metasploit-unleashed/)

11. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине.

Программное обеспечение обучения включает в себя:

- система электронного образовательного контента БФУ им. И. Канта – www.lms-3.kantiana.ru, обеспечивающую разработку и комплексное использование электронных образовательных ресурсов;
- серверное программное обеспечение, необходимое для функционирования сервера и связи с системой электронного обучения через Интернет;
- корпоративная платформа Microsoft Teams;
- установленное на рабочих местах студентов ПО: Microsoft Windows 7-11.
- специализированное ПО:
- Свободно распространяемая версия проигрывателя виртуальных машин (актуальная версия Oracle Virtual Box или VMware Workstation Player).
- Свободно распространяемая версия СУБД «Oracle XE» версии 11 или выше.
- Свободно распространяемая версия Oracle SQL Developer.

12. Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине.

Для проведения занятий лекционного типа, практических и семинарских занятий используются специальные помещения (учебные аудитории), оборудованные техническими средствами обучения – мультимедийной проекционной техникой. Для проведения занятий лекционного типа используются наборы демонстрационного оборудования.

Для проведения лабораторных работ, (практических занятий – при необходимости) используются специальные помещения (учебные аудитории), оснащенные специализированным лабораторным оборудованием: персональными компьютерами с возможностью выхода в интернет и с установленным программным обеспечением, заявленным в п.11.

Для проведения групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации используются специальные помещения (учебные аудитории), оборудованные специализированной мебелью (для обучающихся), меловой / маркерной доской.

Для организации самостоятельной работы обучающимся предоставляются помещения, оснащенные компьютерной техникой с возможностью подключения к сети «Интернет» и обеспечением доступа в электронную информационно-образовательную среду университета.

Для обучения инвалидов и лиц с ограниченными возможностями здоровья университетом могут быть представлены специализированные средства обучения, в том числе технические средства коллективного и индивидуального пользования.

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
федеральное государственное автономное образовательное учреждение высшего образования «Балтийский федеральный университет имени Иммануила Канта»
Институт физико-математических наук и информационных технологий

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

«Основы машинного обучения»

Шифр: 10.05.01
Специальность: «Компьютерная безопасность»
Специализация: «Математические методы защиты информации»
Квалификация (степень) выпускника: специалист по защите информации

Калининград
2022

Лист согласования

Составитель: Ширкин А., ассистент

Рабочая программа утверждена на заседании учебно-методического совета института физико-математических наук и информационных технологий

Протокол № 01/22 от «01» февраля 2022 г.

Председатель учебно-методического совета института физико-математических наук и информационных технологий
Первый заместитель директора ИФМНиИТ, к. ф.-м. н., доцент — Шпилевой А. А

Ведущий менеджер — Е.П.Ставицкая

Содержание

1.Наименование дисциплины: «Основы машинного обучения»

Целью дисциплины «Основы машинного обучения» является формирование у студентов теоретических знаний и практических навыков по основам машинного обучения, овладение студентами инструментарием, моделями и методами машинного обучения, а также приобретение навыков исследователя.

2. Перечень планируемых результатов обучения по дисциплине, соотнесенных с планируемыми результатами освоения образовательной программы

Код компетенции	Результаты освоения образовательной программы (ИДК)	Результаты обучения по дисциплине
УК-1. Способен осуществлять критический анализ проблемных ситуаций на основе системного подхода, вырабатывать стратегию действий	УК.1.1. Анализирует проблемную ситуацию как систему, выявляя ее составляющие и связи между ними. УК.1.2. Критически оценивает надежность источников информации, работает с противоречивой информацией из разных источников. УК.1.3. Разрабатывает и содержательно аргументирует стратегию решения проблемной ситуации на основе системного и междисциплинарных подходов.	В результате освоения дисциплины студент должен: − Знать ключевые понятия, цели и задачи использования машинного обучения; методологические основы применения алгоритмов машинного обучения. − Уметь визуализировать результаты работы алгоритмов машинного обучения, выбирать метод машинного обучения, соответствующий исследовательской задаче, интерпретировать полученные результаты. − Иметь навыки (приобрести опыт) чтения и анализа академической литературы по применению методов машинного обучения, построения и оценки качества моделей.
ПКС-4 Способность осуществлять подбор, изучение и обобщение научно-технической информации, методических материалов отечественного и зарубежного опыта по проблемам компьютерной безопасности, а также нормативных	ПКС-4.1. Осуществляет подбор, изучение и обобщение научно-технической информации, методических материалов отечественного и зарубежного опыта по проблемам компьютерной безопасности. ПКС-4.2. Знает основные руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации. ПКС-4.3. Применяет действующую законодательную базу в	В результате освоения дисциплины обучающийся должен: Знать: - принципы построения векторов признаков, решающих правил и классификации; - основные виды классификаторов; - принципы построения линейных классификаторов; - принципы построения нелинейных классификаторов; - особенности выбора признаков классификации и предварительной обработки данных. Уметь: - выбирать подходящий вид классификатора в зависимости от решаемой задачи;

правовых актов в сфере профессиональной деятельности	области обеспечения защиты информации.	- выбирать набор признаков для классификации и проводить предварительную обработку данных; - уметь применять алгоритмы построения и обучения классификатора по выборке. Владеть: - навыками выбора, построения, обучения и использования основных классификаторов при решении задач

3. Место дисциплины в структуре образовательной программы

«Основы машинного обучения» представляет собой факультативную дисциплину (ФТД.01) части, формируемой участниками образовательных отношений подготовки студентов.

4. Виды учебной работы по дисциплине.

Виды учебной работы по дисциплине зафиксированы учебным планом основной профессиональной образовательной программы по указанному направлению и профилю, выражаются в академических часах. Часы контактной работы и самостоятельной работы обучающегося и часы, отводимые на процедуры контроля, могут различаться в учебных планах ОПОП по формам обучения. Объем контактной работы включает часы контактной аудиторной работы (лекции/практические занятия/ лабораторные работы), контактной внеаудиторной работы (контроль самостоятельной работы), часы контактной работы в период аттестации. Контактная работа, в том числе может проводиться посредством электронной информационно-образовательной среды университета с использованием ресурсов сети Интернет и дистанционных технологий

5. Содержание дисциплины, структурированное по темам (разделам)

Исходя из рамок, установленных учебным планом по трудоемкости и видам учебной работы по дисциплине, преподаватель самостоятельно выбирает тематику занятий по формам и количеству часов проведения контактной работы: лекции и иные учебные занятия, предусматривающие преимущественную передачу учебной информации преподавателем и (или) занятия семинарского типа (семинары, практические занятия, практикумы, лабораторные работы, коллоквиумы и иные аналогичные занятия), и (или) групповые консультации, и (или) индивидуальную работу обучающихся с преподавателем, в том числе индивидуальные консультации (по курсовым работам/проектам – при наличии курсовой работы/проекта по данной дисциплине в учебном плане). Рекомендуемая тематика занятий максимально полно реализуется в контактной работе с обучающимися очной формы обучения. В случае реализации образовательной программы в заочной / очно-заочной форме трудоемкость дисциплины сохраняется, однако объем учебного материала в значительной части осваивается обучающимися в форме самостоятельной работы. При этом требования к ожидаемым образовательным результатам обучающихся по данной дисциплине не зависят от формы реализации образовательной программы.

№	Наименование раздела	Содержание раздела

1	Типы задач. Метрические классификаторы. Алгоритмы кластеризации	Предмет и задачи машинного обучения и анализа данных. Основные принципы, задачи и подходы, использование в различных областях науки и индустрии. Основные этапы эволюции алгоритмов машинного обучения. Общий вид метрического классификатора. Алгоритм K ближайших соседей. Алгоритмы отбора эталонов. Алгоритмы кластеризации с фиксированным количеством кластеров. Алгоритмы кластеризации по плотности. Иерархическая кластеризация.
2	Деревья решений, линейные классификаторы. Нейронные сети	Правила и анализ качества (точность, полнота). Анализ с помощью ROC кривой. Алгоритм построения деревьев решений. Критерий информационного выигрыша и критерий Джини. Леса решающих деревьев. Перцептрон и разделяющая гиперплоскость. Переход в пространство повышенной размерности. Метод опорных векторов Логистическая регрессия. Градиентный спуск. Нейронные сети и алгоритм обратного распространения градиента. Глубокое обучение, свертки и пулинг
3	Регрессионный анализ, Ансамблевые методы. Стохастический поиск	Линейная регрессия. Полиномиальная регрессия. Смещение и дисперсия. Гребневая регрессия. Голосование. Бутстраппинг. Бустинг, адаптивный бустинг, градиентный бустинг. Поиск Монте-Карло. Алгоритм симулированного отжига. Генетический алгоритм.

6. Рекомендуемая тематика учебных занятий в форме контактной работы

Рекомендуемая тематика учебных занятий *лекционного* типа (предусматривающих преимущественную передачу учебной информации преподавателями):

№	Наименование раздела	Тема лекции
1	Типы задач. Метрические классификаторы. Алгоритмы кластеризации	Лекция 1. Предмет и задачи машинного обучения и анализа данных. Основные принципы, задачи и подходы, использование в различных областях науки и индустрии. Основные этапы эволюции алгоритмов машинного обучения. Лекция 2. Общий вид метрического классификатора. Алгоритм K ближайших соседей. Алгоритмы отбора эталонов. Лекция 3. Алгоритмы кластеризации с фиксированным количеством кластеров. Алгоритмы кластеризации по плотности. Иерархическая кластеризация.
2	Деревья решений, линейные классификаторы. Нейронные сети	Лекция 4. Правила и анализ качества (точность, полнота). Анализ с помощью ROC кривой. Лекция 5. Алгоритм построения деревьев решений. Критерий информационного выигрыша и критерий Джини. Леса решающих деревьев.

		Лекция 6. Перцептрон и разделяющая гиперплоскость. Переход в пространство повышенной размерности. Метод опорных векторов. Лекция 7. Логистическая регрессия. Градиентный спуск. Нейронные сети и алгоритм обратного распространения градиента. Лекция 8. Глубокое обучение, свертки и пулинг
3	Регрессионный анализ, Ансамблевые методы. Стохастический поиск	Лекция 9. Линейная регрессия. Полиномиальная регрессия. Лекция 10. Смещение и дисперсия. Гребневая регрессия. Лекция 11. Голосование. Бутстраппинг. Лекция 12. Бустинг, адаптивный бустинг, градиентный бустинг. Лекция 13. Поиск Монте-Карло. Лекция 14. Алгоритм симулированного отжига. Лекция 15. Генетический алгоритм.

Рекомендуемая тематика *практических* занятий:

№ п/п	**Наименование Темы**	**Содержание темы**
1	Основные понятия и определения. Примеры прикладных задач	Признаки, вектора признаков. Объекты, классы. Классификация. Классификатор. Обучение, виды обучения "с учителем" и "без учителя". Разбор примеров прикладных задач.
2	Линейные классификаторы	Разбор примеров и решение задач по темам: линейная модель классификации, метод стохастического градиента, алгоритм Персептрона.
3	Метод опорных векторов	Основы метода опорных векторов. Случай линейно разделимой выборки. Случай линейно неразделимой выборки. Ядра и спрямляющие пространства. Разбор примеров и решение задач.
4	Методы восстановления регрессии	Метод наименьших квадратов. Непараметрическая регрессия: ядерное сглаживание. Линейная регрессия. Метод главных компонент. Разбор примеров и решение задач по этим темам.
5	Искусственные нейронные сети	Проблема полноты. Задача исключающего "или". Вычислительные возможности двух- и трехслойных сетей. Метод обратного распространения ошибки. Изучение на лабораторном занятии алгоритма постройки нейронных сетей.
6	Выбор признаков и подготовка данных	Влияние выбора набора признаков на результаты классификации. Предварительная обработка данных. Недостающие значения. Выбор признаков на основе проверки гипотез. Выбор подмножества признаков.
7	Контекстно-зависимая классификация	Марковские цепи. Алгоритм Витерби. Скрытые марковские модели. Применение в задачах распознавания голоса. Решение задач по теории марковских моделей в машинном обучении.

На практических занятиях решаются задачи по теме занятия.

Требования к самостоятельной работе обучающихся

1. Работа с лекционным материалом, предусматривающая проработку конспекта лекций и учебной литературы, по всем темам из п. 6 настоящей рабочей программы.

2. Выполнение домашнего задания, предусматривающего решение задач, выполнение упражнений, выдаваемых на практических занятиях, по всем темам из п. 6 настоящей рабочей программы.

Руководствуясь положениями статьи 47 и статьи 48 Федерального закона от 29 декабря 2012 г. N 273-ФЗ «Об образовании в Российской Федерации» научно-педагогические работники и иные лица, привлекаемые университетом к реализации данной образовательной программы, пользуются предоставленными академическими правами и свободами в части свободы преподавания, свободы от вмешательства в профессиональную деятельность; свободы выбора и использования педагогически обоснованных форм, средств, методов обучения и воспитания; права на творческую инициативу, разработку и применение авторских программ и методов обучения и воспитания в пределах реализуемой образовательной программы и отдельной дисциплины.

Исходя из рамок, установленных учебным планом по трудоемкости и видам учебной работы по дисциплине, преподаватель самостоятельно выбирает тематику занятий по формам и количеству часов проведения контактной работы: лекции и иные учебные занятия, предусматривающие преимущественную передачу учебной информации преподавателем и (или) занятия семинарского типа (семинары, практические занятия, практикумы, лабораторные работы, коллоквиумы и иные аналогичные занятия), и (или) групповые консультации, и (или) индивидуальную работу обучающихся с преподавателем, в том числе индивидуальные консультации (по курсовым работам/проектам – при наличии курсовой работы/проекта по данной дисциплине в учебном плане).

Рекомендуемая тематика занятий максимально полно реализуется в контактной работе с обучающимися очной формы обучения. В случае реализации образовательной программы в заочной / очно-заочной форме трудоемкость дисциплины сохраняется, однако объем учебного материала в значительной части осваивается обучающимися в форме самостоятельной работы. При этом требования к ожидаемым образовательным результатам обучающихся по данной дисциплине не зависят от формы реализации образовательной программы.

7. Методические рекомендации по видам занятий

Лекционные занятия.

В ходе лекционных занятий обучающимся рекомендуется выполнять следующие действия. Вести конспектирование учебного материала. Обращать внимание на категории, формулировки, раскрывающие содержание тех или иных явлений и процессов, научные выводы и практические рекомендации по их применению. Задавать преподавателю уточняющие вопросы с целью уяснения теоретических положений, разрешения спорных ситуаций.

Желательно оставить в рабочих конспектах поля, на которых во внеаудиторное время можно сделать пометки из рекомендованной литературы, дополняющие материал прослушанной лекции, а также подчеркивающие особую важность тех или иных теоретических положений.

Практические и семинарские занятия.

На практических и семинарских занятиях в зависимости от темы занятия выполняется поиск информации по решению проблем, практические упражнения, контрольные работы, выработка индивидуальных или групповых решений, итоговое обсуждение с обменом знаниями, участие в круглых столах, разбор конкретных ситуаций, командная работа, представление портфолио и т.п.

Самостоятельная работа.

Самостоятельная работа осуществляется в виде изучения литературы, эмпирических данных по публикациям и конкретных ситуаций из практики, подготовке индивидуальных работ, работа с лекционным материалом, самостоятельное изучение отдельных тем дисциплины; поиск и обзор литературы и электронных источников; чтение и изучение учебника и учебных пособий.

8. Фонд оценочных средств

8.1. Перечень компетенций с указанием этапов их формирования в процессе освоения образовательной программы в рамках учебной дисциплины

Основными этапами формирования указанных компетенций при изучении обучающимися дисциплины являются последовательное изучение содержательно связанных между собой тем учебных занятий. Изучение каждой темы предполагает овладение обучающимися необходимыми компетенциями. Результат аттестации обучающихся на различных этапах формирования компетенций показывает уровень освоения компетенций.

Контролируемые разделы (темы) дисциплины	Индекс контролируемой компетенции (или её части)	Оценочные средства по этапам формирования компетенций
		текущий контроль по дисциплине
Типы задач. Метрические классификаторы. Алгоритмы кластеризации	ПКС-4 УК-1	Тестирование
Деревья решений, линейные классификаторы. Нейронные сети	ПКС-4 УК-1	Тестирование
Регрессионный анализ, Ансамблевые методы. Стохастический поиск	ПКС-4 УК-1	Тестирование

8.2. Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений и навыков и (или) опыта деятельности процессе текущего контроля

1. Какие из этих задач типичны для машинного обучения с учителем?

1. Группировка сообщений от пользователей;
2. Оценка тона комментария: положительный или отрицательный;
3. Группировка изображений по визуальным признакам на неразмеченных данных;
4. Оценка вероятности, кликнет ли человек на рекламный баннер.

1. 1 и 2
2. 2 и 4
3. 1 и 3

2. Выберите все задачи, которые характерны для обучения без учителя.

1. Прогноз стоимости недвижимости;
2. Предсказание пола автора комментария;
3. Рекомендация друзей, контента и пабликов в социальных сетях;
4. Сегментация пользователей интернет-магазина по неявным интересам.

1. 1 и 3
2. 1 и 2
3. 3 и 4
4. 1 и 4

3. Вы хотите предсказать суммы, которые клиенты потратят на оплату трафика в разные месяцы, исходя из истории их предыдущего потребления. Это задача:

1. Регрессии
2. Классификации
3. Классификации и регрессии

4. В базе данных есть следующие записи: длительность звонков, общее число звонков, общее число переданных сообщений, количество потраченных гигабайтов трафика. Вы хотите предсказывать объем трафика, который потратят клиенты. Что будет объектом модели в этой задаче?

1. Длительность звонков
2. Общее число звонков
3. Клиент
4. Количество трафика

5. Вы хотите выявлять клиентов, которые, вероятно, перестанут пользоваться услугами компании в ближайшую неделю. Это задача:

1. Классификации
2. Регрессии
3. Кластеризации

6. Что будет объектом в задаче поиска уходящих от компании клиентов?

1. Уход клиента
2. Количество дней, через которые клиент уйдет
3. Клиент
4. Услуга, от которой отказывается клиент

7. Что будет целевой переменной (y) в задаче поиска уходящих от компании клиентов?

1. Уход клиента
2. Количество дней, через которые клиент уйдет
3. Клиент
4. Услуга, от которой отказывается клиент

8. Какие метрики можно использовать, чтобы оценить, насколько качественно модель решает задачу поиска уходящих клиентов?

1. Долю правильных ответов, полноту, точность
2. RMSE, MAE, MAPE
3. Долю правильных ответов, MAPE, MSE

9. Какой алгоритм не подходит для решения задачи, объекты в которой нужно разделить на классы?

1. Случайный лес
2. Дерево принятия решений
3. Линейная регрессия
4. Логистическая регрессия

10. Оцените метрики и решите, какую модель стоит выбрать для пилотного внедрения.

	Точность	Полнота	Доля правильных ответов
Логистическая регрессия	0.7	0.78	0.79
Решающее дерево	0.72	0.77	0.78
Случайный лес	0.82	0.79	0.88

1. Логистическая регрессия
2. Решающее дерево
3. Случайный лес

11. Компания запускает пилотный проект, чтобы проверить, помогают ли прогнозы модели лучше находить клиентов, которых можно удержать. Какой способ проверки подойдет:

1. Предлагать скидку 15% на услуги, как в компании всегда делали в этих случаях
2. Предлагать улучшенный пакет услуг — так делает конкурент, да и вообще, давно хотели такое попробовать

12. Компания отобрала клиентов, которых модель посчитала уходящими, в тестовую группу, а тех, кого уходящими посчитали маркетологи, — в контрольную. Тестовая группа получила предложение о скидке 15% в четверг вечером, а контрольная — в субботу. Будете ли вы доверять результатам такого эксперимента?

1. Да, ведь скидка одинакова
2. Нет, ведь они получили предложения в разное время

13. Как можно бороться с переобучением модели?

1. С помощью кросс-валидации;
2. С помощью отложенных выборок;
3. С помощью A/B-тестирований;
4. С помощью композиции алгоритмов.

1. 1 и 2
2. 3 и 4
3. 1 и 4
4. 2 и 4

14. Ваши клиенты активно пишут в онлайн-чаты техподдержки по любому поводу. Вы хотите в первую очередь работать с негативом, а значит, вам нужно научиться по тону сообщения отделять жалобы от стандартных вопросов, чтобы жалобы автоматически получали приоритет. Вы решаете делить сообщения на два класса. Дата-сайентист спрашивает, какая метрика будет ключевой?
Какую метрику вы выберете с учетом того, что вам важно научиться точно находить жалобы?

	y = 1 жалоба	y = 0 обычный вопрос
y прогнозное = 1	TP	FP
y прогнозное = 0	FN	TN

1. Доля правильных ответов (TP+TN)/(TP+TN+FN+FP)
2. Точность TP/(TP+FP)
3. Полнота TP/(TP+FN)

15. Если вы хотите, чтобы каждый объект попал в обучающую выборку и алгоритм стал учитывать его особенности, надо выбрать:

1. Метод многих отложенных выборок
2. Метод кросс-валидации (k-блоки)

16. К персональным данным относится:

1. Только та информация, которая непосредственно указывает физическое лицо
2. Любая информация, которая прямо либо косвенно может быть соотнесена с физическим лицом
3. Любая информация, которая прямо либо косвенно может быть соотнесена с физическим или юридическим лицом

17. Какая информация о пациентах, находящаяся в распоряжении медицинской организации, относится к персональным данным?

1. Диагнозы конкретных пациентов
2. Количество пациентов медицинской организации
3. Данные из электронной медицинской карты без Ф.И.О.: дата рождения, адрес регистрации и пр.
4. Динамика роста случаев конкретного заболевания.

1. 2 и 4
2. 1 и 4
3. 1 и 2
4. 1 и 3

8.3. Перечень вопросов и заданий для промежуточной аттестации по дисциплине

Вопросы для промежуточного контроля (зачета)

1. Препроцессинг. Масштабирование. Нормировка. Полиномиальные признаки. One-hot encoding.
2. Кластеризация. kMeans, MeanShift, DBSCAN, Affinity Propagation.
3. Смещение и дисперсия (bias and variance). Понятие средней гипотезы.

4. Ансамблевые методы. Soft and Hard Voting. Bagging. Случайные леса. AdaBoost.
5. Типы обучения: с учителем, без учителя, с подкреплением, с частичным участием учителя, активное обучение.
6. Бустинг деревьев решений.
7. Ошибка внутри и вне выборки. Ошибка обобщения. Неравенство Хёфдинга. Валидация и кросс-валидация.
8. Линейная регрессия. Полиномиальная регрессия. Гребневая регрессия.
9. Размерность Вапника-Червоненкиса. Размерность Вапника-Червоненкиса для перцептрона.
10. Логистическая регрессия. Градиентный спуск.
11. Пороговые условия. Эффективность по Парето. Presicion-Recall и ROC кривые. AUC.
12. Ансамблевые методы регрессии. RANSAC. Theil-Sen. Huber.
13. Перцептрон. Перцептрон с карманом.
14. Метод опорных векторов. Постановка задачи. Формулировка и решение двойственной задачи. Типы опорных векторов. Ядра.
15. Гипотезы и дихотомии. Функция роста. Точка поломки. Доказательство полиномиальности функции роста в присутствии точки поломки.
16. Деревья решений. Информационный выигрыш, критерий Джини. Регуляризация деревьев. Небрежные решающие деревья.
17. Байесовский классификатор. Типы оценки распределений признаков (Gaussian, Bernoulli, Multinomial). EM алгоритм.
18. Нейронные сети. Перцептрон Розенблатта. Функции активации. Обратное распространение градиента. Softmax.
19. Стохастическая оптимизация. Hill Climb. Отжиг. Генетический алгоритм.
20. Метрические классификаторы. kNN. WkNN. Отбор эталонов. DROP5. Kdtree.

8.4. Планируемые уровни сформированности компетенций обучающихся и критерии оценивания

Уровни	Содержательное описание уровня	Основные признаки выделения уровня (этапы формирования компетенции, критерии оценки сформированности)	Пятибалльная шкала (академическая) оценка	Двухбалльная шакала, зачет	БРС, % освоения (рейтинговая оценка)
Повышенный	Творческая деятельность	*Включает нижестоящий уровень.* Умение самостоятельно принимать решение, решать проблему/задачу теоретического и прикладного характера на основе изученных методов, приемов, технологий	отлично	зачтено	86-100
Базовый	Применение знаний и умений в более широких контекстах	*Включает нижестоящий уровень.* Способность собирать, систематизировать, анализировать и грамотно использовать	хорошо		71-85

	учебной и профессиональной деятельности, нежели по образцу с большей степени самостоятельности и инициативы	информацию из самостоятельно найденных теоретических источников и иллюстрировать ими теоретические положения или обосновывать практику применения			
Удовлетворительный (достаточный)	Репродуктивная деятельность	Изложение в пределах задач курса теоретически и практически контролируемого материала	удовлетворительно		55-70
Недостаточный	Отсутствие признаков удовлетворительного уровня		неудовлетворительно	не зачтено	Менее 55

9. Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины.

Основная литература

1. Коэльо, Луис Педро Построение систем машинного обучения на языке Python / Луис Педро Коэльо, Вилли Ричарт ; пер. с англ. А. А. Слинкина. - 2-е изд. - Москва : ДМК Пресс, 2016. - 302 с. - ISBN 978-5-97060-330-7. - Текст : электронный. - URL: https://znanium.com/catalog/product/1027824 (дата обращения: 02.04.2022). – Режим доступа: по подписке.

Дополнительная литература

1. Рашка, С. Python и машинное обучение: крайне необходимое пособие по новейшей предсказательной аналитике, обязательное для более глубокого понимания методологии машинного обучения / С. Рашка ; пер. с англ. А.В. Логунова. - Москва : ДМК Пресс, 2017. - 418 с. - ISBN 978-5-97060-409-0. - Текст : электронный. - URL: https://znanium.com/catalog/product/1027758 (дата обращения: 02.04.2022). – Режим доступа: по подписке.

10. Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины (модуля).

- НЭБ Национальная электронная библиотека, диссертации и прочие издания
- eLIBRARY.RU Научная электронная библиотека, книги, статьи, тезисы докладов конференций
- Гребенников Электронная библиотека ИД журналы
- ЭБС ZNANIUM.COM
- РГБ Информационное обслуживание по МБА
- БЕН РАН
- Электронно-библиотечная система (ЭБС) Кантитана (https://elib.kantiana.ru/)

11. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине.

Программное обеспечение обучения включает в себя:

- система электронного образовательного контента БФУ им. И. Канта – www.lms-3.kantiana.ru, обеспечивающую разработку и комплексное использование электронных образовательных ресурсов;
- серверное программное обеспечение, необходимое для функционирования сервера и связи с системой электронного обучения через Интернет;
- корпоративная платформа Microsoft Teams;
- установленное на рабочих местах обучающихся ПО: Microsoft Windows 7, Microsoft Office Standart 2010, антивирусное программное обеспечение Kaspersky Endpoint Security.
- GNU C++;
- Oracle Java;
- Python;
- Deductor.

12. Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине.

Для проведения занятий лекционного типа, практических и семинарских занятий используются специальные помещения (учебные аудитории), оборудованные техническими средствами обучения – мультимедийной проекционной техникой. Для проведения занятий лекционного типа используются наборы демонстрационного оборудования.

Для проведения лабораторных работ, (практических занятий – при необходимости) используются специальные помещения (учебные аудитории), оснащенные специализированным лабораторным оборудованием: персональными компьютерами с возможностью выхода в интернет и с установленным программным обеспечением, заявленным в п.11.

Для проведения групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации используются специальные помещения (учебные аудитории), оборудованные специализированной мебелью (для обучающихся), меловой / маркерной доской.

Для организации самостоятельной работы обучающимся предоставляются помещения, оснащенные компьютерной техникой с возможностью подключения к сети «Интернет» и обеспечением доступа в электронную информационно-образовательную среду университета.

Для обучения инвалидов и лиц с ограниченными возможностями здоровья университетом могут быть представлены специализированные средства обучения, в том числе технические средства коллективного и индивидуального пользования.

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
федеральное государственное автономное образовательное учреждение высшего образования «Балтийский федеральный университет имени Иммануила Канта»
Институт физико-математических наук и информационных технологий

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

«Управление командой»

Шифр: 10.05.01
Специальность: «Компьютерная безопасность»
Специализация: «Математические методы защиты информации»
Квалификация (степень) выпускника: специалист по защите информации

Калининград
2022

Лист согласования

Составитель: Мищук Б.Р., к. ф.-м. н., доцент.

Рабочая программа утверждена на заседании учебно-методического совета института физико-математических наук и информационных технологий

Протокол № 01/22 от «01» февраля 2022 г.

Председатель учебно-методического совета института физико-математических наук и информационных технологий
Первый заместитель директора ИФМНиИТ, к. ф.-м. н., доцент — Шпилевой А. А

Ведущий менеджер — Е.П.Ставицкая

Содержание

1.Наименование дисциплины: «Управление командой».

Целью изучения дисциплины «Управление командой» является приобретение студентами-бакалаврами теоретических знаний в области управления человеческими ресурсами проектами, позволяющую в дальнейшем самостоятельно расширить знания в данной предметной области, и современное управленческое мышление, способствующее управлению проектом на всех стадиях его жизненного цикла.

Необходимость изучения дисциплины заключается в подготовке студентов для практической деятельности в области управления проектами и командами.

Основные **задачи** изучения дисциплины:

- формирование у обучающихся навыков управления командой;
- формирование у обучающихся навыков формирования и развития команд.

2. Перечень планируемых результатов обучения по дисциплине, соотнесенных с планируемыми результатами освоения образовательной программы

Код компетенции	Результаты освоения образовательной программы (ИДК)	Результаты обучения по дисциплине
УК-1. Способен осуществлять критический анализ проблемных ситуаций на основе системного подхода, вырабатывать стратегию действий	УК.1.1. Анализирует проблемную ситуацию как систему, выявляя ее составляющие и связи между ними. УК.1.2. Критически оценивает надежность источников информации, работает с противоречивой информацией из разных источников. УК.1.3. Разрабатывает и содержательно аргументирует стратегию решения проблемной ситуации на основе системного и междисциплинарных подходов.	Студент, изучивший данный курс, должен: **Знать:** критерии постановки задач в соответствии с целью **Уметь:** анализировать информацию и работать с большим количеством источников информации **Владеть:** технологиями поиска решений поставленной задачи и анализа последствий возможных решений задачи
УК-3. Способен организовывать и руководить работой команды, вырабатывая командную стратегию для достижения поставленной цели	УК.3.1. Умеет организовать команду для достижения поставленной цели и взаимодействовать с другими участниками проекта для решения текущих задач. УК.3.2. Планирует последовательность шагов для достижения заданного результата; понимает эффективность использования стратегии сотрудничества для достижения поставленной цели, определяет свою роль в команде.	**Знать** основные правила и приемы работы в команде **Уметь** выявлять, согласовывать и осуществлять социальное взаимодействие **Владеть практически** средствами управления и работы в команде в различных ролях

	УК.3.3. Осуществляет обмен информацией с другими членами команды, осуществляет презентацию результатов работы команды	
ПКС-4 Способность осуществлять подбор, изучение и обобщение научно-технической информации, методических материалов отечественного и зарубежного опыта по проблемам компьютерной безопасности, а также нормативных правовых актов в сфере профессиональной деятельности	ПКС-4.1. Осуществляет подбор, изучение и обобщение научно-технической информации, методических материалов отечественного и зарубежного опыта по проблемам компьютерной безопасности. ПКС-4.2. Знает основные руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации. ПКС-4.3. Применяет действующую законодательную базу в области обеспечения защиты информации.	**Знать** методики формирования команд и определения ее эффективности, основные приемы создания и использования программных модулей и компонент для управления проектами; **Уметь** использовать основные методики для формирования устойчивой команды для работы в ИТ-сфере, выявлять, согласовывать и осуществлять управление информационными системами управления проектами; **Владеть практически** формирования эффективной команды разработчиков ПО, средствами создания и использования программных средств и компонент для управления проектами.

3. Место дисциплины в структуре образовательной программы

Курс «Управление командой» представляет собой факультативную дисциплину (ФТД.01) части, формируемой участниками образовательных отношений подготовки студентов.

4. Виды учебной работы по дисциплине.

Виды учебной работы по дисциплине зафиксированы учебным планом основной профессиональной образовательной программы по указанному направлению и профилю, выражаются в академических часах. Часы контактной работы и самостоятельной работы студента и часы, отводимые на процедуры контроля, могут различаться в учебных планах ОПОП по формам обучения. Объем контактной работы включает часы контактной аудиторной работы (лекции/практические занятия/ лабораторные работы), контактной внеаудиторной работы (контроль самостоятельной работы), часы контактной работы в период аттестации. Контактная работа, в том числе может проводиться посредством электронной информационно-образовательной среды университета с использованием ресурсов сети Интернет и дистанционных технологий

5. Содержание дисциплины, структурированное по темам (разделам)

Исходя из рамок, установленных учебным планом по трудоемкости и видам учебной работы по дисциплине, преподаватель самостоятельно выбирает тематику занятий по формам и количеству часов проведения контактной работы: лекции и иные учебные занятия, предусматривающие преимущественную передачу учебной информации преподавателем и (или) занятия семинарского типа (семинары, практические занятия, практикумы, лабораторные работы, коллоквиумы и иные аналогичные занятия), и (или) групповые консультации, и (или) индивидуальную работу обучающихся с преподавателем, в том числе индивидуальные консультации (по курсовым работам/проектам – при наличии курсовой работы/проекта по данной дисциплине в учебном плане). Рекомендуемая тематика занятий максимально полно реализуется в контактной работе со студентами очной формы обучения. В случае реализации образовательной программы в заочной / очно-заочной форме трудоемкость дисциплины сохраняется, однако объем учебного материала в значительной части осваивается студентами в форме самостоятельной работы. При этом требования к ожидаемым образовательным результатам студентов по данной дисциплине не зависят от формы реализации образовательной программы.

№	Наименование раздела	Содержание раздела
1	Тема 1. Управление человеческими ресурсами проекта. Команда проекта.	Управление человеческими ресурсами проекта. Процессы управления человеческими ресурсами проекта. План управления человеческими ресурсами проекта. Определение команды, типология команд, цели команды. Тип мышления: типологический опросник Майерс-Бригс. Четыре пары основных характеристик типов личности: экстраверсия-интроверсия, сенсорика-интуиция, мышление-чувствование, решение - восприятие.
2	Тема 2. Социально-психологическая структура команды. Формирование эффективных команд	Социальная группа, ее структура. Малая группа. Основные характеристики коллектива. Формальные и неформальные коллективы. Внутренняя социально-психологическая структура. Социальная структура группы: статусно-ролевые отношения, профессионально-квалификационные характеристики и половозрастной состав. Схема ролевого поведения человека американского психолога Олпорта. Особенности женской и мужской психологии. Женские, мужские и смешанные команды. Социометрия и психологический климат коллектива. Жизненный цикл команды проекта. Этапы формирования и параметры образования команды. Принципы проектирования эффективных организаций. Влияние внешних факторов на проектирование эффективной

		организации. Внутренние элементы структуры организации. Стадии развития команды. Лидерство в коллективе. Типология лидерства. Лидерство и руководство. Качества и функции руководителя. Базовые критерии эффективной работы лидера. Стили управления.
3	Тема 3. Конфликт. Управление конфликтом. Переговоры. Эффективное ведение переговоров.	Конфликт. Структурно-содержательные характеристики конфликта: образы конфликтной ситуации, возможные действия участников конфликтного взаимодействия, варианты его исходов, сферы возникновения и проявления. Пространственно-временные характеристики конфликта: условия, повод, частота и форма конфликтного взаимодействия. Динамика конфликта. Функции и механизм конфликта. Классификация конфликтов. Характеристика основных видов конфликтов. Стратегии и тактики конфликтного взаимодействия. Типы поведения в конфликтной ситуации. Классификация стратегий конфликтного взаимодействия. Классификация тактик в ситуации конфликта. Характеристика основных стилей поведения в конфликтной ситуации. Типология конфликтного поведения. Модель конструктивного поведения в конфликте. Понятие переговорного процесса. Виды и функции переговоров. Субъекты и предмет переговоров. Понятие «результат переговоров». Морально-этическая сторона ведения переговоров. Планирование переговорного процесса. Постановка целей. Определение пределов возможностей сторон. Сбор информации. Методы подготовки к переговорам. Подготовка к международным переговорам. Размещение участников переговоров. Интересы сторон в переговорном процессе. Различие в понятиях «позиция» и «интересы». Ожидания и намерения в переговорах. Решение проблем на переговорах. Стратегия и тактика переговорного процесса. Сущность понятий «стратегия» и «тактика» переговорного процесса. Психологическая сущность понятия «манипуляция». Психологические механизмы манипулятивного воздействия на переговорах.

		Распознавание манипуляции. Психологическая защита от манипуляций.
4	Тема 4. Проблемы управления командой проекта.	Основные понятия конфликтного взаимодействия: социальная и психическая напряженность, ранг или значимость оппонента в социальном пространстве, дистанция, социальная мобильность. Межличностная коммуникация. Манипулирование как реализация корыстных интересов. Виды манипулирования: экономическое, политическое, бюрократическое, идеологическое, психологическое. Стрессы и управление эмоциональным состоянием. Эффективность работы группы. Факторы, влияющие на эффективность работы группы

6. Рекомендуемая тематика учебных занятий в форме контактной работы

Рекомендуемая тематика учебных занятий *лекционного* типа (предусматривающих преимущественную передачу учебной информации преподавателями):

№	Наименование раздела	Темы лекций
1	Тема 1. Управление человеческими ресурсами проекта. Команда проекта.	Лекция 1. Управление человеческими ресурсами проекта. Лекция 2. Команда проекта.
2	Тема 2. Социально-психологическая структура команды. Формирование эффективных команд	Лекция 3. Социально-психологическая структура команды. Лекция 4. Формирование эффективных команд.
3	Тема 3. Конфликт. Управление конфликтом. Переговоры. Эффективное ведение переговоров.	Лекции 5. Конфликт. Управление конфликтом Лекция 6. Переговоры. Эффективное ведение переговоров.
4	Тема 4. Проблемы управления командой проекта.	Лекция 7. Проблемы управления командой проекта.

Практические занятия не предусмотрены.

Перечень тем *практических занятий:*

Практическое занятие 1. Управление человеческими ресурсами проекта
1.1 Видеофильм «Кто нам нужен для реализации проекта?».

Практическое занятие 2. Команда проекта
Определение команды, типология команд, цели команды. Тип мышления: типологический опросник Майерс-Бригс.
2.1 Определение своего типа мышления на основе опросника Майерс-Бригс.

Практическое занятие 3. Социально-психологическая структура команды

Социальная группа. Социальная структура группы: статусно-ролевые отношения, профессионально-квалификационные характеристики и половозрастной состав.
2.1 Видеофильм «Типы ролей в команде» (по И. Адизесу).
2.2 Определение ролевой структуры по Р.Белбину (тест).
2.3 Игра «Таможня».

Практическое занятие 4. Формирование эффективных команд
Жизненный цикл команды проекта. Этапы формирования и параметры образования команды.
2.1 Видеофильм «Команда проекта».
2.2 Игра на командообразование «Дигикон».

Практическое занятие 5. Конфликт. Управление конфликтом
Конфликт. Характеристика основных видов конфликтов. Стратегии и тактики конфликтного взаимодействия. Типы поведения в конфликтной ситуации. Классификация
стратегий конфликтного взаимодействия. Модель конструктивного поведения в конфликте.
5.1 Мультфильм «Конфликт».
5.2 Разбор ситуации «Жизнь чиновника».
5.3 Деловая игра «Конфликтная ситуация на железной дороге».

Практическое занятие 6. Переговоры. Эффективное ведение переговоров
Понятие переговорного процесса. Стратегия и тактика переговорного процесса.
6.1 Разбор 3-х видеофрагментов из фильма «Троя».
6.2 Просмотр учебного фильма «Переговоры» («Тренинг-медиа»).
6.3 Игра «Черное-красное».

Практическое занятие 7. Проблемы управления командой проекта
Межличностная коммуникация. Эффективность работы группы. Факторы, влияющие на эффективность работы группы. Активное слушание.
7.1 Разбор видеофрагментов «Слушаю Вас, сэр» и «Да-да».

Требования к самостоятельной работе студентов

1. Работа с лекционным материалом, предусматривающая проработку конспекта лекций и учебной литературы, по всем темам из п. 6 настоящей рабочей программы.

2. Выполнение лабораторных работ, предусматривающих решение задач, по соответствующим темам из п. 6 настоящей рабочей программы.

Руководствуясь положениями статьи 47 и статьи 48 Федерального закона от 29 декабря 2012 г. N 273-ФЗ «Об образовании в Российской Федерации» научно-педагогические работники и иные лица, привлекаемые университетом к реализации данной образовательной программы, пользуются предоставленными академическими правами и свободами в части свободы преподавания, свободы от вмешательства в профессиональную деятельность; свободы выбора и использования педагогически обоснованных форм, средств, методов обучения и воспитания; права на творческую инициативу, разработку и применение авторских программ и методов обучения и воспитания в пределах реализуемой образовательной программы и отдельной дисциплины.

Исходя из рамок, установленных учебным планом по трудоемкости и видам учебной работы по дисциплине, преподаватель самостоятельно выбирает тематику занятий по формам и количеству часов проведения контактной работы: лекции и иные учебные

занятия, предусматривающие преимущественную передачу учебной информации преподавателем и (или) занятия семинарского типа (семинары, практические занятия, практикумы, лабораторные работы, коллоквиумы и иные аналогичные занятия), и (или) групповые консультации, и (или) индивидуальную работу обучающихся с преподавателем, в том числе индивидуальные консультации (по курсовым работам/проектам – при наличии курсовой работы/проекта по данной дисциплине в учебном плане).

Рекомендуемая тематика занятий максимально полно реализуется в контактной работе со студентами очной формы обучения. В случае реализации образовательной программы в заочной / очно-заочной форме трудоемкость дисциплины сохраняется, однако объем учебного материала в значительной части осваивается студентами в форме самостоятельной работы. При этом требования к ожидаемым образовательным результатам студентов по данной дисциплине не зависят от формы реализации образовательной программы.

7. Методические рекомендации по видам занятий

Лекционные занятия.

В ходе лекционных занятий обучающимся рекомендуется выполнять следующие действия. Вести конспектирование учебного материала. Обращать внимание на категории, формулировки, раскрывающие содержание тех или иных явлений и процессов, научные выводы и практические рекомендации по их применению. Задавать преподавателю уточняющие вопросы с целью уяснения теоретических положений, разрешения спорных ситуаций.

Желательно оставить в рабочих конспектах поля, на которых во внеаудиторное время можно сделать пометки из рекомендованной литературы, дополняющие материал прослушанной лекции, а также подчеркивающие особую важность тех или иных теоретических положений.

Практические и семинарские занятия.

На практических и семинарских занятиях в зависимости от темы занятия выполняется поиск информации по решению проблем, практические упражнения, контрольные работы, выработка индивидуальных или групповых решений, итоговое обсуждение с обменом знаниями, участие в круглых столах, разбор конкретных ситуаций, командная работа, представление портфолио и т.п.

Самостоятельная работа.

Самостоятельная работа осуществляется в виде изучения литературы, эмпирических данных по публикациям и конкретных ситуаций из практики, подготовке индивидуальных работ, работа с лекционным материалом, самостоятельное изучение отдельных тем дисциплины; поиск и обзор литературы и электронных источников; чтение и изучение учебника и учебных пособий.

8. Фонд оценочных средств

8.1. Перечень компетенций с указанием этапов их формирования в процессе освоения образовательной программы в рамках учебной дисциплины

Основными этапами формирования указанных компетенций при изучении обучающимися дисциплины являются последовательное изучение содержательно связанных между собой тем учебных занятий. Изучение каждой темы предполагает овладение обучающимися необходимыми компетенциями. Результат аттестации обучающихся на различных этапах формирования компетенций показывает уровень освоения компетенций.

Контролируемые разделы (темы) дисциплины	Индекс контроли-руемой компетенции (или её части)	Оценочные средства по этапам формирования компетенций
		текущий контроль по дисциплине
Тема 1. Управление человеческими ресурсами проекта. Команда проекта.	УК-1, УК-3 ПКС-4	Опрос. Тест
Тема 2. Социально-психологическая структура команды. Формирование эффективных команд	УК-1, УК-3 ПКС-4	Опрос. Тест
Тема 3. Конфликт. Управление конфликтом. Переговоры. Эффективное ведение переговоров.	УК-1, УК-3 ПКС-4	Опрос. Тест
Тема 4. Проблемы управления командой проекта.	УК-1, УК-3 ПКС-4	Опрос. Тест

8.2. Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений и навыков и (или) опыта деятельности процессе текущего контроля

Темы лабораторных работ

1. Определение потребностей в человеческих ресурсах.
2. Урегулирование конфликта между подчиненными.
3. Урегулирование конфликта с подчиненным.
4. Урегулирование конфликта между группировками.
5. Выработка стратегии развития персонала.
6. Анализ конфликта.

Лабораторная работа №1
Определение потребностей в человеческих ресурсах.
Цель работы: научиться рассчитывать потребности в человеческих ресурсах.
Задания:

1. Исходные данные. Компания «Русса» занимается оптовой реализацией продовольственных товаров. В 2013 году компания имела 5 коммерческих агентов и объем реализации 500.000 тыс.руб. В 2014 году компания намерена достичь объема реализации 700.000 тыс.руб. С помощью метода экстраполяции определить, сколько коммерческих агентов понадобится компании «Русса» для достижения ее целей.
2. Исходные данные. Организация по техническому обслуживанию лифтов использует метод скорректированной экстраполяции для определения потребностей в персонале на следующий год. Данные об организации в текущем году: Число лифтов на техническом обслуживании 12564. Общее число производительных часов, отработанных на обслуживании 224.000. Численность работников: производственные (механики) – 140; непроизводственные – 18
3. При расчете численности на следующий год руководство организации основывается на следующих предположениях:

a. Производительность труда механиков по обслуживанию увеличится на 15%.
b. Эффективность использования рабочего времени возрастет на 10%.
c. Портфель заказов (количество обслуживаемых лифтов) останется без изменения.
d. Соотношение между производственными и непроизводственными работниками не изменится.

4. На основании результатов текущего года рассчитать основные пропорции. С учетом плановых параметров рассчитать основные показатели на следующий год. Определить плановую численность механиков и численность непроизводительных работников на следующий год.

Лабораторная работа №2

Урегулирование конфликта между подчиненными.

Цель работы: научиться регулировать конфликтные ситуации между подчиненными.

Задания.

Исходные данные. Между двумя высшими подчиненными (коллегами) возник конфликт, который мешает им успешно работать. Каждый из них в отдельности обращался к Вам с просьбой разобраться и поддержать его позицию.

Постановка задачи. Выберите и обоснуйте свой вариант поведения в этой ситуации:

а) пресечь конфликт на работе и порекомендовать разрешить конфликтные взаимоотношения в неслужебное время;

б) попросить разобраться в конфликте специалистов лаборатории социологических исследований или другого подразделения службы управления персона, чьей функцией это является;

в) лично попытаться разобраться в мотивах конфликта и найти приемлемый для обеих сторон вариант примирения;

г) выяснить, кто из членов коллектива служит авторитетом для конфликтующих, и попытаться через него воздействовать на этих людей.

Лабораторная работа №3

Урегулирование конфликта с подчиненным.

Цель работы: научиться регулировать конфликтные ситуации с подчиненными.

Задания.

Исходные данные. Подчиненный (коллега) игнорирует Ваши советы и указания, делает все по-своему, не обращая внимания на замечания, не исправляя того, на что Вы ему указываете.

Постановка задачи. Как Вы будете поступать с этим подчиненным (коллегой) в дальнейшем:

а) разобравшись в мотивах упорства и видя их несостоятельность, применить обычные административные меры наказания;

б) в интересах дела постараться вызвать его на откровенный разговор, попытаться найти с ним общий язык, настроить на деловой контакт;

в) обратиться к коллективу - пусть обратит внимание на неправильное поведение коллеги и применит меры общественного воздействия;

г) попытаться разобраться в том, не делаете ли Вы сами ошибок во взаимоотношениях с этим подчиненным (коллегой), потом решить, как поступить.

Лабораторная работа №4

Урегулирование конфликта между группировками.

Цель работы: научиться регулировать конфликтные ситуации между группировками.

Задания.

Исходные данные. В трудовой коллектив, где имеется конфликт между двумя группировками по поводу внедрения нового стиля руководства, пришел новый руководитель, приглашенный со стороны.

Постановка задачи. Каким образом, по Вашему мнению, ему лучше действовать, чтобы нормализовать психологический климат в коллективе:

а) установить контакт с приверженцами нового стиля и, не принимая всерьез доводы сторонников старого порядка, вести работу по внедрению новшеств, воздействуя на противников силой своего примера и примера других;

б) попытаться разубедить и привлечь на свою сторону приверженцев прежнего стиля работы, противников новаций, воздействовать на них убеждением в процессе дискуссии; в) выбрать наиболее авторитетных членов трудового коллектива, поручить им, разобраться и предложить меры по нормализации обстановки, опираясь на поддержку администрации, профсоюза и т. д.;

г) изучить перспективы развития коллектива, поставить перед коллективом новые стратегические задачи совместной трудовой деятельности, опираясь на лучшие достижения и трудовые традиции коллектива и не противопоставлять новое старому.

Лабораторная работа №5

Выработка стратегии развития персонала.

Цель работы: овладеть навыками развития персонала.

Задания.

Исходные данные. Ирина Хромова, директор по человеческим ресурсам ООО «Графика», получила свой персональный компьютер три дня назад. После того, как естественная радость от этого долгожданного события несколько утихла, Ирина начала думать о том, что же она будет с ним делать. Согласно, приложенным к компьютеру документам в нем уже были установлены и текстовый редактор, и программа Лотус, и система анализа базы данных «Директор по персоналу». Однако Ирина никогда прежде не пользовалась компьютерами. Во вчерашней газете она видела объявление университета, который предлагал недельные компьютерные курсы для начинающих. Цена обучения – 5000 руб. В той же газете было опубликовано маленькое объявление о частных уроках компьютерной грамотности, стоящих 200 рублей за час. Начальник отдела информатизации ООО «Графика» предложил Ирине свою помощь, но признался, что не знаком с базой данных «Директор по персоналу». В подчинении у Ирины находится пять человек, получивших такие же компьютеры, но, к сожалению, также не имеющих опыта работы на них

Вопросы для обсуждения:

1.Определите потребности в профессиональном обучении в данной ситуации.

2.Определите цели программы профессионального обучения.

3. Что должна сделать Ирина?

Лабораторная работа №6

Анализ конфликта.

Цель работы: овладеть навыками анализа конфликтных ситуаций.

Задания.

Описание ситуаций и постановка задачи:

1. Изучить описание приведенных ниже ситуаций и составить карты конфликта.

2. Обсудить опыт, приобретенный при выполнении упражнения.

3. Обсудить достоинства изученного метода, области его применения и ограничения.

Ситуация 1. В организации освободилась должность начальника одного из отделов. На нее претендуют два сотрудника, имеющих высокую квалификацию и солидный стаж работы на этом предприятии, – Иванов и Сидоров. Руководитель поручает секретарю вызвать того и другого на совещание, на котором должно быть принято решение. В назначенное время появляется только Иванов. Руководитель очень удивился и стал выяснять в чем дело. Оказалось, что секретарь сообщил о вызове только Иванову и попросил того уведомить Сидорова. Иванов 23 обещал передать, но сразу Сидорова не застал, а позже не смог этого сделать, так как ему самому пришлось срочно выехать в другую организацию. Руководитель послал секретаря за Сидоровым, но того на месте не оказалось, и совещание отложили на следующую неделю. Руководитель строго отчитал секретаря и велел ему лично известить второго претендента о времени встречи. Узнав от секретаря о случившемся, Сидоров решил, что его соперник намеренно не сообщил ему о совещании, и поделился этими соображениями с коллегами. Мнения сослуживцев разделились: кто-то согласился с Сидоровым, другие посчитали, что во всем виноват секретарь. А кто-то сообщил Иванову, что Сидоров настраивает сотрудников против него. И началось. Оба претендента «за глаза» обвиняли друг друга в клевете, вспоминали старые обиды, скрупулезно учитывали новые. К моменту решающего совещания, которое вновь было отложено, на сей раз из-за занятости руководителя, Иванов с Сидоровым производили впечатление давних врагов

Ситуация 2. Как-то наш начальник распределил очередную работу между тремя исполнителями, одним из которых был я. К назначенному сроку я выполнил свою часть задания, а мои напарники – нет. И тогда начальник велел мне заняться их недоработками. Я мог бы молча проигнорировать это поручение, и ничего бы не случилось. Но я пошел на принцип и отказался его выполнять, мотивируя это тем, что при одинаковой зарплате не должно быть различной нагрузки. Этот довод не понравился начальнику. Он заявил, что мы не хотим работать, а зарплату требуем. Я возразил, что его замечание не по существу. Разговор происходил на глазах у всего коллектива, и все понимали, что начальник несправедлив ко мне. Просто я попал под горячую руку. За предшествовавшие шесть лет ничего подобного не случалось. Я всегда относился к нему с уважением (он намного старше меня), но в этот момент мне стало обидно, что вместо похвалы я получил нагоняй. Если бы он просто по-человечески попросил поработать дополнительно, чтобы выручить фирму, я бы, конечно, не отказался. Но, по словам начальника, выходило, что мы все бездельники. И я сознательно пошел на обострение ситуации. После бурной «дискуссии» я вышел из кабинета. Успокоившись, я вернулся, подошел к начальнику и извинился. По-моему, он удивился. Но постарался скрыть это. И, к моему удивлению, сам извинился передо мной. Вот уже несколько лет я «прокручиваю» эту ситуацию в разных вариантах. Я понимаю, что вел себя неправильно. Ни по форме, ни по сути дела у меня не было серьезных оснований вступать в пререкания с начальником. И все-таки я не вижу лучшего выхода для себя, чем «обострение». Ведь если бы я сделал самое простое (как позже мне советовали некоторые) и не стал бы возражать, но потом не ударил бы пальцем о палец, то пошел бы против своих принципов, потому что это был бы обман. А я считаю себя достаточно сильным человеком, чтобы не прибегать к хитрости и лжи. Я мог бы безропотно выполнить чужую работу, но потом просто сходил бы с ума от несправедливости и злости. Я же дал понять, что готов защищать свою честь и достоинство, и заставил начальника отнестись ко мне с уважением. В результате я пошел на рабочее место и с легкой душой сделал все, что требовалось. Думаю, и начальник извлек для себя полезный урок. Я ощутил это по себе: с того раза я не услышал в свой адрес ни одного грубого слова.

Ситуация 3. Фирма занимается импортом продовольственных товаров и оптовыми поставками предприятиям розничной торговли. Она имеет отдел сбыта, задачей которого является совершение торговых операций Перед отделом стоит задача ежегодного увеличения оборота не менее чем на 30%. Фирма работает на высококонкурентном рынке, клиенты имеют возможность выбирать поставщика, поэтому менеджерам сбытового отдела

приходится работать очень интенсивно. Фирма существует уже несколько лет, поэтому у каждого поставщика есть налаженная сеть клиентов. На ее поддержку уходит основная часть рабочего времени и усилий. Кроме того, задача увеличения оборота требует поиска новых каналов сбыта. Около полутора лет назад в отдел был принят еще один сотрудник на должность менеджера. Хорошо образованный, эрудированный и не лишенный обаяния молодой человек быстро вошел в коллектив. Вокруг него образовался кружок молодежи, объединенный общими спортивными интересами. Ему была 24 передана часть клиентской базы, но она была недостаточна для выполнения плановых заданий. Поэтому ему надо было направить свои силы на поиск и привлечение новых клиентов. Обладая средним уровнем развития коммуникативных навыков и незначительным опытом работы на этом рынке, новый сотрудник едва справлялся со своими задачами. Он тратил значительно больше усилий на получение тех же результатов, которых опытные менеджеры добиваются с легкостью. Начальник отдела несколько раз указывал ему на просчеты и упущения в работе. Поскольку оплата труда в фирме зависит от объема продаж, то и заработок у него был меньше, чем у остальных менеджеров, показывающих лучшие результаты. Но у этого сотрудника возникло впечатление, что начальник отдела относится к нему предвзято, оценивая его заслуги несправедливо. Сначала обиженный ограничивался «кулуарными» проявлениями своего недовольства, а затем занял открыто конфронтационную позицию. Несколько раз он в присутствии других сотрудников упрекал начальника отдела в мелочных придирках, скептически высказывался о его способности руководить отделом, язвительно критиковал его распоряжения. Попытки начальника Отдела выяснить отношения успеха не имели. В коллективе отдела наметился раскол, поскольку часть молодых сотрудников явно сочувствовала своему коллеге и была готова принять его сторону, если конфликт будет иметь развитие.

Методические указания:

Этап 1. Определение предмета конфликта. Опишите проблему в общих чертах. Из-за чего возник спор, по поводу чего высказывались разные мнения? Не надо глубоко вдаваться в проблему или находить выход. Опишите, что является предметом конфликта, не что надо делать, а что является «яблоком раздора». Предмет может быть не один.

Этап 2. Определение оппонентов, вовлеченных в конфликт. Решите, кто является главными сторонами в конфликте. Составьте список действующих лиц. Если группа имеет однородные требования, потребности. Дайте каждому из участников конфликта какое-либо веселое (ни в коем случае необидное) определение, которое подчеркнет их сильные стороны и их позитивные намерения в этом конфликте. Определите в каком организационном и социальном пространстве происходит конфликт, в каких бизнес-процессах участвуют конфликтующие стороны, какие цели и задачи ими решаются?

Этап 3. Определение подлинных интересов оппонентов — какова мотивация, стоящая за позициями оппонентов. Необходимо перечислить потребности и опасения каждого участника. Так формируются возможности для создания большего количества взаимовыгодных решений. Одна и та же потребность может относиться к нескольким или ко всем участникам. Тогда она записывается всем, свидетельствуя об общности интересов. Не путайте потребности с позициями! Предметом опасений часто бывают физическая безопасность, финансовые потери, потеря членства в группе, потеря контроля и власти, нежелание попадать в зависимость от кого-либо, потеря уважения, осуждение, унижение, утрата возможности реализовать себя и т.д.

Вопросы для устного опроса

1. Различие между группой и командой.
2. Классификация видов команд.
3. Ролевые позиции в команде.
4. Стадии развития группы и команды.
5. Структура межличностной коммуникации в команде

6. Классификация основных видов конфликтов.
7. Особенности конфликтного взаимодействия «личность и группа».
8. Основные признаки межличностных конфликтов.
9. Основные проявления внутриличностного конфликта.
10. Понятие внутриличностного конфликта и его основные виды.
11. Понятие урегулирования и разрешение конфликта.
12. Психологические основы групповых конфликтов (понятие, причины, проявления).
13. Стили поведения в конфликте. Особенности выбора эффективного стиля поведения.
14. Стратегии поведения в конфликтном взаимодействии.
15. Структурно-содержательные характеристики конфликта (понятие, структура, динамика, функции).
16. Характеристика конструктивного вида поведения в конфликте

8.3. Перечень вопросов и заданий для промежуточной аттестации по дисциплине

Перечень вопросов для промежуточного контроля (зачета).

1. Организация управления персоналом в проекте.
2. Набор команды проекта.
3. Развитие команды проекта.
4. Личные качества и компетенции руководителя проекта.
5. Подготовка персонала в области управления проектами.
6. Внедрение корпоративной системы управления проектами.
7. Процессы управления проектами.
8. Команда проекта и проектная группа – есть ли между ними разница?
9. Что означает жизненный цикл развития команды проекта?
10. Как сдать эффективную команду?
11. Зачем нужна матрица компетенций?
12. Что такое лидерство? Почему хороший менеджер должен обладать качествами лидера?
13. Какими компетенциями должен обладать менеджер проекта?
14. Дайте определение переговорам.
15. Раскройте основные функции переговоров в современном обществе.
16. Что такое планирование переговоров?
17. Назовите основные источники информационной подготовки к переговорам.
18. Каковы основные стадии переговоров и их характеристики.
19. Раскройте различие в понятиях «позиция» и «интересы».
20. Назовите основные характеристики начала переговоров.
21. Назовите особенности этапа подготовки к переговорам.
22. Какие разногласия могут возникать на переговорах?
23. Назовите основные стратегии и тактики переговорного процесса.
24. Назовите основные модели поведения сторон в переговорах.
25. Раскройте содержание понятия «манипуляция».
26. Раскройте содержание психологических механизмов манипулятивного воздействия на переговорах.
27. Назовите основные критерии успешных переговоров.
28. Назовите основные преимущества ведения переговоров командой и одним человеком.
29. Охарактеризуйте специфику проведения переговоров на «своей», «чужой» и нейтральной территории

8.4. Планируемые уровни сформированности компетенций обучающихся и критерии оценивания

Уровни	Содержательное описание уровня	Основные признаки выделения уровня (этапы формирования компетенции, критерии оценки сформированности)	Пятибалльная шкала (академическая) оценка	Двухбалльная шакала, зачет	БРС, % освоения (рейтинговая оценка)
Повышенный	Творческая деятельность	*Включает нижестоящий уровень.* Умение самостоятельно принимать решение, решать проблему/задачу теоретического и прикладного характера на основе изученных методов, приемов, технологий	отлично	зачтено	86-100
Базовый	Применение знаний и умений в более широких контекстах учебной и профессиональной деятельности, нежели по образцу с большей степени самостоятельности и инициативы	*Включает нижестоящий уровень.* Способность собирать, систематизировать, анализировать и грамотно использовать информацию из самостоятельно найденных теоретических источников и иллюстрировать ими теоретические положения или обосновывать практику применения	хорошо		71-85
Удовлетворительный (достаточный)	Репродуктивная деятельность	Изложение в пределах задач курса теоретически и практически контролируемого материала	удовлетворительно		55-70
Недостаточный	Отсутствие признаков удовлетворительного уровня		неудовлетворительно	не зачтено	Менее 55

9. Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины.

Основная литература

1. Попов, Ю. И. Управление проектами: учебное пособие / Ю. И. Попов, О. В.

Яковенко. — Москва: ИНФРА-М, 2021. — 208 с. — (Учебники для программы МВА). - ISBN 978-5-16-002337-3. - Текст: электронный. - URL: https://znanium.com/catalog/product/1153780 (дата обращения: 11.01.2022). – Режим доступа: по подписке.
2. Цителадзе, Д. Д. Управление проектами: учебник / Д.Д. Цителадзе. — Москва: ИНФРА-М, 2022. — 361 с. — (Высшее образование: Бакалавриат). — DOI 10.12737/1817091. - ISBN 978-5-16-017166-1. - Текст: электронный. - URL: https://znanium.com/catalog/product/1817091 (дата обращения: 11.01.2022). – Режим доступа: по подписке.

Дополнительная литература

1. Управление проектами: учебник / под ред. Н.М. Филимоновой, Н.В. Моргуновой, Н.В. Родионовой. — Москва: ИНФРА-М, 2022. — 349 с. — (Высшее образование: Бакалавриат). — DOI 10.12737/textbook_5a2a2b6fa850b2.17424197. - ISBN 978-5-16-013197-9. - Текст: электронный. - URL: https://znanium.com/catalog/product/1836589 (дата обращения: 11.01.2022). – Режим доступа: по подписке.
2. Поташева, Г. А. Управление проектами (проектный менеджмент): учебное пособие / Г.А. Поташева. — Москва: ИНФРА-М, 2022. — 224 с. + Доп. материалы [Электронный ресурс]. — (Высшее образование: Бакалавриат). — DOI 10.12737/17508. - ISBN 978-5-16-010873-5. - Текст: электронный. - URL: https://znanium.com/catalog/product/1840953 (дата обращения: 11.01.2022). – Режим доступа: по подписке.

10. Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины (модуля).

- НЭБ Национальная электронная библиотека, диссертации и прочие издания
- eLIBRARY.RU Научная электронная библиотека, книги, статьи, тезисы докладов конференций
- Гребенников Электронная библиотека ИД журналы
- ЭБС Лань книги, журналы
- ЭБС Консультант студента
- ПРОСПЕКТ ЭБС
- ЭБС ZNANIUM.COM
- РГБ Информационное обслуживание по МБА
- БЕН РАН
- Электронно-библиотечная система (ЭБС) Кантитана (https://elib.kantiana.ru/)

11. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине.

Программное обеспечение обучения включает в себя:

- система электронного образовательного контента БФУ им. И. Канта – www.lms-3.kantiana.ru, обеспечивающую разработку и комплексное использование электронных образовательных ресурсов;
- серверное программное обеспечение, необходимое для функционирования сервера и связи с системой электронного обучения через Интернет;
- корпоративная платформа Microsoft Teams;

- установленное на рабочих местах студентов ПО: Microsoft Windows 7, Microsoft Office Standart 2010, антивирусное программное обеспечение Kaspersky Endpoint Security.
- MS Project v. 2013 и выше

12. Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине.

Для проведения занятий лекционного типа, практических и семинарских занятий используются специальные помещения (учебные аудитории), оборудованные техническими средствами обучения – мультимедийной проекционной техникой. Для проведения занятий лекционного типа используются наборы демонстрационного оборудования.

Для проведения лабораторных работ, (практических занятий – при необходимости) используются специальные помещения (учебные аудитории), оснащенные специализированным лабораторным оборудованием: персональными компьютерами с возможностью выхода в интернет и с установленным программным обеспечением, заявленным в п.11.

Для проведения групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации используются специальные помещения (учебные аудитории), оборудованные специализированной мебелью (для обучающихся), меловой / маркерной доской.

Для организации самостоятельной работы обучающимся предоставляются помещения, оснащенные компьютерной техникой с возможностью подключения к сети «Интернет» и обеспечением доступа в электронную информационно-образовательную среду университета.

Для обучения инвалидов и лиц с ограниченными возможностями здоровья университетом могут быть представлены специализированные средства обучения, в том числе технические средства коллективного и индивидуального пользования.

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
федеральное государственное автономное образовательное учреждение высшего образования «Балтийский федеральный университет имени Иммануила Канта»
Институт физико-математических наук и информационных технологий

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

«Элективные курсы по физической культуре и спорту»

Шифр: 10.05.01
Специальность: «Компьютерная безопасность»
Специализация: «Математические методы защиты информации»
Квалификация (степень) выпускника: Специалист по защите информации

Калининград
2022

Лист согласования

Составитель: Томашевская О.Б. к.п.н, доцент; Доценты, к.п.н: Юшков.В.И., Семенив Д.А., Никитина А.А., Ст. преподаватели: Бекаури М.В., Барановский В.Н., Головина Е.А., Грудько Л.С, Долматов Б.В., Калягин В.И., Коваленко Т.А., Макиенко В.В., Маркелова Е.Б., Мартынова В.И., Моржухин А.Н., Кравченко И.А., Пасевина В.В., Писаренко Е.Г., Попова И.В., Покровская Н.В., Романов С.С., Румянцева О.В., Созинова Л.Л., Споденко С.В., Станчик Т.И., Тюпа П.И., , Ассистенты: Мусейчук С.В., Ястребова О.С., Сыч Р.К.

Рабочая программа утверждена на заседании учебно-методического совета института физико-математических наук и информационных технологий

Протокол № 01/22 от «01» февраля 2022 г.

Председатель учебно-методического совета института физико-математических наук и информационных технологий
Первый заместитель директора ИФМНиИТ, к. ф.-м. н., доцент — Шпилевой А. А

Ведущий менеджер — Е.П.Ставицкая

Содержание

1.Наименование дисциплины: «Элективные курсы по физической культуре и спорту».

Элективные дисциплины по физической культуре и спорту как составная часть общей культуры и профессиональной подготовки студента в период обучения в университете, входит обязательным разделом в базовую часть дисциплин, значимость которого проявляется через гармонизацию духовных и физических сил, формирование таких общечеловеческих ценностей, как здоровье, физическое и психическое благополучие, физическое совершенство.

Результатом образования в области элективных дисциплин по физической культуре и спорту должно быть создание у студентов устойчивой мотивации и потребности в выборе здорового образа жизни, в физическом самосовершенствовании, приобретении личного опыта творческого использования средств и методов физической культуры, в достижении достаточного уровня психофизической подготовленности.

Реализация программы по модулю «Элективные дисциплины по физической культуре и спорту» направлена на:

- повышение уровня теоретических знаний студентов в формировании навыков здорового образа жизни;
- достижение целостности знаний в области физической культуры, направленных на профессионально-личностное развитие будущего специалиста, его профессиональной компетенции;
- ориентацию всех видов программного материала на решение задач обучения студентов умениям физической самоподготовки, самосовершенствованию средствами физической культуры;
- учет профессиональной направленности университета, кадрового потенциала преподавателей физической культуры, специфики организации учебного процесса и возможностей материально-технической базы.

2. Перечень планируемых результатов обучения по дисциплине, соотнесенных с планируемыми результатами освоения образовательной программы

Код компетенции	Результаты освоения образовательной программы (ИДК)	Результаты обучения по дисциплине
УК-7. Способен поддерживать должный уровень физической подготовленности для обеспечения полноценной социальной и профессиональной деятельности	УК.7.1. Поддерживает должный уровень физической подготовленности для обеспечения полноценной социальной и профессиональной деятельности и соблюдает нормы здорового образа жизни. УК.7.2. Использует основы физической культуры для осознанного выбора здоровьесберегающих технологий с учётом внутренних и внешних условий реализации конкретной профессиональной	Знать: Роль физической культуры в подготовке будущего специалиста; Методику использования видов двигательной активности в процессе учебной и профессиональной деятельности; Основы обучения двигательным действиям; Основы развития и совершенствования физических качеств; Правила техники безопасности при выполнеии упражнений; Уметь: Применять средства физической культуры для освоения основных двигательных действий; Применять средства и методы для развития и

	деятельности.	совершенствования физических качеств; Владеть средствами и методами физической культуры необходимыми для обеспечения полноценной жизнедеятельности;

3. Место дисциплины в структуре образовательной программы

Данная дисциплина представляет собой дисциплину части, формируемой участниками образовательных отношений Блока 1 Дисциплины (модули) подготовки студентов.

4. Виды учебной работы по дисциплине.

Виды учебной работы по дисциплине зафиксированы учебным планом основной профессиональной образовательной программы по указанному направлению и профилю, выражаются в академических часах. Часы контактной работы и самостоятельной работы обучающегося и часы, отводимые на процедуры контроля, могут различаться в учебных планах ОПОП по формам обучения. Объем контактной работы включает часы контактной аудиторной работы (практические занятия), контактной внеаудиторной работы (контроль самостоятельной работы), часы контактной работы в период аттестации. Контактная работа, в том числе может проводиться посредством электронной информационно-образовательной среды университета с использованием ресурсов сети Интернет и дистанционных технологий

5. Содержание дисциплины, структурированное по темам (разделам)

Исходя из рамок, установленных учебным планом по трудоемкости и видам учебной работы по дисциплине, преподаватель самостоятельно выбирает тематику занятий по формам и количеству часов проведения контактной работы: лекции и иные учебные занятия, предусматривающие преимущественную передачу учебной информации преподавателем и (или) занятия семинарского типа (семинары, практические занятия, практикумы, лабораторные работы, коллоквиумы и иные аналогичные занятия), и (или) групповые консультации, и (или) индивидуальную работу обучающихся с преподавателем, в том числе индивидуальные консультации (по курсовым работам/проектам – при наличии курсовой работы/проекта по данной дисциплине в учебном плане). Рекомендуемая тематика занятий максимально полно реализуется в контактной работе с обучающимися очной формы обучения. В случае реализации образовательной программы в заочной / очно-заочной форме трудоемкость дисциплины сохраняется, однако объем учебного материала в значительной части осваивается обучающимися в форме самостоятельной работы. При этом требования к ожидаемым образовательным результатам обучающихся по данной дисциплине не зависят от формы реализации образовательной программы.

№ п/п	Наименование вида двигательной активности	Содержание
1.	Общефизическая подготовка с основами атлетической гимнастики	Ознакомление с правилами техники безопасности. Общая физическая подготовка (совершенствование двигательных действий, воспитание физических качеств). Средства и методы ОФП: строевые упражнения, общеразвивающие упражнения без предметов, с предметами.

		Упражнения для воспитания силы: упражнения с отягощением, соответствующим собственному весу, весу партнера и его противодействию, с сопротивлением упругих предметов (эспандеры и резиновые амортизаторы), с отягощением (гантели, набивные мячи). Упражнения для воспитания выносливости: упражнения или элементы с постепенным увеличением времени их выполнения. Упражнения для воспитания гибкости. Методы развития гибкости: активные (простые, пружинящие, маховые), пассивные (с самозахватами или с помощью партнера). Упражнения для воспитания ловкости. Методы воспитания ловкости. Использование подвижных игр, гимнастических упражнений. Упражнения для воспитания быстроты. Совершенствование двигательных реакций повторным реагированием на различные (зрительные, звуковые, тактильные) сигналы. Методика оценки уровня функционального и физического состояния организма.
2.	Атлетическая гимнастика	Ознакомление с правилами техники безопасности. Изучение методических основ выполнения упражнений на тренажерах. Техника безопасности выполнения отдельных упражнений на тренажерах. Локальность воздействия отдельных упражнений на группы мышц. Разучивание и выполнение комплексов упражнений различного уровня воздействия. Упражнения для укрепления мышц из положения лёжа и сидя с партнёром и без (нижнего, верхнего и среднего отделов брюшного пресса). Использование тренажёрных снарядов (набивные мячи, эспандеры, гимнастические скакалки) для работы на мышцы брюшного пресса и спины. Работа на специализированных тренажёрах.
3.	Плавание. Начальное обучение	Ознакомление с правилами техники безопасности. Изучение подготовительных упражнений для освоения с водой, подводящие, имитационные упражнения для освоения гребковых движений работы рук и ног, согласования движений в способах плавания. Изучение основ техники спортивных способов плавания, кроль на груди и кроль на спине. Обучение технике стартов поворотов. Игры развлечения на воде. Общеразвивающие упражнения в воде для развития основных физических качеств.
4.	Спортивное плавание	Ознакомление с правилами техники безопасности. Общеразвивающие упражнения в воде для развития основных физических качеств. Имитационные упражнения. Упражнения для разучивания и совершенствования техники спортивных способов плавания, старта с тумбочки, старта в плавании кролем на спине, поворотов в данных спортивных способах плавания. Упражнения спортивной тренировки пловца. Плавание с использованием равномерного, переменного, интервального методов. Проплывание отрезков и дистанций с использованием повторного метода. Соревновательный и контрольный методы. Игровые задания. Правила соревнований. Судейство. Профессионально-

		прикладная физическая подготовка обучающихся средствами плавания.
5	ОФП с основами волейбола	Ознакомление с правилами техники безопасности. Общая физическая подготовка (совершенствование двигательных действий, воспитание физических качеств). Средства и методы ОФП: строевые упражнения, общеразвивающие упражнения без предметов, с предметами. Техника перемещений (ходьба; бег; скачок). Подачи (нижняя прямая; нижняя боковая; верхняя прямая; верхняя боковая). Передачи (вперед; назад). Нападающий удар. Прием мяча (снизу двумя руками; снизу одной рукой). Блок. Тактика игры (тактика защиты; тактика нападения). Учебная игра. Общая физическая и специальная физическая подготовка волейболиста. Профессионально-прикладная физическая подготовка обучающихся средствами волейбола.
6.	Волейбол	Ознакомление с правилами техники безопасности. Правила соревнований. Техника перемещений (ходьба; бег; скачок). Подачи (нижняя прямая; нижняя боковая; верхняя прямая; верхняя боковая). Передачи (вперед; назад). Нападающий удар. Прием мяча (снизу двумя руками; снизу одной рукой). Блок. Тактика игры (тактика защиты; тактика нападения). Учебная игра. Общая физическая и специальная физическая подготовка волейболиста. Профессионально-прикладная физическая подготовка обучающихся средствами волейбола.
7.	ОФП с основами с баскетбола	Ознакомление с правилами техники безопасности. Общая физическая подготовка (совершенствование двигательных действий, воспитание физических качеств). Средства и методы ОФП: строевые упражнения, общеразвивающие упражнения без предметов, с предметами. Правила соревнований. Техника перемещений (ходьба; бег; приставные шаги; прыжки; остановки; повороты). Техника нападения (ловля мяча; передача мяча; ведение мяча; броски). Техника защиты (выбивание; вырывание; накрывание; перехват; овладение мячом, отскочившим от щита или корзины). Тактика игры (тактика нападения; индивидуальные действия с мячом и без мяча; групповые взаимодействия). Учебная игра. Общая физическая и специальная физическая подготовка баскетболиста. Профессионально-прикладная физическая подготовка студентов средствами баскетбола.
8.	Баскетбол	Ознакомление с правилами техники безопасности. Правила соревнований. Техника перемещений (ходьба; бег; приставные шаги; прыжки; остановки; повороты). Техника нападения (ловля мяча; передача мяча; ведение мяча; броски). Техника защиты (выбивание; вырывание; накрывание; перехват; овладение мячом, отскочившим от щита или корзины). Тактика игры (тактика нападения; индивидуальные действия с мячом и без мяча; групповые взаимодействия). Учебная игра. Общая физическая и специальная физическая подготовка баскетболиста. Профессионально-прикладная физическая подготовка

		студентов средствами баскетбола.
9.	Мини - футбол	Ознакомление с правилами техники безопасности. Правила соревнований. Техника игры (передвижения: бег, ходьба, остановки, повороты, прыжки; удары по мячу: ногой, головой; ведение мяча; обманные движения (финты); прием мяча (остановка). Тактика игры. Учебная игра. Общая физическая и специальная физическая подготовка футболиста. Профессионально-прикладная физическая подготовка студентов средствами футбола.
10.	ОФП с основами с бадминтона	Ознакомление с правилами техники безопасности. Общая физическая подготовка (совершенствование двигательных действий, воспитание физических качеств). Средства и методы ОФП: строевые упражнения, общеразвивающие упражнения без предметов, с предметами. Правила соревнований. Освоение техники основных технических приемов в бадминтоне (стойки, подачи, удары, перемещения). Тактика игры, особенности парной игры. Особенности смешанной игры. Профессионально-прикладная физическая подготовка студентов средствами бадминтона.
11.	Бадминтон	Ознакомление с правилами техники безопасности. Освоение техники основных технических приемов в бадминтоне. (стойки, подачи, удары, перемещения. Тактика игры, Особенности парной игры. Особенности смешанной игры. Профессионально-прикладная физическая подготовка студентов средствами бадминтона.
12.	ОФП с основами настольного тенниса	Ознакомление с правилами техники безопасности. Общая физическая подготовка (совершенствование двигательных действий, воспитание физических качеств). Средства и методы ОФП: строевые упражнения, общеразвивающие упражнения без предметов, с предметами. Правила соревнований. Упражнения с мячом и ракеткой. Основные положения теннисиста. Способы удержания ракетки. Удары по мячу. Вращение мяча. Исходные положения, выбор места. Способы перемещения. Шаги, прыжки, выпады, броски. Подачи. Тактика одиночных игр. Игра в защите. Основные тактические комбинации. Основы тренировки теннисиста. Тренировка двигательных реакций. Игра у стола. Игровые комбинации.
13.	Настольный теннис	Ознакомление с правилами техники безопасности. Правила соревнований. Способы удержания ракетки. Жесткий хват, мягкий хват, хват «пером». Разновидности хватки «пером», «малые клещи», «большие клещи». Удары по мячу накатом. Удар по мячу с полулета, удар подрезкой, срезка, толчок. Игра в ближней и дальней зонах. Вращение мяча. Основные положения теннисиста. Исходные положения, выбор места. Способы перемещения. Шаги, прыжки, выпады, броски. Одношажные и двухшажные перемещения. Подача (четыре группы подач: верхняя, боковая, нижняя и со смешанным вращением). Подачи: короткие и длинные. Подача накатом, удары слева, справа,

		контрнакат (с поступательным вращением). Удары: накатом с подрезанного мяча, накатом по короткому мячу, крученая «свеча» в броске. Тактика одиночных игр. Игра в защите. Основные тактические комбинации. Применение подач с учетом атакующего и защищающего соперника. Основы тренировки теннисиста. Специальная физическая подготовка. Упражнения с мячом и ракеткой. Вращение мяча в разных направлениях. Тренировка двигательных реакций. Атакующие удары (имитационные упражнения) и в игре. Передвижения у стола (скрестные и приставные шаги, выпады вперед, назад и в стороны). Тренировка удара: накатом у стенки, удары на точность. Игра у стола. Игровые комбинации. Подготовка к соревнованиям (разминка общая и игровая).
14.	ОФП с основами ритмической гимнастики	Ознакомление с правилами техники безопасности. Общая физическая подготовка (совершенствование двигательных действий, воспитание физических качеств). Средства и методы ОФП: строевые упражнения, общеразвивающие упражнения без предметов, с предметами. Изучение базовых элементов техники движений. Построение занятия, требования к частям. Развитие основных физических качеств, разучивание и совершенствование различных комбинаций в ритмической гимнастики. Общеразвивающие упражнения в сочетании с танцевальными движениями на основе базовых шагов под музыкальное сопровождение. Разучивание комплексов упражнений силовой направленности, локального воздействия на различные группы мышц. Упражнения локального и регионального характера, упражнения на равновесие, изометрические упражнения с максимальным мышечным напряжением из различных исходных положений. Основы методики развития гибкости. Разучивание и совершенствование упражнений из различных видов стретчинга: пассивного и активного, динамического и статического. Рекомендации к составлению комплексов упражнений по совершенствованию отдельных физических качеств с учетом имеющихся отклонений в состоянии здоровья.
15.	Ритмическая гимнастика	Ознакомление с правилами техники безопасности. Изучение базовых элементов техники движений. Построение занятия, требования к частям. Развитие основных физических качеств, разучивание и совершенствование различных комбинаций в ритмической гимнастики. Общеразвивающие упражнения в сочетании с танцевальными движениями на основе базовых шагов под музыкальное сопровождение. Разучивание комплексов упражнений силовой направленности, локального воздействия на различные группы мышц. Упражнения локального и регионального характера, упражнения на равновесие, изометрические упражнения с максимальным мышечным напряжением из различных

		исходных положений. Основы методики развития гибкости. Разучивание и совершенствование упражнений из различных видов стретчинга: пассивного и активного, динамического и статического. Рекомендации к составлению комплексов упражнений по совершенствованию отдельных физических качеств с учетом имеющихся отклонений в состоянии здоровья.
16.	ОФП с основами Микс-Аэробики	Ознакомление с правилами техники безопасности. Общая физическая подготовка (совершенствование двигательных действий, воспитание физических качеств). Средства и методы ОФП: строевые упражнения, общеразвивающие упражнения без предметов, с предметами. Изучение базовых элементов техники движений. Построение занятия, требования к частям. Развитие основных физических качеств, разучивание и совершенствование различных комбинаций аэробики различных направлений. Средства танцевальной аэробики с элементами шейпинга: общеразвивающие упражнения в сочетании с танцевальными движениями на основе базовых шагов под музыкальное сопровождение. Разучивание комплексов упражнений силовой направленности, локального воздействия на различные группы мышц. Фитбол-аэробика: Особенности содержания занятий по фитбол-аэробике. Упражнения локального и регионального характера, упражнения на равновесие, изометрические упражнения с максимальным мышечным напряжением из различных исходных положений. Степ-аэробика: обучение различным вариантам шагов с подъемом на платформу (гимнастическую скамейку) и спуском с нее, танцевальным движениям, переходам с изменением ритма и направления движений. Основы методики развития гибкости. Разучивание и совершенствование упражнений из различных видов стретчинга: пассивного и активного, динамического и статического. Рекомендации к составлению комплексов упражнений по совершенствованию отдельных физических качеств с учетом имеющихся отклонений в состоянии здоровья.
17.	Микс-Аэробика	Ознакомление с правилами техники безопасности. Изучение базовых элементов техники движений. Построение занятия, требования к частям. Развитие основных физических качеств, разучивание и совершенствование различных комбинаций аэробики различных направлений. Средства танцевальной аэробики с элементами шейпинга: общеразвивающие упражнения в сочетании с танцевальными движениями на основе базовых шагов под музыкальное сопровождение. Разучивание комплексов упражнений силовой направленности, локального воздействия на различные группы мышц. Фитбол-аэробика: Особенности содержания занятий по фитбол-аэробике. Упражнения локального и регионального

		характера, упражнения на равновесие, изометрические упражнения с максимальным мышечным напряжением из различных исходных положений. Степ-аэробика: обучение различным вариантам шагов с подъемом на платформу (гимнастическую скамейку) и спуском с нее, танцевальным движениям, переходам с изменением ритма и направления движений. Основы методики развития гибкости. Разучивание и совершенствование упражнений из различных видов стретчинга: пассивного и активного, динамического и статического. Рекомендации к составлению комплексов упражнений по совершенствованию отдельных физических качеств с учетом имеющихся отклонений в состоянии здоровья.
18.	Самооборона	Общеразвивающие упражнения без предметов и с предметами. Упражнения для формирования правильной осанки. Упражнения для развития координации и точности движений. Упражнения для развития вестибулярного аппарата. Упражнения для развития ловкости. Развитие быстроты. Бег на короткие дистанции. Челночный бег. Развитие выносливости. Бег на длинные дистанции. Овладение навыками самостраховки. Кувырки, падения. Удары рукой и ногой. Прямой удар. Удар снизу. Удар сбоку. Удары ногой сбоку и назад. Защитные действия руками и ногами. Подставка предплечья. Болевые приемы. Загиб руки за спину. Сваливание для связывания. Рычаг руки наружу и внутрь. Броски. Задняя подножка. Бросок через спину. Освобождение от захватов противника. Освобождение от захвата рук. Освобождение от захвата за шею спереди. Освобождение от захвата туловища и рук сзади. Освобождение от захвата туловища спереди.
19.	Рукопашный бой	Основные стойки и позиции: ритуальные, информационные, тренировочные, боевые. Удары руками: прямой, боковой, апперкот, удары локтем. Удары в движении. Серии ударов. Удары ногами. Передвижение с нанесением ударов руками и ногами. Обучение защите от ударов руками и ногами. Блоки, уклоны, нырки, сбивы, уходы, захваты, встречные удары. Приемы страховки и самостраховки при падении. Борьба в стойке: приемы выведения из равновесия, бросковая техника, освобождение от захватов. Борьба в партере: позиции удержания, контроль, перевороты, болевые и удушающие приемы.
20.	ОФП с основами Zumba-fitness	Ознакомление с правилами техники безопасности. Общая физическая подготовка (совершенствование двигательных действий, воспитание физических качеств). Средства и методы ОФП: строевые упражнения, общеразвивающие упражнения без предметов, с предметами. Разучивание базовых шагов ритмов программы зумба: танго, кебрадита, сока, фламенко, самба. Разучивание техники фитнес танцев. Разучивание силового комплекса и стрейтчинга на гимнастических ковриках. – Кардиотренировка.

21.	Zumba-fitness	Разучивание базовых шагов ритмов программы зумба: танго, кебрадита, сока, фламенко, самба. Разучивание техники фитнес танцев "Habaneros", сока "Zoka Zumba"; кебрадита "Quiebra"; фламенко "Lolita"; самба "Alegria", меренга"El amore, el amore", кумбия "Bla bla bla", реггетон "Zumba mami", сальса "Gozando". Разучивание силового комплекса и стрейтчинга на гимнастических ковриках. Кардиотренировка.

Для обучающихся специальной медицинской группы используются средства корригирующей и оздоровительно-профилактической направленности. В занятиях используется индивидуально-дифференцированный подход в зависимости от уровня функциональной и физической подготовленности, характера и выраженности структурных и функциональных нарушений в организме, вызванных временными или постоянными патологическими факторами. Для данной категории обучающихся в занятиях есть ограничения двигательной нагрузки с учетом имеющихся противопоказаний, обусловленных конкретным заболеванием и в соответствии с рекомендациями врача. Используются статические и динамические дыхательные упражнения, общеразвивающие упражнения, упражнения в расслаблении, статико-динамические упражнения, упражнения в равновесии, на координацию движений, подвижные игры с различной психофизической нагрузкой, элементы стретчинга, фитбола, аэробики, пилатеса, йоги. Методики дыхательных гимнастик.

Студенты, временно освобожденные по состоянию здоровья (четвертой функциональной группы здоровья) выполняют индивидуальные проектные задания по темам:

1 семестр. Диагноз и краткая характеристика заболевания студента. Влияние заболевания на личную работоспособность и самочувствие. Место ЛФК в поддержании здоровья.

2 семестр. Медицинские противопоказания при занятиях физическими упражнениями и применения других средств физической культуры при данном заболевании (диагнозе). Физическая реабилитация и рекомендуемые средства лечебной и оздоровительной физической культуры при данном заболевании (диагнозе).

4 семестр. Реализация компонентов здорового образа жизни студента с учетом имеющихся отклонений в состоянии здоровья.

5 семестры. Оздоровительная физическая культура и ее место в поддержании работоспособности.

6 семестр. Реализация здоровьесберегащих технологий с учетом показателей физического состояния и имеющегося отклонения в здоровье.

6. Рекомендуемая тематика учебных занятий в форме контактной работы

–Материалы лекций;

–Учебно-методическая литература;

–Информационные ресурсы «Интернета»;

–Методические рекомендации и указания;

–Фонды оценочных средств.

Требования к самостоятельной работе обучающихся

Руководствуясь положениями статьи 47 и статьи 48 Федерального закона от 29 декабря 2012 г. N 273-ФЗ «Об образовании в Российской Федерации» научно-педагогические работники и иные лица, привлекаемые университетом к реализации данной образовательной программы, пользуются предоставленными академическими правами и свободами в части свободы преподавания, свободы от вмешательства в профессиональную деятельность; свободы выбора и использования педагогически обоснованных форм, средств, методов обучения и воспитания; права на творческую инициативу, разработку и применение авторских программ и методов обучения и воспитания в пределах реализуемой образовательной программы и отдельной дисциплины.

Исходя из рамок, установленных учебным планом по трудоемкости и видам учебной работы по дисциплине, преподаватель самостоятельно выбирает тематику занятий по формам и количеству часов проведения контактной работы: лекции и иные учебные занятия, предусматривающие преимущественную передачу учебной информации преподавателем и (или) занятия семинарского типа (семинары, практические занятия, практикумы, лабораторные работы, коллоквиумы и иные аналогичные занятия), и (или) групповые консультации, и (или) индивидуальную работу обучающихся с преподавателем, в том числе индивидуальные консультации (по курсовым работам/проектам – при наличии курсовой работы/проекта по данной дисциплине в учебном плане).

Рекомендуемая тематика занятий максимально полно реализуется в контактной работе с обучающимися очной формы обучения. В случае реализации образовательной программы в заочной / очно-заочной форме трудоемкость дисциплины сохраняется, однако объем учебного материала в значительной части осваивается обучающимися в форме самостоятельной работы. При этом требования к ожидаемым образовательным результатам обучающихся по данной дисциплине не зависят от формы реализации образовательной программы.

7. Методические рекомендации по видам занятий

Оценка знаний, умений, навыков, характеризующая этапы формирования компетенций по модулю «Элективные дисциплины по физической культуре и спорту» проводится в форме текущей, промежуточной аттестации. Осуществляется на основе:

- Требований к проведению занятий по физической культуре на учебный год;
- Положения о балльно-рейтинговой системе оценки учебных достижений студентов по модулям дисциплины «Физическая культура и спорт» Балтийского федерального университета имени Иммануила Канта.

Текущая проверка успеваемости проводиться выборочно на протяжении семестра. К ней относится проверка знаний, умений и навыков обучающихся:

- результатов освоения основных двигательных умений и навыков в соответствии с функциональной группой здоровья.
- результатов выполнения заданий (индивидуальных проектов).

Промежуточная аттестация – проводится в конце семестра с целью определения уровня овладения компетенциями, обучающимися (усвоения знаний; формирования умений и навыков); своевременного выявления преподавателем недостатков в практической и методической подготовке и принятия необходимых мер по ее корректировке; совершенствованию методики обучения; организации учебной работы и оказания индивидуальной помощи.

К контролю промежуточной успеваемости относятся:

- результаты посещаемости практических занятий.
- результаты тестирования физической подготовленности.

Особенностью преподавания данной дисциплины является систематичность занятий физическими упражнениями, т.к. это объясняется физиологическими процессами организма студента, которые обеспечивают развитие оптимального уровня развития физической и функциональной подготовленности. Поэтому необходимо систематически, два раза в неделю посещать учебные занятия, согласно выбранного вида двигательной активности, в течение модуля.

Формами организации учебных занятий по дисциплине являются: практические занятия, самостоятельная работа.

У студентов формируются знания, навыки и умения применения оздоровительной физической культуры, видов спорта в практической, физкультурно-оздоровительной и профессионально-прикладной деятельности.

На практических занятиях студенты осваивают техники основных базовых видов спорта и видов двигательной активности, формируются навыки для самостоятельного использования в повседневной жизни различных физических упражнений для сохранения здоровья и обеспечения высокой профессиональной работоспособности и профилактики профессиональных заболеваний будущего специалиста.

Самостоятельная работа студентов включает в себя: составление комплексов упражнений производственной и утренней гигиенической гимнастики, вопросы профессионально-прикладной физической культуры с учетом будущей профессии.

№ п/п	Наименование темы	Тематика самостоятельной работы
1	Практические занятия на основе вида двигательной активности	Методические основы самостоятельных занятий физическими упражнениями. Составление комплекса упражнений оздоровительной направленности.
		Методы самоконтроля в занятиях физическими упражнениями
		Методика составления комплексов упражнений в избранном виде двигательной активности
		Профессионально-прикладная физическая подготовка студентов. Физическая культура и спорт в профессиональной деятельности специалиста. Составление комплекса упражнений производственной гимнастики.

8. Фонд оценочных средств

8.1. Перечень компетенций с указанием этапов их формирования в процессе освоения образовательной программы в рамках учебной дисциплины

Основными этапами формирования указанных компетенций при изучении обучающимися дисциплины являются последовательное изучение содержательно связанных между собой тем учебных занятий. Изучение каждой темы предполагает овладение обучающимися необходимыми компетенциями. Результат аттестации обучающихся на различных этапах формирования компетенций показывает уровень освоения компетенций.

Контролируемые модули, разделы (темы) дисциплины	**Индекс контролируемой**	**Оценочные средства по этапам формирования компетенций**			**Способ контроля**
		текущий	**рубежный**	**итогов**	

	компетенции (или ее части)	контроль по дисциплине	контроль по дисциплине	ый контроль по дисциплине	
«Элективная дисциплина по физической культуре и спорту» Практические занятия на основе вида двигательной активности	УК –7	Контрольные упражнения - задания Учебные проекты	Тестирование	зачет	Контрольные упражнения по виду двигательной активности Тесты для оценки физической подготовленности

Перечень компетенций с указанием этапов их формирования в процессе освоения образовательной программы в рамках учебной дисциплины.

Основными этапами формирования указанных компетенций при изучении студентами дисциплины являются последовательное изучение содержательно связанных между собой разделов (тем) учебных занятий. Изучение каждого раздела (темы) предполагает овладение студентами необходимыми компетенциями. Результат аттестации студентов на различных этапах формирования компетенций показывает уровень освоения компетенций студентами.

Контролируемые модули, разделы (темы) дисциплины	Индекс контролируемой компетенции (или ее части)	Оценочные средства по этапам формирования компетенций			Способ контроля
		текущий контроль по дисциплине	рубежный контроль по дисциплине	итоговый контроль по дисциплине	
«Элективная дисциплина по физической культуре и спорту» Практические занятия на основе вида двигательной активности	УК –7	Контрольные упражнения - задания Учебные проекты	Тестирование	зачет	Контрольные упражнения по виду двигательной активности Тесты для оценки физической подготовленности

Показатели и критерии определения сформированности компетенций на различных этапах их формирования

Критерии оценки формируются в два этапа:

1-й этап: определение критериев оценки отдельно формируемой компетенции. Сущность 1-го этапа состоит в определении критериев для оценивания компетенции на основе продемонстрированного обучаемым уровня самостоятельности в применении полученных в ходе изучения учебной дисциплины, знаний, умений и навыков.

2-й этап: определение критериев для оценки уровня обученности по учебной дисциплине на основе комплексного подхода к уровню сформированности всех компетенций, обязательных к формированию в процессе изучения предмета. Сущность 2-го этапа определения критерия оценки по учебной дисциплине заключена в определении подхода к оцениванию на основе ранее полученных данных о сформированности каждой компетенции, обязательной к выработке в процессе изучения предмета. В качестве основного критерия при оценке обучаемого при определении уровня освоения учебной дисциплины наличие сформированных у него компетенций по результатам освоения учебной дисциплины.

Критерии определения сформированности компетенций на итоговой аттестации по дисциплине

Компетенции	**Этапы формирования**	**Показатели сформированности**	**Средства и критерии оценки**
УК - 7	Ориентировочный (начальный)	**Знать:** Роль физической культуры в подготовке будущего специалиста; Методику использования видов двигательной активности в процессе учебной и профессиональной деятельности; Основы обучения двигательным действиям; Основы развития и совершенствования физических качеств; Правила техники безопасности при выполнении упражнений;	Посещение практических занятий не менее 80%
	Деятельностный (Основной)	**Уметь:** Применять средства физической культуры для освоения основных двигательных действий; Применять средства и методы для развития и совершенствования	Комплексы упражнений Контрольных упражнений

		физических качеств;	
	Контрольно-корректировочный (завершающий)	**Владеть** средствами и методами физической культуры необходимыми для обеспечения полноценной жизнедеятельности;	Выполнение тестов физической подготовленности

8.2. Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений и навыков и (или) опыта деятельности процессе текущего контроля

КОНТРОЛЬНЫЕ УПРАЖНЕНИЯ ДЛЯ ОЦЕНКИ ФИЗИЧЕСКОЙ И ТЕХНИЧЕСКОЙ ПОДГОТОВЛЕННОСТИ
для студентов 1 – 3 курсов
Элективная дисциплина БАСКЕТБОЛ

1 курс

Контрольное упражнение		Нормативы и оценки									
		Мужчины					женщины				
		5	**4**	**3**	**2**	**1**	**5**	**4**	**3**	**2**	**1**
1.	Прыжок в длину с места (см)	**235**	**225**	**220**	**205**	**190**	**190**	**180**	**170**	**160**	**150**
2.	Ведение с последующим броском после двух шагов	**5**	**4**	**3**	**2**	**1**	**5**	**4**	**3**	**2**	**1**
3.	Штрафные броски. Количество попаданий из 10 бросков	**5**	**4**	**3**	**2**	**1**	**5**	**4**	**3**	**2**	**1**

2 курс

Контрольное упражнение		Нормативы и оценки									
		Мужчины					женщины				
		5	**4**	**3**	**2**	**1**	**5**	**4**	**3**	**2**	**1**
1.	Перемещения различными способами вокруг штрафной зоны	**16,0**	**16,5**	**17,5**	**18,5**	**19,5**	**17,5**	**18,0**	**18,5**	**19,5**	**20,5**
2.	Ведение с изменением направления (змейка) с последующим броском после двух шагов	**5**	**4**	**3**	**2**	**1**	**5**	**4**	**3**	**2**	**1**
3.	Штрафные броски. Количество попаданий из 10 бросков	**6**	**5**	**4**	**3**	**1**	**6**	**5**	**4**	**3**	**1**

3 курс

Контрольное упражнение	Нормативы и оценки	
	Мужчины	женщины

		5	4	3	2	1	5	4	3	2	1
1.	Перемещения различными способами вокруг штрафной зоны	**15,5**	**16,0**	**17,0**	**18,0**	**19,0**	**17,5**	**18,0**	**18,5**	**19,0**	**20,0**
2.	Ведение с изменением направления (змейка) с последующим броском после двух шагов	**6**	**5**	**3**	**2**	**1**	**6**	**4**	**3**	**2**	**1**
3.	Штрафные броски. Количество попаданий из 10 бросков	**6**	**5**	**4**	**3**	**2**	**6**	**5**	**4**	**3**	**2**

Требования к выполнению контрольных упражнений
По элективной дисциплине баскетбол

1. Прыжок в длину с места. (для 1 курса)

Прыжок выполняется толчком двумя ногами в соответствующем секторе для прыжков. Место отталкивания должно обеспечивать хорошее сцепление с обувью. Участник принимает ИП: ноги на ширине плеч, ступни параллельно, носки ног перед линией отталкивания. Одновременным толчком двух ног выполняется прыжок вперед. Мах руками допускается.

Измерение производится по перпендикулярной прямой от места отталкивания любой ногой до ближайшего следа, оставленного любой частью тела участника. Участнику предоставляются три попытки. В зачет идет лучший результат.

Ошибки (попытка не засчитывается): заступ за линию отталкивания или касание ее; выполнение отталкивания с предварительного подскока; отталкивание ногами поочередно.

1. Перемещения различными способами вокруг штрафной зоны. (для 2 и 3 курса)

По периметру баскетбольной штрафной зоны стандартного размера расставить 4 конуса (по внешним углам зоны). Все перемещения выполнять лицом к противоположному щиту. Высокий старт из-за лицевой линии слева от щита, правая рука на конусе. По сигналу начинать перемещения приставным шагом в защитной стойке правым боком (коснуться конуса левой рукой), затем вперед до штрафной линии (коснуться конуса левой рукой), затем приставным шагом левым боком в защитной стойке вдоль штрафной линии (коснуться конуса правой рукой), затем спиной вперед до лицевой линии (коснуться конуса правой рукой). Второй круг выполнять в обратном направлении: вперед, правым боком, спиной вперед, левым боком. На каждой смене передвижения – коснуться конуса рукой.

Время выполнения в секундах: от стартового сигнала до последнего касания конуса.

Ошибки: Перемещения неуказанным способом, нарушение границ штрафной зоны.

2. Ведение с последующим броском после двух шагов. (для 1 курсов)

Ведение мяча справа и слева от центральной линии с последующим выполнением броска после двух шагов соответствующей рукой. Выполнять по 3 раза с левой и правой стороны. Считается количество попаданий (из 6 бросков). Засчитываются попадания, выполненные без игровых нарушений. Каждый участник выполняет по 3 попытки. Фиксируется лучший результат.

Ошибки: Нарушение двушажного ритма (1 или 3 шага), выполнение шагов не в той последовательности, броски в кольцо разноименной рукой, пробежки, нарушения техники ведения.

2. Ведение с изменением направления (змейка) с последующим броском после двух шагов. (для 2 и 3 курсов)

Поставить по 5 конусов с правой и левой стороны площадки (расстояние между конусами 2 метра). Выполнять по 3 раза с левой и правой стороны. Ведение мяча с изменением направления (змейка) дальней рукой от конуса и бросок после двух шагов соответствующей рукой. Считается количество попаданий (из 6 бросков). Засчитываются попадания, выполненные без игровых нарушений. Каждый участник выполняет по 3 попытки. Фиксируется лучший результат.

Ошибки: Нарушение двушажного ритма (1 или 3 шага), выполнение шагов не в той последовательности, броски в кольцо разноименной рукой, пробежки, нарушения техники ведения.

3. Штрафные броски. Количество попаданий из 10 бросков.

Выполнить 10 штрафных бросков без игровых нарушений. Попадание с нарушением не засчитывается. Каждый участник выполняет по 3 попытки. Фиксируется лучший результат.

Ошибки: Заступ штрафной линии.

КОНТРОЛЬНЫЕ УПРАЖНЕНИЯ ДЛЯ ОЦЕНКИ ФИЗИЧЕСКОЙ И ТЕХНИЧЕСКОЙ ПОДГОТОВЛЕННОСТИ
для студентов 1 – 3 курсов
Элективная дисциплина БАДМИНТОН

Контрольное упражнение		Нормативы и оценки				
		1 КУРС				
		5	**4**	**3**	**2**	**1**
1.	Выполнение подачи открытой стороной ракетки, количество попаданий в квадрат подачи	10	8	6	3	Менее 3

2.	Выполнение подачи закрытой стороной ракетки, количество попаданий в квадрат подачи	10	8	6	3	Менее 3
3.	Двустороняя игра через сетку, количество ударов над сеткой без потери волана	50 ударов без потери волана	35	20	10	Менее 10
Контрольное упражнение						
		2 КУРС				
		5	**4**	**3**	**2**	**1**
1.	Выполнение подачи открытой стороной ракетки, количество попаданий в квадрат подачи	10	9	8	7	Менее 5
2.	Выполнение подачи закрытой стороной ракетки, количество попаданий в квадрат подачи	10	9	8	7	Менее 5
3.	Двустороняя игра через сетку, количество ударов над сеткой без потери волана	60 ударов без потери волана	50	40	30	Менее 20
Контрольное упражнение						
		3 КУРС				
		5	**4**	**3**	**2**	**1**
1.	Выполнение подачи открытой стороной ракетки, количество попаданий в квадрат подачи	10	9	8	7	Менее 6
2.	Выполнение подачи закрытой стороной ракетки, количество попаданий в квадрат подачи	10	9	8	7	Менее 6
3.	Двустороняя игра через сетку, количество ударов над сеткой без потери волана	70 ударов без потери волана	60	50	40	Менее 30

Требования к выполнению контрольных упражнений

По элективной дисциплине бадминтон

1. **Подача открытой стороной ракетки (кол-во попаданий в зону подачи)**

— введение волана в игру. Хватка «Открытая» — это значит, при любом ударе этой стороной рука с ракеткой как бы открывает туловище.

Основная стойка, ноги на ширине плеч. Левое плечо развернуто вперед. Волан держится в левой вытянутой вперед руке. Правая рука отведена назад вниз в сторону, потом энергичное движение кисти руки, и ракетка бьет по волану, выпущенному из левой руки. Одновременно с ударом корпус поворачивается влево, и тяжесть тела передается на левую ногу. Ракетка движется по инерции вперед вверх. (Движения похожи на те, которые проделывает волейболист при нижней подаче мяча.)

Выполнить 10 подач через сетку в правый квадрат подачи (без ошибок). Правильной считается подача, без технических ошибок, при которой волан приземляется в поле подачи. Попадание волана с нарушением не засчитывается. Каждый участник выполняет 1 подход. Фиксируется количество попаданий.

Ошибки при подаче:

1. Нельзя отрывать ногу от пола.
2. В момент удара ракетка не должна подниматься выше пояса игрока.

2. **Подача закрытой стороной ракетки (кол-во попаданий в зону подачи)**

— введение волана в игру. «Закрытая» сторона — рука с ракеткой как бы закрывает туловище.

Основная стойка, ноги на ширине плеч. Правое плечо развернуто вперед. Волан держится в левой вытянутой вперед руке. Правая рука отведена назад вниз в сторону, потом энергичное движение кисти руки, и ракетка бьет по волану, выпущенному из левой руки. Одновременно с ударом корпус поворачивается вправо, и тяжесть тела передается на правую ногу. Ракетка движется по инерции вперед вверх.

Выполнить 10 подач через сетку в левый квадрат подачи (без ошибок). Правильной считается подача, без технических ошибок, при которой волан приземляется в поле подачи. Попадание волана с нарушением не засчитывается. Каждый участник выполняет 1 подход. Фиксируется количество попаданий.

Ошибки при подаче:

1. Нельзя отрывать ногу от пола.
2. В момент удара ракетка не должна подниматься выше пояса игрока.

3. **Двухсторонняя игра справа/слева в парах без потери волана (кол-во раз)**

Откидка - удар открытой и закрытой стороной ракетки по волану, находящемуся на уровне кромки сетки и ниже, который затем летит по высокой траектории.

Удар справа выполняют открытой стороной ракетки.

Из основной стойки разверните корпус вправо и немного отклоните его назад. Тяжесть тела на отставленной назад правой ноге. Рука с ракеткой чуть согнута в локте и отведена назад вверх. Ракетка должна встретить волан немного впереди корпуса. Когда волан приближается, рука с ракеткой делает хлесткий, свободный удар. Все время смотрите на подлетающий волан — это избавит от промахов.

Удар слева выполняют закрытой стороной ракетки.

Корпус поворачивается влево. Тяжесть тела переносится на левую ногу. Затем правая нога делает шаг вперед навстречу подлетающему волану. Одновременно ракетка отводится назад влево.

Вы смотрите на подлетающий волан и начинаете разворот корпуса в направлении удара. Руку с ракеткой выносите локтем вперед навстречу волану, распрямляете ее и хлестким движением бьете по волану.

С партнером через сетку технически правильно выполнить удары справа, слева. Уметь сочетать оба приема в двухсторонней игре через сетку. Учитывается количество ударов без потери волана.

Ошибки:

1. Одному и тому же испытуемому нельзя касаться волана (выполнять удар) подряд дважды.
2. Волан не должен коснуться пола (потеря волана).

Контрольные упражнения по модулю «Элективные дисциплины по физической культуре». «ОФП с элементами атлетической гимнастики» 1 курс

Контрольные нормативы для девушек

Упражнение	**Оценка в баллах**				
	5	**4**	**3**	**2**	**1**
Сгибание-разгибание рук в упоре лежа, количество	12	11	9	7	4
Приседания за 30 с, раз	25	23	21	19	17
Гиперэкстензия из положения лежа на животе, раз	55	47	36	25	20

Контрольные нормативы для юношей

Упражнение	Оценка в баллах				
	5	**4**	**3**	**2**	**1**
Сгибание-разгибание рук на брусьях, количество	20	17	14	10	6
Выпрыгивания из положения присед, количество раз в мин.	45	35	25	20	10
Гиперэкстензия из положения лежа на животе, раз	55	45	35	30	20

Контрольные упражнения по модулю «Элективные дисциплины по физической культуре». «Атлетическая гимнастика» 2-3 курс

Контрольные нормативы для девушек

Упражнение	Оценка в баллах				
	5	**4**	**3**	**2**	**1**
Сгибание-разгибание рук в упоре лежа, количество	15	13	11	8	4
Приседания за 30 с, раз	30	28	26	24	22
Гиперэкстензия из положения лежа на животе, раз	60	50	40	30	20

Контрольные нормативы для юношей

Упражнение	Оценка в баллах				
	5	**4**	**3**	**2**	**1**
Сгибание-разгибание рук на брусьях, количество	25	21	17	13	9
Выпрыгивания из положения присед, количество раз в мин.	50	40	30	20	10
Гиперэкстензия из положения лежа на животе, раз	60	50	40	30	20

КОНТРОЛЬНЫЕ УПРАЖНЕНИЯ ДЛЯ ОЦЕНКИ ФИЗИЧЕСКОЙ ПОДГОТОВЛЕННОСТИ
для студентов 1-3 курсов
Элективная дисциплина <u>ВОЛЕЙБОЛ</u>
1 курс

Контрольное упражнение		Нормативы и оценки									
		Мужчины					женщины				
		5	**4**	**3**	**2**	**1**	**5**	**4**	**3**	**2**	**1**
1.	Передача мяча сверху двумя руками над собой	15	13	11	9	7	15	13	11	9	7
2.	Передача мяча снизу двумя руками в стену	15	13	11	9	7	15	13	11	9	7
3.	Верхняя прямая подача	10	8	6	4	2	10	8	6	4	2

2 курс

Контрольное упражнение		Нормативы и оценки									
		Мужчины					женщины				
		5	**4**	**3**	**2**	**1**	**5**	**4**	**3**	**2**	**1**
1.	Передача мяча сверху двумя	18	15	13	11	9	18	15	13	11	9

	руками над собой										
2.	Передача мяча снизу двумя руками в стену	18	15	13	11	9	18	15	13	11	9
3.	Верхняя прямая подача	11	9	7	5	3	11	9	7	5	3

3 курс

Контрольное упражнение		Нормативы и оценки									
		Мужчины					женщины				
		5	**4**	**3**	**2**	**1**	**5**	**4**	**3**	**2**	**1**
1.	Передача мяча сверху двумя руками над собой	20	17	15	13	11	20	17	15	13	11
2.	Передача мяча снизу двумя руками в стену	20	17	15	13	11	20	17	15	13	11
3.	Верхняя прямая подача	12	10	8	6	4	12	10	8	6	4

Требования к выполнению контрольных упражнений
По элективной дисциплине волейбол

1. **Передача мяча сверху двумя руками над собой.** Выполняется в кругу диаметром 3 м. Норматив: 15 передач над собой, высота передачи не менее 1,5 м.
2. **Передача мяча снизу двумя руками в стену.** Выполняется на расстоянии 3 м. от стены.
3. **Верхняя прямая подача.** Норматив из 15 подач необходимо результативное попадание в площадку.

Ошибки:

1. **Передача мяча сверху двумя руками над собой.**
- большие пальцы направлены вперёд;
- локти слишком широко разведены или наоборот;
- кисти рук встречают мяч при почти выпрямленных в локтевых суставах руках.

2. **Передача мяча снизу двумя руками в стену.**
- в момент приёма руки согнуты в локтевых суставах;
- руки почти параллельны полу;
- резкое встречное движение рук к мячу;
- приём мяча на «кулаки».

3. <u>Верхняя прямая подача</u>.

- в исходном положении вперёд ставится нога, одноимённая бьющей руке;
- подброс мяча не оптимален по высоте;
- удар по мячу неточный (сверху, сбоку);
- скорость бьющей руки незначительна;
- удар по мячу выполняется рукой, согнутой в локтевом суставе.

КОНТРОЛЬНЫЕ УПРАЖНЕНИЯ ДЛЯ ОЦЕНКИ ФИЗИЧЕСКОЙ ПОДГОТОВЛЕННОСТИ
для студентов 1-3 курсов
Элективная дисциплина <u>МИНИФУТБОЛ</u>

1 курс

Контрольное упражнение		Нормативы и оценки									
		Мужчины					женщины				
		5	**4**	**3**	**2**	**1**	**5**	**4**	**3**	**2**	**1**
1.	Удар по воротам	6	5	4	3	2	5	4	3	2	1
2.	Жонглирование	21	19	17	15	13	13	11	10	9	8
3.	Удар на дальность - сумма ударов правой и левой ногой (м)	80	75	70	65	60	60	55	50	45	40

2 курс

Контрольное упражнение		Нормативы и оценки									
		Мужчины					женщины				
		5	**4**	**3**	**2**	**1**	**5**	**4**	**3**	**2**	**1**
1.	Удар по воротам	7	6	5	4	3	6	5	4	3	2
2.	Жонглирование	23	21	19	17	15	14	12	11	10	9
3.	Удар на дальность - сумма ударов правой и левой ногой (м)	85	80	75	70	65	60	55	50	45	40

3 курс

Контрольное упражнение		Нормативы и оценки									
		Мужчины					женщины				
		5	**4**	**3**	**2**	**1**	**5**	**4**	**3**	**2**	**1**
1.	Удар по воротам (10 раз)	8	7	6	5	4	7	6	5	4	3
2.	Жонглирование (3 попытки)	25	23	21	19	17	15	13	12	11	10
3.	Удар на дальность - сумма ударов правой и левой ногой (м)	90	85	80	75	70	60	55	50	45	40

Требования к выполнению контрольных упражнений
По элективной дисциплине мини-футбол

1. **Удар по воротам.** (для 1,2,3 курсов)

Удар по воротам выполняется футбольным мячом с расстояния 10м, любой ногой и любым удобным для студента способом. Попытка является результативной, если мяч после удар пересекает линию ворот, не коснувшись поверхности площадки (по воздуху).

Ошибки:
- не бить по катящемуся мячу;
- один удар - одна попытка;
- линия ворот не входит в створ ворот;
-мяч должен пересечь линию ворот полностью.

2. **Жонглирование.** (для 1,2,3 курсов)

Жонглирование ногами, коленями, головой, и плечами. **Держать мяч перед собой на уровне груди.** Подбросить руками вверх. Когда мяч начнет снижаться, подбросьте его ногой обратно в воздух, не дав ему опуститься на землю.

Ошибки:
- касание мяча земли
- касание мяча руки

3. **Удар на дальность.** (для 1,2,3 курсов)

На выполнение данного упражнения дается по одной попытке (с левой и правой ноги). Удар осуществляется ногой по неподвижному мячу. Суммируются оба удара. Результат фиксируется по ближайшему касанию мяча с землей.

Ошибки:
-касание потолка или стен мячом
- не выполнять удар по движущемуся мячу

КОНТРОЛЬНЫЕ УПРАЖНЕНИЯ ДЛЯ ОЦЕНКИ ТЕХНИЧЕСКОЙ ПОДГОТОВЛЕННОСТИ
для студентов 1, 3 курсов
Элективная дисциплина НАСТОЛЬНЫЙ ТЕННИС

Контрольное упражнение		Нормативы и оценки				
		1 КУРС				
		5	**4**	**3**	**2**	**1**
1.	Подачи («откидкой», «подрезкой») справа и слева, количество подач.	15	10	8	6	4
2.	Сочетание «откидки» справа и слева, количество ударов	20	15	10	8	6
3.	Сочетание «наката» справа и слева, количество ударов	15	10	8	6	4
Контрольное упражнение						
		2 КУРС				
		5	**4**	**3**	**2**	**1**
1.	Подачи («откидкой», «подрезкой») справа и слева, количество подач.	18	13	10	8	6
2.	Сочетание «откидки» справа и слева, количество ударов	25	17	13	10	8
3.	Сочетание «наката» справа и слева, количество ударов	18	13	10	8	6
Контрольное упражнение						
		3 КУРС				
		5	**4**	**3**	**2**	**1**
1.	Подачи («откидкой», «подрезкой») справа и слева, количество подач.	20	15	13	10	8
2.	Сочетание «откидки» справа и слева, количество ударов	30	20	15	13	10
3.	Сочетание «наката» справа и слева, количество ударов	20	15	13	10	8

Требования к выполнению контрольных упражнений
По элективной дисциплине настольный теннис

1. **Подачи «откидкой» «подрезкой» справа и слева, количество подач**

«Окидкой» слева выполняется плоским ударом по мячу без вращения.
«Окидкой» справа также выполняется плоским ударом по мячу без вращения.
«Подрезкой» слева – подача, при которой мячу придается сильное нижнее левое боковое вращение.
«Подрезкой» справа – подача, при которой мячу придается сильное нижнее правое боковое вращение.
Подача — это удар с двойным отскоком мяча. Мяч должен, отскочив от стороны подающего, перелететь через сетку на сторону принимающего. Подача считается поданной, как только мяч оторвался от ладони подающего.

Ошибки при подаче:

1) Не выполняется из статического положения.
2) Не соблюдается правило подброса мяча.
3) При подаче мяч не должен коснуться сетки.

2. **Игра «откидкой» справа и слева, количество ударов**

«Откидка» справа, слева – удары без вращения мяча (плоские удары).
«Откидка» слева. Стойка: ноги не напряжены, согнуты в коленях, вес тела переносится вперед на впереди стоящую ногу. Замах делается согнутой рукой. Носик ракетки идет за мячом. Удар плоский, выполняется строго перед собой. Перенос веса тела производится в момент удара ракеткой по мячу.
«Откидка» справа. Удар плоский без вращения. При его нанесении рука согнута примерно на 45 градусов. Левая нога стоит впереди, и при ударе на нее переносится вес тела. При ударе ракетка аккуратно подводится к мячу и переносит мяч на другую сторону стола. Удар наносится перед собой.

Ошибки при игре «откидкой»:

1) Нельзя запускать мяч за себя при игре «откидкой» справа.
2) Удары выполняются строго перед собой.

3. **Игра «накатом» справа и слева, количество ударов**

«Накат» справа - атакующий удар. До удара необходимо занять развернутую позицию: левая нога впереди, плечи развернуты, правое плечо несколько ниже, чем левое. При замахе рука согнута в локте примерно на 45 градусов, носик ракетки смотрит в сторону. Удар наносится согнутой в локте рукой. В момент контакта ракетки с мячом происходит окончательное сгибание локтя, что позволяет придать мячу максимальную скорость. Обгоняя мяч по задней верхней части, носик ракетки направляет его на другую сторону стола. Вес тела переносится с правой ноги на стоящую впереди левую ногу. «Накат» справа наносится по восходящему мячу в высшей точке полета мяча.

«Накат» слева - атакующий удар с верхним вращением. Ракетка обгоняет мяч по верхней его части. Удар наносится по восходящему мячу или по высшей точке отскока. Ракетка опущена немного ниже локтя, замах производится снизу. Ракетка играет по задней верхней части мяча. При замахе носик ракетки смотрит в сторону. Во время удара кисть быстро поворачивает ракетку, а носик сопровождает движение мяча на другую сторону стола. Стойка одинаковая для всех ударов слева. Мяч играется строго перед собой. В момент удара по мячу игровое плечо опускается, а локоть разгибается. Скорость полета мяча зависит от того, насколько быстро сыграет предплечье и кисть. Необходимо строго занимать выгодную позицию перед ударом, подходить к мячу так, чтобы он находился прямо перед собой. В момент замаха колени сгибаются, а в момент удара разгибаются.

Ошибки при игре «накатом»:

3) Удар «накатом» справа наносится по восходящему мячу в высшей точке полета мяча.
4) При игре «накатом» слева удары выполняются строго перед собой.

КОНТРОЛЬНЫЕ УПРАЖНЕНИЯ ДЛЯ ОЦЕНКИ ФИЗИЧЕСКОЙ ПОДГОТОВЛЕННОСТИ
для студентов 1 курсов
Элективная дисциплина «ОФП+MIX АЭРОБИКА»

Контрольное упражнение		Нормативы и оценки									
		Мужчины					женщины				
		5	**4**	**3**	**2**	**1**	**5**	**4**	**3**	**2**	**1**
1.	Комбинация на 32 счета с использованием степ-платформы	выполнение без ошибок	1-2 ошибки	3-4 ошибки	5-6 ошибок	более 6 ошибок	выполнение без ошибок	1-2 ошибки	3-4 ошибки	5-6 ошибок	более 6 ошибок
2.	Прыжки на двух ногах через скакалку, кол-во раз за 1 мин.	130 и более	120-129	110-119	100-110	100-99	140 и более	130-139	120-129	110-119	100-109
3.	Упор лежа «Планка», (сек)	150 сек	120 сек	90 сек	60 сек	45 сек	120 сек	90 сек	60 сек	45 сек	30 сек

Требования к выполнению контрольных упражнений
По элективной дисциплине ОФП+MIX аэробика
для студентов 1 курса

Методические рекомендации по выполнению контрольных упражнений:

1. Комбинация на 32 счета.

Упражнение проводится на любой ровной площадке с твердым покрытием с использованием степ-платформы. Студент выполняет последовательно в заданном музыкальном ритме комбинацию из элементов ритмической гимнастики: шаги, повороты, подскоки, бег и т.д., сопровождающиеся работой рук, туловища, головы с правой и левой ноги на 32 счета. Оценивается техника выполнения элементов, амплитуда движений, музыкальность, чувство ритма.

Ошибки: сбой в темпе и ритме упражнений, непопадание в музыку, повтор выполнения элементов более чем на 8 счетов.

2. Прыжки на двух ногах через скакалку.

Прыжки через скакалку проводятся на любой ровной площадке с твердым покрытием, обеспечивающим хорошее сцепление с обувью. По команде «На старт!» студент принимает положение основная стойка, скакалка за спиной на полу в двух руках. По команде «Марш!» (с одновременным включением секундомера) начинает прыжки на двух ногах с прокручиванием скакалки на каждый прыжок. Фиксируется количество прыжков без сбоев за 1 минуту.

Скорость увеличиваем, стараясь добиться результата 180 оборотов в минуту, что равноценно трем прыжкам в секунду. Направление вращения скакалки не меняется.

Ошибки: напрыгивание перед отталкиванием, вращение прямыми руками, сбой.

3. Упор лежа «Планка»

Статическое упражнение «ПЛАНКА» проводится на любой ровной площадке с твердым покрытием, обеспечивающим хорошее сцепление с обувью. По команде «Марш!» (с одновременным включением секундомера) участник принимает положение «УПОР ЛЕЖА» на прямых руках, фиксируется время неподвижного удержания прямого положения тела без провисания живота и прогиба в спине, ноги прямые с опорой на носок, стопы на ширине таза.

Ошибки: кисть не под плечом, прогиб в пояснице, высокое положение таза.

Результаты выполнения контрольных упражнения суммируются и их сумма переводится в бонусные баллы учебного раздела БРС:

КОНТРОЛЬНЫЕ УПРАЖНЕНИЯ ДЛЯ ОЦЕНКИ ФИЗИЧЕСКОЙ ПОДГОТОВЛЕННОСТИ
для студентов 2,3 курсов
Элективная дисциплина «MIX АЭРОБИКА»

Контрольное упражнение		Нормативы и оценки									
		Мужчины					женщины				
		5	**4**	**3**	**2**	**1**	**5**	**4**	**3**	**2**	**1**
1.	Комбинация на 64 счета с использованием степ-платформы	выполнение без ошибок	1-2 ошибки	3-4 ошибки	5-6 ошибок	более 6 ошибок	выполнение без ошибок	1-2 ошибки	3-4 ошибки	5-6 ошибок	более 6 ошибок
2.	Прыжки на двух ногах через скакалку, кол-во раз за 20 сек.	50 и более	40-49	30-39	20-29	10-19	60 и более	50-59	40-49	30-39	20-29
3.	Упор лежа «Планка», (сек)	150 сек	120 сек	90 сек	60 сек	45 сек	120 сек	90 сек	60 сек	45 сек	30 сек

Требования к выполнению контрольных упражнений

По элективной дисциплине «MIX аэробика»
для студентов 2,3 курсов
Методические рекомендации по выполнению контрольных упражнений:

1. Комбинация на 64 счета.

Упражнение проводится на любой ровной площадке с твердым покрытием с использованием степ-платформы. Студент выполняет последовательно в заданном музыкальном ритме комбинацию из элементов ритмической гимнастики: шаги, повороты, подскоки, бег и т.д., сопровождающиеся работой рук, туловища, головы с правой и левой ноги на 32 счета. Оценивается техника выполнения элементов, амплитуда движений, музыкальность, чувство ритма.

Ошибки: сбой в темпе и ритме упражнений, непопадание в музыку, повтор выполнения элементов более чем на 8 счетов.

2. Прыжки на двух ногах через скакалку.

Прыжки через скакалку проводятся на любой ровной площадке с твердым покрытием, обеспечивающим хорошее сцепление с обувью. По команде «На старт!» студент принимает положение основная стойка, скакалка за спиной на полу в двух руках. По команде «Марш!» (с одновременным включением секундомера) начинает прыжки на двух ногах с прокручиванием скакалки на каждый прыжок. Фиксируется количество прыжков без сбоев за 20 секунд.

Скорость увеличиваем, стараясь добиться результата 180 оборотов в минуту, что равноценно трем прыжкам в секунду. Направление вращения скакалки не меняется.

Ошибки: напрыгивание перед отталкиванием, вращение прямыми руками, сбой.

3. Упор лежа «Планка»

Статическое упражнение «ПЛАНКА» проводится на любой ровной площадке с твердым покрытием, обеспечивающим хорошее сцепление с обувью. По команде «Марш!» (с одновременным включением секундомера) участник принимает положение «УПОР ЛЕЖА» на прямых руках, фиксируется время неподвижного удержания прямого положения тела без провисания живота и прогиба в спине, ноги прямые с опорой на носок, стопы на ширине таза.

Ошибки: кисть не под плечом, прогиб в пояснице, высокое положение таза.

КОНТРОЛЬНЫЕ УПРАЖНЕНИЯ ДЛЯ ОЦЕНКИ ФИЗИЧЕСКОЙ ПОДГОТОВЛЕННОСТИ
для студентов 1 курсов
Элективная дисциплина ОФП+РИТМИЧЕСКАЯ ГИМНАСТИКА

Контрольное упражнение		Нормативы и оценки									
		Мужчины					женщины				
		5	**4**	**3**	**2**	**1**	**5**	**4**	**3**	**2**	**1**
1.	Комбинация на 32 счета без степ-платформы	выполнение без ошибок	1-2 ошибки	3-4 ошибки	5-6 ошибок	более 6 ошибок	выполнение без ошибок	1-2 ошибки	3-4 ошибки	5-6 ошибок	более 6 ошибок
2.	Прыжки на двух ногах через скакалку, кол-во раз за 1 мин.	130 и более	120-129	110-119	100-110	100-99	140 и более	130-139	120-129	110-119	100-109
3.	Упор лежа «Планка», (сек)	150 сек	120 сек	90 сек	60 сек	45 сек	120 сек	90 сек	60 сек	45 сек	30 сек

Требования к выполнению контрольных упражнений
По элективной дисциплине офп+ритмическая гимнастика
для студентов 1 курсов

Методические рекомендации по выполнению контрольных упражнений:

1. Комбинация на 32 счета.

Упражнение проводится на любой ровной площадке с твердым покрытием. Студент выполняет последовательно в заданном музыкальном ритме комбинацию из элементов ритмической гимнастики: шаги, повороты, подскоки, бег и т.д., сопровождающиеся работой рук, туловища, головы с правой и левой ноги на 32 счета. Оценивается техника выполнения элементов, амплитуда движений, музыкальность, чувство ритма.

Ошибки: сбой в темпе и ритме упражнений, непопадание в музыку, повтор выполнения элементов более чем на 8 счетов.

2. Прыжки на двух ногах через скакалку.

Прыжки через скакалку проводятся на любой ровной площадке с твердым покрытием, обеспечивающим хорошее сцепление с обувью. По команде «На старт!» студент принимает положение основная стойка, скакалка за спиной на полу в двух руках. По команде «Марш!» (с одновременным включением секундомера) начинает прыжки на двух ногах с прокручиванием скакалки на каждый прыжок. Фиксируется количество прыжков без сбоев за 1 минуту.

Скорость увеличиваем, стараясь добиться результата 180 оборотов в минуту, что равноценно трем прыжкам в секунду. Направление вращения скакалки не меняется.

Ошибки: напрыгивание перед отталкиванием, вращение прямыми руками, сбой.

3. Упор лежа «Планка»

Статическое упражнение «ПЛАНКА» проводится на любой ровной площадке с твердым покрытием, обеспечивающим хорошее сцепление с обувью. По команде «Марш!» (с одновременным включением секундомера) участник принимает положение «УПОР ЛЕЖА» на прямых руках, фиксируется время неподвижного удержания прямого положения тела без провисания живота и прогиба в спине, ноги прямые с опорой на носок, стопы на ширине таза.

Ошибки: кисть не под плечом, прогиб в пояснице, высокое положение таза.

КОНТРОЛЬНЫЕ УПРАЖНЕНИЯ ДЛЯ ОЦЕНКИ ФИЗИЧЕСКОЙ ПОДГОТОВЛЕННОСТИ
для студентов 2,3 курсов
Элективная дисциплина РИТМИЧЕСКАЯ ГИМНАСТИКА

Контрольное упражнение		Нормативы и оценки									
		Мужчины					женщины				
		5	**4**	**3**	**2**	**1**	**5**	**4**	**3**	**2**	**1**
1.	Комбинация на 64 счета без степ-платформы	выполнение без ошибок	1-2 ошибки	3-4 ошибки	5-6 ошибок	более 6 ошибок	выполнение без ошибок	1-2 ошибки	3-4 ошибки	5-6 ошибок	более 6 ошибок
2.	Прыжки на двух ногах через скакалку, кол-во раз за 20 сек.	50 и более	40-49	30-39	20-29	10-19	60 и более	50-59	40-49	30-39	20-29
3.	Упор лежа «Планка», (сек)	150 сек	120 сек	90 сек	60 сек	45 сек	120 сек	90 сек	60 сек	45 сек	30 сек

Требования к выполнению контрольных упражнений
По элективной дисциплине ритмическая гимнастика
для студентов 2,3 курсов
Методические рекомендации по выполнению контрольных упражнений:

1. Комбинация на 64 счета.

Упражнение проводится на любой ровной площадке с твердым покрытием. Студент выполняет последовательно в заданном музыкальном ритме комбинацию из элементов ритмической гимнастики: шаги, повороты, подскоки, бег и т.д., сопровождающиеся работой рук, туловища, головы с правой и левой ноги на 32 счета. Оценивается техника выполнения элементов, амплитуда движений, музыкальность, чувство ритма.

Ошибки: сбой в темпе и ритме упражнений, непопадание в музыку, повтор выполнения элементов более чем на 8 счетов.

2. Прыжки на двух ногах через скакалку.

Прыжки через скакалку проводятся на любой ровной площадке с твердым покрытием, обеспечивающим хорошее сцепление с обувью. По команде «На старт!» студент принимает положение основная стойка, скакалка за спиной на полу в двух руках. По команде «Марш!» (с одновременным включением секундомера) начинает прыжки на двух ногах с прокручиванием скакалки на каждый прыжок. Фиксируется количество прыжков без сбоев за 20 секунд.

Скорость увеличиваем, стараясь добиться результата 180 оборотов в минуту, что равноценно трем прыжкам в секунду. Направление вращения скакалки не меняется.

Ошибки: напрыгивание перед отталкиванием, вращение прямыми руками, сбой.

3. Упор лежа «Планка»

Статическое упражнение «ПЛАНКА» проводится на любой ровной площадке с твердым покрытием, обеспечивающим хорошее сцепление с обувью. По команде «Марш!» (с одновременным включением секундомера) участник принимает положение «УПОР ЛЕЖА» на прямых руках, фиксируется время неподвижного удержания прямого положения тела без провисания живота и прогиба в спине, ноги прямые с опорой на носок, стопы на ширине таза.

Ошибки: кисть не под плечом, прогиб в пояснице, высокое положение таза.

КОНТРОЛЬНЫЕ УПРАЖНЕНИЯ ДЛЯ ОЦЕНКИ ФИЗИЧЕСКОЙ ПОДГОТОВЛЕННОСТИ
для студентов 1курсов
Элективная дисциплина «Плавание. Начальное обучение»

Нормативы Для студентов основной и подготовительной групп здоровья	Курс	Оценки в баллах									
		Юноши					Девушки				
		5	4	3	2	1	5	4	3	2	1
плавание 50 м кроль на спине (с)	1	0.55	1.05	1.15	1.25	1.40	1.15	1.20	1.30	1.40	1.50
плавание 50 м в/ст. (с)		0.50	1.00	1.10	1.20	1.35	1.00	1.15	1.25	1.35	1.50
12 минутное плавание (м)		450	400	350	300	250	400	350	300	250	200
Нормативы Для студентов специальной медицинской группы здоровья	Курс	Оценки в баллах									
		Юноши					Девушки				
		5	4	3	2	1	5	4	3	2	1
плавание 50 м кроль на спине (с)	1	1.00	1.10	1.20	1.30	1.50	1.20	1.25	1.35	1.45	2.00
плавание 50 м в/ст. (с)		0.55	1.05	1.15	1.25	1.40	1.10	1.20	1.30	1.40	2.00
12 минутное плавание (м)		400	350	300	250	200	350	300	250	200	150

Требования к выполнению контрольных упражнений «Плавание. Начальное обучение»

Контрольные нормативы по плаванию (50м, 12 мин) проводятся в бассейне БФУ им.И.Канта. Бассейн 25 метров.

Старт осуществляется с тумбочки (вольный стиль) или из воды (вольный стиль и кроль на спине). Способ плавания – кроль на спине и вольный стиль (произвольный). Завершив дистанцию, коснитесь бортика. Запрещено останавливаться, ставить ноги на дно, поправлять очки, держаться за дорожку. При плавании на 50 метров выполните поворот любым удобным способом, но обязательно коснитесь бортика бассейна руками или ногами. Перед сдачей контрольных нормативов следует провести небольшую разминку. При любых неприятных ощущениях (чрезмерная одышка, боли в области сердца и др.) контрольное упражнение следует прекратить.

КОНТРОЛЬНЫЕ УПРАЖНЕНИЯ ДЛЯ ОЦЕНКИ ФИЗИЧЕСКОЙ ПОДГОТОВЛЕННОСТИ
для студентов 2,3 курсов
Элективная дисциплина «Спортивное Плавание».

Нормативы Для студентов основной и подготовительной групп здоровья	Курс	Оценки в баллах									
		Юноши					Девушки				
		5	4	3	2	1	5	4	3	2	1
плавание 50 м кроль на спине (с)	2-3	0.50	0.55	1.00	1.05	1.10	1.05	1.10	1.15	1.20	1.25
плавание 50 м в/ст. (с)		0.44	0.50	0.55	1.00	1.05	1.00	1.05	1.10	1.15	1.20
12 минутное плавание (м)		600	550	500	450	400	550	500	450	400	350
Нормативы Для студентов специальной медицинской группы здоровья	Курс	Оценки в баллах									
		Юноши					Девушки				
		5	4	3	2	1	5	4	3	2	1
плавание 50 м кроль на спине (с)	2-3	0.55	1.00	1.08	1.28	1.35	1.15	1.20	1.25	1.30	1.35
плавание 50 м в/ст. (с)		50.0	57.0	1.05	1.24	1.30	1.10	1.15	1.20	1.25	1.30
12 минутное плавание (м)		500	450	400	350	250	450	400	350	300	200

Требования к выполнению контрольных упражнений «Спортивное Плавание».

Контрольные нормативы по плаванию (50м, 12 мин) принимаются в бассейне (25м) БФУ им.И.Канта по заранее утвержденному графику. К сдаче нормативов допускаются студенты, прошедшие курс начального обучения плаванию. Перед сдачей контрольных нормативов выполняется самостоятельная разминка. На дистанции 50м вольный стиль применяется способ плавания кроль на груди. Останавливаться, ставить ноги на дно, висеть на дорожке запрещено. Старт, по желанию студента, осуществляется с тумбочки или из воды. Во время 12 минутного плавания стили можно менять, можно останавливаться и поправлять очки. Во время поворота, на любой дистанции, нельзя хвататься руками за бортик и ставить ноги на дно. Завершая дистанцию, необходимо коснуться бортика рукой для фиксации результата.

КОНТРОЛЬНЫЕ УПРАЖНЕНИЯ ДЛЯ ОЦЕНКИ ФИЗИЧЕСКОЙ ПОДГОТОВЛЕННОСТИ
для студентов 2,3 курсов
ZUMBA ® FITNESS

	Упражнение	Оценка в баллах				
		5	4	3	2	1
ZUMBA ® FITNESS	Фитнес танец (для 1ого курса основные шаги)	Выполнена связка полностью, движения четкие, музыкальные (все виды шагов в комбинации с руками).	Связка выполнена полностью, есть нечеткости в выполнении или музыкальности (все виды шагов).	Выполнены две части связки (два вида шагов).	Выполнена одна из частей связки (один вид шагов).	Связка (шаги) не выполнена
	Фиксация в приседе у стены, угол в коленных суставах 90°(сек).	30 и более	25-30	20-25	15-20	До 15
	Бег на месте с высоким подниманием бедра (мин).	2.30	2.20	2.00	1.30	Меньше 1

ФИТНЕС ТАНЕЦ

Студентам предлагается выбор одного фитнес танца из изученного за модуль фитнес блока. По результату выполнения студент получает соответствующий балл по шкале оценки. **Запрещено:**1. Повторное выполнение танца или перевыбор.

Ошибки:

1. Отсутствие типичных для каждого ритма движений рук и ног.
2. Не соблюдение музыкального сопровождения.
3. Нарушения в технике выполнения и комбинации элементов.
4. Невозможность удержания правильной осанки и линий частей туловища.

КОНТРОЛЬНОЕ УПРАЖНЕНИЕ - ФИКСАЦИЯ В ПРИСЕДЕ У СТЕНЫ

Испытуемый становится спиной к стене, выполняет присед до угла в коленных суставах 90° с выносом рук вперед. Фиксируется время (секунды) удержания статического положения. **Запрещено:**1. Ставить руки в упор на бедра.2. Уменьшать или увеличивать угол в коленных суставах.

Ошибки:1. Отклоняться от вертикали стены и опускать голову. 2. Менять положение.

БЕГ НА МЕСТЕ С ВЫСОКИМ ПОДНИМАНИЕМ БЕДРА

Исходное положение – основная стойка, предплечья параллельны полу, ладони вниз, плечи прижаты к туловищу. По команде преподавателя испытуемый начинает выполнять бег с высоким подниманием бедра, касаясь ладоней. Фиксируется время выполнения упражнения.

Запрещено:1. Переходить на шаг. **Ошибки:** 1. Не касаться ногами рук. 2. Изменение темпа бега.

КОНТРОЛЬНЫЕ УПРАЖНЕНИЯ ДЛЯ ОЦЕНКИ ФИЗИЧЕСКОЙ ПОДГОТОВЛЕННОСТИ
для студентов 1-3 курсов
Элективная дисциплина специальная медицинская групп

Контрольное упражнение		Нормативы и оценки									
		Мужчины					женщины				
		5	**4**	**3**	**2**	**1**	**5**	**4**	**3**	**2**	**1**
1.	Сгибание и разгибание рук в упоре лежа на коленях (девушки), в упоре лёжа (юноши)	40	30	20	10	5	30	20	10	5	2
2.	Поднимание туловища из положения лежа на спине, руки за головой, ноги закреплены	60	50	40	30	20	50	40	30	20	10

	(девушки и юноши)										
3.	Наклон вперёд стоя на гимнастической скамейке (девушки и юноши)	9	7	5	3	1	15	10	8	6	2

Требования к выполнению контрольных упражнений
По элективной дисциплине специальная медицинская группа
Основные требования

1. Сгибание и разгибание рук в упоре лежа на коленях (девушки), в упоре лёжа (юноши)

Исходное положение**:** примите упор лежа на плоскости, поставьте руки на ширине плеч, кисти смотрят вперед, локти разведены, но не больше, чем на 45 гр., плечи, корпус и бедро выстроены в прямую линию, стопы упираются прямо в плоскость.

Ошибки:

1. прикосновение к полу бедрами или тазом
2. «перелом» прямой линии от плеч до туловища;
3. не было фиксации с исходной позиции
4. руки разгибались поочередно;
5. было касание грудью поверхности;
6. локти развелись в стороны больше, чем на 45 гр.

2. Поднимание туловища из положения лежа на спине, руки за головой, ноги закреплены (девушки и юноши)

Поднимание туловища из положения лежа выполняется из ИП: лежа на спине на гимнастическом мате, руки за головой, пальцы сцеплены в «замок», лопатки касаются мата, ноги согнуты в коленях под прямым углом, ступни прижаты партнером к полу. Участник выполняет максимальное количество подниманий за 1 мин., касаясь локтями бедер (коленей), с последующим возвратом в ИП.

Засчитывается количество правильно выполненных подниманий туловища. Для выполнения тестирования создаются пары, один из партнеров выполняет упражнение, другой удерживает его ноги за ступни и голени. Затем участники меняются местами.

Ошибки:

1. отсутствие касания локтями бедер (коленей);
2. отсутствие касания лопатками мата;
3. пальцы разомкнуты “из замка”;
4. смещение таза.

3. Наклон вперёд стоя на гимнастической скамейке (девушки и юноши)

Наклон вперед из положения стоя с прямыми ногами выполняется из ИП: стоя на полу или гимнастической скамье, ноги выпрямлены в коленях, ступни ног расположены параллельно на ширине 10 - 15 см.

При выполнении испытания (теста) на полу участник по команде выполняет два предварительных наклона. При третьем наклоне касается пола пальцами или ладонями двух рук и фиксирует результат в течение 2 с.

При выполнении испытания (теста) на гимнастической скамье по команде участник выполняет два предварительных наклона, скользя пальцами рук по линейке измерения. При третьем наклоне участник максимально сгибается и фиксирует результат в течение 2 с. Величина гибкости измеряется в сантиметрах. Результат выше уровня гимнастической скамьи определяется знаком «-» , ниже - знаком «+».

Ошибки:

1. сгибание ног в коленях;
2. фиксация результата пальцами одной руки;
3. отсутствие фиксации результата в течение 2 с.

Результаты выполнения контрольных упражнения суммируются и их сумма переводится в бонусные баллы учебного раздела БРС:

Сумма оценки трех контрольных упражнений	Бонусные баллы
15-13	3
12 – 10	2
8 - 9	1

Практический раздел реализуется в виде учебно-тренировочных. Критерием успешности освоения учебного материала является выполнение контрольных упражнений и тестов физической подготовленности для основной и подготовительной групп (Приложение 1), для специальной медицинской группы (Приложение 2).

Студенты временно освобожденные по состоянию здоровья выполняют индивидуальные проектные задания по темам представленные в разделе 2.2.

Критерии оценивания

«зачтено» Задание выполнено и оформлено полностью в соответствии с требованиями, отражены все компоненты.

«не зачтено» Задание выполнено и оформлено с ошибками, не раскрыто содержание выделенных в заданиях компонентов.

Промежуточный контроль по дисциплине

Промежуточной формой контроля знаний, умений и навыков по дисциплине «Элективные дисциплины физической культуры и спорта» является зачет. Условием получения зачета является выполнение практического раздела, сдачи контрольных упражнений, тестов физической подготовленности, в которых учитывается наличие медицинского осмотра, регулярность посещения занятий по расписанию, достаточный уровень физической подготовленности и функционального состояния, участие в соревнованиях, научно-исследовательская деятельность. Промежуточная аттестация осуществляется на основе Положение балльно-рейтинговой оценки учебных достижений обучающихся в БФУ им.И.Канта.

9. Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины.

Основная литература

1. Чертов, Н. В. Физическая культура : учебное пособие / Н. В. Чертов. - Ростов-на-Дону : Издательство ЮФУ, 2012. - 118 с. - ISBN 978-5-9275-0896-9. - Текст : электронный. - URL: https://znanium.com/catalog/product/551007 (дата обращения: 29.03.2022). – Режим доступа: по подписке.

Дополнительная литература

1.Булгакова, Н. Ж. Теория и методика плавания [Электронный ресурс]: учеб. для высш. проф. образования/ Н. Ж. Булгакова, О. И. Попов, Е. А. Распопова ; под ред. Н. Ж. Булгаковой. - 2-е изд., стер.. - Москва: Академия, 2014. - 1 эл. опт. диск (CD-ROM), 318, [1] с.: ил.. - Библиогр. в конце гл... Имеются экземпляры в отделах: ЭБС Кантиана(1)

2.Петров, П. К. Информационные технологии в физической культуре и спорте [Электронный ресурс]: учебник/ П. К. Петров. - 4-е изд., стер.. - Москва: Академия, 2014. - 1 эл. опт. диск (CD-ROM), 288 с.: рис.. - (Высшее образование - бакалавриат). - Библиогр.: с. 278-283 (80 назв.). - Лицензия до 31.12.2020 г.. Имеются экземпляры в отделах: ЭБС Кантиана(1)

10. Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины (модуля).

- НЭБ Национальная электронная библиотека, диссертации и прочие издания
- eLIBRARY.RU Научная электронная библиотека, книги, статьи, тезисы докладов конференций
- Гребенников Электронная библиотека ИД журналы
- ЭБС Лань книги, журналы
- ЭБС Консультант студента
- ПРОСПЕКТ ЭБС
- ЭБС ZNANIUM.COM
- РГБ Информационное обслуживание по МБА
- БЕН РАН
- Электронно-библиотечная система (ЭБС) Кантитана (https://elib.kantiana.ru/)

11. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине.

Программное обеспечение обучения включает в себя:

- система электронного образовательного контента БФУ им. И. Канта – www.lms-3.kantiana.ru, обеспечивающую разработку и комплексное использование электронных образовательных ресурсов;
- серверное программное обеспечение, необходимое для функционирования сервера и связи с системой электронного обучения через Интернет;
- корпоративная платформа Microsoft Teams;
- установленное на рабочих местах обучающихся ПО: Microsoft Windows 7, Microsoft Office Standart 2010, антивирусное программное обеспечение Kaspersky Endpoint Security.

12. Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине.

Для осуществления образовательного процесса по дисциплине «Элективные дисциплины по физической культуре и спорту» необходимо соответствующий аудиторный фонд и материально-спортивная база, которая продуктивно развивается в БФУ им. И. Канта. Учебные аудитории оснащены мультимедийным оборудованием, которые используются для лекционных и методико-практических занятий. К материально-техническому обеспечению относим также используемые мультимедийные средства обучения: электронные презентации к лекциям, иллюстрированные упражнения тестового типа, комплект дополнительных структурно-логических схем.

Характеристика материально-технического обеспечения практических занятий «Элективные дисциплины по физической культуре»:

Материально-спортивная база	Обеспечение учебного процесса по дисциплине «Элективные дисциплины по физической культуре и спорту» спортивным инвентарем
Учебно-физкультурный корпус с бассейном, Корпус	Бассейн: плавательные доски, плавательные ласты, нудлы, плавательные лопатки, Электронное табло,

№22 236000 Калининградская область. г. Калининград ул. А. Невского, 14 Бассейн, Фитнес-зал, Тренажерный зал.	настенный секундомер, колобашки. Раздевалки. Фитнес – зал: Степы, Гимнастические палки, Гимнастические мячи, металлические обручи, коврики гимнастические, гантели 9 кг, 1,5 кг,3 кг, 2 кг, утяжелители для рук- ног 1,5, утяжелители для рук-ног 3 кг., скакалки, мини степы, гимнастические маты. Музыкальный центр.
Физкультурно-оздоровительный комплекс, корпус №9 Калининградская область. г. Калининград ул. А. Невского, 14	Гимнастические маты, баскетбольные щиты, волейбольные стойки, волейбольная сетка с креплениями, гимнастические палки, баскетбольные мячи, волейбольные мячи, ракетки для бадминтона, воланы. медицинболы, скакалки, раздевалки для мужчин и женщин, гимнастические скамейки,
Корпус №4 спортивный зал № 2236000 Калининградская обл., г. Калининград ул. Чернышевского, 56А	Гимнастические скамейки, гимнастические маты, шведская стенка, фишки, гимнастические палки деревянные, гимнастические палки пластиковые, скакалки, ракетки для бадминтона, воланы, теннисные мячи, волейбольные мячи, баскетбольные мячи, музыкальный центр, коврики гимнастические, флорбольные клюшки, медицинболы. Баскетбольные щиты, волейбольные стойки и сетка.
Спортивный зал №1 236000 Калининградская обл., г. Калининград ул. Чернышевского, 56А	Борцовский ковер, гимнастические маты, гимнастические брусья, бревно гимнастическое напольное, гимнастическое бревно постоянной высоты, мостик гимнастический пружинный, перекладина гимнастическая, брусья гимнастические разновысокие, конь гимнастический маховый, козел гимнастический, гимнастические скамейки, шведские стенки, зеркала, скакалки, теннисные мячи, гимнастические палки, обручи, медицинболы.
Корпус №15 236000 Калининградская обл., г. Калининград Адрес: ул. Соммера, 23.	Зал аэробики: степы, металлические обручи, гимнастические палки, гантели 1 кг, гимнастические мячи, музыкальный центр, гимнастические скамейки, коврики гимнастические.
Корпус № 15 Тренажерный зал 236000 Калининградская обл., г. Калининград Адрес: ул. Соммера, 23.	Кардиотренажеры, блочные тренажеры, рычажные , тренажер с собственным весом, Велотренажеры, железные блины 5, 10,15,20,25кг.; гантели от 1 кг – 3 кг.; резиновые блины 10, 15, 20,50 кг., гири.
Стадион «Кантиана»	Беговые дорожки, сектор для прыжков, сектор для

236000 Калининградская обл., г. Калининград Адрес: ул. Озерова,57.	метаний, футбольное поле, футбольные мячи,

Приложение 1

Тесты по физической подготовленности для студентов 1-3 курсов основной и подготовительной групп.

Виды упражнений***	**Нормативы и оценка в баллах**									
	Мужчины					**Женщины**				
	5	**4**	**3**	**2**	**1**	**5**	**4**	**3**	**2**	**1**
1. Бег 3000 м, мин/сек (муж) **Бег 2000 м**, мин/сек (жен)	**12,30**	**13,30**	**14,00**	**15,00**	**16,50**	**10,30**	**11,15**	**11,50**	**12,30**	**14.00**
2. Бег 100 м, сек	**13,5**	**14,0**	**14,5**	**15,1**	**15,8**	**16,5**	**17,0**	**17,5**	**18,2**	**19,0**
3. Подтягивание из виса на высокой перекладине (муж.) Кол-во раз.) **Сгибание разгибание рук в упоре лежа на полу** (кол-во раз)	**13** **45**	**10** **40**	**9** **35**	**6** **30**	**4** **25**					
3. Подтягивание из виса на низкой перекладине (жен.) Кол-во раз **или** **Поднимание туловища из положения лежа на спине за 1 мин** (жен.) Кол-во раз.						**14** **47**	**12** **40**	**10** **35**	**5** **30**	**3** **25**
4. Наклон туловища из положения стоя на гимнастической скамейке (муж., жен.),см	**13**	**7**	**6**	**5**	**3**	**16**	**11**	**8**	**6**	**4**

***** Три теста на выбор.**

Приложение 2

ТЕСТЫ ДЛЯ ОЦЕНКИ ФИЗИЧЕСКОЙ ПОДГОТОВЛЕННОСТИ
для студентов 1-3 курсов специальной медицинской группы

Контрольное упражнение***		Нормативы и оценки									
		Юноши					Девушки				
		5	4	3	2	1	5	4	3	2	1
1.	Сгибание и разгибание рук в упоре лежа на коленях (девушки), в упоре лёжа (юноши)	35	25	20	10	5	25	20	15	10	5
2.	Поднимание туловища из положения лежа на спине, руки за головой, ноги закреплены за 1 мин. (девушки и юноши)	50	40	30	25	20	40	35	30	25	15
3.	Наклон вперёд стоя на гимнастической скамейке (девушки и юноши)	9	7	5	3	1	15	10	8	6	2
4.	Ходьба 2 км, мин., с (девушки, юноши)	14.00	14.30	15.30	16.00	16.30	16.30	17.30	18.40	20.00	20.30
5.	Прыжки в длину с места, см (девушки, юноши.)	210	205	200	190	180	170	165	160	155	150
6.	Подтягивание (юноши) количество раз	8	6	5	3	1	-	-	-	-	-

***** Обязательный тест: ходьба 2 км и 2 теста на выбор**

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
федеральное государственное автономное образовательное учреждение высшего образования «Балтийский федеральный университет имени Иммануила Канта»
Институт физико-математических наук и информационных технологий

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

«Введение в специальность»

Шифр: 10.05.01
Специальность: «Компьютерная безопасность»
Специализация: «Математические методы защиты информации»
Квалификация (степень) выпускника: Специалист по защите информации

Калининград
2022

Лист согласования

Составитель: Ветров Игорь Анатольевич, к.т.н., доцент

Рабочая программа утверждена на заседании учебно-методического совета института физико-математических наук и информационных технологий
Протокол № 01/22 от «01» февраля 2022 г.

Председатель учебно-методического совета института физико-математических наук и информационных технологий
Первый заместитель директора ИФМНиИТ, к. ф.-м. н., доцент — Шпилевой А. А

Ведущий менеджер — Е.П.Ставицкая

Содержание

1. Наименование дисциплины: «ВВЕДЕНИЕ В СПЕЦИАЛЬНОСТЬ»

Целью изучения дисциплины «***Введение в специальность***» является:

- освоение студентами основ обучения в высшей школе, знакомство с ФГОС и учебными планами по направлению подготовки, учебной образовательной программой, структурами университета, института ФМНиИТ, истории развития Института, а также базовых понятий – специальность, бакалавриат, магистратура, аспирантура, лекции, семинары, практические занятия, лабораторные работы;

- овладение первичными знаниями в области защиты информации и выработка методики изучения специальных и других дисциплин в области защиты информации, выработка практических навыков работы со специальной литературой и литературой общего назначения.

2. Перечень планируемых результатов обучения по дисциплине, соотнесенных с планируемыми результатами освоения образовательной программы

Код компетенции	Результаты освоения образовательной программы (ИДК)	Результаты обучения по дисциплине
ПКС-4: Способность осуществлять подбор, изучение и обобщение научно-технической информации, методических материалов отечественного и зарубежного опыта по проблемам компьютерной безопасности, а также нормативных правовых актов сфере профессиональной деятельности	ПКС-4.1. Осуществляет подбор, изучение и обобщение научно-технической информации, методических материалов отечественного и зарубежного опыта по проблемам компьютерной безопасности. ПКС-4.2. Знает основные руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации. ПКС-4.3. Применяет действующую законодательную базу в области обеспечения защиты информации	**Знать**: - основные закономерности исторического процесса, этапы исторического развития России, место и роль России в истории человечества и в современном мире, правовые основы обеспечения национальной безопасности Российской Федерации; - основные требования и положения «Закона о высшем профессиональном образовании» РФ, ФГОС и учебные планы по направлению подготовки своей специальности; - основные руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации. **Уметь**: - осуществлять подбор, изучение и обобщение научно-технической информации, методических материалов отечественного и зарубежного опыта по проблемам компьютерной безопасности; - применять действующую законодательную базу в области обеспечения защиты информации **Владеть**: - навыками поиска нормативной правовой информации, необходимой для

		профессиональной деятельности; - навыками поиска и обработки информации по профилю деятельности в глобальных компьютерных сетях, библиотечных фондах и иных источниках информации.

3. Место дисциплины в структуре образовательной программы

«*Введение в специальность*» представляет собой дисциплину вариативной части, формируемой участниками образовательных отношений Блока 1 Дисциплины (модули) дисциплин специальности 10.05.01 «Компьютерная безопасность», специализация «Математические методы защиты информации».

4. Виды учебной работы по дисциплине

Виды учебной работы по дисциплине зафиксированы учебным планом основной профессиональной образовательной программы по указанному направлению и профилю, выражаются в академических часах. Часы контактной работы и самостоятельной работы обучающегося и часы, отводимые на процедуры контроля, могут различаться в учебных планах ОПОП по формам обучения. Объем контактной работы включает часы контактной аудиторной работы (лекции/практические занятия/ лабораторные работы), контактной внеаудиторной работы (контроль самостоятельной работы), часы контактной работы в период аттестации. Контактная работа, в том числе может проводиться посредством электронной информационно-образовательной среды университета с использованием ресурсов сети Интернет и дистанционных технологий

5. Содержание дисциплины, в том числе практической подготовки в рамках дисциплины, структурированное по темам

Исходя из рамок, установленных учебным планом по трудоемкости и видам учебной работы по дисциплине, преподаватель самостоятельно выбирает тематику занятий по формам и количеству часов проведения контактной работы: лекции и иные учебные занятия, предусматривающие преимущественную передачу учебной информации преподавателем и (или) занятия семинарского типа (семинары, практические занятия, практикумы, лабораторные работы, коллоквиумы и иные аналогичные занятия), и (или) групповые консультации, и (или) индивидуальную работу обучающихся с преподавателем, в том числе индивидуальные консультации (по курсовым работам/проектам – при наличии курсовой работы/проекта по данной дисциплине в учебном плане). Рекомендуемая тематика занятий максимально полно реализуется в контактной работе с обучающимися очной формы обучения. В случае реализации образовательной программы в заочной / очно-заочной форме трудоемкость дисциплины сохраняется, однако объем учебного материала в значительной части осваивается обучающимися в форме самостоятельной работы. При этом требования к ожидаемым образова-

тельным результатам обучающихся по данной дисциплине не зависят от формы реализации образовательной программы.

№ п/п	Наименование темы	Содержание темы
1	Организация высшего образования в области информационной безопасности	Задачи и программа курса. Место курса «*Введение в специальность*» в ряду других дисциплин. Формы самостоятельной работы студентов по изучению курса. Литература к курсу. Характер специальности «Компьютерная безопасность». Задачи, решаемые специалистами по защите информации. Многоаспектность защиты информации в компьютерных системах. Методологические основы освоения математических методов защиты информации. Роль теории познания и философии в целом в понимании специальности «Компьютерная безопасность». Основные положения Доктрины информационной безопасности РФ. Роль и значение компьютерной безопасности в обеспечении интересов России и её граждан. Краткая история развития криптографии в России и за рубежом. Общая характеристика теории информации и теории кодирования. Правовые аспекты высшего образования: правовое регулирование отношений в сфере образования (Конституция РФ, Закон об образовании РФ), права и обязанности студента; государственная регламентация образовательной деятельности: лицензирование образовательной деятельности, государственная аккредитация образовательной деятельности, государственный контроль (надзор) в сфере образования; Федеральные государственные образовательные стандарты, направления подготовки (специальность, бакалавриат, магистратура, аспирантура), ФГОС по направлению подготовки «Информационная безопасность». Организация учебного процесса в университете: Университет, структура, основные направления подготовки; Институт физико-математических наук и информационных технологий, руководство, структура и образовательные программы института; организация учебного процесса в Институте (расписание, лекции, практические занятия, лабораторные работы, планирование и организация самостоятельной работы студентов, экзамены, зачёты, курсовые работы (проекты); студенческие общественные организации и общественная деятельность студентов.
2	Введение в информационную безопасность	История развития проблемы защиты информации, понятия национальной безопасности, анализ угроз информационной безопасности, проблемы информационной защиты, понятия информационной войны. Общее представление о защищаемой информации: понятие об информации как предмете защиты, основные виды информации, свойства информации,, основные положения информационного законодательства.
3	Человек и информация. Общие понятия о передаче информации на расстояние	Информация, сообщение, сигнал; канал обработки и передачи информации; виды сигналов и их свойства. Спектры сигналов и их характеристики. Основные каналы утечки информации: актуальность вопроса, основные каналы утечки информации при её обработке в информационно-телекоммуникационных системах, другие виды каналов утечки информации. Виды модуляции, их свойства и отличия.

4	Информационные угрозы. Методы и средства защиты информации.	Информационная безопасность, виды информационных угроз, вирусы, методы защиты информации. Организация защиты информации на предприятиях (учреждениях, организациях): содержание концепции и политики информационной безопасности, стратегия защиты организации (предприятия), структура и функции службы безопасности организации, организация физической защиты и пропускного режима на предприятии.

6. **Рекомендуемая тематика учебных занятий в форме контактной работы**

Учебно-методическое обеспечение для самостоятельной работы обучающихся составляют:

1. Материалы лекций.
2. Материалы практических занятий.
3. Информационные ресурсы «Интернет» (сайты ФСТЭК России, ФСБ России, Консультант плюс и др.)
4. Методические рекомендации и указания.
5. Фонды оценочных средств.
6. Учебники и учебно-методические пособия.

Рекомендуемая тематика учебных занятий *лекционного* типа (предусматривающих преимущественную передачу учебной информации преподавателями):

№ п/п	Наименование темы	Содержание темы
1	Организация высшего образования в области информационной безопасности	Задачи и программа курса. Место курса «*Введение в специальность*» в ряду других дисциплин. Формы самостоятельной работы студентов по изучению курса. Литература к курсу. Характер специальности «Компьютерная безопасность». Задачи, решаемые специалистами по защите информации. Многоаспектность защиты информации в компьютерных системах. Методологические основы освоения математических методов защиты информации. Роль теории познания и философии в целом в понимании специальности «Компьютерная безопасность». Основные положения Доктрины информационной безопасности РФ. Роль и значение компьютерной безопасности в обеспечении интересов России и её граждан. Краткая история развития криптографии в России и за рубежом. Общая характеристика теории информации и теории кодирования. Правовые аспекты высшего образования: правовое регулирование отношений в сфере образования (Конституция РФ, Закон об образовании РФ), права и обязанности студента; государственная регламентация образовательной деятельности: лицензирование образовательной деятельности, государственная аккредитация образовательной деятельности, государственный контроль (надзор) в сфере образования; Федеральные государственные образовательные стандарты, направления подготовки (специальность, ба-

		калавриат, магистратура, аспирантура), ФГОС по направлению подготовки «Информационная безопасность». Организация учебного процесса в университете: Университет, структура, основные направления подготовки; Институт физико-математических наук и информационных технологий, руководство, структура и образовательные программы института; организация учебного процесса в Институте (расписание, лекции, практические занятия, лабораторные работы, планирование и организация самостоятельной работы студентов, экзамены, зачёты, курсовые работы (проекты); студенческие общественные организации и общественная деятельность студентов.
2	Введение в информационную безопасность	История развития проблемы защиты информации, понятия национальной безопасности, анализ угроз информационной безопасности, проблемы информационной защиты, понятия информационной войны. Общее представление о защищаемой информации: понятие об информации как предмете защиты, основные виды информации, свойства информации,, основные положения информационного законодательства.
3	Человек и информация. Общие понятия о передаче информации на расстояние	Информация, сообщение, сигнал; канал обработки и передачи информации; виды сигналов и их свойства. Спектры сигналов и их характеристики. Основные каналы утечки информации: актуальность вопроса, основные каналы утечки информации при её обработке в информационно-телекоммуникационных системах, другие виды каналов утечки информации. Виды модуляции, их свойства и отличия.
4	Информационные угрозы. Методы и средства защиты информации.	Информационная безопасность, виды информационных угроз, вирусы, методы защиты информации. Организация защиты информации на предприятиях (учреждениях, организациях): содержание концепции и политики информационной безопасности, стратегия защиты организации (предприятия), структура и функции службы безопасности организации, организация физической защиты и пропускного режима на предприятии.

Тематика практических занятий

№ п/п	**Наименование Темы**	**Содержание темы**
1	Организация высшего образования в области информационной безопасности	Изучение законодательных документов Высшей школы. Изучение образовательных стандартов, учебных планов, программ дисциплин. Отработка методик написания конспектов лекций, особенностей самостоятельной подготовки к практическим и лабораторным работам.
2	Введение в информационную безопасность	Изучение основных положений законодательства в области защиты информации. Расчёт угроз информационной безопасности на простейших примерах. Описание основных свойств защищаемой информации.
3	Человек и информация. Общие понятия о передаче информации на расстояние	Задачи на расчёт и построение спектров сигналов, определение полосы пропускания устройства формирования и передачи информации, спектры АМС, АМС с балансной и однополосной модуляцией
	Информационные	Отработка задач на изучение вопросов: что такое мобильная радио-

4	угрозы. Методы и средства защиты информации.	связь, что такое сотовая связь, принцип действия сотовой связи, как происходит связь между мобильными телефонами, кто такие сотовые операторы. Изучение и практическая работа с мобильным интернетом, каналом передачи GPRS , с WAP – браузерами, WAP – сайтами, особенностями работы с интернет – мессенджеры, социальными сетями и их подвидами.

Тематика самостоятельных работ

№ п/п	Наименование темы	Тематика самостоятельных работ
1	Организация высшего образования в области информационной безопасности	Повторение теоретического материала к практическим занятиям. Решение задач домашнего задания по теме. Ознакомление с литературой по курсу. Выбор темы групповой практической работы. Чтение литературы по теме групповой практической работы. Подготовка к контрольной работе.
2	Введение в информационную безопасность	Повторение теоретического материала к практическим занятиям. Решение задач домашнего задания по теме. Подготовка краткой сводки теоретических результатов групповой практической работы. Подготовка к контрольной работе.
3	Человек и информация. Общие понятия о передаче информации на расстояние	Повторение теоретического материала к практическим занятиям. Решение задач домашнего задания по теме. Разработка компьютерной программы для групповой практической работы. Проведение компьютерных вычислительных экспериментов. Подготовка к контрольной работе.
4	Информационные угрозы. Методы и средства защиты информации.	Повторение теоретического материала к практическим занятиям. Решение задач домашнего задания по теме. Подготовка к демонстрации результатов групповой практической работы. Подготовка к контрольной работе. Подготовка к промежуточной аттестации – зачёту с оценкой.

7. Методические рекомендации по видам занятий

Лекционные занятия.

В ходе лекционных занятий обучающимся рекомендуется выполнять следующие действия. Вести конспектирование учебного материала. Обращать внимание на категории, формулировки, раскрывающие содержание тех или иных явлений и процессов, научные выводы и практические рекомендации по их применению. Задавать преподавателю уточняющие вопросы с целью уяснения теоретических положений, разрешения спорных ситуаций.

Желательно оставить в рабочих конспектах поля, на которых во внеаудиторное время можно сделать пометки из рекомендованной литературы, дополняющие материал прослушанной лекции, а также подчеркивающие особую важность тех или иных теоретических положений.

Практические и семинарские занятия.

На практических и семинарских занятиях в зависимости от темы занятия выполняется поиск информации по решению проблем, практические упражнения, контрольные работы,

выработка индивидуальных или групповых решений, итоговое обсуждение с обменом знаниями, участие в круглых столах, разбор конкретных ситуаций, командная работа, представление портфолио и т.п.

Самостоятельная работа.

Самостоятельная работа осуществляется в виде изучения литературы, эмпирических данных по публикациям и конкретных ситуаций из практики, подготовке индивидуальных работ, работа с лекционным материалом, самостоятельное изучение отдельных тем дисциплины; поиск и обзор литературы и электронных источников; чтение и изучение учебника и учебных пособий.

8. Фонд оценочных средств

8.1. Перечень компетенций с указанием этапов их формирования в процессе освоения образовательной программы в рамках учебной дисциплины

Код компетенции	Содержание компетенций
ПКС - 4	Способность осуществлять подбор, изучение и обобщение научно-технической информации, методических материалов отечественного и зарубежного опыта по проблемам компьютерной безопасности, а также нормативных правовых актов сфере профессиональной деятельности

Основными этапами формирования указанной компетенции при изучении студентами дисциплины являются последовательное изучение содержательно связанных между собой *разделов* (*тем*) учебных занятий. Изучение каждого раздела (темы) предполагает овладение студентами необходимыми компетенциями. Результат аттестации студентов на различных этапах формирования компетенций показывает уровень освоения компетенций студентами.

Паспорт фонда оценочных средств по дисциплине «Введение в специальность»

Контролируемые модули, разделы (темы) дисциплины	Индекс контролируемой компетенции (или её части)	Оценочные средства по этапам формирования компетенций
		текущий контроль по дисциплине
Тема 1. Организация высшего образования в области информационной безопасности	ПКС - 4	решение задач, контрольная работа, устный опрос
Тема 2. Введение в информационную безопасность	ПКС - 4	решение задач, контрольная работа
Тема 3. Человек и информация. Общие понятия о передаче информации на расстояние	ПКС - 4	решение задач, контрольная работа
Тема 4. Информационные угрозы. Методы и средства защиты информации.	ПКС - 4	решение задач, контрольная работа

8.2. Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений и навыков и (или) опыта деятельности в процессе текущего контроля

8.2.1. Оценочные средства для текущего контроля успеваемости

Текущий контроль может включать следующие процедуры (методики) контроля успеваемости: устные или письменные опросы. Вопросы представлены без вариантов ответов.

1. Безопасность – это
2. Информационная безопасность Российской Федерации – это
3. Компьютерная система – это
4. Компьютерная безопасность – это
5. Структура понятия «Безопасность»
6. Три составляющие понятия «безопасность информации»
7. Что понимается под конфиденциальностью информации
8. Что понимается под целостностью информации
9. Что понимается под доступностью информации
10. Две составляющие безопасности функций КС
11. Причина и год возникновения задач по обеспечению компьютерной безопасности.
12. Этапы развития концепций обеспечения ИБ
13. Принцип разумной достаточности
14. Принцип целенаправленности
15. Принцип системности
16. Принцип комплексности
17. Принцип непрерывности
18. Принцип управляемости
19. Принцип сочетания унификации и оригинальности
20. Принцип открытости алгоритмов и механизмов защиты
21. Принцип простоты применения средств защиты
22. Какая информация подлежит защите
23. Систематика методов и механизмов обеспечения компьютерной безопасности
24. Что такое идентификация и аутентификация
25. Методы протоколирования и аудита событий это
26. Как происходит фиксирование процессов изменения данных в журналах событий
27. Угроза безопасности КС – это
28. Систематизация – это
29. Классификация – это
30. Классификации угроз компьютерной безопасности по различным критериям
31. Что такое таксономическое деление
32. Что такое мереологическое деление
33. Что представляет собой *каталогизация* угроз
34. ГОСТ 5127599 "Защита информации. Объект информатизации. Факторы, воздействующие на информацию"
35. Классификации угроз по ГОСТ Р 51275-99

8.2.2. Типовые контрольные задания

1. История развития проблемы защиты информации
2. Основные понятия национальной безопасности
3. Источники угроз информационной безопасности РФ
4. Методы обеспечения ИБ (организационно-технические, правовые, экономические - таблица)
5. Информационные войны
6. Регуляторы в области ЗИ (рисунок)
7. Понятие об информации как предмете защиты (определения)
8. Виды информации
9. Свойства информации
10. Основные положения информационного законодательства
11. Радиотехнический канал передачи информации
12. Понятие информационной безопасности
13. Источники и виды информационных угроз
14. Вирусы (классификация вирусов)
15. Вредоносные программы, антивирусные программы (виды)
16. Основные каналы утечки информации (в общем)
17. Содержание концепции и политики информационной безопасности предприятия
18. Кратко – защита предприятия

8.2.3. Устные опросы

Устный опрос имеет целью проверить теоретическую подготовку студентов к практическому занятию, знание основных определений, формулировок, свойств, используемых при решении задач.

1. Что такое мобильная радиосвязь
2. Что такое сотовая связь
3. Принцип действия сотовой связи
4. Как происходит связь между мобильными телефонами
5. Кто такие сотовые операторы
6. Схемы, рисунки, определения, поясняющие тему практического занятия
7. Что такое мобильный интернет
8. Что такое канал передачи GPRS
9. Информационные ресурсы мобильного интернета
10. Что такое WAP – браузеры, WAP - сайты
11. Что такое интернет – мессенджеры, для чего нужны, самые популярные. Их сравнение по достоинствам и недостаткам
12. Что такое файрвол
13. Что такое брандмауэр
14. Что такое межсетевой экран

15. Что такое персональный файрвол
16. Их основное назначение, отличия, для чего нужны, самые популярные. Их сравнение по достоинствам и недостаткам

8.2.4. Групповое задание

Для развития у обучающихся навыков командной работы, межличностной коммуникации, принятия решений, лидерских качеств, развития навыков творческой исследовательской деятельности студентам предлагается выполнить групповое задание.

Групповое задание - творческая практическая работа, направленная на формирования практических навыков в области применения элементарных математических методов в компьютерном моделировании простых задач защиты информации.

Для развития у обучающихся навыков командной работы, межличностной коммуникации, принятия решений, лидерских качеств задание получает группа из 2-3 человек.

Защита группового задания происходит в виде публичного выступления с презентаций (по требованию преподавателя).

Темы практических групповых заданий

1. Изучение законодательных документов Высшей школы. Изучение образовательных стандартов, учебных планов, программ дисциплин. Отработка методик написания конспектов лекций, особенностей самостоятельной подготовки к практическим и лабораторным работам.
2. Изучение основных положений законодательства в области защиты информации. Расчёт угроз информационной безопасности на простейших примерах. Описание основных свойств защищаемой информации.
3. Задачи на расчёт и построение спектров сигналов, определение полосы пропускания устройства формирования и передачи информации, спектры АМС, АМС с балансной и однополосной модуляцией
4. Отработка задач на изучение вопросов: что такое мобильная радиосвязь, что такое сотовая связь, принцип действия сотовой связи, как происходит связь между мобильными телефонами, кто такие сотовые операторы. Изучение и практическая работа с мобильным интернетом, каналом передачи GPRS , с WAP – браузерами, WAP – сайтами, особенностями работы с интернет – мессенджеры, социальными сетями и их подвидами.

8.3. Перечень вопросов и заданий для промежуточной аттестации по дисциплине

Промежуточной формой контроля знаний, умений и навыков по дисциплине во 2 семестре является **зачёт с оценкой**. Промежуточный контроль по дисциплине служит для оценки работы студента в течение семестра и призван выявить уровень, прочность и систематичность полученных им теоретических и практических знаний, приобретения навыков самостоятельной работы, развития творческого мышления, умение синтезировать полученные знания и применять их в решении практических задач.

Вопросы предполагают контроль общих методических знаний и умений, способность студентов проиллюстрировать их примерами, индивидуальными материалами, составленными студентами в течение курса.

По итогам зачёта с оценкой выставляется оценка по шкале порядка: «отлично», «хорошо», «удовлетворительно», «неудовлетворительно».

Вопросы для промежуточного контроля (зачёта с оценкой)

1. История теории и практики компьютерной безопасности;
2. Структура понятия «компьютерная безопасность»;
3. Основные направления обеспечения компьютерной безопасности;
4. Содержание понятия «компьютерная безопасность»;
5. Понятие защищенности (безопасности) компьютерной информации;
6. Конфиденциальность, целостность и доступность информации;
7. Принципы обеспечения компьютерной безопасности;
8. Методы обеспечения компьютерной безопасности;
9. Механизмы обеспечения компьютерной безопасности;
10. Понятие угроз безопасности компьютерной информации и их классификация;
11. Классификация угроз компьютерной безопасности по природе происхождения;
12. Классификация угроз компьютерной безопасности по направлению осуществления;
13. Классификация угроз компьютерной безопасности по объекту воздействия;
14. Классификация угроз компьютерной безопасности по способу осуществления;
15. Классификация угроз компьютерной безопасности по жизненному циклу информационной системы;
16. Процесс создания компьютерной системы с учетом обеспечения информационной безопасности;
17. Таксономия угроз безопасности и изъянов (брешей) систем защиты по ГОСТ Р 51275-99

8.4. Планируемые уровни сформированности компетенций обучающихся и критерии оценивания

Уровни	Содержательное описание уровня	Основные признаки выделения уровня (этапы формирования компетенции, критерии оценки сформированности)	Пятибалльная шкала (академическая) оценка	Двухбалльная шакала, зачет	БРС, % освоения (рейтинговая оценка)
Повышенный	Творческая деятельность	*Включает нижестоящий уровень.* Умение самостоятельно принимать решение, решать проблему/задачу теоретического и прикладного характера на основе изученных методов, приемов, технологий	отлично	зачтено	86-100

Базовый	Применение знаний и умений в более широких контекстах учебной и профессиональной деятельности, нежели по образцу с большей степени самостоятельности и инициативы	*Включает нижестоящий уровень.* Способность собирать, систематизировать, анализировать и грамотно использовать информацию из самостоятельно найденных теоретических источников и иллюстрировать ими теоретические положения или обосновывать практику применения	хорошо		71-85
Удовлетворительный (достаточный)	Репродуктивная деятельность	Изложение в пределах задач курса теоретически и практически контролируемого материала	удовлетворительно		55-70
Недостаточный	Отсутствие признаков удовлетворительного уровня		неудовлетворительно	не зачтено	Менее 55

9. Перечень основной и дополнительной литературы, необходимой для освоения дисциплины

9.1. Основная литература

1. Белов, Е. Б. Основы информационной безопасности: Учебное пособие для вузов / Е.Б. Белов и др. - Москва : Гор. линия-Телеком, 2011. - 558 с.: ил.; . - (Специальность; Учебное пособие для высших учебных заведений). ISBN 5-93517-292-5, 100 экз. - Текст : электронный. - URL: https://znanium.com/catalog/product/405159 (дата обращения: 13.01.2022). – Режим доступа: по подписке.
2. Введение в информационную безопасность: Учебное пособие для вузов / А.А. Малюк, В.И. Королев, В.М. Фомичев; Под ред. В.С. Горбатов. - Москва : Гор. линия-Телеком, 2011. - 288 с.: ил.; . - (Специальность). ISBN 978-5-9912-0160-5, 1000 экз. - Текст : электронный. - URL: https://znanium.com/catalog/product/265558 (дата обращения: 13.01.2022). – Режим доступа: по подписке.

9.2. Дополнительная литература:

1. Башлы, П. Н. Информационная безопасность и защита информации [Электронный ресурс] : учебник / П. Н. Башлы, А. В. Бабаш, Е. К. Баранова. - Москва : РИОР, 2013. - 222 с. - ISBN 978-5-369-01178-2. - Текст : электронный. - URL: https://znanium.com/catalog/product/405000 (дата обращения: 13.01.2022). – Режим доступа: по подписке.

2. Бахаров, Л. Е. Информационная безопасность и защита информации : сборник тестов / Л. Е. Бахаров. - Москва : Изд. Дом МИСиС, 2015. - 43 с. - Текст : электронный. - URL: https://znanium.com/catalog/product/1232263 (дата обращения: 13.01.2022). – Режим доступа: по подписке.

10. Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины

- НЭБ Национальная электронная библиотека, диссертации и прочие издания
- eLIBRARY.RU Научная электронная библиотека, книги, статьи, тезисы докладов конференций
- Гребенников Электронная библиотека ИД журналы
- ЭБС Лань книги, журналы
- ЭБС Консультант студента
- ПРОСПЕКТ ЭБС
- ЭБС ZNANIUM.COM
- РГБ Информационное обслуживание по МБА
- БЕН РАН
- Электронно-библиотечная система (ЭБС) Кантитана (https://elib.kantiana.ru/)
- История математики (http://www-history.mcs.st-andrews.ac.uk/).

11. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине

Программное обеспечение обучения включает в себя:

- система электронного образовательного контента БФУ им. И. Канта – www.lms-3.kantiana.ru, обеспечивающую разработку и комплексное использование электронных образовательных ресурсов;
- серверное программное обеспечение, необходимое для функционирования сервера и связи с системой электронного обучения через Интернет;
- корпоративная платформа Microsoft Teams;
- установленное на рабочих местах студентов ПО: Microsoft Windows 7, Microsoft Office Standart 2010, антивирусное программное обеспечение Kaspersky Endpoint Security.

12. Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине

Для проведения занятий лекционного типа, практических и семинарских занятий используются специальные помещения (учебные аудитории), оборудованные техническими средствами обучения – мультимедийной проекционной техникой. Для проведения занятий лекционного типа используются наборы демонстрационного оборудования.

Для проведения лабораторных работ, (практических занятий – при необходимости) используются специальные помещения (учебные аудитории), оснащенные специализированным лабораторным оборудованием: персональными компьютерами с возможностью выхода в интернет и с установленным программным обеспечением, заявленным в п.11.

Для проведения групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации используются специальные помещения (учебные аудитории), оборудованные специализированной мебелью (для обучающихся), меловой / маркерной доской.

Для организации самостоятельной работы обучающимся предоставляются помещения, оснащенные компьютерной техникой с возможностью подключения к сети «Интернет» и обеспечением доступа в электронную информационно-образовательную среду университета.

Для обучения инвалидов и лиц с ограниченными возможностями здоровья университетом могут быть представлены специализированные средства обучения, в том числе технические средства коллективного и индивидуального пользования.

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
федеральное государственное автономное образовательное учреждение высшего образования
«Балтийский федеральный университет имени Иммануила Канта»
Институт физико-математических наук и информационных технологий

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

«Теория чисел»

Шифр: 10.05.01
Специальность: «Компьютерная безопасность»
Специализация: «Математические методы защиты информации»
Квалификация (степень) выпускника: Специалист по защите информации

Калининград
2022

Лист согласования

Составитель: Малыгина Екатерина Сергеевна, к.ф.-м.н., доцент

Рабочая программа утверждена на заседании учебно-методического совета института физико-математических наук и информационных технологий

Протокол № 01/22 от «01» февраля 2022 г.

Председатель учебно-методического
совета института физико-
математических наук и информационных
технологий

Первый заместитель директора Шпилевой А. А
ИФМНиИТ, к. ф.-м. н., доцент

Ведущий менеджер Е.П.Ставицкая

Содержание

1.Наименование дисциплины: «Теория чисел».

Цель дисциплины: целью освоения дисциплины «Теория чисел» является фундаментальная подготовка обучающихся в области теории чисел.

2. Перечень планируемых результатов обучения по дисциплине, соотнесенных с планируемыми результатами освоения образовательной программы

Код компетенции	Результаты освоения образовательной программы (ИДК)	Результаты обучения по дисциплине
ПКС-5 Способность участвовать в теоретических и экспериментальных научно-исследовательских работах по оценке защищенности информации в компьютерных системах.	ПКС-5.1. Знает тенденции развития теоретических и экспериментальных исследований в области защиты информации. ПКС-5.2. Участвует в теоретических научно-исследовательских работах по оценке защищенности информации в компьютерных системах. ПКС-5.3. Участвует в экспериментальных научно-исследовательских работах по аудиту безопасности в компьютерных системах.	- **знать** основные понятия теории чисел и основные типы задач, возникающие в теории чисел; - **уметь** использовать полученные теоретические знания для решения конкретных прикладных задач, производить математические расчеты в стандартных постановках, производить содержательный анализ результатов вычислений; - **владеть** навыками применения понятий и методов дисциплины для решения различных задач, используемых в дальнейшей учебной и профессиональной деятельности.

3. Место дисциплины в структуре образовательной программы

Дисциплина «Теория чисел» представляет собой дисциплину части, формируемой участниками образовательных отношений, блока дисциплин подготовки обучающихся.

4. Виды учебной работы по дисциплине.

Виды учебной работы по дисциплине зафиксированы учебным планом основной профессиональной образовательной программы по указанному направлению и профилю, выражаются в академических часах. Часы контактной работы и самостоятельной работы обучающегося и часы, отводимые на процедуры контроля, могут различаться в учебных планах ОПОП по формам обучения. Объем контактной работы включает часы контактной аудиторной работы (лекции/практические занятия/ лабораторные работы), контактной внеаудиторной работы (контроль самостоятельной работы), часы контактной работы в период аттестации. Контактная работа, в том числе, может проводиться посредством электронной информационно-образовательной среды университета с использованием ресурсов сети Интернет и дистанционных технологий

5. Содержание дисциплины, структурированное по темам (разделам)

Исходя из рамок, установленных учебным планом по трудоемкости и видам учебной работы по дисциплине, преподаватель самостоятельно выбирает тематику занятий по формам и количеству часов проведения контактной работы: лекции и иные учебные занятия, предусматривающие преимущественную передачу учебной информации преподавателем и (или) занятия семинарского типа (семинары, практические занятия, практикумы, лабораторные работы, коллоквиумы и иные аналогичные занятия), и (или) групповые консультации, и (или) индивидуальную работу обучающихся с преподавателем, в том числе индивидуальные консультации (по курсовым работам/проектам – при наличии курсовой работы/проекта по данной дисциплине в учебном плане). Рекомендуемая тематика занятий максимально полно реализуется в контактной работе с обучающимися очной формы обучения. В случае реализации образовательной программы в заочной / очно-заочной форме трудоемкость дисциплины сохраняется, однако объем учебного материала в значительной части осваивается обучающимися в форме самостоятельной работы. При этом требования к ожидаемым образовательным результатам обучающихся по данной дисциплине не зависят от формы реализации образовательной программы.

№	Наименование раздела	Содержание раздела
1	Теория делимости целых чисел	Алгоритм деления целых чисел. Наибольший общий делитель и его свойства. Алгоритм Евклида. Наименьшее общее кратное. Простейшие диофантовы уравнения.
2	Простые числа	Фундаментальная теорема арифметики и ее следствия. Решето Эратосфена. Гипотеза Гольдбаха
3	Теория сравнений	Основные свойства сравнений. Специальные тесты делимости. Линейные сравнения. Китайская теорема об остатках. Системы сравнений.
4	Теорема Ферма	Метод Ферма разложения числа на множители. Малая теорема Ферма. Теорема Вильсона.
5	Теоретико-числовые функции	Функции τ и σ. Формула обращения Мёбиуса. Наибольшая целая функция. Функция Эйлера. Теорема Эйлера. Свойства функции Эйлера.
6	Примитивные корни и индексы	Порядок числа по модулю n. Свойства порядка. Примитивные корни по простому модулю и их свойства. Примитивные корни по составному модулю и их свойства. Теория индексов.
7	Цепные дроби	Конечные цепные дроби. Бесконечные цепные дроби. Уравнение Пелля.

6. Рекомендуемая тематика учебных занятий в форме контактной работы

Рекомендуемая тематика учебных занятий *лекционного* типа (предусматривающих преимущественную передачу учебной информации преподавателями):

№	Наименование раздела	Темы лекций
1	Теория делимости целых	Лекция 1. Алгоритм деления. Наибольший общий

	чисел	делитель. Лекция 2. Алгоритм Евклида. Лекция 3. Простейшие диофантовы уравнения.
2	Простые числа	Лекция 4. Основная теорема арифметики. Лекция 5. Решето Эратосфена. Гипотеза Гольдбаха.
3	Теория сравнений	Лекция 6. Основные свойства сравнений. Некоторые признаки делимости. Лекция 7. Линейные сравнения.
4	Теорема Ферма	Лекция 8. Метод Ферма разложения числа на множители. Малая теорема Ферма. Теорема Вильсона.
5	Теоретико-числовые функции	Лекция 9. Функции тау и сигма. Лекция 10. Функция Мёбиуса и формула обращения. Функция наибольшего целого. Лекция 11. Функции Эйлера и ее свойства. Приложения.
6	Примитивные корни и индексы	Лекция 12. Порядок числа по модулю n. Примитивные корни по простому модулю. Лекция 13. Примитивные корни по составному модулю. Индексы.
7	Цепные дроби	Лекция 14. Конечные и бесконечные цепные дроби. Лекция 14. Уравнения Пелля.

Рекомендуемая тематика *практических* занятий:

1. Вычисление наибольшего общего делителя целых чисел. Решение задач на деление чисел с помощью свойств наибольшего общего делителя. Вычисление наименьшего общего кратного целых чисел.
2. Решение простейших диофантовых уравнений.
3. Решение задач на делимость чисел с использованием простых чисел.
4. Нахождение простых чисел с помощью решета Эратосфена. Построение небольших простых чисел.
5. Определение составных и простых чисел с помощью гипотезы Гольдбаха.
6. Решение сравнений с использованием их свойств.
7. Установление делимости целых чисел.
8. Решение линейных сравнений. Решение систем сравнений.
9. Разложение чисел на множители с помощью метода Ферма.
10. Решение сравнений с помощью малой теоремы Ферма.
11. Определение простоты числа с помощью теоремы Вильсона.
12. Вычисление функций τ и σ.
13. Решение задач на простоту с использованием функций τ и σ.
14. Вычисление функции Мёбиуса. Вычисление целой части числа.
15. Вычисление функции Эйлера. Решение сравнений с использованием теоремы Эйлера.
16. Вычисление порядков элементов в кольце классов вычетов по модулю n.
17. Вычисление примитивных корней в конечном поле.
18. Вычисление примитивных корней по составному модулю.
19. Вычисление индексов.
20. Решение степенных сравнений с помощью индексов.
21. Представление рациональных и действительных чисел в виде конечных и бесконечных цепных дробей.
22. Решение уравнений Пелля.

На практических занятиях решаются задачи по теме занятия.

Требования к самостоятельной работе обучающихся

1. Работа с лекционным материалом, предусматривающая проработку конспекта лекций и учебной литературы, по всем темам из п. 6 настоящей рабочей программы.
2. Выполнение домашнего задания, предусматривающего решение задач, выполнение упражнений, выдаваемых на практических занятиях, по всем темам из п. 6 настоящей рабочей программы.

Руководствуясь положениями статьи 47 и статьи 48 Федерального закона от 29 декабря 2012 г. N 273-ФЗ «Об образовании в Российской Федерации» научно-педагогические работники и иные лица, привлекаемые университетом к реализации данной образовательной программы, пользуются предоставленными академическими правами и свободами в части свободы преподавания, свободы от вмешательства в профессиональную деятельность; свободы выбора и использования педагогически обоснованных форм, средств, методов обучения и воспитания; права на творческую инициативу, разработку и применение авторских программ и методов обучения и воспитания в пределах реализуемой образовательной программы и отдельной дисциплины.

Исходя из рамок, установленных учебным планом по трудоемкости и видам учебной работы по дисциплине, преподаватель самостоятельно выбирает тематику занятий по формам и количеству часов проведения контактной работы: лекции и иные учебные занятия, предусматривающие преимущественную передачу учебной информации преподавателем и (или) занятия семинарского типа (семинары, практические занятия, практикумы, лабораторные работы, коллоквиумы и иные аналогичные занятия), и (или) групповые консультации, и (или) индивидуальную работу обучающихся с преподавателем, в том числе индивидуальные консультации (по курсовым работам/проектам – при наличии курсовой работы/проекта по данной дисциплине в учебном плане).

Рекомендуемая тематика занятий максимально полно реализуется в контактной работе с обучающимися очной формы обучения. В случае реализации образовательной программы в заочной / очно-заочной форме трудоемкость дисциплины сохраняется, однако объем учебного материала в значительной части осваивается обучающимися в форме самостоятельной работы. При этом требования к ожидаемым образовательным результатам обучающихся по данной дисциплине не зависят от формы реализации образовательной программы.

7. Методические рекомендации по видам занятий

Лекционные занятия.

В ходе лекционных занятий обучающимся рекомендуется выполнять следующие действия. Вести конспектирование учебного материала. Обращать внимание на категории, формулировки, раскрывающие содержание тех или иных явлений и процессов, научные выводы и практические рекомендации по их применению. Задавать преподавателю уточняющие вопросы с целью уяснения теоретических положений, разрешения спорных ситуаций.

Желательно оставить в рабочих конспектах поля, на которых во внеаудиторное время можно сделать пометки из рекомендованной литературы, дополняющие материал

прослушанной лекции, а также подчеркивающие особую важность тех или иных теоретических положений.

Практические и семинарские занятия.

На практических и семинарских занятиях в зависимости от темы занятия выполняется поиск информации по решению проблем, практические упражнения, контрольные работы, выработка индивидуальных или групповых решений, итоговое обсуждение с обменом знаниями, участие в круглых столах, разбор конкретных ситуаций, командная работа, представление портфолио и т.п.

Самостоятельная работа.

Самостоятельная работа осуществляется в виде изучения литературы, эмпирических данных по публикациям и конкретных ситуаций из практики, подготовке индивидуальных работ, работа с лекционным материалом, самостоятельное изучение отдельных тем дисциплины; поиск и обзор литературы и электронных источников; чтение и изучение учебника и учебных пособий.

8. Фонд оценочных средств

8.1. Перечень компетенций с указанием этапов их формирования в процессе освоения образовательной программы в рамках учебной дисциплины

Основными этапами формирования указанных компетенций при изучении обучающимися дисциплины являются последовательное изучение содержательно связанных между собой тем учебных занятий. Изучение каждой темы предполагает овладение обучающимися необходимыми компетенциями. Результат аттестации обучающихся на различных этапах формирования компетенций показывает уровень освоения компетенций.

Контролируемые разделы (темы) дисциплины	Индекс контроли-руемой компетенции (или её части)	Оценочные средства по этапам формирования компетенций
		текущий контроль по дисциплине
1. Теория делимости целых чисел	ПКС-5	Опрос, решение задач.
2. Простые числа		
3. Теория сравнений		
4. Теорема Ферма		
5. Теоретико-числовые функции		
6. Примитивные корни и индексы		
7. Цепные дроби		
Итоговая контрольная работа по всем темам дисциплины		Контрольная работа

8.2. Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений и навыков и (или) опыта деятельности процессе текущего контроля

Примеры вопросов для устного опроса:

По Теме 1. Теория делимости целых чисел

1. Объяснить работу алгоритма деления целых чисел.
2. Дать определение наибольшего общего делителя двух чисел.
3. Сформулировать основные свойства наибольшего общего делителя.
4. Объяснить работу алгоритма Евклида.
5. Дать определение наименьшего общего кратного двух чисел.
6. Сформулировать основные свойства наименьшего общего кратного.

По Теме 2. Простые числа

1. Дать определения простому и составному числам.
2. Сформулировать основные свойства простых чисел.
3. Объяснить принцип работы решета Эратосфена.
4. Сформулировать гипотезу Гольдбаха.

По Теме 3. Теория сравнений

1. Дать определение сравнимости двух целых чисел по модулю n.
2. Сформулировать основные свойства сравнений.
3. Сформулировать теорему о решении линейного сравнения.
4. Сформулировать китайскую теорему об остатках.

По Теме 4. Теорема Ферма

1. Объяснить суть метода Ферма разложения целых чисел на множители.
2. Сформулировать малую теорему Ферма.
3. Сформулировать теорему Вильсона.

По Теме 5. Теоретико-числовые функции

1. Дать определение функциям σ и τ. Записать формулы для функций σ и τ.
2. Дать определение мультипликативной функции.
3. Дать определение функции Мёбиуса.
4. Дать определение наибольшей целой функции.
5. Дать определение функции Эйлера. Записать формулы для вычисления функции Эйлера.
6. Сформулировать терему Эйлера.
7. Сформулировать основные свойства функции Эйлера.

По Теме 6. Примитивные корни и индексы

1. Дать определение порядка числа по модулю n.
2. Сформулировать основные свойства порядка.
3. Дать определение примитивному корню.
4. Сформулировать в каких случаях примитивный корень существует, а в каких нет.
5. Дать определение индекса. Сформулировать основные свойства индекса.

По Теме 7. Цепные дроби.

1. Дать определение конечной цепной дроби.
2. Дать определение подходящей цепной дроби.

3. Сформулировать свойства конечных цепных дробей.
4. Дать определение бесконечной цепной дроби.

Типовые контрольные задания:

1. Для $n \geq 1$ доказать, что $n(n + 1)(2n + 1)/6$ – целое.
2. Найти НОД(143, 227) и НОК(143, 227).
3. Используя алгоритм Евклида, найти x и y: НОД(56, 72) = $56x + 72y$.
4. Определить все решения в целых числах для диофантового уравнения: $56x + 72y = 40$.
5. Если $p \geq 5$ – простое число, то показать, что $p^2 + 2$ – составное.
6. Найти все простые числа, делящие 50!.
7. Найти разложение на простые множители чисел 1234, 10140 и 36000.
8. Используя решето Эратосфена, найти все простые числа между 100 и 200.
9. Пусть $a \equiv b \pmod{n}$. Доказать, что НОД(a, n) = НОД(b, n).
10. Проверить, выполняется ли для нечетного целого a условие: $a^{2^n} \equiv 1 \ (mod \ 2^{n+2})$.
11. Используя теорию сравнений проверить, что $8|2^{44} - 1$.
12. Решить линейное сравнение: $25x \equiv 15 \pmod{29}$.
13. Решить систему сравнений: $\begin{cases} x \equiv 1 \ (mod \ 3), \\ x \equiv 2 \ (mod \ 5), \\ x \equiv 3 \ (mod \ 7). \end{cases}$
14. Используя метод Ферма, разложить на множители 2279.
15. Проверить, что $18^6 \equiv 1 \ (mod \ 7^k)$ для $k = 1, 2, 3$.
16. Для целого $n \geq 1$ проверить выполнимость неравенства $\tau(n) \leq 2\sqrt{n}$.
17. Показать, что $\sum_{d|n} 1/d = \sigma(n)/n$.
18. Пусть N – целое положительное. Показать, что $\sum_{n=1}^{N} \mu(n)[N/n] = 1$.
19. Представить -19/51 в виде цепной дроби.
20. Какому иррациональному числу соответствует цепная дробь $[0; \overline{1, 2, 3}]$?
21. Решить уравнение Пелля: $x^2 - 7y^2 = 1$.

8.3. Перечень вопросов и заданий для промежуточной аттестации по дисциплине

Вопросы для промежуточного контроля (зачета)

1. Алгоритм деления целых чисел.
2. Наибольший общий делитель и его свойства.
3. Алгоритм Евклида.
4. Наименьшее общее кратное и его свойства.
5. Простейшие диофантовы уравнения.
6. Фундаментальная теорема арифметики и ее следствия.
7. Решето Эратосфена.
8. Гипотеза Гольдбаха.
9. Основные свойства сравнений.
10. Специальные тесты делимости.
11. Линейные сравнения.
12. Китайская теорема об остатках.
13. Системы сравнений.
14. Метод Ферма разложения числа на множители.
15. Малая теорема Ферма.
16. Теорема Вильсона.
17. Функции τ и σ.

18. Формула обращения Мёбиуса.
19. Наибольшая целая функция.
20. Функция Эйлера.
21. Теорема Эйлера.
22. Свойства функции Эйлера.
23. Порядок числа по модулю n.
24. Свойства порядка.
25. Примитивные корни по простому модулю и их свойства.
26. Примитивные корни по составному модулю и их свойства.
27. Теория индексов.
28. Конечная цепная дробь.
29. Бесконечная цепная дробь.

8.4. Планируемые уровни сформированности компетенций обучающихся и критерии оценивания

Уровни	Содержательное описание уровня	Основные признаки выделения уровня (этапы формирования компетенции, критерии оценки сформированности)	Пятибалльная шкала (академическая) оценка	Двухбалльная шакала, зачет	БРС, % освоения (рейтинговая оценка)
Повышенный	Творческая деятельность	*Включает нижестоящий уровень.* Умение самостоятельно принимать решение, решать проблему/задачу теоретического и прикладного характера на основе изученных методов, приемов, технологий	отлично	зачтено	86-100
Базовый	Применение знаний и умений в более широких контекстах учебной и профессиональной деятельности, нежели по образцу с большей степени самостоятельности и инициативы	*Включает нижестоящий уровень.* Способность собирать, систематизировать, анализировать и грамотно использовать информацию из самостоятельно найденных теоретических источников и иллюстрировать ими теоретические положения или обосновывать практику применения	хорошо		71-85
Удовлетвори	Репродуктивн	Изложение в пределах	удовлетвор		55-70

тельный (достаточный)	ая деятельность	задач курса теоретически и практически контролируемого материала	ительно		
Недостаточный	Отсутствие признаков удовлетворительного уровня		неудовлетворительно	не зачтено	Менее 55

9. Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины.

Основная литература

1. Смолин, Ю.Н. *Алгебра и теория чисел* : учеб. пособие / Ю.Н. Смолин. — 5-е изд., стер.—Москва : ФЛИНТА, 2017. — 464 с. - ISBN 978-5-9765-0050-1. - Текст : электронный. - URL: https://znanium.com/catalog/product/1034573.

Дополнительная литература

1. Пилиди, В. С. Математические основы зашиты информации : учебное пособие / В. С. Пилиди ; Южный федеральный университет. - Ростов-на-Дону ; Таганрог : Издательство Южного федерального университета, 2019. - 308 с. - ISBN 978-5-9275-3363-3. - Текст : электронный. - URL: https://znanium.com/catalog/product/1088209 (дата обращения: 26.04.2022). – Режим доступа: по подписке.

10. Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины (модуля).

- НЭБ Национальная электронная библиотека, диссертации и прочие издания
- eLIBRARY.RU Научная электронная библиотека, книги, статьи, тезисы докладов конференций
- Гребенников Электронная библиотека ИД журналы
- ЭБС Лань книги, журналы
- ЭБС Консультант студента
- ПРОСПЕКТ ЭБС
- ЭБС ZNANIUM.COM
- РГБ Информационное обслуживание по МБА
- БЕН РАН
- Электронно-библиотечная система (ЭБС) Кантитана (https://elib.kantiana.ru/)

11. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине.

Программное обеспечение обучения включает в себя:

- система электронного образовательного контента БФУ им. И. Канта – www.lms-3.kantiana.ru, обеспечивающую разработку и комплексное использование электронных образовательных ресурсов;
- серверное программное обеспечение, необходимое для функционирования сервера и связи с системой электронного обучения через Интернет;

- корпоративная платформа Microsoft Teams;
- установленное на рабочих местах обучающихся ПО: Microsoft Windows 7, Microsoft Office Standart 2010, антивирусное программное обеспечение Kaspersky Endpoint Security.
- специализированное ПО не требуется.

12. Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине.

Для проведения занятий лекционного типа, практических и семинарских занятий используются специальные помещения (учебные аудитории), оборудованные техническими средствами обучения – мультимедийной проекционной техникой. Для проведения занятий лекционного типа используются наборы демонстрационного оборудования.

Для проведения лабораторных работ, (практических занятий – при необходимости) используются специальные помещения (учебные аудитории), оснащенные специализированным лабораторным оборудованием: персональными компьютерами с возможностью выхода в интернет и с установленным программным обеспечением, заявленным в п.11.

Для проведения групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации используются специальные помещения (учебные аудитории), оборудованные специализированной мебелью (для обучающихся), меловой / маркерной доской.

Для организации самостоятельной работы обучающимся предоставляются помещения, оснащенные компьютерной техникой с возможностью подключения к сети «Интернет» и обеспечением доступа в электронную информационно-образовательную среду университета.

Для обучения инвалидов и лиц с ограниченными возможностями здоровья университетом могут быть представлены специализированные средства обучения, в том числе технические средства коллективного и индивидуального пользования.

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
федеральное государственное автономное образовательное учреждение высшего образования «Балтийский федеральный университет имени Иммануила Канта»
Институт физико-математических наук и информационных технологий

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

«ИСТОРИЯ КРИПТОГРАФИИ»

Шифр: 10.05.01
специальность «Компьютерная безопасность»,
специализация «Математические методы защиты информации»
Квалификация (степень) выпускника: специалист по защите информации

Калининград
2022

Лист согласования

Составитель: БОЛТНЕВ ЮРИЙ ФЕДОРОВИЧ. старший преподаватель

Рабочая программа утверждена на заседании учебно-методического совета института физико-математических наук и информационных технологий
Протокол № 01/22 от «01» февраля 2022 г.

Председатель учебно-методического совета института физико-математических наук и информационных технологий
Первый заместитель директора ИФМНиИТ, к. ф.-м. н., доцент — Шпилевой А. А

Ведущий менеджер — Е.П.Ставицкая

СОДЕРЖАНИЕ

1. Наименование дисциплины: «ИСТОРИЯ КРИПТОГРАФИИ»

Целями освоения дисциплины «***История криптографии***» являются:

- раскрытие процессов, движущих сил и закономерности исторического процесса, исследование роли личности в истории криптографии и тайных политических организаций.
- изучение ретроспективного развития приемов шифрования от древнейших времен до наших дней;
- ознакомление с историческими примерами тайных операций в криптографической деятельности;
- воспитание социальной значимости своей будущей профессии, цели и смысла государственной службы, установка на обладание высокой мотивации к выполнению патриотического долга.

2. Перечень планируемых результатов обучения по дисциплине, соотнесенных с планируемыми результатами освоения образовательной программы

Код компетенции	Результаты освоения образовательной программы (ИДК)	Результаты обучения по дисциплине
ПКС-4. Способность осуществлять подбор, изучение и обобщение научно-технической информации, методических материалов отечественного и зарубежного опыта по проблемам компьютерной безопасности, а также нормативных правовых актов сфере профессиональной деятельности.	ПКС-4.1. Осуществляет подбор, изучение и обобщение научно-технической информации, методических материалов отечественного и зарубежного опыта по проблемам компьютерной безопасности ПКС-4.2. Знает основные руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации ПКС-4.3. Применяет действующую законодательную базу в области обеспечения защиты информации	**Знать** перечень необходимой проектной и технической документации, регламентирующей построение эффективных систем защиты информации; правила и этапы разработки проектной и технической документации в области обеспечения информационной безопасности компьютерных систем **Уметь** выполнять расчётные работы и подготовку текстовых и графических документов средствами Microsoft Office и/или иными средствами; **Владеть** практическими навыками применения компьютерных средств создания текстов и презентаций; навыками выступления с докладами и ведения научных дискуссий в профессиональной сфере защиты информации.

3. Место дисциплины в структуре ООП ВО

Дисциплина «История криптографии» представляет собой дисциплину Части, формируемой участниками образовательных отношений блока дисциплин подготовки обучающихся.

4. Виды учебной работы по дисциплине.

Виды учебной работы по дисциплине зафиксированы учебным планом основной профессиональной образовательной программы по указанному направлению и профилю, выражаются в академических часах. Часы контактной работы и самостоятельной работы студента и часы, отводимые на процедуры контроля, могут различаться в учебных планах ОПОП по формам обучения. Объем контактной работы включает часы контактной аудиторной работы (лекции/практические занятия/ лабораторные работы), контактной внеаудиторной работы (контроль самостоятельной работы), часы контактной работы в период аттестации. Контактная работа, в том числе может проводиться посредством электронной информационно-образовательной среды университета с использованием ресурсов сети Интернет и дистанционных технологий

5. Содержание дисциплины, структурированное по темам (разделам)

Исходя из рамок, установленных учебным планом по трудоемкости и видам учебной работы по дисциплине, преподаватель самостоятельно выбирает тематику занятий по формам и количеству часов проведения контактной работы: лекции и иные учебные занятия, предусматривающие преимущественную передачу учебной информации преподавателем и (или) занятия семинарского типа (семинары, практические занятия, практикумы, лабораторные работы, коллоквиумы и иные аналогичные занятия), и (или) групповые консультации, и (или) индивидуальную работу обучающихся с преподавателем, в том числе индивидуальные консультации (по курсовым работам/проектам – при наличии курсовой работы/проекта по данной дисциплине в учебном плане). Рекомендуемая тематика занятий максимально полно реализуется в контактной работе со студентами очной формы обучения. В случае реализации образовательной программы в заочной / очно-заочной форме трудоемкость дисциплины сохраняется, однако объем учебного материала в значительной части осваивается студентами в форме самостоятельной работы. При этом требования к ожидаемым образовательным результатам студентов по данной дисциплине не зависят от формы реализации образовательной программы.

Тема 1. Криптография в античные времена. Начала криптоанализа (коды и шифр простой замены)

Язык жестов. Петроглифы и пиктограммы. Геродот о тайнописи на восковых дощечках. Аристотель и спартанский шифр скитала. Доска Полибия. Шифр (код) сдвига Цезаря.

Понятие кода. Коды, состоящие из одной и двух частей. Понятие шифра. Шифр перестановки. Шифр простой замены. Частотный анализ. Арабские ученые Аль-Кинди (или Алькиндус) и Омар Хайям.

Тема 2. Дешифровка египетских иероглифов. Дешифровка слогового линейного письма Б

Древнейшее зашифрованное сообщение (дошедшее до нас): надпись, вырезанная на гробнице Хнумхотепа, примерно в 1900 г. до Р. Х. Иероглифика, иератика и демотика.

Афанасий Кирхер, Иоганн Георг Цоэга. Розеттский камень, Птолемей V Эпифан.

Томас Юнг. Жан Франсуа Шампольон. Картуши Рамсеса и Тутмоса.

Линейное письмо А (Фестский диск). Линейное письмо Б. Артур Эванс и Кносский дворец. Первые шаги в дешифровке линейного письма Б (Джордж Смит, А.

Э. Каули). Статистический анализ окончаний падежей (Алиса Кобер). Окончательная дешифровка (Майкл Вентрис и Джон Чедвик).

Тема 3. Криптография в Западной Европе в новое время

Леон Батиста Альберти и его диск. Квадрат (таблица) Блеза де Виженера. Автоключ Джероламо Кардано. Бегущий автоключ и первичный ключ Блеза де Виженера. Дешифровка «невскрываемого шифра» Чарльзом Бэббиджом. Алгоритм взлома шифра Виженера. Засекречивание алгоритма взлома из-за Крымской войны (1853-1856 гг.) между Великобританией и Россией. Первая публикация о взломе шифра Виженера (Фридрих Вильгельм Касиски, 1863 г.). Неведение об этом Чарльза Лютвиджа Доджсона (Льюиса Кэрролла), 1868 г.

Тема 4. История шифровального дела в России.

Цифирь. Двойная цифирь (Александр Сергеевич Грибоедов). Мудрая литторея. Декабристы (тюремный шифр). Шифр графа Льва Николаевича Толстого. Книжный шифр русских революционеров (на примере анархиста, князя Петра Алексеевича Кропоткина).

История теории чисел. Нерешенные проблемы в теории чисел.

6. Рекомендуемая тематика учебных занятий в форме контактной работы

Рекомендуемая тематика учебных занятий лекционного типа (предусматривающих преимущественную передачу учебной информации преподавателями):

№	Наименование раздела	Содержание раздела
1	Криптография в античные времена. Начала криптоанализа	Язык жестов. Петроглифы и пиктограммы. Геродот о тайнописи на восковых дощечках. Аристотель и спартанский шифр скитала. Доска Полибия. Шифр (код) сдвига Цезаря. Понятие кода. Коды, состоящие из одной и двух частей. Понятие шифра. Шифр перестановки. Шифр простой замены. Частотный анализ. Арабские ученые Аль-Кинди (или Алькиндус) и Омар Хайям
2	Дешифровка египетских иероглифов. Дешифровка слогового линейного письма Б.	Древнейшее зашифрованное сообщение (дошедшее до нас): надпись, вырезанная на гробнице Хнумхотепа, примерно в 1900 г. до Р. Х. Иероглифика, иератика и демотика. Афанасий Кирхер, Иоганн Георг Цоэга. Розеттский камень, Птолемей V Эпифан. Томас Юнг. Жан Франсуа Шампольон. Картуши Рамсеса и Тутмоса. Линейное письмо А (Фестский диск). Линейное письмо Б. Артур Эванс и Кносский дворец. Первые шаги в дешифровке линейного письма Б (Джордж Смит, А. Э. Каули). Статистический анализ окончаний падежей (Алиса Кобер). Окончательная дешифровка (Майкл Вентрис и Джон Чедвик).

3	Криптография в Западной Европе в новое время.	Леон Батиста Альберти и его диск. Квадрат (таблица) Блеза де Виженера. Автоключ Джероламо Кардано. Бегущий автоключ и первичный ключ Блеза де Виженера. Дешифровка «невскрываемого шифра» Чарльзом Бэббиджом. Алгоритм взлома шифра Виженера. Засекречивание алгоритма взлома из-за Крымской войны (1853-1856 гг.) между Великобританией и Россией. Первая публикация о взломе шифра Виженера (Фридрих Вильгельм Касиски, 1863 г.). Неведение об этом Чарльза Лютвиджа Доджсона (Льюиса Кэрролла), 1868 г
4	История шифровального дела в России	Цифирь. Двойная цифирь (Александр Сергеевич Грибоедов). Мудрая литторея. Декабристы (тюремный шифр). Шифр графа Льва Николаевича Толстого. Книжный шифр русских революционеров (на примере анархиста, князя Петра Алексеевича Кропоткина). История теории чисел. Нерешенные проблемы в теории чисел

Тематика практических занятий

Введение. Исторические задачи и примеры.
1. Криптография в античные времена. Шифр Цезаря со сдвигом.
2. Дешифровка древних письменностей. Расшифровка картушей древнеегипетских фараонов. Линейное письмо В.
3. Криптография в средние века. «Шифр Виженера. Шифр Pigpen.
4. Криптография в XVIII-XX веках. Шифр Плейфера. Шифр ADFGVX
5. Криптографическая деятельность в России. Шифр «Мудрая литторея».
6. Использования криптография в тайных операциях спецслужб. Шифр замены, применяемый советскими партизанами во время ВОВ с внесенными намеренно грамматическими ошибками.
7. Развитие методов криптографии в XXI веке. Шифр RSA.
8. **История теории чисел. Нерешенные проблемы в теории чисел**

Требования к самостоятельной работе обучающихся

1. Работа с лекционным материалом, предусматривающая проработку конспекта лекций и учебной литературы, по всем темам из п. 6 настоящей рабочей программы.

2. Выполнение домашнего задания, предусматривающего решение задач, выполнение упражнений, выдаваемых на практических занятиях, по всем темам из п. 6 настоящей рабочей программы.

Руководствуясь положениями статьи 47 и статьи 48 Федерального закона от 29 декабря 2012 г. N 273-ФЗ «Об образовании в Российской Федерации» научно-педагогические работники и иные лица, привлекаемые университетом к реализации данной образовательной программы, пользуются предоставленными академическими

правами и свободами в части свободы преподавания, свободы от вмешательства в профессиональную деятельность; свободы выбора и использования педагогически обоснованных форм, средств, методов обучения и воспитания; права на творческую инициативу, разработку и применение авторских программ и методов обучения и воспитания в пределах реализуемой образовательной программы и отдельной дисциплины.

Исходя из рамок, установленных учебным планом по трудоемкости и видам учебной работы по дисциплине, преподаватель самостоятельно выбирает тематику занятий по формам и количеству часов проведения контактной работы: лекции и иные учебные занятия, предусматривающие преимущественную передачу учебной информации преподавателем и (или) занятия семинарского типа (семинары, практические занятия, практикумы, лабораторные работы, коллоквиумы и иные аналогичные занятия), и (или) групповые консультации, и (или) индивидуальную работу обучающихся с преподавателем, в том числе индивидуальные консультации (по курсовым работам/проектам – при наличии курсовой работы/проекта по данной дисциплине в учебном плане).

Рекомендуемая тематика занятий максимально полно реализуется в контактной работе с обучающимися очной формы обучения. В случае реализации образовательной программы в заочной / очно-заочной форме трудоемкость дисциплины сохраняется, однако объем учебного материала в значительной части осваивается обучающимися в форме самостоятельной работы. При этом требования к ожидаемым образовательным результатам обучающихся по данной дисциплине не зависят от формы реализации образовательной программы.

7. Методические рекомендации по видам занятий

Лекционные занятия.

В ходе лекционных занятий обучающимся рекомендуется выполнять следующие действия. Вести конспектирование учебного материала. Обращать внимание на категории, формулировки, раскрывающие содержание тех или иных явлений и процессов, научные выводы и практические рекомендации по их применению. Задавать преподавателю уточняющие вопросы с целью уяснения теоретических положений, разрешения спорных ситуаций.

Желательно оставить в рабочих конспектах поля, на которых во внеаудиторное время можно сделать пометки из рекомендованной литературы, дополняющие материал прослушанной лекции, а также подчеркивающие особую важность тех или иных теоретических положений.

Практические и семинарские занятия.

На практических и семинарских занятиях в зависимости от темы занятия выполняется поиск информации по решению проблем, практические упражнения, контрольные работы, выработка индивидуальных или групповых решений, итоговое обсуждение с обменом знаниями, участие в круглых столах, разбор конкретных ситуаций, командная работа, представление портфолио и т.п.

Самостоятельная работа.

Самостоятельная работа осуществляется в виде изучения литературы, эмпирических данных по публикациям и конкретных ситуаций из практики, подготовке индивидуальных работ, работа с лекционным материалом, самостоятельное изучение отдельных тем дисциплины; поиск и обзор литературы и электронных источников; чтение и изучение учебника и учебных пособий.

8. Фонд оценочных средств

8.1 Перечень компетенций с указанием этапов их формирования в процессе освоения образовательной программы

Основными этапами формирования указанных компетенций при изучении студентами дисциплины являются последовательное изучение содержательно связанных между собой *разделов* (*тем*) учебных занятий. Изучение каждого раздела (темы) предполагает овладение студентами необходимыми компетенциями. Результат аттестации студентов на различных этапах формирования компетенций показывает уровень освоения компетенций студентами.

Контролируемые модули, разделы (темы) дисциплины	Индекс контролируемой компетенции (или её части)	Оценочные средства по этапам формирования компетенций
Тема 1. Криптография в античные времена. Начала криптоанализа	ПКС-4	Реферат. Презентация доклада
Тема 2. Дешифровка египетских иероглифов. Дешифровка слогового линейного письма Б.	ПКС-4	Реферат. Презентация доклада
Тема 3 Криптография в Западной Европе в новое время.	ПКС-4	Реферат. Презентация доклада
Тема 4. История шифровального дела в России	ПКС-4	Реферат. Презентация доклада

8.2. Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений и навыков и (или) опыта деятельности процессе текущего контроля

Примеры задач для решения

Тема 1. Криптография в античные времена. Начала криптоанализа

	Задача
Оценка «удовлетворительно» или низкой уровень освоения компетенции	Расшифруйте текст, зашифрованный кодом сдвига (шифр Цезаря): ЙСХЦГЯЩРЪНГОАЩКЁВГПЪХГКАРМОЩКАОЖКГ
Оценка «хорошо» или повышенный уровень освоения компетенции	На реализацию древнеспартанского шифра перестановки скитала накладываются чисто физические ограничения. Естественно предположить, что диаметр жезла не превосходил 10 сантимет-

	ров. При высоте узкой накладываемой ленты (строки) в 1 сантиметр на одном витке найти максимальное число перестановок, реализуемых шифром.
Оценка «отлично» или высокий уровень освоения компетенции	Дешифруйте криптограмму, составленную с помощью шифра скитала: СЗНЛВЛАОЮОЫРЧБЕХОНВЙАЩОИПЛЕЙПЕЙЙ-ПЕЧЛГЕВАЬЛВЦЛВАЦАИЫСАС

Тема 2. Дешифровка египетских иероглифов. Дешифровка слогового линейного письма Б

	Задача
Оценка «удовлетворительно» или низкой уровень освоения компетенции	Определить, сколькими различными способами можно зашифровать слово “загадка” шифром перестановки
Оценка «хорошо» или повышенный уровень освоения компетенции	Разгадайте древнеегипетский картуш. Иероглиф  1 2 3 4 5 6 7 8
Оценка «отлично» или высокий уровень освоения компетенции	Ниже дан текст, образованный в соответствии с правилами линейного письма Б. В приведенном тексте опущены все гласные буквы – восстановите его. Здесь * — пропуск гласной. **Правила:** **1)** Слова разбиты на слоги: СЛОГ = Согласная + Гласная. **2)** Начальная гласная пишется не в слоге, а отдельно. **3)** Конечные гласные могут опускаться. **4)** Для образования слога между двумя гласными вставляется немое «и». Текст. 1. М*-м* м*-л* р*-м*. 2. * р*-з* *-п*-л* н* л*-п* *-з*-р*. (Афанасий Фет?) 3. М*-з*, р*-н* ш*-л*-м* *-п*-т*, т* п*-м*-л*-ш*-с* н* р*-з*. 4. *-з*-м* *-ч*-л* — * з*-м*-ч*-л*. 5. Н* *-с*-к*-ш*-л* — н*-с* * с*-к*ш*-л*. 6. Л*-з* с*-к*-к*-л*. «*-б*-р*-в*...» — *-б*-л*-к* с*-к*-з*-л*. 7. Т*-л*-т*-л* т*-с*-т* ж*-н* * н*-в*-с*-т*. 8. П*-к* л*-ч*-л* – п*-к*-л*-ч*-л*. 9. Р*-ж* ф*-г*-р*-к* — к*-н* * р*-б*-к*, к*-к* б* р*-с*-н*-к*— * к*-р* * ф*-ж*. 10.Разгадайте стихотворную **загадку** от поэта Державина Гаврилы Романовича (1743 – 1816): * р*-з*-м* *-м* з*-р*, // * *-д* с* м*-ч*-м* с*-д*-*. // С н*-ч*-л* т* ж* * * с* к*-н*-ц* //* в*-с*-м* ч*-т*-с* з* *-т*-ц*.

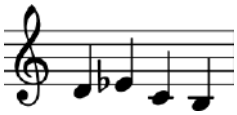
Тема 3. Криптография в Западной Европе в новое время

	Задача

Оценка «удовлетворительно» или низкой уровень освоения компетенции	Поросячья латынь. Переведите с поросячьей латыни на русский язык фразу: Посорососясячьяся ласатыньсы эсэтосо засабасавносо. Укажите "правила" перевода.
Оценка «хорошо» или повышенный уровень освоения компетенции	Некоторый алфавит состоит из шести букв, которые для передачи по телеграфу кодированы так: ·, —, · ·, — —, · —, — ·. При передаче одного слова не сделали промежутков, отделяющих букву от буквы, так что получилась сплошная цепочка точек и тире, состоящая из 12 знаков. Сколькими способами можно прочитать переданное слово? (например, буква «а» в азбуке Морзе всегда кодируется знаками · —).
Оценка «отлично» или высокий уровень освоения компетенции	Код Бэкона. Английский философ, историк, лорд-канцлер Великобритании Фрэнсис Бэкон (Francis Bacon, 1st Viscount St Albans, 1561-1626) разработал код, который бы позволял передавать секретные сообщения в обычных текстах так, чтобы никто не знал об этом сообщении. Впрочем, для его вскрытия требуется всего лишь внимательность. Итак, пусть дана обычная фраза (кодовое слово): вот и Наступила ДолГОжДаННая зима. Дешифровав её, получим секретное сообщение: bacon. Укажите алгоритм дешифровки.

Тема 4. История шифровального дела в России

	Задача
Оценка «удовлетворительно» или низкой уровень освоения компетенции	В начале рукописи, найденной в Вологде, и относящейся к 1643 г., писец сделал следующую приписку ppppp aaaaa aaaa o iiiiiiiii ъ, в которой зашифровал своё имя. Дешифруйте вышеприведённую мудрую литторею.
Оценка «хорошо» или повышенный уровень освоения компетенции	В романе графа Л. Н. Толстого "Анна Каренина" можно встретить страницы, на которых описывается шифр влюблённых друг в друга людей: «Константин Левин на новом зелёном сукне карточного стола начертил мелком следующие буквы, которые были предназначены княжне Кити Щербацкой: "к, в, м, о: э, н, м, б, з, л, э, н, и, т?"» Что «эти начальные буквы вопрошали»?

Оценка «отлично» или высокий уровень освоения компетенции	Нотная монограмма. Ре – Ми (бемоль) – До – Си (второй октавы)  Дешифруйте монограмму и назовите фамилию композитора, чья нотная монограмма здесь представлена. Подсказка: Прокофьев Сергей Сергеевич. Рахманинов Сергей Васильевич. Скрябин Александр Николаевич. Шостакович Дмитрий Дмитриевич.

8.3. Перечень вопросов и заданий для промежуточной аттестации по дисциплине

Вопросы для промежуточного контроля (зачета)

1. Язык жестов. Петроглифы и пиктограммы.
2. Геродот о тайнописи на восковых дощечках.
3. Аристотель и спартанский шифр скитала.
4. Доска Полибия.
5. Шифр (код) сдвига Цезаря.
6. Понятие код. Коды, состоящие из одной и двух частей.
7. Понятие шифра.
8. Шифр перестановки.
9. Шифр простой замены.
10. Частотный анализ. Арабские ученые Аль-Кинди (или Алькиндус) и Омар Хайям.
11. Древнейшее зашифрованное сообщение (дошедшее до нас): надпись, вырезанная на гробнице Хнумхотепа, примерно в 1900 г. до Р. Х.
12. Иероглифика, иератика и демотика.
13. Афанасий Кирхер, Иоганн Георг Цоэга.
14. Розеттский камень, Птолемей V Эпифан.
15. Томас Юнг.
16. Жан Франсуа Шампольон.
17. Картуши Рамсеса и Тутмоса.
18. Линейное письмо А (Фестский диск).
19. Линейное письмо Б.
20. Артур Эванс и Кносский дворец.
21. Первые шаги в дешифровке линейного письма Б (Джордж Смит, А. Э. Каули).
22. Статистический анализ окончаний падежей линейного письма Б (Алиса Кобер).

23. Окончательная дешифровка линейного письма Б (Майкл Вентрис и Джон Чедвик).
24. Леон Батиста Альберти и его диск.
25. Квадрат (таблица) Блеза де Виженера.
26. Автоключ Джероламо Кардано.
27. Бегущий автоключ и первичный ключ Блеза де Виженера.
28. Дешифровка «невскрываемого шифра» Чарльзом Бэббиджом.
29. Алгоритм взлома шифра Виженера.
30. Засекречивание алгоритма взлома из-за Крымской войны (1853-1856 гг.) между Великобританией и Россией.
31. Цифирь.
32. Двойная цифирь (Александр Сергеевич Грибоедов).
33. Мудрая литторея.
34. Декабристы (тюремный шифр).
35. Шифр графа Льва Николаевича Толстого.
36. Книжный шифр русских революционеров (на примере анархиста, князя Петра Алексеевича Кропоткина).

8.4. Планируемые уровни сформированности компетенций обучающихся и критерии оценивания

Уровни	Содержательное описание уровня	Основные признаки выделения уровня (этапы формирования компетенции, критерии оценки сформированности)	Пятибалльная шкала (академическая) оценка	Двухбалльная шакала, зачет	БРС, % освоения (рейтинговая оценка)
Повышенный	Творческая деятельность	*Включает нижестоящий уровень.* Умение самостоятельно принимать решение, решать проблему/задачу теоретического и прикладного характера на основе изученных методов, приемов, технологий	отлично	зачтено	86-100
Базовый	Применение знаний и умений в более широких контекстах учебной и профессиональной деятельности, нежели по образцу с большей степени самостоятельности и инициативы	*Включает нижестоящий уровень.* Способность собирать, систематизировать, анализировать и грамотно использовать информацию из самостоятельно найденных теоретических источников и иллюстрировать ими теоретические положения или обосновывать практику применения	хорошо		71-85

Удовлетворительный (достаточный)	Репродуктивная деятельность	Изложение в пределах задач курса теоретически и практически контролируемого материала	удовлетворительно		55-70
Недостаточный	Отсутствие признаков удовлетворительного уровня		неудовлетворительно	не зачтено	Менее 55

9. Перечень основной и дополнительной литературы, необходимой для освоения дисциплины

Основная литература.

1. *Фомичев, В. М.* Криптография — наука о тайнописи : учебное пособие / В. М. Фомичев. - Москва : Прометей, 2020. - 66 с. - ISBN 978-5-00172-040-9. - Текст : электронный. - URL: https://znanium.com/catalog/product/1851305

Дополнительная литература

1. Криптографическая защита информации : учебное пособие / С. О. Крамаров, О. Ю. Митясова, С. В. Соколов [и др.] ; под ред. С. О. Крамарова. — Москва : РИОР : ИНФРА-М, 2021. — 321 с. — (Высшее образование). - ISBN 978-5-369-01716-6. - Текст : электронный. - URL: https://znanium.com/catalog/product/1153156 (дата обращения: 25.04.2022). – Режим доступа: по подписке.
2. Фомичев, В. М. Криптография — наука о тайнописи : учебное пособие / В. М. Фомичев. - Москва : Прометей, 2020. - 66 с. - ISBN 978-5-00172-040-9. - Текст : электронный. - URL: https://znanium.com/catalog/product/1851305 (дата обращения: 25.04.2022). – Режим доступа: по подписке.

10. Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины

- НЭБ Национальная электронная библиотека, диссертации и прочие издания https://rusneb.ru/
- eLIBRARY.RU Научная электронная библиотека, книги, статьи, тезисы докладов конференций http://elibrary.ru/defaultx.asp
- Гребенников Электронная библиотека ИД журналы
- ЭБС Лань книги, журналы http://e.lanbook.com/
- ЭБС Консультант студента
- ПРОСПЕКТ ЭБС
- ЭБС ZNANIUM.COM https://znanium.com
- РГБ Информационное обслуживание по МБА
- БЕН РАН

– Электронно-библиотечная система (ЭБС) Кантиана (https://lib.kantiana.ru/jirbis2/)

Дополнительные ресурсы

1. Библиотека научной литературы. Раздел «Криптография» http://lib.org.by/_djvu/Cs_Computer%20science/CsCr_Cryptography/
2. Сайт Семьянова «Криптографический ликбез» http://www.ssl.stu.neva.ru/psw/crypto.html
3. Электронная библиотека механико-математического факультета Московского государственного университета. Раздел Криптография http://lib.mexmat.ru/catalogue.php?dir=02_06
4. Домашняя страница Алана Тьюринга http://www.turing.org.uk

Электронные книги

1. Гребенников В. В. История криптологии и секретного сыска. — Ужгород, 2012. — 659 с.: ил. http://www.cryptohistory.ru
2. *Павлов, Е. А.* История отечественной математики : учебное пособие / Е. А. Павлов. — 2-е изд., испр. — Санкт-Петербург : Лань, 2020. — 92 с. — ISBN 978-5-8114-4664-3. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/142332

11. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине

Программное обеспечение обучения включает в себя:

- система электронного образовательного контента БФУ им. И. Канта – www.lms-3.kantiana.ru, обеспечивающую разработку и комплексное использование электронных образовательных ресурсов;
- серверное программное обеспечение, необходимое для функционирования сервера и связи с системой электронного обучения через Интернет;
- корпоративная платформа Microsoft Teams;
- установленное на рабочих местах обучающихся ПО: Microsoft Windows 7, Microsoft Office Standart 2010, антивирусное программное обеспечение Kaspersky Endpoint Security.
- специализированное ПО – не требуется.

12. Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине

Для проведения занятий лекционного типа, практических и семинарских занятий используются специальные помещения (учебные аудитории), оборудованные технически-

ми средствами обучения – мультимедийной проекционной техникой. Для проведения занятий лекционного типа используются наборы демонстрационного оборудования.

Для проведения лабораторных работ, (практических занятий – при необходимости) используются специальные помещения (учебные аудитории), оснащенные специализированным лабораторным оборудованием: персональными компьютерами с возможностью выхода в интернет и с установленным программным обеспечением, заявленным в п.11.

Для проведения групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации используются специальные помещения (учебные аудитории), оборудованные специализированной мебелью (для обучающихся), меловой / маркерной доской.

Для организации самостоятельной работы обучающимся предоставляются помещения, оснащенные компьютерной техникой с возможностью подключения к сети «Интернет» и обеспечением доступа в электронную информационно-образовательную среду университета.

Для обучения инвалидов и лиц с ограниченными возможностями здоровья университетом могут быть представлены специализированные средства обучения, в том числе технические средства коллективного и индивидуального пользования.

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ
федеральное государственное автономное образовательное учреждение высшего образования «Балтийский федеральный университет имени Иммануила Канта»
Институт физико-математических наук и информационных технологий

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

«СИСТЕМЫ КОМПЬЮТЕРНОЙ АЛГЕБРЫ И РЕАЛИЗАЦИЯ КРИПТОГРАФИЧЕСКИХ АЛГОРИТМОВ»

Шифр: 10.05.01
Специальность: «Компьютерная безопасность»
Специализация: «Математические методы защиты информации»
Квалификация (степень) выпускника: специалист по защите информации

Калининград
2022

Лист согласования

Составитель: БОЛТНЕВ ЮРИЙ ФЕДОРОВИЧ. старший преподаватель

Рабочая программа утверждена на заседании учебно-методического совета института физико-математических наук и информационных технологий
Протокол № 01/22 от «01» февраля 2022 г.

Председатель учебно-методического совета института физико-математических наук и информационных технологий
Первый заместитель директора ИФМНиИТ, к. ф.-м. н., доцент — Шпилевой А. А

Ведущий менеджер — Е.П.Ставицкая

СОДЕРЖАНИЕ

1. Наименование дисциплины: «СИСТЕМЫ КОМПЬЮТЕРНОЙ АЛГЕБРЫ И РЕАЛИЗАЦИЯ КРИПТОГРАФИЧЕСКИХ АЛГОРИТМОВ»

Целями освоения дисциплины «Системы компьютерной алгебры и реализация криптографических алгоритмов» являются:

- формирование знаний и навыков, необходимых для эксплуатации программного обеспечения и программно-аппаратных средств обеспечения информационной безопасности компьютерных систем;
- ознакомление с современными тенденциями развития информатики и вычислительной техники, компьютерных технологий в области защиты информации;
- изучение основных методов применения систем компьютерной алгебры для реализации теоретико-числовых алгоритмов;
- овладение методами современной теории чисел, применяемыми в криптографии, теории кодирования и общих моделях безопасности компьютерных систем.

2. Перечень планируемых результатов обучения по дисциплине, соотнесенных с планируемыми результатами освоения образовательной программы

Код компетенции	Результаты освоения образовательной программы (ИДК)	Результаты обучения по дисциплине
ПКС-5. Способность участвовать в теоретических и экспериментальных научно-исследовательских работах по оценке защищенности информации в компьютерных системах	ПКС-5.1. Знает тенденции развития теоретических и экспериментальных исследований в области защиты информации. ПКС-5.2. Участвует в теоретических научно-исследовательских работах по оценке защищенности информации в компьютерных системах ПКС-5.3. Участвует в экспериментальных научно-исследовательских работах по аудиту безопасности в компьютерных системах	В результате освоения дисциплины студент должен: *Знать:* – современные информационные методики и технологии, методы математической обработки информации – методы решения стандартных задач алгебры и теории чисел; – алгоритмы вычислений в конечных полях: – основные теоретико-числовые алгоритмы, имеющие приложения в криптографии; – основные типы криптографических алгоритмов и типовые уязвимости криптосистем. – современные методы математической обработки информации, методы теоретического и экспериментального исследования. *Уметь:* – разрабатывать вычислительные алгоритмы, реализующие современные математические методы защиты информации; – грамотно применять изученные математические методы, математические пакеты Maple, SAGE, PARI-GP для обработки, детального анализа и систематизации криптографической информации; – моделировать алгоритмы в системах компьютерной алгебры, оценивать их работоспособность и эффективность; – ориентироваться в современных и перспективных математических методах защиты информации, оценивать возможности и эффективность их применения в кон-

		кретных задачах защиты информации. *Владеть:* − построением математических моделей информационных потоков, возникающих при построении криптографической инфраструктуры и оценивать возможность и эффективность их применения в криптографии; − практическими навыками применения пакетов компьютерной алгебры Maple, Sage, PARI-GP для решения криптографических задач, владеть навыками исследования алгоритмов применительно к криптографии; − приемами реализации стандартных теоретико-числовых алгоритмов; приемами работы с программными средствами прикладного, системного и специального назначения; − методами оценки корректности и стойкости соответствующих алгоритмов; навыками математического моделирования в криптографии.

3. Место дисциплины в структуре ООП ВО

Дисциплина «Системы компьютерной алгебры и реализация криптографических алгоритмов» представляет собой дисциплину части, формируемой участниками образовательных отношений блока дисциплин подготовки обучающихся

4. Виды учебной работы по дисциплине.

Виды учебной работы по дисциплине зафиксированы учебным планом основной профессиональной образовательной программы по указанному направлению и профилю, выражаются в академических часах. Часы контактной работы и самостоятельной работы студента и часы, отводимые на процедуры контроля, могут различаться в учебных планах ОПОП по формам обучения. Объем контактной работы включает часы контактной аудиторной работы (лекции/практические занятия/ лабораторные работы), контактной внеаудиторной работы (контроль самостоятельной работы), часы контактной работы в период аттестации. Контактная работа, в том числе может проводиться посредством электронной информационно-образовательной среды университета с использованием ресурсов сети Интернет и дистанционных технологий

5. Содержание дисциплины, структурированное по темам (разделам)

Исходя из рамок, установленных учебным планом по трудоемкости и видам учебной работы по дисциплине, преподаватель самостоятельно выбирает тематику занятий по формам и количеству часов проведения контактной работы: лекции и иные учебные занятия, предусматривающие преимущественную передачу учебной информации преподавателем и (или) занятия семинарского типа (семинары, практические занятия, практикумы, лабораторные работы, коллоквиумы и иные анало-

гичные занятия), и (или) групповые консультации, и (или) индивидуальную работу обучающихся с преподавателем, в том числе индивидуальные консультации (по курсовым работам/проектам – при наличии курсовой работы/проекта по данной дисциплине в учебном плане). Рекомендуемая тематика занятий максимально полно реализуется в контактной работе со студентами очной формы обучения. В случае реализации образовательной программы в заочной / очно-заочной форме трудоемкость дисциплины сохраняется, однако объем учебного материала в значительной части осваивается студентами в форме самостоятельной работы. При этом требования к ожидаемым образовательным результатам студентов по данной дисциплине не зависят от формы реализации образовательной программы.

Тема 1. Решение задач алгебры и математического анализа. Графика в Maple

Обзор программ символьной математики. Возможности алгебраического пакета Maple. Его структура и интерфейс. Программные средства работы с числами, со строчными и символьными выражениями пакета. Программные средства работы со списками, множествами и таблицами пакета.

Аналитические преобразования в Maple. Операции с полиномами и рациональными дробями. Способы упрощения выражений. Решение алгебраических уравнений и неравенств в среде пакета Maple. Возможности пакета при решении тригонометрических уравнений и неравенств. Особенности преобразования тригонометрических выражений в среде пакета.

Решение задач математического анализа в среде пакета Maple: вычисление пределов, производных, интегралов, нахождение суммы ряда. Решение прикладных задач. Линейная алгебра в Maple. Базовые средства линейной алгебры в среде linalg-модуля пакета и в среде модуля LinearAlgebra. Примеры решения задач линейной алгебры в среде Maple.

Опции и команды двумерной графики (функции, заданной явно, неявно, параметрически, в полярной системе координат). Сохранение рисунка в текстовом документе. Команды и структуры трехмерной графики. Цилиндрическая и сферическая системы координат. Анимация.

Тема 2. Решение задач прикладной математики средствами математических пакетов

Назначение пакетов и обращение к ним. Обзор некоторых пакетов: комбинаторика, финансово-экономических функций, ортогональных многочленов, реализации степенных разложений, работы с полиномами, приближения кривых. Структура и возможности пакета «Student» . Работа с самоучителями (Tutors) в интерактивном режиме.

Аналитические решения обыкновенных дифференциальных уравнений (ОДУ) в среде пакета Maple. Приближенные решения ОДУ. Численные решения ОДУ.

Решение задач теории графов. Команды модуля «Graph Theory». Задание графа, определение его вершин и ребер. Команды, реализующие основные операции работы с графами: вычисление потоков в сетях, определение связности, поиск покрывающих деревьев, расчет кратчайших путей.

Программирование в Maple. Условный оператор, операторы цикла. Виды циклов: «Перечислительный» цикл, цикл «while», цикл, работающий с символьными выражениями, бесконечные циклы, вложенные циклы. Управление ходом выполнения цикла. Процедуры.

Тема 3. Алгоритмы элементарной теории чисел.

Алгоритм Евклида. Расширенный алгоритм Евклида. Решение сравнений и систем сравнений. Вычисление квадратных корней по простому и по составному модулю.

Вычисления в кольце целых гауссовых чисел. Решение сравнений. Наибольший общий делитель гауссовых чисел. Разложение на неприводимые множители в евклидовых кольцах.

Разложение рациональных чисел в конечные цепные дроби Разложение действительных чисел в бесконечные цепные дроби. Приближение иррациональных чисел подходящими дробями.

Тема 4. Вычисления в конечных полях.

Построение конечного поля. Таблица индексов конечного поля. Алгоритмы возведения в степень в конечном поле. Построение неприводимых многочленов над полем. Вычисление круговых многочленов. Разложение многочленов на неприводимые множители над заданным полем. Вычисление норм и следов. Построение минимальных многочленов.

Тема 5. Криптосистемы с открытым ключом

Криптосистема RSA. Выбор параметров. Алгоритмы маркировки сообщений. Типовые атаки на RSA. Атака на малую шифрующую экспоненту. Факторизация модуля. Атака Винера. Атака повторным шифрованием. Альтернативные ключи в RSA. Криптосистемы, основанные на дискретном логарифме: Диффи–Хеллмана, Месси–Омуры, Эль-Гамаля.

6. Рекомендуемая тематика учебных занятий в форме контактной работы

Рекомендуемая тематика учебных занятий лекционного типа (предусматривающих преимущественную передачу учебной информации преподавателями):

№	Наименование раздела	Темы лекций
1	Решение задач алгебры и математического анализа. Графика в Maple	Обзор программ символьной математики. Возможности алгебраического пакета Maple. Его структура и интерфейс. Программные средства работы с числами, со строчными и символьными выражениями пакета. Программные средства работы со списками, множествами и таблицами пакета. Аналитические преобразования в Maple. Операции с полиномами и рациональными дробями. Способы упрощения выражений. Решение алгебраических уравнений и неравенств в среде пакета Maple. Возможности пакета при решении тригонометрических уравнений и неравенств. Особенности преобразования тригонометрических выражений в среде пакета. Решение задач математического анализа в среде пакета Maple: вычисление пределов, производных, интегралов, нахождение суммы ряда. Решение прикладных задач. Линейная алгебра в Maple. Базовые средства линейной алгебры в среде linalg-модуля пакета и в среде модуля LinearAlgebra. Примеры решения задач линейной алгебры в среде Maple. Опции и команды двумерной графики (функции, заданной явно, неявно, параметрически, в полярной системе координат). Сохранение рисунка в текстовом документе. Команды и структуры трехмерной графики. Цилиндрическая и сферическая системы координат. Анимация
2	Решение задач прикладной математики средствами математических пакетов.	Назначение пакетов и обращение к ним. Обзор некоторых пакетов: комбинаторика, финансово-экономических функций, ортогональных многочленов, реализации степенных разложений, работы с полиномами, приближения кривых. Структура и

		возможности пакета «Student» . Работа с самоучителями (Tutors) в интерактивном режиме. Аналитические решения обыкновенных дифференциальных уравнений (ОДУ) в среде пакета Maple. Приближенные решения ОДУ. Численные решения ОДУ. Решение задач теории графов. Команды модуля «Graph Theory». Задание графа, определение его вершин и ребер. Команды, реализующие основные операции работы с графами: вычисление потоков в сетях, определение связности, поиск покрывающих деревьев, расчет кратчайших путей. Программирование в Maple. Условный оператор, операторы цикла. Виды циклов: «Перечислительный» цикл, цикл «while», цикл, работающий с символьными выражениями, бесконечные циклы, вложенные циклы. Управление ходом выполнения цикла. Процедуры
3	Алгоритмы элементарной теории чисел	Алгоритм Евклида. Расширенный алгоритм Евклида. Решение сравнений и систем сравнений. Вычисление квадратных корней по простому и по составному модулю. Вычисления в кольце целых гауссовых чисел. Решение сравнений. Наибольший общий делитель гауссовых чисел. Разложение на неприводимые множители в евклидовых кольцах. Разложение рациональных чисел в конечные цепные дроби Разложение действительных чисел в бесконечные цепные дроби. Приближение иррациональных чисел подходящими дробями.
4	4. Вычисления в конечных полях.	Построение конечного поля. Таблица индексов конечного поля. Алгоритмы возведения в степень в конечном поле. Построение неприводимых многочленов над полем. Вычисление круговых многочленов. Разложение многочленов на неприводимые множители над заданным полем. Вычисление норм и следов. Построение минимальных многочленов
5	Криптосистемы с открытым ключом.	Криптосистема RSA. Выбор параметров. Алгоритмы маркировки сообщений. Типовые атаки на RSA. Атака на малую шифрующую экспоненту. Факторизация модуля. Атака Винера. Атака повторным шифрованием. Альтернативные ключи в RSA. Криптосистемы, основанные на дискретном логарифме: Диффи–Хеллмана, Месси–Омуры, Эль-Гамаля

Тематика практических занятий

1. Работа с обучающей программой «Самоучитель пользователя Maple».
2. Алгебраические преобразования.
3. Решение задач элементарной математики средствами пакета.
4. Решение задач математического анализа.
5. Применение пакета «Student».
6. Двумерная графика. Трехмерная графика.

7. Математические пакеты.
8. Линейная алгебра.
9. Решение дифференциальных уравнений
10. Теория графов.
11. Программирование в Maple.
12. Вычисления над конечными полями.
13. Решение учебно-исследовательской задачи элементарной теории чисел.
14. Вычисление наибольшего общего делителя. Исследование сложности алгоритма Евклида.
15. Решение сравнений и систем сравнений.
16. Разложение рациональных и иррациональных чисел в цепные дроби.
17. Построение конечного поля.
18. Вычисление кругового многочлена. Разложение многочленов на множители над конечным полем.
19. Вычисление следа в конечном поле.
20. Определение числа решений уравнения гиперэллиптического типа.
21. Построение минимальных многочленов элементов конечного поля.
22. Реализация криптосистемы RSA.
23. Атака Винера на RSA.
24. Атака повторным шифрованием.
25. Альтернативные ключи в RSA.
26. Реализация криптосистем, основанных на дискретном логарифме в простом конечном поле.
27. Реализация криптосистем Диффи–Хеллмана, Месси–Омуры, Эль-Гамаля в расширении простого конечного поля.
28. Реализация типовых теоретико-числовых алгоритмов средствами специализированных алгебраических систем (с открытым кодом) PARI-GP и SAGE.
29. Реализация вычислений в конечных полях средствами специализированных алгебраических систем (с открытым кодом) PARI-GP и SAGE.
30. Проведение деловой игры: определение типа уязвимости системы RSA на основании открытой информации. Дешифрование секретного сообщения путем проведения атаки на обнаруженную уязвимость

Темы заданий на лабораторные работы

1. Разработать программу для вычисления обратного элемента, используя расширенный алгоритм Евклида. Рассчитать примеры. Сделать оценку сложности алгоритма. Дать краткое описание методики.
2. Разработать программу для быстрого возведения в степень (методом слева направо или справа налево). Рассчитать примеры. Сделать оценку сложности алгоритма. Дать краткое описание методики.
3. Разработать программу, производящую потенцирование в криптосистеме RSA на основе китайской теоремы об остатках. Дать краткое описание методики. Сделать оценку сложности алгоритма.
4. Разработать программу для построения ЛРП на основе линейного регистра сдвига с обратной связью (LFSR). Определить период построенной ЛРП. Дать краткое описание методики.

5. Построить компьютерную модель протокола Диффи – Хеллмана в системе CrypTool. Продемонстрировать атаку на протокол. Сделать оценку сложности атаки.
6. Построить компьютерную модель протокола Диффи – Хеллмана в системе SAGE. Реализовать атаку на протокол путем вычисления дискретного логарифма. Сделать оценку сложности атаки.
7. Построить компьютерную модель криптосистемы Эль-Гамаля в системе SAGE. Реализовать атаку на криптосистему путем вычисления дискретного логарифма. Сделать оценку сложности атаки.
8. Разработать программу, производящую зашифрование и расшифрование текстового сообщения в криптосистеме RSA. Дать краткое описание методики.
9. Разработать программу, позволяющую провести атаку повторным шифрованием на криптосистему RSA. Исследовать возможность проведения атаки при подходящем выборе ключа шифрования. Сделать оценку сложности атаки
10. Разработать программу, позволяющую провести атаку Винера на криптосистему RSA. Исследовать возможность проведения атаки при превышении границы Винера. Сделать оценку сложности атаки.
11. Проведение деловой игры: определение типа уязвимости системы RSA на основании открытой информации. Дешифрование секретного сообщения путем проведения атаки на обнаруженную уязвимость

Требования к самостоятельной работе обучающихся

1. Работа с лекционным материалом, предусматривающая проработку конспекта лекций и учебной литературы, по всем темам из п. 6 настоящей рабочей программы.
2. Выполнение домашнего задания, предусматривающего решение задач, выполнение упражнений, выдаваемых на практических занятиях, по всем темам из п. 6 настоящей рабочей программы.

Руководствуясь положениями статьи 47 и статьи 48 Федерального закона от 29 декабря 2012 г. N 273-ФЗ «Об образовании в Российской Федерации» научно-педагогические работники и иные лица, привлекаемые университетом к реализации данной образовательной программы, пользуются предоставленными академическими правами и свободами в части свободы преподавания, свободы от вмешательства в профессиональную деятельность; свободы выбора и использования педагогически обоснованных форм, средств, методов обучения и воспитания; права на творческую инициативу, разработку и применение авторских программ и методов обучения и воспитания в пределах реализуемой образовательной программы и отдельной дисциплины.

Исходя из рамок, установленных учебным планом по трудоемкости и видам учебной работы по дисциплине, преподаватель самостоятельно выбирает тематику занятий по формам и количеству часов проведения контактной работы: лекции и иные учебные занятия, предусматривающие преимущественную передачу учебной информации преподавателем и (или) занятия семинарского типа (семинары, практические занятия, практикумы, лабораторные работы, коллоквиумы и иные аналогичные занятия), и (или) групповые консультации, и (или) индивидуальную работу обучающихся с преподавателем, в том числе индивидуальные консультации (по курсовым работам/проектам – при наличии курсовой работы/проекта по данной дисциплине в учебном плане).

Рекомендуемая тематика занятий максимально полно реализуется в контактной работе с обучающимися очной формы обучения. В случае реализации образовательной программы в заочной

/ очно-заочной форме трудоемкость дисциплины сохраняется, однако объем учебного материала в значительной части осваивается обучающимися в форме самостоятельной работы. При этом требования к ожидаемым образовательным результатам обучающихся по данной дисциплине не зависят от формы реализации образовательной программы.

7. Методические рекомендации по видам занятий

Лекционные занятия.

В ходе лекционных занятий обучающимся рекомендуется выполнять следующие действия. Вести конспектирование учебного материала. Обращать внимание на категории, формулировки, раскрывающие содержание тех или иных явлений и процессов, научные выводы и практические рекомендации по их применению. Задавать преподавателю уточняющие вопросы с целью уяснения теоретических положений, разрешения спорных ситуаций.

Желательно оставить в рабочих конспектах поля, на которых во внеаудиторное время можно сделать пометки из рекомендованной литературы, дополняющие материал прослушанной лекции, а также подчеркивающие особую важность тех или иных теоретических положений.

Практические и семинарские занятия.

На практических и семинарских занятиях в зависимости от темы занятия выполняется поиск информации по решению проблем, практические упражнения, контрольные работы, выработка индивидуальных или групповых решений, итоговое обсуждение с обменом знаниями, участие в круглых столах, разбор конкретных ситуаций, командная работа, представление портфолио и т.п.

Самостоятельная работа.

Самостоятельная работа осуществляется в виде изучения литературы, эмпирических данных по публикациям и конкретных ситуаций из практики, подготовке индивидуальных работ, работа с лекционным материалом, самостоятельное изучение отдельных тем дисциплины; поиск и обзор литературы и электронных источников; чтение и изучение учебника и учебных пособий.

8. Фонд оценочных средств

8.1 Перечень компетенций с указанием этапов их формирования в процессе освоения образовательной программы

Основными этапами формирования указанных компетенций при изучении студентами дисциплины являются последовательное изучение содержательно связанных между собой *разделов* (*тем*) учебных занятий. Изучение каждого раздела (темы) предполагает овладение студентами необходимыми компетенциями. Результат аттестации студентов на различных этапах формирования компетенций показывает уровень освоения компетенций студентами.

Контролируемые модули, разделы (темы) дисциплины	Индекс контролируемой компетенции (или её части)	Оценочные средства по этапам формирования компетенций
1. Решение задач алгебры и математического анализа. Графика в Maple	ПКС-5	Защита лабор. работ
2. Решение задач прикладной математики средствами математических пакетов.	ПКС-5	Защита лабор. работ

3. Алгоритмы элементарной теории чисел	ПКС-5	Защита лабор. работ
4. Вычисления в конечных полях.	ПКС-5	Защита лабор. работ
5. Криптосистемы с открытым ключом.	ПКС-5	Защита лабор. работ

8.2. Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений и навыков и (или) опыта деятельности процессе текущего контроля

Типовые контрольные задания

Лабораторная работа

«Решение задач теории дифференциальных уравнений в среде пакета Maple.»

Найти приближенное решение в виде степенного ряда до 6-го порядка и точное решение задачи Коши. Построить на одном рисунке графики точного и приближенного решений.

$$dif := \frac{d^2}{dx^2} y(x) - 4\left(\frac{d}{dx} y(x)\right) + 13\, y(x) = e^{2x}\cos(3x)$$

$$ic := y(0) = 1, D(y)(0) = -1$$

Задания к проверочной работе по теме «Алгоритмы теории чисел»

1.Разложите на множители число $10^{10}+1$.
2.Проверьте, является ли число $10^{100}+1$ простым.
3.Найдите наибольший общий делитель чисел $10^{10}+1$ и $10^{18}+1$.
4.Найдите 100-е по счету простое число.
5.Пьер Ферма считал, что все числа вида $2^{2\wedge n}$, где n целое неотрицательное число – простые. Опровергните утверждение Ферма.
6.Найдите ближайшие сверху и снизу простые числа к 10^{100}.
7.Сколько существует простых чисел, не превосходящих 10^6?
8.Найдите общий вид решения в целых числах уравнения 3x+5y=179.
9.Найдите общий вид решения в натуральных числах уравнения $x^2-2y^2=-1$. Найдите первые три наименьших его решения.
10.Для отрезка $[10^3,10^3+50]$ постройте графики функций pi(x), tau(x), sigma(x), phi(x).
11.Асимптотический закон распределения простых чисел гласит, что количество простых чисел не превосходящих x стремится к x/ln(x). Проверьте это утверждение, построив график отношения pi(x) к x/ln(x) на отрезке $[10^5 ,10^6]$.

Перечисленные задания выполнить средствами трех систем: Maple, PARI-GP и SAGE

Примеры задач для решения

Тема 1. Решение задач алгебры и математического анализа. Графика в Maple

	Задача
Оценка «удовлетворительно» или низкой уровень освоения компетенции	Дана тригонометрическая функция *y := cos(x)*. Проверить тип. Преобразовать данную функцию в экспоненциальную и присвоить ее переменной *ex*. Конвертировать экспоненциальную функцию в тригонометрическую и присвоить ее переменной *tr*. Опре-

	делить тип каждого полученного выражения.
Оценка «хорошо» или повышенный уровень освоения компетенции	Найти корни полиномиального уравнения $x\text{^}4 + 3*x\text{^}3 - 8*x + 3 = 0$ Представить решение в виде приближенного числового значения. Найти численное решение. Найти вещественные и комплексные корни. Найти корень, заданный на интервале от 1 до бесконечности. Найти один наименьший корень полинома. Найти корень из множества корней, который находится вблизи значения: -2 + *i* и 2. Представить решение, используя радикалы. Проверить правильность полученного решения с помощью команды map.
Оценка «отлично» или высокий уровень освоения компетенции	Решить систему из двух уравнений с двумя неизвестными $\{x y + 3x = 8\ ,\ 3x^2 + (y+3)^2 = 28\ \}$ Представить решение, используя радикалы, если потребуется. Представить решение в виде списка множеств. Проверить правильность полученного решения.

Тема 2. Решение задач прикладной математики средствами математических пакетов

	Задача
Оценка «удовлетворительно» или низкой уровень освоения компетенции	Найти общее решение дифференциального уравнения первого порядка: $\frac{\mathrm{d}}{\mathrm{d}x} y(x) = \frac{y(x)\ln(y(x))}{\sqrt{1-x^2}\ \arcsin(x)}$
Оценка «хорошо» или повышенный уровень освоения компетенции	Найти общие решения дифференциального уравнения второго порядка и найти частное решение, удовлетворяющее указанным начальным условиям, которые определены как множество: $\frac{\mathrm{d}^2}{\mathrm{d}x^2} y(x) - \frac{\frac{\mathrm{d}}{\mathrm{d}x} y(x)}{x-1} = x\,(x-1)$ $\{y(0) = 0, \mathrm{D}(y)(0) = -1\}$
Оценка «отлично» или высокий уровень освоения компетенции	Найти решение задачи Коши в виде степенного ряда с точностью до 5-го порядка. $\frac{\mathrm{d}}{\mathrm{d}x} y(x) = y(x) + x\,\mathrm{e}^{y(x)}$ $y(0) = 0$

Тема 3. Алгоритмы элементарной теории чисел

	Задача
Оценка «удовлетворительно» или низкой уровень освоения компетенции	Реализовать расширенный алгоритм Евклида
Оценка «хорошо» или повышенный уровень освоения компетенции	Реализовать алгоритм разложения рационального числа в цепную дробь
Оценка «отлично» или высокий уровень освоения компетенции	Реализовать алгоритм решения системы сравнений по китайской теореме об остатках

Тема 4. Вычисления в конечных полях

	Задача
Оценка «удовлетворительно» или низкой уровень освоения компетенции	Реализовать алгоритм построения таблицы индексов конечного поля F_{16}
Оценка «хорошо» или повышенный уровень освоения компетенции	Реализовать алгоритм построения таблицы следов в конечном поле F_{16}
Оценка «отлично» или высокий уровень освоения компетенции	Реализовать алгоритм разложения многочлена $\Phi_{15}(x)$ на неприводимые множители над полем разложения

Тема 5. Криптосистемы с открытым ключом

	Задача
Оценка «удовлетворительно» или низкой уровень освоения компетенции	Написать процедуру, реализующую криптосистему RSA
Оценка «хорошо» или повышенный уровень освоения компетенции	Написать процедуру маркировки текстового сообщения целыми числами (элементами кольца Z/nZ).
Оценка «отлично» или высокий уровень освоения компетенции	Написать процедуру, реализующую атаку Винера на RSA.

8.3. Перечень вопросов и заданий для промежуточной аттестации по дисциплине

Вопросы для промежуточного контроля (зачета)

1. Программы для символьной математики (Mathematica, Maple, MatLab, MathCad) и альтернативные проекты. Спектр решаемых задач.
2. Общая структурная организация пакета Maple. Открытие, сохранение, создание нового, просмотр, редактирование, закрытие текущего документа.
3. Интерфейс пакета Maple.
4. Простейшие объекты в Maple.
5. Типы переменных, выражения, команды Maple.
6. Синтаксис пакета, стандартные функции.
7. Использование справочной системы.
8. Команды преобразования и упрощения. Операции с формулами.
9. Преобразования типов. Операции оценивания.
10. Операции с полиномами.
11. Решение уравнений и неравенств элементарной математики.
12. Программные средства для решения задач мат. анализа.
13. Использование пакета Student.

14. Программные средства библиотек LinearAlgebra и linalg.
15. Программные средства для решения дифференциальных уравнений.
16. Графические возможности Maple.
17. Опции, структуры и команды трехмерной графики.
18. Возможности пакета при работе с графами.
19. Программные средства для задач теории чисел.
20. Программирование в Maple.
21. Некоторые алгоритмы проверки на простоту.
22. Алгоритм Евклида. Расширенный Алгоритм Евклида.
23. Решение сравнений и систем сравнений.
24. Разложение действительных чисел в конечные и бесконечные цепные дроби.
25. Вычисление квадратных корней по простому и по составному модулю
26. Наибольший общий делитель целых гауссовых чисел
27. Разложение на неприводимые множители в кольце целых гауссовых чисел
28. Построение конечного поля. Таблица индексов конечного поля.
29. Алгоритмы возведения в степень в конечном поле.
30. Вычисление круговых многочленов. Разложение многочленов на неприводимые множители над заданным полем.
31. Вычисление норм и следов.
32. Построение минимальных многочленов
33. Алгоритмы факторизации.
34. Криптосистема RSA. Особенности выбора параметров криптосистемы.
35. Типовые уязвимости RSA.
36. Атака на малую шифрующую экспоненту. Факторизация модуля.
37. Атака Винера на криптосистему RSA.
38. Атака повторным шифрованием.
39. Альтернативные ключи в RSA.
40. Криптосистемы, основанные на дискретном логарифме: Диффи–Хеллмана, Месси–Омуры.
41. Криптосистема Эль-Гамаля.
42. Схема цифровой подписи.

8.4. Планируемые уровни сформированности компетенций обучающихся и критерии оценивания

Уровни	Содержательное описание уровня	Основные признаки выделения уровня (этапы формирования компетенции, критерии оценки сформированности)	Пятибалльная шкала (академическая) оценка	Двухбалльная шакала, зачет	БРС, % освоения (рейтинговая оценка)
Повышенный	Творческая деятельность	*Включает нижестоящий уровень.* Умение самостоятельно принимать решение, решать проблему/задачу теоретиче-	отлично	зачтено	86-100

		ского и прикладного характера на основе изученных методов, приемов, технологий			
Базовый	Применение знаний и умений в более широких контекстах учебной и профессиональной деятельности, нежели по образцу с большей степени самостоятельности и инициативы	*Включает нижестоящий уровень.* Способность собирать, систематизировать, анализировать и грамотно использовать информацию из самостоятельно найденных теоретических источников и иллюстрировать ими теоретические положения или обосновывать практику применения	хорошо		71-85
Удовлетворительный (достаточный)	Репродуктивная деятельность	Изложение в пределах задач курса теоретически и практически контролируемого материала	удовлетворительно		55-70
Недостаточный	Отсутствие признаков удовлетворительного уровня		неудовлетворительно	не зачтено	Менее 55

9. Перечень основной и дополнительной литературы, необходимой для освоения дисциплины

Основная литература.

1. *Алешников С.И., Козьминых Е.В.* Математические методы защиты информации. Ч. 3. Вычислительный практикум по числовым полям и криптографии в квадратичных полях: Практическое пособие. – Калининград: Изд-во РГУ им. И. Канта, 2006, . Переиздано: электронное издание, Изд-во БФУ, 2015 г ЭБС Кантиана
   http://medialib.kantiana.ru/MediaPlayerTestPage.html?id=83e91cb3-b256-4860-948c-f0171a2d95a8

Дополнительная литература

2. *Алешников С.И., Болтнев Ю.Ф.* Математические методы защиты информации. Часть 1. Алгебраические методы: Учебное пособие / Калинингр. ун-т. – Калининград, 2000. Переиздано: электронное издание, Изд-во БФУ, 2015 г ЭБС Кантиана
3. *Авдошин, С.М.* Дискретная математика. Модулярная алгебра, криптография, кодирование / С.М. Авдошин, А.А. Набебин. - Москва : ДМК Пресс, 2017. - 352 с. - ISBN 978-5-94074-408-3. - Текст : электронный. - URL:
   https://znanium.com/catalog/product/1027855

10. Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины

- НЭБ Национальная электронная библиотека, диссертации и прочие издания https://rusneb.ru/
- eLIBRARY.RU Научная электронная библиотека, книги, статьи, тезисы докладов конференций http://elibrary.ru/defaultx.asp
- Гребенников Электронная библиотека ИД журналы
- ЭБС Лань книги, журналы http://e.lanbook.com/
- ЭБС Консультант студента
- ПРОСПЕКТ ЭБС
- ЭБС ZNANIUM.COM https://znanium.com
- РГБ Информационное обслуживание по МБА
- БЕН РАН
- Электронно-библиотечная система (ЭБС) Кантиана (https://lib.kantiana.ru/jirbis2/)

Дополнительные ресурсы

1. Библиотека научной литературы. Раздел «Криптография» http://lib.org.by/_djvu/Cs_Computer%20science/CsCr_Cryptography/
2. Сайт Семьянова «Криптографический ликбез» http://www.ssl.stu.neva.ru/psw/crypto.html
3. Электронная библиотека механико-математического факультета Московского государственного университета. Раздел Криптография http://lib.mexmat.ru/catalogue.php?dir=02_06
4. *Шнайер Б.* Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си http://www.ssl.stu.neva.ru/psw/crypto/appl_rus/appl_cryp.htm
5. *A. Menezes, P. van Oorschot, S. Vanstone.* Handbook of Applied Cryptography. — http://www.cacr.math.uwaterloo.ca/hac/

Электронные книги

1. *Аграновский А.В. Хади Р.А.* Практическая криптография: алгоритмы и их программирование http://e.lanbook.com/books/element.php?pl1_id=13653
2. *Василенко О.Н.* Теоретико-числовые алгоритмы в криптографии http://e.lanbook.com/books/element.php?pl1_id=9303
3. *Глухов М.М., Круглов И.А., Пичкур А.Б., Черемушкин А.В.* Введение в теоретико-числовые методы криптографии http://e.lanbook.com/books/element.php?pl1_id=1540
4. *Лапонина О.Р.* Криптографические основы безопасности http://www.intuit.ru/goods_store/ebooks/8170
5. Фороузан Б.А. Криптография и безопасность сетей http://www.intuit.ru/goods_store/ebooks/361

11. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине

Программное обеспечение обучения включает в себя:

- система электронного образовательного контента БФУ им. И. Канта – www.lms-3.kantiana.ru, обеспечивающую разработку и комплексное использование электронных образовательных ресурсов;
- серверное программное обеспечение, необходимое для функционирования сервера и связи с системой электронного обучения через Интернет;
- корпоративная платформа Microsoft Teams;
- установленное на рабочих местах обучающихся ПО: Microsoft Windows 7, Microsoft Office Standart 2010, антивирусное программное обеспечение Kaspersky Endpoint Security.
- специализированное ПО - Система компьютерной алгебры SAGE версии 9.0 и выше. (с открытым кодом) http://www.sagemath.org/

Программное обеспечение для электронного обучения в области криптографии

- CRYPTOOL (в свободном доступе) https://www.cryptool.org/en/

12. Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине

Для проведения занятий лекционного типа, практических и семинарских занятий используются специальные помещения (учебные аудитории), оборудованные техническими средствами обучения – мультимедийной проекционной техникой. Для проведения занятий лекционного типа используются наборы демонстрационного оборудования.

Для проведения лабораторных работ, (практических занятий – при необходимости) используются специальные помещения (учебные аудитории), оснащенные специализированным лабораторным оборудованием: персональными компьютерами с возможностью выхода в интернет и с установленным программным обеспечением, заявленным в п.11.

Для проведения групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации используются специальные помещения (учебные аудитории), оборудованные специализированной мебелью (для обучающихся), меловой / маркерной доской.

Для организации самостоятельной работы обучающимся предоставляются помещения, оснащенные компьютерной техникой с возможностью подключения к сети «Интернет» и обеспечением доступа в электронную информационно-образовательную среду университета.

Для обучения инвалидов и лиц с ограниченными возможностями здоровья университетом могут быть представлены специализированные средства обучения, в том числе технические средства коллективного и индивидуального пользования.

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
федеральное государственное автономное образовательное учреждение высшего образования «Балтийский федеральный университет имени Иммануила Канта»
Институт физико-математических наук и информационных технологий

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

«Основы технической физик»

Шифр: 10.05.01
Специальность: «Компьютерная безопасность»
Специализация: «Математические методы защиты информации»
Квалификация (степень) выпускника: специалист по защите информации

Калининград
2022

Лист согласования

Составитель: Горбачев Андрей Александрович к.т.н., доцент

Рабочая программа утверждена на заседании учебно-методического совета института физико-математических наук и информационных технологий

Протокол № 01/22 от «01» февраля 2022 г.

Председатель учебно-методического
совета института физико-
математических наук и информационных
технологий

Первый заместитель директора Шпилевой А. А
ИФМНиИТ, к. ф.-м. н., доцент

Ведущий менеджер Е.П.Ставицкая

Содержание

1.Наименование дисциплины: «Основы технической физики».

Цель дисциплины: формирование необходимых знаний для глубокого понимания физических процессов, лежащих в основе образования технических каналов утечки информации, а также для грамотной организации защиты информации при помощи технических средств.

2. Перечень планируемых результатов обучения по дисциплине, соотнесенных с планируемыми результатами освоения образовательной программы

Код компетенции	Результаты освоения образовательной программы (ИДК)	Результаты обучения по дисциплине
ПКС-3 Способность организовывать и проводить работы по технической защите информации.	ПКС-3.1. Разрабатывает модели угроз безопасности информации в организации; разрабатывает техническое задание на создание системы защиты информации в организации. ПКС-3.2. Организует установку и настройку технических, программных (программно-технических) средств защиты информации, входящих в состав системы защиты информации организации, в соответствии с техническим проектом и инструкциями по эксплуатации. ПКС-3.3. Организовывает ввод системы защиты информации в эксплуатацию.	***Знать***: фундаментальные физические законы и явления, лежащие в основе образования технических каналов утечки информации. ***Уметь***: формировать требования по технической защите информации; применять наиболее эффективные методы и средства технической защиты информации; контролировать эффективность мер защиты информации. ***Владеть***: методами технической защиты информации; навыками расчета и инструментального контроля показателей технической защиты информации; методиками проверки защищенности объектов информатизации на соответствие требованиям нормативных документов.

3. Место дисциплины в структуре образовательной программы

Дисциплина "Основы технической физики" представляет собой дисциплину части, формируемой участниками образовательных отношений блока 1 дисциплины (модули) подготовки студентов.

4. Виды учебной работы по дисциплине.

Виды учебной работы по дисциплине зафиксированы учебным планом основной профессиональной образовательной программы по указанному направлению и профилю, выражаются в академических часах. Часы контактной работы и самостоятельной работы обучающегося и часы, отводимые на процедуры контроля, могут различаться в учебных планах ОПОП по формам обучения. Объем контактной работы включает часы контактной аудиторной работы (лекции/практические занятия/лабораторные работы), контактной внеаудиторной работы (контроль самостоятельной работы), часы контактной работы в

период аттестации. Контактная работа, в том числе может проводиться посредством электронной информационно-образовательной среды университета с использованием ресурсов сети Интернет и дистанционных технологий

5. Содержание дисциплины, структурированное по темам (разделам)

Исходя из рамок, установленных учебным планом по трудоемкости и видам учебной работы по дисциплине, преподаватель самостоятельно выбирает тематику занятий по формам и количеству часов проведения контактной работы: лекции и иные учебные занятия, предусматривающие преимущественную передачу учебной информации преподавателем и (или) занятия семинарского типа (семинары, практические занятия, практикумы, лабораторные работы, коллоквиумы и иные аналогичные занятия), и (или) групповые консультации, и (или) индивидуальную работу обучающихся с преподавателем, в том числе индивидуальные консультации (по курсовым работам/проектам – при наличии курсовой работы/проекта по данной дисциплине в учебном плане). Рекомендуемая тематика занятий максимально полно реализуется в контактной работе с обучающимися очной формы обучения. В случае реализации образовательной программы в заочной / очно-заочной форме трудоемкость дисциплины сохраняется, однако объем учебного материала в значительной части осваивается обучающимися в форме самостоятельной работы. При этом требования к ожидаемым образовательным результатам обучающихся по данной дисциплине не зависят от формы реализации образовательной программы.

№	Наименование раздела	Содержание раздела
1	Введение.	Взаимосвязь источника информации с компонентами окружающей среды.
2	Основы теории электрических цепей и сигналов.	Основные понятия и определения. Основные законы электрических цепей. Уравнения пассивных элементов. Основные методы расчета электрических цепей.
3	Гармонические сигналы в линейных электрических цепях.	Гармонический сигнал и его характеристики. Представление гармонических функций комплексными величинами. Основные законы электрических цепей в комплексной форме. Уравнения пассивных элементов в комплексной форме. Энергетические характеристики гармонических сигналов.
4	Избирательные свойства электрических цепей.	Последовательный колебательный контур и его характеристики. Резонанс напряжений. Параллельный колебательный контур и его характеристики. Резонанс токов. Связанные контуры и их характеристики. Сложный резонанс.
5	Основы теории линейных четырехполюсников.	Понятие и классификация четырехполюсников. Системы уравнений четырехполюсника. Основные параметры четырехполюсника. Эквивалентные схемы замещения четырехполюсников.
6	Аналоговые электрические фильтры.	Понятие электрического фильтра. Фильтры нижних частот, их типовые схемы и характеристики. Фильтры верхних частот, их типовые схемы и характеристики. Полосовые фильтры, их типовые схемы и характеристики. Заграждающие фильтры, их типовые схемы и характеристики.
7	Длинные линии и волноводы.	Понятие длинной линии и погонных параметров. Модель длинной линии. Первичные параметры

		длиной линии. Телеграфные уравнения. Волны напряжений и токов в длинной линии. Вторичные параметры длинной линии. Режимы работы длинной линии. КПД длинной линии. Волноводы и их свойства.
8	Сигналы и их свойства.	Типы сигналов. Периодические сигналы. Спектры периодических сигналов. Спектр видеоимпульса. Преобразование непрерывных сообщений в дискретные сигналы.
9	Модуляция сигналов.	Основные понятия и определения. Амплитудная модуляция. Частотная модуляция. Фазовая модуляция. Одновременная модуляция по амплитуде и частоте. Импульсная модуляция (амплитудно-импульсная, фазоимпульсная, широтно-импульсная).

6. Рекомендуемая тематика учебных занятий в форме контактной работы

Рекомендуемая тематика учебных занятий *лекционного* типа (предусматривающих преимущественную передачу учебной информации преподавателями):

№	Наименование раздела	Темы лекций
1	Введение.	Лекция 1. Физические эффекты в технических каналах утечки информации.
2	Основы теории электрических цепей и сигналов.	Лекция 1. Основные законы электрических цепей. Лекция 2. Методы расчета электрических цепей.
3	Гармонические сигналы в линейных электрических цепях.	Лекция 3. Представление гармонических функций комплексными величинами. Основные законы электрических цепей в комплексной форме.
4	Избирательные свойства электрических цепей.	Лекция 4. Последовательный колебательный контур и его характеристики. Лекция 5. Параллельный колебательный контур и его характеристики. Лекция 6. Связанные контуры и их характеристики.
5	Основы теории линейных четырехполюсников.	Лекция 7. Системы уравнений четырехполюсников. Основные параметры четырехполюсников. Лекция 8. Схемы замещения четырехполюсника. Характеристические параметры четырехполюсника.
6	Аналоговые электрические фильтры.	Лекция 9. Понятие электрического фильтра. Фильтры нижних и верхних частот и их характеристики. Лекция 10. Полосовые и заграждающие фильтры, их типовые схемы и характеристики.
7	Длинные линии и волноводы.	Лекция 11. Модель длинной линии. Телеграфные уравнения. Волны напряжений и токов. Лекция 12. Вторичные параметры длинной линии. Режимы работы длинной линии. КПД длинной линии.
8	Сигналы и их свойства.	Лекция 13. Понятие сигнала. Периодические сигналы. Спектры периодических сигналов. Лекция 14. Преобразование непрерывных сообщений в

		дискретные сигналы.
9	Модуляция сигналов.	Лекция 14. Понятие модуляции. Амплитудная модуляция. Частотная модуляция. Фазовая модуляция. Лекция 15. Одновременная модуляция по амплитуде и частоте. Импульсная модуляция (амплитудно-импульсная, фазоимпульсная, широтно-импульсная).
10		

Рекомендуемый перечень *лабораторных* работ:

№	Наименование раздела	Темы лабораторной работы
1	Введение.	Лабораторная работа № 1. Знакомство со средой схемотехнического моделирования Multisim
2	Основы теории электрических цепей и сигналов.	Лабораторная работа № 1. Исследование делителей напряжения и токов. Лабораторная работа № 2. Изучение законов Кирхгофа, исследование линейной цепи постоянного напряжения методами токов ветвей и напряжений ветвей. Лабораторная работа № 3. Исследование разветвленной цепи постоянного напряжения методом узловых напряжений.
3	Гармонические сигналы в линейных электрических цепях.	Лабораторная работа № 4. Определение реактивных сопротивлений и сдвига фаз в цепях с гармоническими сигналами. Лабораторная работа № 5. Определение параметров разветвленных цепей с гармоническими сигналами.
4	Избирательные свойства электрических цепей.	Лабораторная работа № 6. Исследование резонансов в колебательных контурах. Лабораторная работа № 7. Исследование связанных колебательных цепей.
5	Основы теории линейных четырехполюсников.	Лабораторная работа № 8. Исследование свойств пассивных четырехполюсников.
6	Аналоговые электрические фильтры.	Лабораторная работа № 9. Исследование частотных характеристик цепей, содержащих реактивные элементы (электрические фильтры).
7	Длинные линии и волноводы.	Лабораторная работа № 10. Исследование цепей с распределенными параметрами.
8	Сигналы и их свойства.	Лабораторная работа № 11. Исследование сигналов и их спектров. Лабораторная работа № 12. Исследование временно*й* дискретизации аналоговых сигналов.
9	Модуляция сигналов.	Лабораторная работа № 13. Исследование методов модуляции сигналов.

Требования к самостоятельной работе обучающихся

1. Работа с лекционным материалом, предусматривающая проработку конспекта лекций и учебной литературы, по всем темам из п. 6 настоящей рабочей программы.

2. Обработка экспериментальных данных, полученных в ходе выполнения лабораторных работ по всем темам из п. 6 настоящей рабочей программы. Проработка теоретического материала к защите лабораторных работ.

Руководствуясь положениями статьи 47 и статьи 48 Федерального закона от 29 декабря 2012 г. N 273-ФЗ «Об образовании в Российской Федерации» научно-педагогические работники и иные лица, привлекаемые университетом к реализации данной образовательной программы, пользуются предоставленными академическими правами и свободами в части свободы преподавания, свободы от вмешательства в профессиональную деятельность; свободы выбора и использования педагогически обоснованных форм, средств, методов обучения и воспитания; права на творческую инициативу, разработку и применение авторских программ и методов обучения и воспитания в пределах реализуемой образовательной программы и отдельной дисциплины.

Исходя из рамок, установленных учебным планом по трудоемкости и видам учебной работы по дисциплине, преподаватель самостоятельно выбирает тематику занятий по формам и количеству часов проведения контактной работы: лекции и иные учебные занятия, предусматривающие преимущественную передачу учебной информации преподавателем и (или) занятия семинарского типа (семинары, практические занятия, практикумы, лабораторные работы, коллоквиумы и иные аналогичные занятия), и (или) групповые консультации, и (или) индивидуальную работу обучающихся с преподавателем, в том числе индивидуальные консультации (по курсовым работам/проектам – при наличии курсовой работы/проекта по данной дисциплине в учебном плане).

Рекомендуемая тематика занятий максимально полно реализуется в контактной работе с обучающимися очной формы обучения. В случае реализации образовательной программы в заочной / очно-заочной форме трудоемкость дисциплины сохраняется, однако объем учебного материала в значительной части осваивается обучающимися в форме самостоятельной работы. При этом требования к ожидаемым образовательным результатам обучающихся по данной дисциплине не зависят от формы реализации образовательной программы.

7. Методические рекомендации по видам занятий

Лекционные занятия.

В ходе лекционных занятий обучающимся рекомендуется выполнять следующие действия. Вести конспектирование учебного материала. Обращать внимание на категории, формулировки, раскрывающие содержание тех или иных явлений и процессов, научные выводы и практические рекомендации по их применению. Задавать преподавателю уточняющие вопросы с целью уяснения теоретических положений, разрешения спорных ситуаций.

Желательно оставить в рабочих конспектах поля, на которых во внеаудиторное время можно сделать пометки из рекомендованной литературы, дополняющие материал прослушанной лекции, а также подчеркивающие особую важность тех или иных теоретических положений.

Лабораторные занятия.

На лабораторных занятиях в зависимости от темы занятия выполняется поиск информации по конкретной теме; подготовка теоретического материала к защите лабораторных работ на основе контрольных вопросов; обсуждение в круглых столах наиболее важных вопросов; разбор конкретных ошибок с группой студентов.

Самостоятельная работа.

Самостоятельная работа осуществляется в виде изучения литературы, эмпирических данных по публикациям и конкретных ситуаций из практики, подготовке индивидуальных работ, работа с лекционным материалом, самостоятельное изучение отдельных тем

дисциплины; поиск и обзор литературы и электронных источников; чтение и изучение учебника и учебных пособий.

8. Фонд оценочных средств

8.1. Перечень компетенций с указанием этапов их формирования в процессе освоения образовательной программы в рамках учебной дисциплины

Основными этапами формирования указанных компетенций при изучении обучающимися дисциплины являются последовательное изучение содержательно связанных между собой тем учебных занятий. Изучение каждой темы предполагает овладение обучающимися необходимыми компетенциями. Результат аттестации обучающихся на различных этапах формирования компетенций показывает уровень освоения компетенций.

	Контролируемые разделы (темы) дисциплины	**Индекс контроли-руемой компетенции (или её части)**	**Оценочные средства по этапам формирования компетенций**
			текущий контроль по дисциплине
1	Введение.	ПКС-3	Опрос
2	Основы теории электрических цепей и сигналов.	ПКС-3	Выполнение и защита лабораторных работ
3	Гармонические сигналы в линейных электрических цепях.	ПКС-3	Выполнение и защита лабораторных работ
4	Избирательные свойства электрических цепей.	ПКС-3	Выполнение и защита лабораторных работ
5	Основы теории линейных четырехполюсников.	ПКС-3	Выполнение и защита лабораторных работ
6	Аналоговые электрические фильтры.	ПКС-3	Выполнение и защита лабораторных работ
7	Длинные линии и волноводы.	ПКС-3	Выполнение и защита лабораторных работ
8	Сигналы и их свойства.	ПКС-3	Выполнение и защита лабораторных работ
9	Модуляция сигналов.	ПКС-3	Выполнение и защита лабораторных работ

8.2. Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений и навыков и (или) опыта деятельности процессе текущего контроля

Основные вопросы для защиты лабораторных работ и собеседования.

Тема 2. Основы теории электрических цепей и сигналов.

Изучение законов Кирхгофа. Исследование линейной цепи постоянного напряжения методом токов ветвей.

1. Сформулировать и записать законы Кирхгофа.
2. Сформулировать и записать закон Джоуля-Ленца для постоянного тока.
3. Как определяется количество независимых уравнений по первому и второму законам Кирхгофа?

4. Записать уравнения по законам Кирхгофа для произвольной цепи, заданной преподавателем.

5. Что понимается по балансом мощностей электрической цепи? Записать в общем виде уравнение баланса мощностей для произвольного контура.

6. Что такое потенциальная диаграмма контура?

7. Совпадает ли напряжение на зажимах источника, измеренное вольтметром, с ЭДС этого источника? Ответ пояснить.

Тема 3. Гармонические сигналы в линейных электрических цепях.

Определение реактивных сопротивлений и сдвига фаз в цепях с гармоническим напряжением.

1. Как определяются реактивные индуктивное и емкостное сопротивления?

2. Чему равен сдвиг фаз между током и напряжением на резисторе, конденсаторе и катушке индуктивности?

3. Как определяется сдвиг фаз между током и напряжением в *RL*-, *RC*- и *RLC*-ветвях?

4. Как экспериментально определяется сдвиг фаз между током и напряжением?

5. Как представляются электрические величины при помощи комплексных чисел? Формы представления.

6. Как соотносятся показания измерительных приборов с комплексными числами для соответствующих электрических величин?

7. Какие величины регистрирует ваттметр?

8. Что называется треугольником сопротивлений?

9. Виды пассивных двухполюсников?

10. Как строятся векторные диаграммы напряжений и токов?

Тема 4. Избирательные свойства электрических цепей.

Исследование резонансов в колебательных контурах.

1. Изобразить на рисунке последовательный колебательный контур.

2. Записать выражение для комплексного сопротивления последовательного колебательного контура, пояснить смысл входящих величин.

3. Каково определение резонанса в последовательном колебательном контуре?

4. Изобразить на рисунке параллельный колебательный контур.

5. Записать выражение для комплексной проводимости параллельного колебательного контура, пояснить смысл входящих величин.

6. Каково определение резонанса в параллельном колебательном контуре?

7. Как определяется резонансная частота в последовательном и параллельном колебательных контурах?

8. Что называется добротностью контура? Что она характеризует?

9. Что такое характеристическое (волновое) сопротивление колебательного контура, как оно определяется?

10. Как производится расчет АЧХ и ФЧХ в последовательном и параллельном колебательном контурах? Изобразить качественно их формы.

11. Что называется полосой пропускания колебательного контура?

Тема 5. Основы теории линейных четырехполюсников.

Исследование свойств пассивных четырехполюсников.

1. Дать определение четырехполюсника.

2. Привести уравнения, связывающие входные и выходные токи и напряжения четырехполюсника (4 пары уравнений).

3. Привести выражения для определения параметров холостого хода четырехполюсника (4 параметра).

4. Привести выражения для определения параметров короткого замыкания четырехполюсника (4 параметра).

5. Как определяются характеристические сопротивления четырехполюсника?

6. Какой четырехполюсник называется согласованно нагруженным?

7. Как определяется комплексное входное сопротивление согласованно нагруженного четырехполюсника?

8. Как определяется характеристическая постоянная передачи согласованно нагруженного четырехполюсника?

9. Что называется собственным затуханием и коэффициентом фазы согласованно нагруженного четырехполюсника? Как они определяется? Единицы измерения.

10. Что называется схемой замещения четырехполюсника? Виды схем замещения.

Тема 6. Аналоговые электрические фильтры.

Исследование фильтров низких и высоких частот.

1. Дать определение фильтрам низких, высоких частот и полосовому и заграждающему фильтрам.

2. Что такое область пропускания и область затухания идеального фильтра?

3. Что такое согласованный режим работы фильтра?

4. Привести П-образную и Т-образную схемы фильтра нижних частот.

5. Привести П-образную и Т-образную схемы фильтра высоких частот.

6. Привести графики амплитудно-частотной и фазочастотной характеристик фильтра нижних частот.

7. Привести графики амплитудно-частотной и фазочастотной характеристик фильтра высоких частот.

8. Методы повышения крутизны амплитудно-частотных характеристик фильтров.

Тема 7. Длинные линии и волноводы.

Исследование цепей с распределенными параметрами.

1. Какие цепи называются цепями с сосредоточенными параметрами, а какие – с распределенными параметрами. Критерий оценки.

2. Что понимается под погонными сопротивлением, проводимостью, емкостью индуктивностью?

4. Записать телеграфные уравнения.

5. Что называется волновым (характеристическим) сопротивлением длинной линии?

6. В чем физический смысл падающих и отраженных волн напряжения и тока?

7. Что называется комплексным коэффициентом отражения по напряжению и току? Их взаимосвязь.

8. Что называется комплексным погонным коэффициентом распространения? Что такое коэффициенты затухания и фазы? Их зависимости от частоты (графическая иллюстрация).

9. Как определяются скорость и длина волны напряжения (тока)?

10. Что понимается под режимом согласованной нагрузки работы длинной линии?

11. Особенности режима холостого хода работы длинной линии.

12. Особенности режима короткого замыкания работы длинной линии.

13. Режим смешанных волн. Как определяются коэффициенты бегущей и стоячей волны?

14. От чего зависит входное сопротивление длинной линии? Как оно определяется?

15. Коэффициент полезного действия длинной линии.

Тема 8. Сигналы и их свойства.

Исследование временной дискретизации аналоговых сигналов.

1. Приведите классификацию и основные характеристики сигналов.
2. Какие сигналы называются дискретными?
3. Как происходит преобразование аналоговых сигналов в дискретные?
4. Что называют отсчетами аналоговых сигналов?
5. Как выбирается величина частоты (периода) дискретизации?
6. Почему частоту дискретизации нельзя выбрать произвольно?

Тема 9. Модуляция сигналов.

Исследование амплитудно-модулированных и частотно-модулированных сигналов.

1. Каков спектральный состав амплитудно-модулированного сигнала?
2. Как расположены спектральные компоненты амплитудно-модулированного сигнала относительно несущей частоты.
3. Покажите, что процесс модуляции связан с переносом спектра сигнала из области низких в область высоких частот?
4. Поясните связь при амплитудной модуляции огибающей сигнала с мгновенным значением низкочастотного модулирующего колебания?
5. Что такое индекс модуляции?
6. Как зависит спектральный состав однотонального частотно-модулированного сигнала от индекса модуляции?
7. Как расположены спектральные компоненты однотонального частотно-модулированного сигнала относительно несущей частоты?
8. Как связаны ширина спектра частотно-модулированного сигнала и индекс модуляции?
9. Поясните различие амплитудной и частотной модуляций?
10. Каков принцип радиосвязи с использованием частотной модуляции?

8.3. Перечень вопросов и заданий для промежуточной аттестации по дисциплине

Вопросы для промежуточного контроля (экзамена)

1. Основные понятия и определения: электрическая цепь, ток, напряжение, энергия тока, мощность.
2. Основные элементы электрических цепей: идеальный резистор, идеальный конденсатор, идеальная катушка индуктивности, идеальный источник напряжения, идеальный источник тока.
3. Уравнения линейных идеальных элементов: резистора, конденсатора, катушки (для каждого их элементов записать связь между током и напряжением, а также выражение для энергии или мощности).
4. Реальные источники напряжения и тока, их представления, взаимозаменяемость.
5. Законы Кирхгофа (1-ый и 2-ой). На примере какой-либо произвольной цепи, имеющей 3-4 контура.
6. Сущность метода контурных токов.
7. Сущность метода узловых напряжений.
8. Гармонические токи и напряжения, их уравнения, смысл параметров (частота, амплитуда, период, фаза, начальная фаза, эффективные (действующие) значения).
9. Комплексное представление гармонических сигналов, векторная диаграмма, понятие комплексной амплитуды.
10. Гармонический ток в элементах электрической цепи, изображение величин (токов, напряжений) на комплексной плоскости: для резистора, для конденсатора, для катушки.
11. Частотные свойства резистора, конденсатора и катушки.
12. Понятия мгновенной, активной, полной и реактивной мощности. Какая из них может быть отрицательной и почему? Единицы измерения.

13. Условие передачи максимума средней мощности от генератора к нагрузке. Коэффициент полезного действия.

14. Последовательный колебательный контур. Входное сопротивление. Напряжения на элементах контура (зависимости от соотношений реактивных сопротивлений), векторные диаграммы.

15. Последовательный колебательный контур. Условие резонанса напряжений. Характеристическое сопротивление.

16. Последовательный колебательный контур. Энергетические соотношения, добротность контура.

17. Последовательный колебательный контур. Зависимость тока от частоты (АЧХ, нормированная АЧХ), полоса пропускания контура.

18. Параллельный колебательный контур. Входная проводимость. Токи в элементах контура (зависимости от соотношений реактивных сопротивлений), векторные диаграммы.

19. Параллельный колебательный контур. Условие резонанса токов. Характеристическое сопротивление.

20. Параллельный колебательный контур. Понятия добротности. АЧХ, нормированная АЧХ, полоса пропускания.

21. Понятие четырехполюсника, уравнения четырехполюсника с Z-, Y-, H-, G-параметрами.

22. Понятие о согласованном включении четырехполюсника, характеристические сопротивления, коэффициент трансформации.

23. Характеристическая постоянная передачи, коэффициент затухания, коэффициент фазы.

24. Эквивалентные схемы замещения четырехполюсников.

25. Понятие электрического фильтра, виды фильтров, их типовые АЧХ, полоса пропускания фильтра.

26. Простейшие схемы ФНЧ, принципы их работы, АЧХ.

27. Простейшие схемы ФВЧ, принципы их работы, АЧХ.

28. Простейшие схемы полосовых фильтров, принципы их работы, АЧХ.

29. Простейшие схемы заграждающих фильтров, принципы их работы, АЧХ.

30. Понятие о цепях с сосредоточенными и распределенными параметрами, погонные характеристики: сопротивление, емкость, индуктивность, проводимость.

31. Модель длинной лини.

32. Телеграфные уравнения, их смысл.

33. Решение телеграфных уравнений для напряжения и тока. Физический смысл волн напряжения и тока и их свойства.

34. Волновое сопротивление. Комплексный погонный коэффициент распространения. Коэффициент затухания, коэффициент фазы. Коэффициент отражения. Понятие фазовой скорости волны.

35. Режим согласованной нагрузки, при каких условиях он реализуется. Зависимости напряжения и тока в длинной линии в режиме согласованной нагрузки от расстояния от нагрузки (или генератора).

36. Режим стоячих волн, при каких условиях он реализуется. Зависимости напряжения и тока в длинной линии в режиме стоячих волн от расстояния от нагрузки (или генератора).

37. Режим смешанных волн, при каких условиях он реализуется. Коэффициенты бегущей волны и стоячей волны. Зависимости напряжения и тока в длинной линии в режиме смешанных волн от расстояния от нагрузки (или генератора).

38. Коэффициент полезного действия длиной линии.

39. Понятие радиотехнического сигнала, классификация, основные характеристики.

40. Представление периодического сигнала с помощью ряда Фурье.

41. Спектры периодических сигналов и необходимая ширина полосы частот.

42. Спектр одиночного прямоугольного импульса.

43. Терема Котельникова.

44. Понятие о модуляции сигналов, способы разделения сигналов, несущая компонента сигнала, модулированная компонента сигнала.

45. Сущность амплитудной модуляции, коэффициент амплитудной модуляции, амплитудный спектр.

46. Сущность фазовой модуляции, индекс фазовой модуляции, мгновенная частота.

47. Сущность частотной модуляции, девиация частоты.

48. Одновременная модуляция по амплитуде и частоте.

49. Сущность амплитудно-импульсной модуляции.

50. Сущность фазоимпульсной модуляции.

51. Сущность Широтно-импульсной модуляции.

8.4. Планируемые уровни сформированности компетенций обучающихся и критерии оценивания

Уровни	Содержательное описание уровня	Основные признаки выделения уровня (этапы формирования компетенции, критерии оценки сформированности)	Пятибалльная шкала (академическая) оценка	Двухбалльная шакала, зачет	БРС, % освоения (рейтинговая оценка)
Повышенный	Творческая деятельность	*Включает нижестоящий уровень.* Умение самостоятельно принимать решение, решать проблему/задачу теоретического и прикладного характера на основе изученных методов, приемов, технологий	отлично	зачтено	86-100
Базовый	Применение знаний и умений в более широких контекстах учебной и профессиональной деятельности, нежели по образцу с большей степени самостоятельности и инициативы	*Включает нижестоящий уровень.* Способность собирать, систематизировать, анализировать и грамотно использовать информацию из самостоятельно найденных теоретических источников и иллюстрировать ими теоретические положения или обосновывать практику применения	хорошо		71-85
Удовлетворительный (достаточны	Репродуктивная деятельность	Изложение в пределах задач курса теоретически и	удовлетворительно		55-70

й)		практически контролируемого материала			
Недостаточный	Отсутствие признаков удовлетворительного уровня		неудовлетворительно	не зачтено	Менее 55

9. Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины.

Основная литература

1. Основы электроники, радиотехники и связи: учеб. пособие для вузов / А. Д. Гуменюк [и др.], 2008. - 479, с. (14 экз)
2. Прянишников В. А. Электротехника и ТОЭ в примерах и задачах: практ. пособие/ В. А. Прянишников, Е. А. Петров, Ю. М. Осипов ; под ред. В. А. Прянишникова. – СПб.: КОРОНА-Век, 2008. - 334 с.: ил. (25 экз)

Дополнительная литература

1. Морозова Н. Ю. Электротехника и электроника: учеб. для вузов/ Н. Ю. Морозова. - М.: Академия, 2007. - 255, с. (59 экз)
2. Сорокин В. С. Материалы и элементы электронной техники: учеб. для вузов : в 2 т./ В. С. Сорокин, Б. Л. Антипов, Н. П. Лазарева. - М.: Академия, 2006.
   Т.1: Проводники, полупроводники, диэлектрики. - 439, с. (19 экз)
   Т.2: Активные диэлектрики, магнитные материалы, элементы электронной техники. - 376 с. (19 экз)

10. Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины (модуля).

- НЭБ Национальная электронная библиотека, диссертации и прочие издания
- eLIBRARY.RU Научная электронная библиотека, книги, статьи, тезисы докладов конференций
- Гребенников Электронная библиотека ИД журналы
- ЭБС Лань книги, журналы
- ЭБС Консультант студента
- ПРОСПЕКТ ЭБС
- ЭБС ZNANIUM.COM
- РГБ Информационное обслуживание по МБА
- БЕН РАН
- Электронно-библиотечная система (ЭБС) Кантитана (https://elib.kantiana.ru/)

11. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине.

Программное обеспечение обучения включает в себя:

- система электронного образовательного контента БФУ им. И. Канта – www.lms-3.kantiana.ru, обеспечивающую разработку и комплексное использование электронных образовательных ресурсов;
- серверное программное обеспечение, необходимое для функционирования сервера и связи с системой электронного обучения через Интернет;
- корпоративная платформа Microsoft Teams;
- установленное на рабочих местах обучающихся ПО: Microsoft Windows 7, Microsoft Office Standart 2010, антивирусное программное обеспечение Kaspersky Endpoint Security.
- система схемотехнического проектирования Multisim

12. Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине.

Для проведения занятий лекционного типа, практических и семинарских занятий используются специальные помещения (учебные аудитории), оборудованные техническими средствами обучения – мультимедийной проекционной техникой. Для проведения занятий лекционного типа используются наборы демонстрационного оборудования.

Для проведения лабораторных работ, (практических занятий – при необходимости) используются специальные помещения (учебные аудитории), оснащенные специализированным лабораторным оборудованием: персональными компьютерами с возможностью выхода в интернет и с установленным программным обеспечением, заявленным в п.11.

Для проведения групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации используются специальные помещения (учебные аудитории), оборудованные специализированной мебелью (для обучающихся), меловой / маркерной доской.

Для организации самостоятельной работы обучающимся предоставляются помещения, оснащенные компьютерной техникой с возможностью подключения к сети «Интернет» и обеспечением доступа в электронную информационно-образовательную среду университета.

Для обучения инвалидов и лиц с ограниченными возможностями здоровья университетом могут быть представлены специализированные средства обучения, в том числе технические средства коллективного и индивидуального пользования.

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ
федеральное государственное автономное образовательное учреждение высшего образования «Балтийский федеральный университет имени Иммануила Канта»
Институт физико-математических наук и информационных технологий

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

«Математические методы диагностики компьютерных систем»

Шифр: 10.05.01
Специальность: «Компьютерная безопасность»
Специализация: «Математические методы защиты информации»
Квалификация (степень) выпускника: Специалист по защите информации

Калининград
2022

Лист согласования

Составитель: Ветров Игорь Анатольевич, к.т.н., доцент

Рабочая программа утверждена на заседании учебно-методического совета института физико-математических наук и информационных технологий
Протокол № 01/22 от «01» февраля 2022 г.

Председатель учебно-методического совета института физико-математических наук и информационных технологий
Первый заместитель директора ИФМНиИТ, к. ф.-м. н., доцент — Шпилевой А. А

Ведущий менеджер — Е.П.Ставицкая

Содержание

1.Наименование дисциплины: «Математические методы диагностики компьютерных систем»

Целью изучения дисциплины **«*Математические методы диагностики компьютерных систем*»** являются:

- приобретение студентами теоретических знаний и практических навыков в области использования математических способов и методов диагностики компьютерных систем (КС), освоение основ методов анализа, расчёта и оценки показателей качества и способов повышения эффективности использования КС; теоретических знаний и практических навыков в области методов и средств технической диагностики;
- выработка методик изучения и использования специальных и других дисциплин для разработки математических моделей безопасности компьютерных систем, выработка практических навыков работы со специальной литературой и литературой общего назначения.

2. Перечень планируемых результатов обучения по дисциплине, соотнесенных с планируемыми результатами освоения образовательной программы

Код компетенции	Результаты освоения образовательной программы (ИДК)	Результаты обучения по дисциплине
ПКС-7: Способность проводить анализ и участвовать в разработке математических моделей безопасности компьютерных систем	ПКС-7.1. Знает математические методы моделирования безопасных компьютерных систем ПКС-7.2. Осуществляет анализ математических моделей безопасности компьютерных систем ПКС-7.3. Участвует в разработке математических моделей безопасности компьютерных систем	**знать:** математические методы моделирования безопасных компьютерных систем **уметь:** разрабатывать математических моделей диагностики компьютерных систем **владеть:** методами анализа математических моделей безопасности компьютерных систем.

3. Место дисциплины в структуре образовательной программы

Дисциплина *«Математические методы диагностики компьютерных систем»* **Б1.В.07** относится к части ООП, формируемой участниками образовательных отношений Блока 1 Дисциплины (модули) для направления подготовки 10.05.01 «Компьютерная безопасность»

4. Виды учебной работы по дисциплине

Виды учебной работы по дисциплине зафиксированы учебным планом основной профессиональной образовательной программы по указанному направлению и профилю, выражаются в академических часах. Часы контактной работы и самостоятельной работы обучающегося и часы, отводимые на процедуры контроля, могут различаться в учебных планах ОПОП по формам обучения. Объем контактной работы включает часы контактной аудиторной работы (лекции/практические занятия/ лабораторные работы), контактной внеаудиторной работы (контроль самостоятельной работы), часы контактной работы в период аттестации. Контактная работа, в том числе может проводиться посредством электронной информационно-образовательной среды университета с использованием ресурсов сети Интернет и дистанционных технологий

5. Содержание дисциплины, в том числе практической подготовки в рамках дисциплины, структурированное по темам

Исходя из рамок, установленных учебным планом по трудоемкости и видам учебной работы по дисциплине, преподаватель самостоятельно выбирает тематику занятий по формам и количеству часов проведения контактной работы: лекции и иные учебные занятия, предусматривающие преимущественную передачу учебной информации преподавателем и (или) занятия семинарского типа (семинары, практические занятия, практикумы, лабораторные работы, коллоквиумы и иные аналогичные занятия), и (или) групповые консультации, и (или) индивидуальную работу обучающихся с преподавателем, в том числе индивидуальные консультации (по курсовым работам/проектам – при наличии курсовой работы/проекта по данной дисциплине в учебном плане). Рекомендуемая тематика занятий максимально полно реализуется в контактной работе с обучающимися очной формы обучения. В случае реализации образовательной программы в заочной / очно-заочной форме трудоемкость дисциплины сохраняется, однако объем учебного материала в значительной части осваивается обучающимися в форме самостоятельной работы. При этом требования к ожидаемым образовательным результатам обучающихся по данной дисциплине не зависят от формы реализации образовательной программы.

№ п/п	Наименование темы	Содержание темы
1	**Тема 1.** Основные понятия и термины теории надёжности компьютерных систем (КС). Количественные показатели и модели надёжности КС. Методы расчёта надежности. Статистическая оценка показателей надёжности. Пути обеспечения надёжности КС. Резервирование.	Понятия качества и надёжности. Состояния и события. Виды отказов. Классификация объектов. Количественные показатели надёжности. Показатели и модели безотказности невосстанавливаемых объектов: интенсивность отказов, вероятность безотказной работы, средняя наработка до отказа, гамма - процентная наработка до отказа. Экспоненциальное распределение, распределение Вейбулла – Гнеденко, нормальное распределение, гамма – распределение. Основной закон надежности, взаимосвязь показателей надежности. Количественные показатели и модели безотказности восстанавливаемых объектов: параметр потока отказов, вероятность безотказной работы, наработка на отказ. Основные законы распределения времени безотказной работы. Показатели и модели ремонтопригодности объектов КС: среднее время восстановления работоспособного состояния, вероятность восстановления, параметр потока восстановления, стоимость ремонта. Экспоненциальное распределение и распределение Эрланга 2-го порядка. Факторы, влияющие на ремонтопригодность КС.
2	**Тема 2.** Основные понятия и термины технической диагностики: объект диагностирования, дефект, неисправность, проверка, глубина поиска и кратность неисправности, тест, система и алгоритм технического диагностирования. Математические модели объектов диагностирования КС непрерывного типа. Алгоритмы технического диагностирования компьютерных систем.	Построение тестов диагностирования: проверяющий тест, тест поиска неисправностей, минимальный проверяющий тест (МПТ) и минимальный тест поиска неисправностей (МТПН) объектов компьютерных систем (КС). Построение оптимизированных условных алгоритмов поиска неисправностей. Понятия оптимального и оптимизированного условного алгоритмов поиска неисправностей. Критерии выбора проверок при построении оптимизированных УАПН: информационный критерий, функции предпочтения, решающие правила выбора оптимальных проверок. Методика построения оптимизированного условного алгоритма поиска неисправностей. Расчет среднего времени отыскания неисправностей по данному условному алгоритму поиска неисправностей. Основные способы построения алгоритмов поиска неисправностей: способ последовательного функционального анализа, способ половинного разбиения, способ «время – вероятность», инженерный способ, способ

№ п/п	Наименование темы	Содержание темы
		на основе иерархического принципа. Определение причин отказа объектов КС.
3	**Тема 3.** Инженерная методика поиска неисправностей объектов КС. Средства контроля и технической диагностики компьютерных систем.	Способы проверок при «ручной» методике поиска неисправностей: способ измерения, способ контрольных переключений и регулировок, способ замены, способ внешнего осмотра, способ сравнения, способ характерных неисправностей. Алгоритм инженерной методики поиска неисправностей. Общая характеристика средств контроля компьютерных систем. Встроенные системы контроля. Диагностические стенды. Автоматизированные диагностические стенды. Применение микропроцессоров и микро-ЭВМ для технического диагностирования объектов КС.
4	**Тема 4.** Сервисное техническое обслуживание компьютерных систем. Ремонт объектов КС. Роль эргономических факторов в решении задач эксплуатации КС. Методы испытаний объектов КС.	Виды сервисного ремонта и их характеристика: плановый и неплановый ремонт. Количественные характеристики системы ремонта: нормативы ремонта, временные показатели, показатели трудозатрат, стоимостные показатели, вероятностные показатели. Категорирование и дефектация компьютерного оборудования. Ремонтный цикл. Организация ремонта КС специалистами и сервисными центрами. Особенности ремонта КС в современных условиях. Основные направления современной инженерной психологии. Роль оператора в системе «человек - машина». Показатели надежности оператора. Вопросы повышения эффективности работы оператора в системе «человек – машина». Инженерно – психологические требования к объектам компьютерных систем. Виды и цели испытаний КС. Типовые программы и методики испытаний объектов КС.

6. Рекомендуемая тематика учебных занятий в форме контактной работы

Учебно-методическое обеспечение для самостоятельной работы обучающихся составляют:

1. Материалы лекций.
2. Материалы практических занятий.
3. Информационные ресурсы «Интернет» (сайты ФСТЭК России, ФСБ России, Консультант плюс и др.)
4. Методические рекомендации и указания.
5. Фонды оценочных средств.
6. Учебники и учебно-методические пособия.

Рекомендуемая тематика учебных занятий *лекционного* типа (предусматривающих преимущественную передачу учебной информации преподавателями):

№ п/п	Наименование темы	Содержание темы
1	**Тема 1.** Основные понятия и термины теории надёжности компьютерных систем (КС). Количественные показатели и	Понятия качества и надёжности. Состояния и события. Виды отказов. Классификация объектов. Количественные показатели надёжности. Показатели и модели безотказности невосстанавливаемых объектов: интенсивность отказов, вероятность безотказной работы, средняя наработка до отказа, гамма - процентная

№ п/п	Наименование темы	Содержание темы
	модели надёжности КС. Методы расчёта надежности. Статистическая оценка показателей надёжности. Пути обеспечения надёжности КС. Резервирование.	наработка до отказа. Экспоненциальное распределение, распределение Вейбулла – Гнеденко, нормальное распределение, гамма – распределение. Основной закон надежности, взаимосвязь показателей надежности. Количественные показатели и модели безотказности восстанавливаемых объектов: параметр потока отказов, вероятность безотказной работы, наработка на отказ. Основные законы распределения времени безотказной работы. Показатели и модели ремонтопригодности объектов КС: среднее время восстановления работоспособного состояния, вероятность восстановления, параметр потока восстановления, стоимость ремонта. Экспоненциальное распределение и распределение Эрланга 2-го порядка. Факторы, влияющие на ремонтопригодность КС.
2	**Тема 2.** Основные понятия и термины технической диагностики: объект диагностирования, дефект, неисправность, проверка, глубина поиска и кратность неисправности, тест, система и алгоритм технического диагностирования. Математические модели объектов диагностирования КС непрерывного типа. Алгоритмы технического диагностирования компьютерных систем.	Построение тестов диагностирования: проверяющий тест, тест поиска неисправностей, минимальный проверяющий тест (МПТ) и минимальный тест поиска неисправностей (МТПН) объектов компьютерных систем (КС). Построение оптимизированных условных алгоритмов поиска неисправностей. Понятия оптимального и оптимизированного условного алгоритмов поиска неисправностей. Критерии выбора проверок при построении оптимизированных УАПН: информационный критерий, функции предпочтения, решающие правила выбора оптимальных проверок. Методика построения оптимизированного условного алгоритма поиска неисправностей. Расчет среднего времени отыскания неисправностей по данному условному алгоритму поиска неисправностей. Основные способы построения алгоритмов поиска неисправностей: способ последовательного функционального анализа, способ половинного разбиения, способ «время – вероятность», инженерный способ, способ на основе иерархического принципа. Определение причин отказа объектов КС.
3	**Тема 3.** Инженерная методика поиска неисправностей объектов КС. Средства контроля и технической диагностики компьютерных систем.	Способы проверок при «ручной» методике поиска неисправностей: способ измерения, способ контрольных переключений и регулировок, способ замены, способ внешнего осмотра, способ сравнения, способ характерных неисправностей. Алгоритм инженерной методики поиска неисправностей. Общая характеристика средств контроля компьютерных систем. Встроенные системы контроля. Диагностические стенды. Автоматизированные диагностические стенды. Применение микропроцессоров и микро-ЭВМ для технического диагностирования объектов КС.
4	**Тема 4.** Сервисное техническое обслуживание компьютерных систем. Ремонт объектов КС. Роль эргономических факторов в решении задач эксплуатации КС. Методы испытаний объектов КС.	Виды сервисного ремонта и их характеристика: плановый и неплановый ремонт. Количественные характеристики системы ремонта: нормативы ремонта, временные показатели, показатели трудозатрат, стоимостные показатели, вероятностные показатели. Категорирование и дефектация компьютерного оборудования. Ремонтный цикл. Организация ремонта КС специалистами и сервисными центрами. Особенности ремонта КС в современных условиях. Основные направления современной инженерной психологии. Роль оператора в системе «человек - машина». Показатели надежности оператора. Вопросы повышения эффективности работы оператора в системе «человек – машина». Инженерно – психоло-

№ п/п	Наименование темы	Содержание темы
		гические требования к объектам компьютерных систем. Виды и цели испытаний КС. Типовые программы и методики испытаний объектов КС.

Рекомендуемая тематика практических занятий:

№ п/п	Наименование темы	Содержание темы
1	**Тема 1.** Основные понятия и термины теории надёжности компьютерных систем (КС). Количественные показатели и модели надёжности КС. Методы расчёта надежности. Статистическая оценка показателей надёжности. Пути обеспечения надёжности КС. Резервирование.	Расчет показателей надежности КС. Расчёт показателей безотказности при последовательном, параллельном и смешанном соединении элементов на структурной схеме надёжности. Приближённые методы расчёта безотказности объектов КС. Определение точечных и интервальных оценок показателей надёжности КС. Определение неизвестных законов распределений в задачах оценки надёжности КС.
2	**Тема 2.** Основные понятия и термины технической диагностики: объект диагностирования, дефект, неисправность, проверка, глубина поиска и кратность неисправности, тест, система и алгоритм технического диагностирования. Математические модели объектов диагностирования КС непрерывного типа. Алгоритмы технического диагностирования компьютерных систем.	Построение таблиц функций неисправностей по заданной логической модели объекта компьютерной системы. Построение оптимизированных условных алгоритмов поиска неисправностей КС. Расчет среднего времени отыскания неисправностей по данному условному алгоритму поиска неисправностей.
3	**Тема 3.** Инженерная методика поиска неисправностей объектов КС. Средства контроля и технической диагностики компьютерных систем.	Расчёт надёжности резервированных КС при нагруженном и ненагруженном резервировании. Расчёт надёжности резервированных систем объектов КС при постоянном резервировании. Построение инженерного алгоритма поиска неисправности для выбранного объекта компьютерной системы.
4	**Тема 4.** Сервисное техническое обслуживание компьютерных систем. Ремонт объектов КС. Роль эргономических факторов в решении задач эксплуатации КС. Методы испытаний объектов КС.	Составление сетевого графика для проведения периодического технического обслуживания компьютерных систем. Выбор и обоснование современных сервисных диагностических программ для обслуживания компьютерных систем и их объектов.

Рекомендуемая тематика самостоятельных работ:

№ п/п	Наименование темы	Тематика самостоятельных работ
1	Основные понятия и термины теории надёжности компьютерных систем (КС). Количественные показатели и модели надёжности КС. Методы расчёта надежности. Статистическая оценка показателей надёжности. Пути обеспечения надёжности КС. Резервирование.	Ознакомление с литературой по курсу. Работа с ресурсами сети Интернет. Выбор темы курсовой работы. Повторение теоретического материала.
2	Основные понятия и термины технической диагностики: объект диагностирования, дефект, неисправность, проверка, глубина поиска и кратность неисправности, тест, система и алгоритм технического диагностирования. Математические модели объектов диагностирования КС непрерывного типа. Алгоритмы технического диагностирования компьютерных систем.	Повторение теоретического материала к практическим занятиям. Ознакомление с литературой по курсу. Работа с ресурсами сети Интернет. Подготовка раздела «Предварительные сведения» курсовой работы
3	Инженерная методика поиска неисправностей объектов КС. Средства контроля и технической диагностики компьютерных систем.	Повторение теоретического материала к практическим занятиям. Ознакомление с литературой по курсу. Работа с ресурсами сети Интернет. Подготовка к выполнению групповых практических работ. Подготовка практической части курсовой работы.
4	Сервисное техническое обслуживание компьютерных систем. Ремонт объектов КС. Роль эргономических факторов в решении задач эксплуатации КС. Методы испытаний объектов КС.	Повторение теоретического материала к практическим занятиям. Ознакомление с литературой по курсу. Работа с ресурсами сети Интернет. Подготовка текста курсовой работы. Подготовка к выполнению групповой практической работы. Подготовка к итоговой аттестации по дисциплине (зачету). Защита курсовой работы.

Требования к самостоятельной работе обучающихся:

1. Работа с лекционным материалом, предусматривающая проработку конспекта лекций и

учебной литературы, по всем темам из п. 6 настоящей рабочей программы.

2. Выполнение домашнего задания, предусматривающего решение задач, выполнение упражнений, выдаваемых на практических занятиях, по всем темам из п. 6 настоящей рабочей программы.

Руководствуясь положениями статьи 47 и статьи 48 Федерального закона от 29 декабря 2012 г. N 273-ФЗ «Об образовании в Российской Федерации» научно-педагогические работники и иные лица, привлекаемые университетом к реализации данной образовательной программы, пользуются предоставленными академическими правами и свободами в части свободы преподавания, свободы от вмешательства в профессиональную деятельность; свободы выбора и использования педагогически обоснованных форм, средств, методов обучения и воспитания; права на творческую инициативу, разработку и применение авторских программ и методов обучения и воспитания в пределах реализуемой образовательной программы и отдельной дисциплины.

Исходя из рамок, установленных учебным планом по трудоемкости и видам учебной работы по дисциплине, преподаватель самостоятельно выбирает тематику занятий по формам и количеству часов проведения контактной работы: лекции и иные учебные занятия, предусматривающие преимущественную передачу учебной информации преподавателем и (или) занятия семинарского типа (семинары, практические занятия, практикумы, лабораторные работы, коллоквиумы и иные аналогичные занятия), и (или) групповые консультации, и (или) индивидуальную работу обучающихся с преподавателем, в том числе индивидуальные консультации (по курсовым работам/проектам – при наличии курсовой работы/проекта по данной дисциплине в учебном плане).

Рекомендуемая тематика занятий максимально полно реализуется в контактной работе с обучающимися очной формы обучения. В случае реализации образовательной программы в заочной / очно-заочной форме трудоемкость дисциплины сохраняется, однако объем учебного материала в значительной части осваивается обучающимися в форме самостоятельной работы. При этом требования к ожидаемым образовательным результатам обучающихся по данной дисциплине не зависят от формы реализации образовательной программы.

7. Методические рекомендации по видам занятий

Лекционные занятия.

В ходе лекционных занятий обучающимся рекомендуется выполнять следующие действия. Вести конспектирование учебного материала. Обращать внимание на категории, формулировки, раскрывающие содержание тех или иных явлений и процессов, научные выводы и практические рекомендации по их применению. Задавать преподавателю уточняющие вопросы с целью уяснения теоретических положений, разрешения спорных ситуаций.

Желательно оставить в рабочих конспектах поля, на которых во внеаудиторное время можно сделать пометки из рекомендованной литературы, дополняющие материал прослушанной лекции, а также подчеркивающие особую важность тех или иных теоретических положений.

Практические и семинарские занятия.

На практических и семинарских занятиях в зависимости от темы занятия выполняется поиск информации по решению проблем, практические упражнения, контрольные работы, выработка индивидуальных или групповых решений, итоговое обсуждение с обменом знаниями, участие в круглых столах, разбор конкретных ситуаций, командная работа, представление портфолио и т.п.

Самостоятельная работа.

Самостоятельная работа осуществляется в виде изучения литературы, эмпирических данных по публикациям и конкретных ситуаций из практики, подготовке индивидуальных работ, работа с лекционным материалом, самостоятельное изучение отдельных тем дисциплины; поиск и обзор литературы и электронных источников; чтение и изучение учебника и учебных пособий.

8. Фонд оценочных средств

8.1. Перечень компетенций с указанием этапов их формирования в процессе освоения образовательной программы в рамках учебной дисциплины

Основными этапами формирования указанных компетенций при изучении обучающимися дисциплины являются последовательное изучение содержательно связанных между собой тем учебных занятий. Изучение каждой темы предполагает овладение обучающимися необходимыми компетенциями. Результат аттестации обучающихся на различных этапах формирования компетенций показывает уровень освоения компетенций.

Контролируемые модули, разделы (темы) дисциплины	Индекс контролируемой компетенции (или её части)	Оценочные средства по этапам формирования компетенций
		текущий контроль по дисциплине
Тема 1. Основные понятия и термины теории надёжности компьютерных систем (КС). Количественные показатели и модели надёжности КС. Методы расчёта надежности. Статистическая оценка показателей надёжности. Пути обеспечения надёжности КС. Резервирование.	ПКС-7	Устный опрос, выполнение практических заданий
Тема 2. Основные понятия и термины технической диагностики: объект диагностирования, дефект, неисправность, проверка, глубина поиска и кратность неисправности, тест, система и алгоритм технического диагностирования. Математические модели объектов диагностирования КС непрерывного типа. Алгоритмы технического диагностирования компьютерных систем.	ПКС-7	Устный опрос, выполнение практических заданий
Тема 3. Инженерная методика поиска неисправностей объектов КС. Средства контроля и технической диагностики компьютерных систем.	ПКС-7	Устный опрос, выполнение практических заданий
Тема 4. Сервисное техническое обслуживание компьютерных систем. Ремонт объектов КС. Роль эргономических факторов в решении задач эксплуатации КС. Методы испытаний объектов КС.	ПКС-7	Устный опрос, выполнение практических заданий

8.2. Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений и навыков и (или) опыта деятельности процессе текущего контроля

Типовые контрольные вопросы:

1. Основные понятия надёжности. Состояния и события. Виды отказов.
2. Классификация объектов надёжности. Количественные показатели надёжности.
3. Количественные показатели безотказности невосстанавливаемых объектов КС. Их сущность, вид и взаимосвязь.
4. Модели безотказности невосстанавливаемых объектов КС.

5. Количественные показатели и модели безотказности восстанавливаемых объектов КС. Их сущность, вид и взаимосвязь
6. Количественные показатели и модели ремонтопригодности объектов КС.
7. Количественные показатели и модели долговечности объектов КС.
8. Комплексные показатели надёжности КС. Их сущность и основные отличия.
9. Формализация описания объектов КС при расчётах надёжности. Приближённый и полный расчёт надёжности.
10. Основные расчётные соотношения для показателей безотказности при последовательном соединении элементов на ССН.
11. Основные расчётные соотношения для показателей безотказности при параллельном соединении элементов на ССН.
12. Методика расчёта показателей безотказности при последовательно-параллельном соединении элементов на ССН.
13. Приближённые методы расчёта показателей безотказности КС. Расчёт безотказности по средней условной интенсивности отказов элементов.
14. Приближённые методы расчёта показателей безотказности КС. Расчёт безотказности по номинальным значениям интенсивностей отказов элементов.
15. Приближённые методы расчёта показателей безотказности КС. Расчёт безотказности с учётом электрических режимов и температуры элементов.
16. Основные понятия и термины технической диагностики.
17. Система технического диагностирования, её виды. Условные и безусловные алгоритмы технического диагностирования.
18. Математическая модель объектов технического диагностирования КС , её описание и виды.
19. Логическая модель объекта диагностирования, её назначение и правила построения.
20. Таблица функций неисправности, её назначение и способ заполнения. Методика построения ТФН по заданной логической модели ОД.
21. Алгоритмы технического диагностирования. Правила и методики построения проверяющих тестов и тестов поиска неисправностей.
22. Понятия оптимального и оптимизированного условного алгоритмов поиска неисправностей. Решающие критерии выбора проверок при построении оптимизированных УАПН.

Темы практических групповых заданий

1. Расчет показателей надежности КС. Расчёт показателей безотказности при последовательном, параллельном и смешанном соединении элементов на структурной схеме надёжности. Приближённые методы расчёта безотказности объектов КС. Определение точечных и интервальных оценок показателей надёжности КС. Определение неизвестных законов распределений в задачах оценки надёжности КС.
2. Построение таблиц функций неисправностей по заданной логической модели объекта компьютерной системы. Построение оптимизированных условных алгоритмов поиска неисправностей КС. Расчет среднего времени отыскания неисправностей по данному условному алгоритму поиска неисправностей.
3. Расчёт надёжности резервированных КС при нагруженном и ненагруженном резервировании. Расчёт надёжности резервированных систем объектов КС при постоянном резервировании. Построение инженерного алгоритма поиска неисправности для выбранного объекта компьютерной системы.
4. Составление сетевого графика для проведения периодического технического обслуживания компьютерных систем.
5. Выбор и обоснование современных сервисных диагностических программ для обслуживания компьютерных систем и их объектов.

8.3. Перечень вопросов и заданий для промежуточной аттестации по дисциплине

Промежуточный контроль по дисциплине служит для оценки работы студента в течение семестра и призван выявить уровень, прочность и систематичность полученных им теоретических и практических знаний, приобретения навыков самостоятельной работы, развития творческого мышления, умение синтезировать полученные знания и применять их в решении практических задач.

Вопросы предполагают контроль общих методических знаний и умений, способность студентов проиллюстрировать их примерами, индивидуальными материалами, составленными студентами в течение курса.

Промежуточный контроль проводится в форме устного собеседования, по результатам которого ставится «зачтено» или «не зачтено» на основе следующих критериев: полноты, структурированности и правильности ответа по сути поставленных вопросов.

Вопросы для промежуточного контроля (зачета)

1. Расчет показателей надежности КС. Расчёт показателей безотказности при последовательном, параллельном и смешанном соединении элементов на структурной схеме надёжности. Приближённые методы расчёта безотказности объектов КС. Определение точечных и интервальных оценок показателей надёжности КС. Определение неизвестных законов распределений в задачах оценки надёжности КС.
2. Построение таблиц функций неисправностей по заданной логической модели объекта компьютерной системы. Построение оптимизированных условных алгоритмов поиска неисправностей КС. Расчет среднего времени отыскания неисправностей по данному условному алгоритму поиска неисправностей.
3. Расчёт надёжности резервированных КС при нагруженном и ненагруженном резервировании. Расчёт надёжности резервированных систем объектов КС при постоянном резервировании. Построение инженерного алгоритма поиска неисправности для выбранного объекта компьютерной системы.
4. Составление сетевого графика для проведения периодического технического обслуживания компьютерных систем.
5. Выбор и обоснование современных сервисных диагностических программ для обслуживания компьютерных систем и их объектов.

8.4. Планируемые уровни сформированности компетенций обучающихся и критерии оценивания

Уровни	Содержательное описание уровня	Основные признаки выделения уровня (этапы формирования компетенции, критерии оценки сформированности)	Пятибалльная шкала (академическая) оценка	Двухбалльная шакала, зачет	БРС, % освоения (рейтинговая оценка)
Повышенный	Творческая деятельность	*Включает нижестоящий уровень.* Умение самостоятельно принимать решение, решать проблему/задачу теоретического и прикладного характера на основе изученных	отлично	зачтено	86-100

		методов, приемов, технологий			
Базовый	Применение знаний и умений в более широких контекстах учебной и профессиональной деятельности, нежели по образцу с большей степени самостоятельности и инициативы	*Включает нижестоящий уровень.* Способность собирать, систематизировать, анализировать и грамотно использовать информацию из самостоятельно найденных теоретических источников и иллюстрировать ими теоретические положения или обосновывать практику применения	хорошо		71-85
Удовлетворительный (достаточный)	Репродуктивная деятельность	Изложение в пределах задач курса теоретически и практически контролируемого материала	удовлетворительно		55-70
Недостаточный	Отсутствие признаков удовлетворительного уровня		неудовлетворительно	не зачтено	Менее 55

9. Перечень основной и дополнительной литературы, необходимой для освоения дисциплины

9.1. Основная литература

1. Пилиди, В. С. Математические основы защиты информации : учебное пособие / В. С. Пилиди ; Южный федеральный университет. - Ростов-на-Дону ; Таганрог : Издательство Южного федерального университета, 2019. - 308 с. - ISBN 978-5-9275-3363-3. - Текст : электронный. - URL: https://znanium.com/catalog/product/1088209 (дата обращения: 13.01.2022). – Режим доступа: по подписке.
2. Богульская, Н. А. Модели безопасности компьютерных систем : учебное пособие / Н. А. Богульская, М. М. Кучеров. - Красноярск : Сиб. федер. ун-т, 2019. - 206 с. - ISBN 978-5-7638-4008-7. - Текст : электронный. - URL: https://znanium.com/catalog/product/1819309 (дата обращения: 13.01.2022). – Режим доступа: по подписке.

9.2. Дополнительная литература

1. Безопасность и надежность технических систем: учебное пособие / Л. Н. Александровская, И. З. Аронов, В. И. Круглов [и др.] - Москва : Логос, 2020. - 376 с: ил. - Текст : электронный. - URL: https://znanium.com/catalog/product/1211589 (дата обращения: 13.01.2022). – Режим доступа: по подписке.

2. Осадчий, Ю. М. Основы теории надежности и диагностики : учебное пособие / Ю.М. Осадчий. — Москва : ИНФРА-М, 2021. — 197 с. — (Военное образование). - ISBN 978-5-16-015733-7. - Текст : электронный. - URL: https://znanium.com/catalog/product/1048706 (дата обращения: 13.01.2022). – Режим доступа: по подписке.
3. Ушаков, Д. М. Введение в математические основы САПР. Курс лекций [Электронный ресурс] / Д. М. Ушаков. - 2-е изд., перераб. и доп. - Москва : ДМК Пресс, 2011. - 208 с. : ил. - ISBN 978-5-94074-829-8. - Текст : электронный. - URL: https://znanium.com/catalog/product/409467 (дата обращения: 13.01.2022). – Режим доступа: по подписке.
4. Смирнов, А. П. Прикладные проблемы надежности и качества систем : курс лекций / А. П. Смирнов. - Москва : Изд. Дом НИТУ «МИСиС», 2018. - 80 с. - ISBN 978-5-87623-783-5. - Текст : электронный. - URL: https://znanium.com/catalog/product/1232202 (дата обращения: 13.01.2022). – Режим доступа: по подписке.

9.3. Нормативные документы

1. Федеральный закон от 29 июля 2004 г. № 98-ФЗ «О коммерческой тайне».
2. Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации».
3. Федеральный закон от 27 июля 2006 г. №152 «О персональных данных».
4. Доктрина информационной безопасности Российской Федерации (утверждена Указом Президента РФ от 5 декабря 2016 г. № 646).
5. Стратегия развития информационного общества в Российской Федерации на 2017 - 2030 годы (утверждена Указом Президента РФ от 9 мая 2017 г. № 203).
6. Перечень сведений конфиденциального характера (утвержден указом Президента Российской Федерации от 6 марта 1997 года №188).
7. Постановление Правительства от 1 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».

10. Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины

- НЭБ Национальная электронная библиотека, диссертации и прочие издания
- eLIBRARY.RU Научная электронная библиотека, книги, статьи, тезисы докладов конференций
- Гребенников Электронная библиотека ИД журналы
- ЭБС Лань книги, журналы
- ЭБС Консультант студента
- ПРОСПЕКТ ЭБС
- ЭБС ZNANIUM.COM
- РГБ Информационное обслуживание по МБА
- БЕН РАН
- Электронно-библиотечная система (ЭБС) Кантитана (https://elib.kantiana.ru/)

11. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине

Программное обеспечение обучения включает в себя:

- система электронного образовательного контента БФУ им. И. Канта – www.lms-3.kantiana.ru, обеспечивающую разработку и комплексное использование электронных образовательных ресурсов;
- серверное программное обеспечение, необходимое для функционирования сервера и связи с системой электронного обучения через Интернет;
- корпоративная платформа Microsoft Teams;
- установленное на рабочих местах студентов ПО: Microsoft Windows 7, Microsoft Office Standart 2010, антивирусное программное обеспечение Kaspersky Endpoint Security.

12. Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине

Для проведения занятий лекционного типа, практических и семинарских занятий используются специальные помещения (учебные аудитории), оборудованные техническими средствами обучения – мультимедийной проекционной техникой. Для проведения занятий лекционного типа используются наборы демонстрационного оборудования.

Для проведения лабораторных работ, (практических занятий – при необходимости) используются специальные помещения (учебные аудитории), оснащенные специализированным лабораторным оборудованием: персональными компьютерами с возможностью выхода в интернет и с установленным программным обеспечением, заявленным в п.11.

Для проведения групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации используются специальные помещения (учебные аудитории), оборудованные специализированной мебелью (для обучающихся), меловой / маркерной доской.

Для организации самостоятельной работы обучающимся предоставляются помещения, оснащенные компьютерной техникой с возможностью подключения к сети «Интернет» и обеспечением доступа в электронную информационно-образовательную среду университета.

Для обучения инвалидов и лиц с ограниченными возможностями здоровья университетом могут быть представлены специализированные средства обучения, в том числе технические средства коллективного и индивидуального пользования.

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
федеральное государственное автономное образовательное учреждение высшего образования «Балтийский федеральный университет имени Иммануила Канта»
Институт физико-математических наук и информационных технологий

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

«Основы криптовалют и блокчейна»

Шифр: 10.05.01
Специальность: «Компьютерная безопасность»
Специализация: «Математические методы защиты информации»
Квалификация (степень) выпускника: специалист по защите информации

Калининград
2022

Лист согласования

Составитель: Мельничук Евгений Михайлович, ассистент Института физико-математических наук и информационных технологий

Рабочая программа утверждена на заседании учебно-методического совета института физико-математических наук и информационных технологий
Протокол № 01/22 от «01» февраля 2022 г.

Председатель учебно-методического
совета института физико-
математических наук и
информационных технологий
Первый заместитель директора Шпилевой А. А
ИФМНиИТ, к. ф.-м. н., доцент

Ведущий менеджер Е.П.Ставицкая

Содержание

1.Наименование дисциплины: «Основы криптовалют и блокчейна».

Цель дисциплины: целью освоения дисциплины «*Основы криптовалют и блокчейна*» является изучение студентами технологии блокчейн и основных принципов построения и работы криптовалют Bitcoin, Ethereum, Monero и Zcash, а также овладение навыками написания простейших смарт-контрактов криптовалют Bitcoin и Ethereum, необходимых для построения, защиты и анализа приложений на базе технологии блокчейн.

2. Перечень планируемых результатов обучения по дисциплине, соотнесенных с планируемыми результатами освоения образовательной программы

Код компетенции	Результаты освоения образовательной программы (ИДК)	Результаты обучения по дисциплине
ПКС-6. Способность проводить анализ безопасности компьютерных систем на соответствие отечественным и зарубежным стандартам в области компьютерной безопасности	ПКС-6.1. Знает отечественные и зарубежные стандарты в области компьютерной безопасности ПКС-6.2. Осуществляет анализ безопасности компьютерных систем на соответствие отечественным и зарубежным стандартам в области компьютерной безопасности ПКС-6.3. Применяет национальные, межгосударственные и международные стандарты в области защиты информации	• ***знать*** принципы построения и работы основных криптовалют и блокчейн технологий, криптографические инструменты, применяемые в криптовалютах Bitcoin, Ethereum, Monero и Zcash, основные уязвимости смарт-контрактов, механизмы анонимизации и деанонимизации в криптовалютах Bitcoin, Ethereum, Monero и Zcash; • ***уметь*** грамотно писать скриптаы криптовалюты Bitcoin, разрабатывать простейшие смарт-контракты на языке Solidity в криптовалюте Ethereum, проверять смарт-контракты на наличие уязвимостей, анализировать уровень анонимности и безопасности в криптовалютах Bitcoin, Ethereum, Monero и Zcash; • ***владеть*** практическими навыками работы с библиотеками языка Python для криптовалюты Bitcoin, навыками программирования на языке

		Solidit, навыками работы с криптографическими инструментами, использующимися в криптовалютах Bitcoin, Ethereum, Monero и Zcash.

3. Место дисциплины в структуре образовательной программы

Дисциплина «Основы криптовалют и блокчейна» представляет собой дисциплину части, формируемой участниками образовательных отношений блока дисциплин подготовки обучающихся.

4. Виды учебной работы по дисциплине.

Виды учебной работы по дисциплине зафиксированы учебным планом основной профессиональной образовательной программы по указанному направлению и профилю, выражаются в академических часах. Часы контактной работы и самостоятельной работы обучающегося и часы, отводимые на процедуры контроля, могут различаться в учебных планах ОПОП по формам обучения. Объем контактной работы включает часы контактной аудиторной работы (лекции/практические занятия/ лабораторные работы), контактной внеаудиторной работы (контроль самостоятельной работы), часы контактной работы в период аттестации. Контактная работа, в том числе может проводиться посредством электронной информационно-образовательной среды университета с использованием ресурсов сети Интернет и дистанционных технологий

5. Содержание дисциплины, структурированное по темам (разделам)

Исходя из рамок, установленных учебным планом по трудоемкости и видам учебной работы по дисциплине, преподаватель самостоятельно выбирает тематику занятий по формам и количеству часов проведения контактной работы: лекции и иные учебные занятия, предусматривающие преимущественную передачу учебной информации преподавателем и (или) занятия семинарского типа (семинары, практические занятия, практикумы, лабораторные работы, коллоквиумы и иные аналогичные занятия), и (или) групповые консультации, и (или) индивидуальную работу обучающихся с преподавателем, в том числе индивидуальные консультации (по курсовым работам/проектам – при наличии курсовой работы/проекта по данной дисциплине в учебном плане). Рекомендуемая тематика занятий максимально полно реализуется в контактной работе с обучающимися очной формы обучения. В случае реализации образовательной программы в заочной / очно-заочной форме трудоемкость дисциплины сохраняется, однако объем учебного материала в значительной части осваивается обучающимися в форме самостоятельной работы. При этом требования к ожидаемым образовательным результатам обучающихся по данной дисциплине не зависят от формы реализации образовательной программы.

№ п/п	**Наименование темы**	**Содержание темы**
1	Введение в криптовалюты	Задачи и программа курса. История создания и развития технологии блокчейн и криптовалют. Современное положение криптовалют в финансовой системе и области применения технологии блокчейн. Криптографическая хеш-функция. Принципы построения. Стойкость к коллизиям. Хеш-функции семейства SHA2(SHA256), SHA3(Keccak). Приложения криптографических хеш-функций. Понятие электронно-цифровой подписи. DSA, ECDSA, проблема malleability ECDSA подписи и способы её решения. Подпись Шнорра и её преимущества перед ECDSA. Мультиподпись, слепая подпись.
2	Bitcoin. UTXO модель	UTXO модель. Адреса и типы адресов, транзакция. Простейшие скрипты сети Bitcoin. Язык Script. Нода. Полная нода. SVP нода. Фильтры Блума. Установка соединения между нодами и их общение. Блок. Организация транзакций в блоке. Merkle tree. Mempool. Proof-of-work. Сложность майнинга. Атака 51%. ASIC и майнинг пулы. Стратегии майнинга. Selfish mining. Преимущества замены подписи ECDSA на подпись Шнорра. BIP340, BIP341, BIP342
3	Ethereum. Аккаунтная модель блокчейна.	Account-based модель. Понятие аккаунта. Адрес в сети Ethereum. Транзакции сети Ethereum. Структура блока. GHOST. Понятие Uncle блок. EVM. Газ. .
4	Смарт-контракты. Основы языка Solidity.	Понятие смарт-контракта. Язык Solidity. Структура смарт-контракта и вызов его функций. Примеры простейших смарт-контрактов. REMIX. DeFi приложения.
5	Основные уязвимости смарт-контрактов	Основные уязвимости смарт-контрактов. Повторный вход. Эффекты исключений. Косвенное выполнение неизвестного кода. Атаки на смарт-контракты.
6	Ethereum 2.0	Этапы перехода с Ethereum на Ethereum 2.0. Proof-of-Stake. Шардинг. Стейкинг и валидаторы.
7	Monero	Кольцевые подписи, Pedersen commitment и доказательства принадлежности интервалу. Stealth-адреса, mix-in’ы. Анонимизация в Monero. RingCT.
8	Основы анонимизации и	Классические Bitcoin и Ethereum миксеры. Coinjoin

	деанонимизации в криптовалютах	транзакции. Анализ уровня анонимности. Ошибки при использовании Coinjoin транзакций. Кластеризация адресов в сети Bitcoin. Эвристики Bitcoin транзакций: Common spending, one-time change

6. Рекомендуемая тематика учебных занятий в форме контактной работы

Рекомендуемая тематика учебных занятий *лекционного* типа (предусматривающих преимущественную передачу учебной информации преподавателями):

№	Наименование раздела	Темы лекций
1	Введение в криптовалюты	Лекция 1. Понятие хеш-функции и электронно-цифровой подписи. SHA-256, Keccack, подпись Шнорра и ECDSA
2	Bitcoin. UTXO модель	Лекция 4. UTXO модель. Адреса и типы адресов, транзакция. Простейшие скрипты сети Bitcoin. Язык Script. Лекция 5. Нода. Полная нода. SVP нода. Фильтры Блума. Установка соединения между нодами и их общение. Лекция 6. Блок. Организация транзакций в блоке. Merkle tree. Mempool. Proof-of-work. Сложность майнинга. Атака 51%. ASIC и майнинг пулы. Стратегии майнинга. Selfish mining. Лекция 7. Преимущества замены подписи ECDSA на подпись Шнорра. BIP340, BIP341, BIP342
3	Ethereum. Аккаунтная модель блокчейна.	Лекция 8. Account-based модель. Понятие аккаунта. Адрес в сети Ethereum. Транзакции сети Ethereum. Лекция 9. Структура блока. GHOST. Понятие Uncle блок. EVM. Газ. .
4	Смарт-контракты. Основы языка Solidity.	Лекция 10. Понятие смарт-контракта. Язык Solidity. Структура смарт-контракта и вызов его функций. Лекция 11. Примеры простейших смарт-контрактов. REMIX. DeFi приложения
5	Основные уязвимости смарт-контрактов	Лекция 12. Основные уязвимости смарт-контрактов. Повторный вход. Эффекты исключений. Косвенное выполнение неизвестного кода. Атаки на смарт-контракты.
6	Ethereum 2.0	Лекция 13. Этапы перехода с Ethereum на Ethereum 2.0. Proof-of-Stake. Шардинг. Стейкинг и валидаторы.
7	Monero	Лекция 14. Кольцевые подписи, Pedersen commitment и доказательства принадлежности интервалу. Stealth-адреса, mix-in’ы. Анонимизация в

		Monero. RingCT.
8	Основы анонимизации и деанонимизации в криптовалютах	Лекции 15. Классические Bitcoin и Ethereum миксеры. Coinjoin транзакции. Анализ уровня анонимности. Лекция 16. Ошибки при использовании Coinjoin транзакций. Кластеризация адресов в сети Bitcoin. Эвристики Bitcoin транзакций: Common spending, one-time change

Рекомендуемая тематика *практических* занятий:

1. Криптографические хеш-функции. Подпись ECDSA и подпись Шнорра.
2. Bitcoin скрипты. Написание парсера биткоин транзакций и скриптов.
3. Формирование блока транзакций.
4. Формирование транзакции и блока транзакций в сети Ethereum.
5. Написание простейших смарт контрактов на языке Solidity. Банковский смарт-контракт.
6. Анализ смарт-контрактов на наличие уязвимостей.
7. Proof-of -stake. Sharding
8. Кольцевая подпись. Генерация стелс-адресов.
9. Coinjoin транзакции, расчёт их уровня анонимности.
10. Кластеризация адресов в сети Bitcoin.

На практических занятиях решаются задачи по теме занятия.

Требования к самостоятельной работе обучающихся

1. Работа с лекционным материалом, предусматривающая проработку конспекта лекций и учебной литературы, по всем темам из п. 6 настоящей рабочей программы.

2. Выполнение домашнего задания, предусматривающего решение задач, выполнение упражнений, выдаваемых на практических занятиях, по всем темам из п. 6 настоящей рабочей программы.

Руководствуясь положениями статьи 47 и статьи 48 Федерального закона от 29 декабря 2012 г. N 273-ФЗ «Об образовании в Российской Федерации» научно-педагогические работники и иные лица, привлекаемые университетом к реализации данной образовательной программы, пользуются предоставленными академическими правами и свободами в части свободы преподавания, свободы от вмешательства в профессиональную деятельность; свободы выбора и использования педагогически обоснованных форм, средств, методов обучения и воспитания; права на творческую инициативу, разработку и применение авторских программ и методов обучения и воспитания в пределах реализуемой образовательной программы и отдельной дисциплины.

Исходя из рамок, установленных учебным планом по трудоемкости и видам учебной работы по дисциплине, преподаватель самостоятельно выбирает тематику занятий по формам и количеству часов проведения контактной работы: лекции и иные учебные занятия, предусматривающие преимущественную передачу учебной

информации преподавателем и (или) занятия семинарского типа (семинары, практические занятия, практикумы, лабораторные работы, коллоквиумы и иные аналогичные занятия), и (или) групповые консультации, и (или) индивидуальную работу обучающихся с преподавателем, в том числе индивидуальные консультации (по курсовым работам/проектам – при наличии курсовой работы/проекта по данной дисциплине в учебном плане).

Рекомендуемая тематика занятий максимально полно реализуется в контактной работе с обучающимися очной формы обучения. В случае реализации образовательной программы в заочной / очно-заочной форме трудоемкость дисциплины сохраняется, однако объем учебного материала в значительной части осваивается обучающимися в форме самостоятельной работы. При этом требования к ожидаемым образовательным результатам обучающихся по данной дисциплине не зависят от формы реализации образовательной программы.

7. Методические рекомендации по видам занятий

Лекционные занятия.

В ходе лекционных занятий обучающимся рекомендуется выполнять следующие действия. Вести конспектирование учебного материала. Обращать внимание на категории, формулировки, раскрывающие содержание тех или иных явлений и процессов, научные выводы и практические рекомендации по их применению. Задавать преподавателю уточняющие вопросы с целью уяснения теоретических положений, разрешения спорных ситуаций.

Желательно оставить в рабочих конспектах поля, на которых во внеаудиторное время можно сделать пометки из рекомендованной литературы, дополняющие материал прослушанной лекции, а также подчеркивающие особую важность тех или иных теоретических положений.

Практические и семинарские занятия.

На практических и семинарских занятиях в зависимости от темы занятия выполняется поиск информации по решению проблем, практические упражнения, контрольные работы, выработка индивидуальных или групповых решений, итоговое обсуждение с обменом знаниями, участие в круглых столах, разбор конкретных ситуаций, командная работа, представление портфолио и т.п.

Самостоятельная работа.

Самостоятельная работа осуществляется в виде изучения литературы, эмпирических данных по публикациям и конкретных ситуаций из практики, подготовке индивидуальных работ, работа с лекционным материалом, самостоятельное изучение отдельных тем дисциплины; поиск и обзор литературы и электронных источников; чтение и изучение учебника и учебных пособий.

8. Фонд оценочных средств

8.1. Перечень компетенций с указанием этапов их формирования в процессе освоения образовательной программы в рамках учебной дисциплины

Основными этапами формирования указанных компетенций при изучении обучающимися дисциплины являются последовательное изучение содержательно связанных между собой тем учебных занятий. Изучение каждой темы предполагает овладение обучающимися необходимыми компетенциями. Результат аттестации

обучающихся на различных этапах формирования компетенций показывает уровень освоения компетенций.

Контролируемые разделы (темы) дисциплины	Индекс контроли-руемой компетенции (или её части)	Оценочные средства по этапам формирования компетенций
		текущий контроль по дисциплине
1. Введение в криптовалюты	ПКС-6	Опрос, решение задач.
2. Bitcoin. UTXO модель	ПКС-6	Опрос, решение задач
3. Ethereum. Аккаунтная модель блокчейна.	ПКС-6	Опрос, решение задач
4. Смарт-контракты. Основы языка Solidity.	ПКС-6	Опрос, решение задач
5. Основные уязвимости смарт-контрактов	ПКС-6	Опрос, решение задач
6. Ethereum 2.0	ПКС-6	Опрос, решение задач
7. Monero	ПКС-6	Опрос, решение задач,
8. Основы анонимизации и деанонимизации в криптовалютах	ПКС-6	Опрос, решение задач, письемнный опрос

8.2. Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений и навыков и (или) опыта деятельности процессе текущего контроля

Примеры вопросов для письменного опроса:

I. Какой размер блока в сети Bitcoin?

A. 1 Мб B. 4 Мб

C. 8 Мб D. 16 Мб

II. Какой из следующих адресов является P2SH адресом?
   A. 13TASu2eYYRn9PfrMZyfwBJFryoV2oqj7m
   B. 371sxtiw12XZTBmKPFJu3WTLKP1ASA4AV2
   C. bc1qggvzm3js0v29j0y485m5n6zquhsx97faeaxx9y

III. Какой алгоритм консенсуса используется в Bitcoin?
   A. Delegated Proof-of-Stake
   B. Proof-of-Stake
   C. Proof-of-Work

IV. Что делает протокол Segregate Witness?
   A. Решает проблему гибкости транзакций(transaction malleability)
   B. Увеличивает максимальный размер блока до 8Мб
   C. Увеличивает максимальный размер блока до 32Мб
   D. Решают проблему масштабируемости через уменьшение размера подписи.

V. Что означает следующая строка из Bitcoin скрипта:

1495652013 OP_CHECKLOCKTIMEVERIFY?

A. Средства не могут быть потрачены до блока номер 1495652013
B. Средства могут быть потрачены после того, как будут замайнены следующие 1495652013 блоков в сети
C. Средства не могут быть потрачены до наступления даты, выраженной в виде Unix timestamp 1495652013

VI. Что такое EOA аккаунты в Ethereum?

A. Аккаунт, контролируемый кодом смарт-контракта
B. Аккаунт на криптовалютной бирже
C. Аккаунт, контролируемый приватным ключом

VII. Какая хеш-функция используется в Ethereum?

A. SHA256
B. Keccak
C. RIPEMD-160
D. MD5

VIII. Что произойдет при недостатке Gas для выполнения транзакции?

A. Транзакция не будет выполнена и средства не уйдут с адреса
B. Весь Gas будет возвращен отправителю
C. Весь Gas не будет возвращен отправителю и останется майнеру
D. Транзакция будет совершена, но дополнительное количество необходимого Gas будет вычтена из суммы транзакции

IX. Можно ли изменить уже развернутый в сети смарт-контракт?

A. Да
B. Нет
C. Да, но только при предварительном добавлении в код специальной функции для смарт-контрактов

X. Какому количеству Wei равен 1 Eth?

A. 10^8 Wei
B. 10^9 Wei
C. 10^{16} Wei
D. 10^{18} Wei

XI. Какие криптовалюты используют UTXO модель?

A. Bitcoin
B. Ethereum
C. Monero

XII. Какие функции может выполнять Bitcoin нода?

A. Маршрутизация
B. Функции кошелька
C. Микширование
D. Майнинг
E. Хранение копии блокчейна

XIII. Какие действия может осуществлять смарт-контракт?

A. Вызывать другие смарт-контракты

B. Отправлять транзакции
C. Позволяют выполнять код, ассоциированный с этим смарт-контрактом, используя EVM
D. Отправлять сообщения другим смарт-контрактам
E. Использовать свой собственный приватный ключ

XIV. В какой тип памяти записываются глобальные переменные(state variables) смарт-контракта?
A. Memory
B. Stack
C. Storage

8.3. Перечень вопросов и заданий для промежуточной аттестации по дисциплине

Вопросы для промежуточного контроля (зачёта)

1. UTXO модель и её основные недостатки и преимущества.
2. Типы адресов в сети Bitcoin
3. Структура транзакции Bitcoin
4. Структура блока Bitcoin
5. Proof-of-work
6. Майнинг. Selfish mining.
7. Протокол Segregate Witness
8. Язык Script. Скрипты ScriptPubkey, ScriptSig.
9. Подпись ECDSA и подпись Шнорра.
10. Протокол Taproot
11. Протокол Lightning Network.
12. Account-based модель
13. EVM. Ethereum как машина состояний
14. Понятие смарт-контракта. Развертывание смарт-контракта в сети Ethereum.
15. Уязвимости смарт-контрактов
16. Этапы перехода на Ethereum 2.0
17. Beacon Chain
18. Sharding
19. Proof-of-Stake
20. Monero.
21. Кольцевая подпись. Стелс адреса.
22. Протокол RingCT.
23. Механизмы анонимизации и деанонимизации в сетях Bitcoin и Ethereum
24. Классические централизованные миксеры в сети Bitcoin
25. Миксеры в сети Ethereum на базе смарт-контрактов
26. Coinjoin транзакции
27. Механизмы кластеризации адресов в сети Bitcoin.

8.4. Планируемые уровни сформированности компетенций обучающихся и критерии оценивания

Уровни	Содержательное описание уровня	Основные признаки выделения уровня (этапы формирования компетенции, критерии оценки сформированности)	Пятибалльная шкала (академическая) оценка	Двухбалльная шакала, зачет	БРС, % освоения (рейтинговая оценка)
Повышенный	Творческая деятельность	*Включает нижестоящий уровень.* Умение самостоятельно принимать решение, решать проблему/задачу теоретического и прикладного характера на основе изученных методов, приемов, технологий	отлично	зачтено	86-100
Базовый	Применение знаний и умений в более широких контекстах учебной и профессиональной деятельности, нежели по образцу с большей степени самостоятельности и инициативы	*Включает нижестоящий уровень.* Способность собирать, систематизировать, анализировать и грамотно использовать информацию из самостоятельно найденных теоретических источников и иллюстрировать ими теоретические положения или обосновывать практику применения	хорошо		71-85
Удовлетворительный (достаточный)	Репродуктивная деятельность	Изложение в пределах задач курса теоретически и практически контролируемого	удовлетворительно		55-70

		материала			
Недостаточный	Отсутствие признаков удовлетворительного уровня		неудовлетворительно	не зачтено	Менее 55

9. Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины.

Основная литература

1. Цихилов, А. М. Блокчейн: принципы и основы / А. М. Цихилов. - Москва : Интеллектуальная Литература, 2019. - 188 с. - ISBN 978-5-6042880-1-6. - Текст : электронный. - URL: https://znanium.com/catalog/product/1220219 (дата обращения: 21.02.2022). ЭБС Znanium(1)

Дополнительная литература

1. Тебернакулов, А. Блокчейн на практике / Александр Табернакулов, Ян Койфманн. - Москва : Альпина Паблишер, 2019. - 260 с. - ISBN 978-5-96142-408-9. - Текст : электронный. - URL: https://znanium.com/catalog/product/1078459 (дата обращения: 21.02.2022). ЭБС Znanium(1)

10. Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины (модуля).

- Сайт по Ethereum (https://ethereum.org/ru/)
- Сайт по Monero (https://www.getmonero.org/resources/research-lab/)
- ЭБС Кантиана (http://lib.kantiana.ru/irbis/standart/ELIB).
- Электронная библиотечная система «Znanium» (https://znanium.com/)

11. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине.

Программное обеспечение обучения включает в себя:

- система электронного образовательного контента БФУ им. И. Канта – www.lms-3.kantiana.ru, обеспечивающую разработку и комплексное использование электронных образовательных ресурсов;
- серверное программное обеспечение, необходимое для функционирования сервера и связи с системой электронного обучения через Интернет;
- корпоративная платформа Microsoft Teams;
- установленное на рабочих местах обучающихся ПО: Microsoft Windows 7, Microsoft Office Standart 2010, антивирусное программное обеспечение Kaspersky Endpoint Security.
- Remix - Solidity IDE, которая используется для написания, компиляции и отладки кода Solidity

12. Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине.

Для проведения занятий лекционного типа, практических и семинарских занятий используются специальные помещения (учебные аудитории), оборудованные техническими средствами обучения – мультимедийной проекционной техникой. Для проведения занятий лекционного типа используются наборы демонстрационного оборудования.

Для проведения лабораторных работ, (практических занятий – при необходимости) используются специальные помещения (учебные аудитории), оснащенные специализированным лабораторным оборудованием: персональными компьютерами с возможностью выхода в интернет и с установленным программным обеспечением, заявленным в п.11.

Для проведения групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации используются специальные помещения (учебные аудитории), оборудованные специализированной мебелью (для обучающихся), меловой / маркерной доской.

Для организации самостоятельной работы обучающимся предоставляются помещения, оснащенные компьютерной техникой с возможностью подключения к сети «Интернет» и обеспечением доступа в электронную информационно-образовательную среду университета.

Для обучения инвалидов и лиц с ограниченными возможностями здоровья университетом могут быть представлены специализированные средства обучения, в том числе технические средства коллективного и индивидуального пользования.

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
федеральное государственное автономное образовательное учреждение высшего образования
«Балтийский федеральный университет имени Иммануила Канта»
Институт физико-математических наук и информационных технологий

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

«Методы алгебраической теории чисел в криптографии»

Шифр: 10.05.01
Специальность: «Компьютерная безопасность»
Специализация: «Математические методы защиты информации»
Квалификация (степень) выпускника: специалист по защите информации

Калининград
2022

Лист согласования

Составитель: Малыгина Екатерина Сергеевна, к.ф.-м.н., доцент

Рабочая программа утверждена на заседании учебно-методического совета института физико-математических наук и информационных технологий

Протокол № 01/22 от «01» февраля 2022 г.

Председатель учебно-методического
совета института физико-
математических наук и информационных
технологий

Первый заместитель директора ИФМНиИТ, к. ф.-м. н., доцент — Шпилевой А. А

Ведущий менеджер — Е.П.Ставицкая

Содержание

1.Наименование дисциплины: «Методы алгебраической теории чисел в криптографии».

Цель дисциплины: целью освоения дисциплины «Методы алгебраической теории чисел в криптографии» является изложение основы теории алгебраических чисел, в частности, теории разложения идеалов; изучение теории вещественных и мнимых квадратичных полей; описание конструкции криптосистем с открытым ключом в квадратичных полях; применение методов алгебраической теории чисел в криптографических приложениях.

2. Перечень планируемых результатов обучения по дисциплине, соотнесенных с планируемыми результатами освоения образовательной программы

Код компетенции	Результаты освоения образовательной программы (ИДК)	Результаты обучения по дисциплине
ПКС-7. Способность проводить анализ и участвовать в разработке математических моделей безопасности компьютерных систем.	ПКС-7.1. Знает математические методы моделирования безопасных компьютерных систем. ПКС-7.2. Осуществляет анализ математических моделей безопасности компьютерных систем. ПКС-7.3. Участвует в разработке математических моделей безопасности компьютерных систем.	- **знать** базовые алгоритмы теории чисел и алгебраической теории чисел; конструкцию криптосистем с открытым ключом в мнимых квадратичных полях; - **уметь** разрабатывать и реализовывать алгоритмы редукции и умножения идеалов квадратичного поля, вычисления числа классов идеалов числового поля, основные криптографические алгоритмы на базе числовых полей; оценивать эффективность криптосистем в квадратичных полях; - **владеть** навыками эффективного вычисления в группе классов идеалов квадратичного поля.

3. Место дисциплины в структуре образовательной программы

Дисциплина «Методы алгебраической теории чисел в криптографии» представляет собой дисциплину части, формируемой участниками образовательных отношений, блока дисциплин подготовки обучающихся.

4. Виды учебной работы по дисциплине.

Виды учебной работы по дисциплине зафиксированы учебным планом основной профессиональной образовательной программы по указанному направлению и профилю, выражаются в академических часах. Часы контактной работы и самостоятельной работы обучающегося и часы, отводимые на процедуры контроля, могут различаться в учебных планах ОПОП по формам обучения. Объем контактной работы включает часы контактной аудиторной работы (лекции/практические занятия/ лабораторные работы), контактной внеаудиторной работы (контроль самостоятельной работы), часы контактной работы в

период аттестации. Контактная работа, в том числе может проводиться посредством электронной информационно-образовательной среды университета с использованием ресурсов сети Интернет и дистанционных технологий.

5. Содержание дисциплины, структурированное по темам (разделам)

Исходя из рамок, установленных учебным планом по трудоемкости и видам учебной работы по дисциплине, преподаватель самостоятельно выбирает тематику занятий по формам и количеству часов проведения контактной работы: лекции и иные учебные занятия, предусматривающие преимущественную передачу учебной информации преподавателем и (или) занятия семинарского типа (семинары, практические занятия, практикумы, лабораторные работы, коллоквиумы и иные аналогичные занятия), и (или) групповые консультации, и (или) индивидуальную работу обучающихся с преподавателем, в том числе индивидуальные консультации (по курсовым работам/проектам – при наличии курсовой работы/проекта по данной дисциплине в учебном плане). Рекомендуемая тематика занятий максимально полно реализуется в контактной работе с обучающимися очной формы обучения. В случае реализации образовательной программы в заочной / очно-заочной форме трудоемкость дисциплины сохраняется, однако объем учебного материала в значительной части осваивается обучающимися в форме самостоятельной работы. При этом требования к ожидаемым образовательным результатам обучающихся по данной дисциплине не зависят от формы реализации образовательной программы.

№	Наименование раздела	Содержание раздела
1	Алгебраические числа	Представление алгебраических чисел. Минимальный многочлен алгебраического числа. Признак алгебраичности. Гомоморфизмы числовых полей.
2	Следы, нормы, дискриминанты	След и норма в числовом поле. Дискриминант набора чисел в числовом поле. Целый базис и дискриминант числового поля.
3	Разложение простых чисел в произведение простых идеалов	Кольцо алгебраических целых. Целый базис. Дробные идеалы. Теорема Дедекинда. Норма идеала. Ветвление и степень. Разложение простых чисел в произведение простых идеалов в алгебраическом числовом поле. Разложение простых чисел в произведение простых идеалов в квадратичном поле.
4	Группа единиц числового поля	Разложение рациональных и иррациональных чисел в цепные дроби. Фундаментальная единица вещественного квадратичного поля. Группа единиц мнимого квадратичного поля.
5	Число классов числового поля	Оценка числа классов числового поля. Число классов квадратичного поля.
6	Редукция и умножение идеалов в квадратичных полях	Примитивные идеалы. Редуцированные идеалы. Редукция идеалов мнимого квадратичного поля. Умножение идеалов.
7	Криптография в квадратичных полях	Криптосистема Бухмана-Вильямса. Криптосистема Вильямса.

6. Рекомендуемая тематика учебных занятий в форме контактной работы

Рекомендуемая тематика учебных занятий *лекционного* типа (предусматривающих преимущественную передачу учебной информации преподавателями):

№	Наименование раздела	Темы лекций
1	Алгебраические числа	Лекция 1. Представление алгебраических чисел. Минимальный многочлен алгебраического числа. Лекция 2. Признак алгебраичности. Гомоморфизмы числовых полей.
2	Следы, нормы, дискриминанты	Лекция 3. След и норма в числовом поле. Дискриминант набора чисел в числовом поле. Лекция 4. Целый базис и дискриминант числового поля.
3	Разложение простых чисел в произведение простых идеалов	Лекция 5. Кольцо алгебраических целых. Целый базис. Лекция 6. Дробные идеалы. Теорема Дедекинда. Норма идеала. Лекция 7. Ветвление и степень. Лекция 8. Разложение простых чисел в произведение простых идеалов в алгебраическом числовом поле. Разложение простых чисел в произведение простых идеалов в квадратичном поле.
4	Группа единиц числового поля	Лекция 9. Разложение рациональных и иррациональных чисел в цепные дроби. Фундаментальная единица вещественного квадратичного поля. Группа единиц мнимого квадратичного поля.
5	Число классов числового поля	Лекция 10-11. Оценка числа классов числового поля. Число классов квадратичного поля.
6	Редукция и умножение идеалов в квадратичных полях	Лекция 12. Примитивные идеалы. Редуцированные идеалы. Лекция 13. Редукция идеалов мнимого квадратичного поля. Умножение идеалов.
7	Криптография в квадратичных полях	Лекция 14-15. Криптосистема Бухмана-Вильямса. Криптосистема Вильямса.

Рекомендуемая тематика *практических* занятий:

1. Проверка чисел на алгебраичность. Построение алгебраических чисел. Вычисление минимального многочлена алгебраического числа.
2. Вычисление следов и норм в числовом поле. Вычисление дискриминанта набора чисел числового поля.
3. Нахождение целого базиса и дискриминанта числового поля.
4. Разложение простых чисел в произведение простых идеалов в алгебраическом числовом поле.
5. Разложение простых чисел в произведение простых идеалов в квадратичном поле.

6. Разложение рациональных и иррациональных чисел в цепные дроби. Вычисление фундаментальных единиц вещественного квадратичного поля. Вычисление группы единиц мнимого квадратичного поля.
7. Вычисление границы Минковского. Подсчет числа классов квадратичного поля и нахождение представителей данных классов.
8. Построение идеалов квадратичного поля. Их исследование на примитивность.
9. Редукция идеалов мнимого квадратичного поля.
10. Умножение идеалов квадратичного поля.
11. Реализация криптосистемы Бухмана-Вильямса.
12. Реализация криптосистемы Вильямса.

На практических занятиях решаются задачи по теме занятия.

Требования к самостоятельной работе обучающихся

1. Работа с лекционным материалом, предусматривающая проработку конспекта лекций и учебной литературы, по всем темам из п. 6 настоящей рабочей программы.
2. Выполнение домашнего задания, предусматривающего решение задач, выполнение упражнений, выдаваемых на практических занятиях, по всем темам из п. 6 настоящей рабочей программы.

Руководствуясь положениями статьи 47 и статьи 48 Федерального закона от 29 декабря 2012 г. N 273-ФЗ «Об образовании в Российской Федерации» научно-педагогические работники и иные лица, привлекаемые университетом к реализации данной образовательной программы, пользуются предоставленными академическими правами и свободами в части свободы преподавания, свободы от вмешательства в профессиональную деятельность; свободы выбора и использования педагогически обоснованных форм, средств, методов обучения и воспитания; права на творческую инициативу, разработку и применение авторских программ и методов обучения и воспитания в пределах реализуемой образовательной программы и отдельной дисциплины.

Исходя из рамок, установленных учебным планом по трудоемкости и видам учебной работы по дисциплине, преподаватель самостоятельно выбирает тематику занятий по формам и количеству часов проведения контактной работы: лекции и иные учебные занятия, предусматривающие преимущественную передачу учебной информации преподавателем и (или) занятия семинарского типа (семинары, практические занятия, практикумы, лабораторные работы, коллоквиумы и иные аналогичные занятия), и (или) групповые консультации, и (или) индивидуальную работу обучающихся с преподавателем, в том числе индивидуальные консультации (по курсовым работам/проектам – при наличии курсовой работы/проекта по данной дисциплине в учебном плане).

Рекомендуемая тематика занятий максимально полно реализуется в контактной работе с обучающимися очной формы обучения. В случае реализации образовательной программы в заочной / очно-заочной форме трудоемкость дисциплины сохраняется, однако объем учебного материала в значительной части осваивается обучающимися в форме самостоятельной работы. При этом требования к ожидаемым образовательным результатам обучающихся по данной дисциплине не зависят от формы реализации образовательной программы.

7. Методические рекомендации по видам занятий

Лекционные занятия.

В ходе лекционных занятий обучающимся рекомендуется выполнять следующие действия. Вести конспектирование учебного материала. Обращать внимание на категории, формулировки, раскрывающие содержание тех или иных явлений и процессов, научные выводы и практические рекомендации по их применению. Задавать преподавателю уточняющие вопросы с целью уяснения теоретических положений, разрешения спорных ситуаций.

Желательно оставить в рабочих конспектах поля, на которых во внеаудиторное время можно сделать пометки из рекомендованной литературы, дополняющие материал прослушанной лекции, а также подчеркивающие особую важность тех или иных теоретических положений.

Практические и семинарские занятия.

На практических и семинарских занятиях в зависимости от темы занятия выполняется поиск информации по решению проблем, практические упражнения, контрольные работы, выработка индивидуальных или групповых решений, итоговое обсуждение с обменом знаниями, участие в круглых столах, разбор конкретных ситуаций, командная работа, представление портфолио и т.п.

Самостоятельная работа.

Самостоятельная работа осуществляется в виде изучения литературы, эмпирических данных по публикациям и конкретных ситуаций из практики, подготовке индивидуальных работ, работа с лекционным материалом, самостоятельное изучение отдельных тем дисциплины; поиск и обзор литературы и электронных источников; чтение и изучение учебника и учебных пособий.

8. Фонд оценочных средств

8.1. Перечень компетенций с указанием этапов их формирования в процессе освоения образовательной программы в рамках учебной дисциплины

Основными этапами формирования указанных компетенций при изучении обучающимися дисциплины являются последовательное изучение содержательно связанных между собой тем учебных занятий. Изучение каждой темы предполагает овладение обучающимися необходимыми компетенциями. Результат аттестации обучающихся на различных этапах формирования компетенций показывает уровень освоения компетенций.

Контролируемые разделы (темы) дисциплины	Индекс контроли-руемой компетенции (или её части)	Оценочные средства по этапам формирования компетенций
		текущий контроль по дисциплине
1. Алгебраические числа	ПКС-7	Опрос, решение задач.
2. Следы, нормы, дискриминанты		Опрос, решение задач.
3. Разложение простых чисел в произведение простых идеалов		Опрос, решение задач, программная реализация алгоритмов.
4. Группа единиц числового поля		Опрос, решение задач.
5. Число классов числового		Опрос, решение задач, контрольная

Контролируемые разделы (темы) дисциплины	Индекс контроли-руемой компетенции (или её части)	Оценочные средства по этапам формирования компетенций
		текущий контроль по дисциплине
поля		работа.
6. Редукция и умножение идеалов в квадратичных полях		Опрос, программная реализация алгоритмов.
7. Криптография в квадратичных полях		Опрос, программная реализация алгоритмов.

8.2. Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений и навыков и (или) опыта деятельности процессе текущего контроля

Примеры вопросов для устного опроса:

1. Дать определение алгебраических и трансцендентных чисел. Привести примеры.
2. Дать определение минимального многочлена. Привести примеры.
3. Сформулировать признак алгебраичности.
4. Сформулировать основные свойства минимального многочлена.
5. Дать определение следа и нормы числового поля. Привести примеры.
6. Сформулировать основные свойства следа и нормы числового поля.
7. Дать определение дискриминанта набора в числовом поле.
8. Дать определение целого базиса числового поля.
9. Дать определение дискриминанта числового поля.
10. Дать определение относительной степени и индекса ветвления. Привести примеры.
11. Дать определение фундаментальной единицы поля. Привести пример.
12. Дать определение группе единиц числового поля, квадратичного поля.
13. Дать определения группы классов числового поля и числа классов числового поля. Дать определения границы и константы Минковского.
14. Дать определение примитивного и редуцированного идеалов.

Типовые контрольные задания:

1. Найти минимальный многочлен числа $z = \sqrt{3} - 2\sqrt{2}$ над полем Θ.

2. Найти степень поля $K = \Theta(\alpha, \beta) = \Theta(\sqrt{2}, \sqrt{3})$. Вычислить $Tr_K(\alpha)$, $Tr_K(\beta)$, $N_K(\alpha)$, $N_K(\beta)$, целый базис и дискриминант поля.

3. Разложить идеалы $2O_K$, $3O_K$, $5O_K$, $7O_K$, в произведение простых идеалов в кольце O_K для $K = \Theta(\sqrt{-7})$.

4. Пусть $\mathfrak{a} = \left[5, \frac{3+\sqrt{-11}}{2}\right]$ – идеал кольца O_K, где $K = \mathbb{Q}(\sqrt{-11})$. Доказать, что этот идеал является примитивным и редуцировать его.

5. Вычислить группу классов O_K поля $K = \Theta(\sqrt{2})$.

8.3. Перечень вопросов и заданий для промежуточной аттестации по дисциплине

Вопросы для промежуточного контроля (зачета)

1. Алгебраические числа. Минимальный многочлен алгебраического числа. Признак алгебраичности.
2. След и норма числового поля. Их свойства. Характеристический многочлен.
3. Дискриминант набора чисел числового поля. Его свойства.
4. Модули, свободные модули, свободные Z-модули.
5. Целые базисы. Дискриминант числового поля. Примеры.
6. Разложение простых чисел в произведение простых идеалов в алгебраическом числовом поле. Пример.
7. Индекс ветвления и относительная степень. Их свойства.
8. Разложение простых чисел в произведение простых идеалов в квадратичном поле. Пример.
9. Определении цепной дроби. Разложение рациональных в цепные дроби. Разложение иррациональных чисел в цепные дроби.
10. Фундаментальная единица вещественного квадратичного поля. Теорема Дирихле. Группа единиц мнимого квадратичного поля.
11. Идеалы квадратичного поля. Их свойства. Примитивные идеалы.
12. Редуцированные идеалы. Их свойства. Алгоритм редукции. Оценка числа шагов алгоритма редукции.
13. Пример редукции идеалов.
14. Алгоритм умножения идеалов. Пример.
15. Группа классов идеалов. Граница Минковского. Число классов числового поля. Пример.
16. Число классов квадратичного поля. Пример вычисления группы классов идеалов.
17. Криптосистема Бухмана-Вильямса.
18. Криптосистема Вильямса.

8.4. Планируемые уровни сформированности компетенций обучающихся и критерии оценивания

Уровни	Содержательное описание уровня	Основные признаки выделения уровня (этапы формирования компетенции, критерии оценки сформированности)	Пятибалльная шкала (академическая) оценка	Двухбалльная шакала, зачет	БРС, % освоения (рейтинговая оценка)
Повышенный	Творческая деятельность	*Включает нижестоящий уровень.* Умение самостоятельно принимать решение, решать проблему/задачу теоретического и прикладного характера на основе изученных методов, приемов, технологий	отлично	зачтено	86-100
Базовый	Применение знаний и умений в более широких контекстах	*Включает нижестоящий уровень.* Способность собирать, систематизировать, анализировать и грамотно использовать	хорошо		71-85

	учебной и профессиональной деятельности, нежели по образцу с большей степени самостоятельности и инициативы	информацию из самостоятельно найденных теоретических источников и иллюстрировать ими теоретические положения или обосновывать практику применения			
Удовлетворительный (достаточный)	Репродуктивная деятельность	Изложение в пределах задач курса теоретически и практически контролируемого материала	удовлетворительно		55-70
Недостаточный	Отсутствие признаков удовлетворительного уровня		неудовлетворительно	не зачтено	Менее 55

9. Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины.

Основная литература

1. Манин, Ю. И. *Введение в современную теорию чисел*: Научное / Манин Ю.И., Панчишкин А.А. - Москва :МЦНМО, 2014. - 552 с.: ISBN 978-5-4439-2027-6. - Текст : электронный. - URL: https://znanium.com/catalog/product/969551.
2. Гречников, Е. А. *Вычислительно сложные задачи теории чисел* : учеб. пособие / Е. А. Гречников [и др.]. - Москва : Издательство Московского университета, 2012. - 312 с. - (Суперкомпьютерное образование). - ISBN 978-5-211-06342-6. - Текст : электронный. - URL: https://znanium.com/catalog/product/1023162.

Дополнительная литература

1. Алешников С. И.. *Математические методы защиты информации* : учеб.пособие/ С. И. Алешников, Ю. Ф. Болтнев ; Балт. федер. ун-т им. И. Канта Ч. 2 : Методы алгебраической теории чисел. on-line, 121 с.

2. Алешников С. И.. *Математические методы защиты информации* : учеб.пособие/ С. И. Алешников, Е.В. Козьминых, Ю. Ф. Болтнев ; Балт. федер. ун-т им. И. Канта Ч. 3 : Вычислительный практикум по числовым полям и криптографии в квадратичных полях. on-line, 93 с.

10. Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины (модуля).

- НЭБ Национальная электронная библиотека, диссертации и прочие издания
- eLIBRARY.RU Научная электронная библиотека, книги, статьи, тезисы докладов конференций

- Гребенников Электронная библиотека ИД журналы
- ЭБС Лань книги, журналы
- ЭБС Консультант студента
- ПРОСПЕКТ ЭБС
- ЭБС ZNANIUM.COM
- РГБ Информационное обслуживание по МБА
- БЕН РАН
- Электронно-библиотечная система (ЭБС) Кантитана (https://elib.kantiana.ru/)

11. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине.

Программное обеспечение обучения включает в себя:

- система электронного образовательного контента БФУ им. И. Канта – www.lms-3.kantiana.ru, обеспечивающую разработку и комплексное использование электронных образовательных ресурсов;
- серверное программное обеспечение, необходимое для функционирования сервера и связи с системой электронного обучения через Интернет;
- корпоративная платформа Microsoft Teams;
- установленное на рабочих местах обучающихся ПО: Microsoft Windows 7, Microsoft Office Standart 2010, антивирусное программное обеспечение Kaspersky Endpoint Security.
- специализированное ПО не требуется.

12. Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине.

Для проведения занятий лекционного типа, практических и семинарских занятий используются специальные помещения (учебные аудитории), оборудованные техническими средствами обучения – мультимедийной проекционной техникой. Для проведения занятий лекционного типа используются наборы демонстрационного оборудования.

Для проведения лабораторных работ, (практических занятий – при необходимости) используются специальные помещения (учебные аудитории), оснащенные специализированным лабораторным оборудованием: персональными компьютерами с возможностью выхода в интернет и с установленным программным обеспечением, заявленным в п.11.

Для проведения групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации используются специальные помещения (учебные аудитории), оборудованные специализированной мебелью (для обучающихся), меловой / маркерной доской.

Для организации самостоятельной работы обучающимся предоставляются помещения, оснащенные компьютерной техникой с возможностью подключения к сети «Интернет» и обеспечением доступа в электронную информационно-образовательную среду университета.

Для обучения инвалидов и лиц с ограниченными возможностями здоровья университетом могут быть представлены специализированные средства обучения, в том числе технические средства коллективного и индивидуального пользования.

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
федеральное государственное автономное образовательное учреждение высшего образования
«Балтийский федеральный университет имени Иммануила Канта»
Институт физико-математических наук и информационных технологий

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

«Квантовая защита и обработка информации»

Шифр: 10.05.01
Специальность: «Компьютерная безопасность»
Специализация: «Математические методы защиты информации»
Квалификация (степень) выпускника: специалист по защите информации

Калининград
2022

Лист согласования

Составитель: Иванов А.И., д.ф.-м.н., профессор

Рабочая программа утверждена на заседании учебно-методического совета института физико-математических наук и информационных технологий

Протокол № 01/22 от «01» февраля 2022 г.

Председатель учебно-методического
совета института физико-
математических наук и информационных
технологий

Первый заместитель директора Шпилевой А. А
ИФМНиИТ, к. ф.-м. н., доцент

Ведущий менеджер Е.П.Ставицкая

Содержание

1.Наименование дисциплины: «Квантовая защита и обработка информации».

Цель дисциплины: углубление и расширение знаний в области новейших перспективных направлений в информационных технологиях, новых принципов кодирования, обработки, передачи информации и вычислений, основанных на квантовой физике.

2. Перечень планируемых результатов обучения по дисциплине, соотнесенных с планируемыми результатами освоения образовательной программы

Код компетенции	Результаты освоения образовательной программы (ИДК)	Результаты обучения по дисциплине
ПКС-5 Способность участвовать в теоретических и экспериментальных научно-исследовательских работах по оценке защищенности информации в компьютерных системах	ПКС-5.1. Знает тенденции развития теоретических и экспериментальных исследований в области защиты информации. ПКС-5.2. Участвует в теоретических научно-исследовательских работах по оценке защищенности информации в компьютерных системах. ПКС-5.3. Участвует в экспериментальных научно-исследовательских работах по аудиту безопасности в компьютерных системах.	Студент, изучивший квантовую защиту и обработку информации, должен: • **Знать** соответствие между логическими цепями класси-ческих и квантовых компьютеров; принципы действия классических и квантовых компьютеров; основные эле-менты логических цепей классических и квантовых компьютеров; свойства необратимых и обратимых гейтов, теорему о неклонируемости кубитов и ее следствия; методы физической реализации и инициализации кубитов; свойства и способы генерации перепутанных состояний, их роль в квантовых вычислениях; особенности протоколов квантовой криптографии и основные трудности их реализации, сравнительные свойства квантовых и клас-сических алгоритмов • **Уметь** истолковывать действия логических цепей классических и квантовых компьютеров, протоколов квантовой криптографии; составлять схемы логических цепей, осуществляющих квантовый параллелизм; составлять схемы логических цепей, осуществляющих квантовые вычисления, коррекцию ошибок, квантовую телепортацию и

		генерацию квантового секретного ключа • Владеть обозначениями элементов квантовых логических цепей; схемами управления кубитами; правилами составления квантовых логических цепей и навыками их изображения; приемами составления протоколов, осуществляющих квантовый параллелизм, квантовые вычисления, коррекцию ошибок, квантовую телепортацию; протоколами генерации квантового секретного ключа

3. Место дисциплины в структуре образовательной программы

Дисциплина «Квантовая защита и обработка информации» представляет собой дисциплину части, формируемой участниками образовательных отношений, блока дисциплин подготовки обучающихся.

4. Виды учебной работы по дисциплине.

Виды учебной работы по дисциплине зафиксированы учебным планом основной профессиональной образовательной программы по указанному направлению и профилю, выражаются в академических часах. Часы контактной работы и самостоятельной работы обучающегося и часы, отводимые на процедуры контроля, могут различаться в учебных планах ОПОП по формам обучения. Объем контактной работы включает часы контактной аудиторной работы (лекции/практические занятия/ лабораторные работы), контактной внеаудиторной работы (контроль самостоятельной работы), часы контактной работы в период аттестации. Контактная работа, в том числе может проводиться посредством электронной информационно-образовательной среды университета с использованием ресурсов сети Интернет и дистанционных технологий.

5. Содержание дисциплины, структурированное по темам (разделам)

Исходя из рамок, установленных учебным планом по трудоемкости и видам учебной работы по дисциплине, преподаватель самостоятельно выбирает тематику занятий по формам и количеству часов проведения контактной работы: лекции и иные учебные занятия, предусматривающие преимущественную передачу учебной информации преподавателем и (или) занятия семинарского типа (семинары, практические занятия, практикумы, лабораторные работы, коллоквиумы и иные аналогичные занятия), и (или) групповые консультации, и (или) индивидуальную работу обучающихся с преподавателем, в том числе индивидуальные консультации (по курсовым работам/проектам – при наличии курсовой работы/проекта по данной дисциплине в учебном плане). Рекомендуемая тематика занятий максимально полно реализуется в контактной работе с обучающимися очной формы обучения. В случае реализации образовательной программы в заочной / очно-заочной форме трудоемкость дисциплины

сохраняется, однако объем учебного материала в значительной части осваивается обучающимися в форме самостоятельной работы. При этом требования к ожидаемым образовательным результатам обучающихся по данной дисциплине не зависят от формы реализации образовательной программы.

№ п/п	**Наименование темы**	**Содержание темы**
1	Аксиомы квантовой механики.	Наблюдаемые и операторы. Собственные значения и собственные функции операторов. Состояние системы и его эволюция. Квантовое измерение. Вероятностное толкование волновой функции. Средние значения физических величин. Соотношение неопределённостей для физических величин. Представление состояний векторами гильбертова пространства. Статистический оператор и матрица плотности. Спин электрона. Спиновые состояния. Сфера Блоха.
2	Квантовая информация.	Информация. Мера информации. Бит. Редуцированная матрица плотности. Квантовая энтропия. Эволюция измеряемой квантовой системы. Кубит. Какое количество информации можно закодировать состояниями кубита? Перепутанные состояния кубитов. ЭПР-пара. Парадокс ЭПР. Теорема о неклонируемости неизвестного квантового состояния.
3	Квантовые коммуникации.	Криптографический ключ. Проблема распространения ключа. Код Вернама. RSA-код. Квантовые поляризационные состояния фотонов. Математические модели приборов квантовой оптики. Квантовая криптография, основанная на теореме Белла. Квантовые криптографические протоколы BB-84, BBM -92 и их практическая реализация. Протокол квантовой телепортации на основе измерения состояний Белла. Протокол квантовой телепортации без измерения состояний Белла.
4	Классические и квантовые логические гейты, квантовые цепи.	Основные понятия алгебры логики. Классический универсальный компьютер и логические гейты. Полусумматор, сумматор. Обратимые логические гейты. Полусумматор и сумматор на обратимых логических гейтах. Квантовые логические гейты. Контролируемые квантовые гейты. CNOT-гейт и невозможность клонирования неизвестного состояния. Универсальные наборы квантовых логических гейтов. Квантовые цепи, реализующие полусумматор и сумматор. Квантовая цепь, реализующая состояния Белла.
5	Квантовые алгоритмы.	Понятие квантового параллельного вычисления. Алгоритм Дойча. Квантовое Фурье-преобразование и нахождение периода функции. Факторизация чисел и алгоритм П. Шора. Поиск в базе данных и алгоритм Гровера.
6	Квантовая коррекция ошибок.	Мажоритарная система исправления ошибок при трёхкубитовом кодировании. Протокол коррекции амплитудной ошибки. Квантовая схема кодирования для защиты от фазовой ошибки.

6. Рекомендуемая тематика учебных занятий в форме контактной работы

Рекомендуемая тематика учебных занятий *лекционного* типа (предусматривающих преимущественную передачу учебной информации преподавателями):

№	Наименование раздела	Темы лекций
1	Тема 1. Аксиомы квантовой механики.	Лекция 1. Аксиомы квантовой механики.
2	Тема 2. Квантовая информация.	Лекция 2. Квантовая информация.
3	Тема 3. Квантовые коммуникации.	Лекция 3. Квантовые коммуникации.
4	Тема 4. Классические и квантовые логические гейты, квантовые цепи.	Лекция 4. Классические и квантовые логические гейты, квантовые цепи.
5	Тема 5. Квантовые алгоритмы.	Лекция 5. Квантовые алгоритмы.
6	Тема 6. Квантовая коррекция ошибок	Лекция 6. Квантовая коррекция ошибок

Рекомендуемая тематика *практических* занятий:

№ п/п	Наименование Темы	Содержание темы
1	Аксиомы квантовой механики.	Определение статистического оператора и матрицы плотности. Работа со сферой Блоха.
2	Квантовая информация.	Составление схем перепутывания состояний кубита. Вычисление квантовой энтропии.
3	Квантовые коммуникации.	Работа с протоколами, основанными на теореме Белла, BB-84 и BBM-92.
4	Классические и квантовые логические гейты, квантовые цепи.	Составление схем сумматора, полусумматора. Построение квантовых цепей.
5	Квантовые алгоритмы.	Составление схем квантового преобразования Фурье, алгоритмом Дойча, алгоритмом Гровера и алгоритмом П.Шора.
6	Квантовая коррекция ошибок.	Работа с протоколом коррекции амплитудной ошибки и квантовой схемой кодирования для защиты от фазовой ошибки.

Требования к самостоятельной работе обучающихся

1. Работа с лекционным материалом, предусматривающая проработку конспекта лекций и учебной литературы, по всем темам из п. 6 настоящей рабочей программы.
2. Выполнение домашнего задания, предусматривающего решение задач, выполнение упражнений, выдаваемых на практических занятиях, по всем темам из п. 6 настоящей рабочей программы.

Руководствуясь положениями статьи 47 и статьи 48 Федерального закона от 29 декабря 2012 г. N 273-ФЗ «Об образовании в Российской Федерации» научно-педагогические работники и иные лица, привлекаемые университетом к реализации данной образовательной программы, пользуются предоставленными академическими правами и свободами в части свободы преподавания, свободы от вмешательства в профессиональную деятельность; свободы выбора и использования педагогически обоснованных форм, средств, методов обучения и воспитания; права на творческую инициативу, разработку и применение авторских программ и методов обучения и воспитания в пределах реализуемой образовательной программы и отдельной дисциплины.

Исходя из рамок, установленных учебным планом по трудоемкости и видам учебной работы по дисциплине, преподаватель самостоятельно выбирает тематику занятий по формам и количеству часов проведения контактной работы: лекции и иные учебные занятия, предусматривающие преимущественную передачу учебной информации преподавателем и (или) занятия семинарского типа (семинары, практические занятия, практикумы, лабораторные работы, коллоквиумы и иные аналогичные занятия), и (или) групповые консультации, и (или) индивидуальную работу обучающихся с преподавателем, в том числе индивидуальные консультации (по курсовым работам/проектам – при наличии курсовой работы/проекта по данной дисциплине в учебном плане).

Рекомендуемая тематика занятий максимально полно реализуется в контактной работе с обучающимися очной формы обучения. В случае реализации образовательной программы в заочной / очно-заочной форме трудоемкость дисциплины сохраняется, однако объем учебного материала в значительной части осваивается обучающимися в форме самостоятельной работы. При этом требования к ожидаемым образовательным результатам обучающихся по данной дисциплине не зависят от формы реализации образовательной программы.

№ п/п	**Наименование темы**	**Тематика самостоятельных работ**
1	Аксиомы квантовой механики.	Повторение теоретического материала к практическим занятиям. Решение задач домашнего задания по теме. Ознакомление с литературой по курсу. Выбор темы реферата.
2	Квантовая информация.	Повторение теоретического материала к практическим занятиям. Решение задач домашнего задания по теме. Чтение литературы по теме реферата. Подготовка краткой сводки предварительных результатов для реферата.
3	Квантовые коммуникации.	Повторение теоретического материала к практическим занятиям. Решение задач домашнего задания по теме. Подготовка основной части реферата.
4	Классические и квантовые логические гейты, квантовые цепи.	Повторение теоретического материала к практическим занятиям. Завершение основной части реферата. Подготовка к письменному опросу.
5	Квантовые алгоритмы.	Повторение теоретического материала к практическим занятиям. Подготовка презентации реферата. Подготовка к письменному опросу. Подготовка к промежуточной аттестации – зачёту.
6	Квантовая коррекция ошибок.	По данной теме самостоятельная работа не предусмотрена.

7. Методические рекомендации по видам занятий

Лекционные занятия.

В ходе лекционных занятий обучающимся рекомендуется выполнять следующие действия. Вести конспектирование учебного материала. Обращать внимание на категории, формулировки, раскрывающие содержание тех или иных явлений и процессов, научные выводы и практические рекомендации по их применению. Задавать преподавателю уточняющие вопросы с целью уяснения теоретических положений, разрешения спорных ситуаций.

Желательно оставить в рабочих конспектах поля, на которых во внеаудиторное время можно сделать пометки из рекомендованной литературы, дополняющие материал прослушанной лекции, а также подчеркивающие особую важность тех или иных теоретических положений.

Практические и семинарские занятия.

На практических и семинарских занятиях в зависимости от темы занятия выполняется поиск информации по решению проблем, практические упражнения, контрольные работы, выработка индивидуальных или групповых решений, итоговое обсуждение с обменом знаниями, участие в круглых столах, разбор конкретных ситуаций, командная работа, представление портфолио и т.п.

Самостоятельная работа.

Самостоятельная работа осуществляется в виде изучения литературы, эмпирических данных по публикациям и конкретных ситуаций из практики, подготовке индивидуальных работ, работа с лекционным материалом, самостоятельное изучение отдельных тем дисциплины; поиск и обзор литературы и электронных источников; чтение и изучение учебника и учебных пособий.

8. Фонд оценочных средств

8.1. Перечень компетенций с указанием этапов их формирования в процессе освоения образовательной программы в рамках учебной дисциплины

Основными этапами формирования указанных компетенций при изучении обучающимися дисциплины являются последовательное изучение содержательно связанных между собой тем учебных занятий. Изучение каждой темы предполагает овладение обучающимися необходимыми компетенциями. Результат аттестации обучающихся на различных этапах формирования компетенций показывает уровень освоения компетенций.

Контролируемые разделы (темы) дисциплины	Индекс контроли-руемой компетенции (или её части)	Оценочные средства по этапам формирования компетенций
		текущий контроль по дисциплине
Тема 1. Аксиомы квантовой механики.		Опрос, решение задач.
Тема 2. Квантовая информация.		Опрос, решение задач.
Тема 3. Квантовые коммуникации.		Опрос, решение задач.
Тема 4. Классические и квантовые логические гейты,		Устный опрос, решение задач,

Контролируемые разделы (темы) дисциплины	Индекс контроли-руемой компетенции (или её части)	Оценочные средства по этапам формирования компетенций
		текущий контроль по дисциплине
квантовые цепи.	ПКС-5	
Тема 5. Квантовые алгоритмы.		Устный опрос, решение задач,
Тема 6. Квантовая коррекция ошибок.		Устный опрос, решение задач,

8.2. Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений и навыков и (или) опыта деятельности процессе текущего контроля

Задачи

Тема 1. Аксиомы квантовой механики

	Задача
Оценка «зачтено» - низкой уровень освоения компетенции	Изобразить условные обозначения необратимых и обратимых элементов логических цепей компьютера.
Оценка «зачтено» - повышенный уровень освоения компетенции	Показать, что произведение унитарных операторов само является унитарным оператором.
Оценка «зачтено» - высокий уровень освоения компетенции	Записать и проанализировать соотношение неопределенностей для случая совместно измеримых величин.

Тема 2. Квантовая информация

	Задача
Оценка «зачтено» - низкой уровень освоения компетенции	Изобразить базисные и суперпозиционные состояния кубита на сфере Блоха.
Оценка «зачтено» - повышенный уровень освоения компетенции	Показать, что, если статистический оператор (матрица плотности) задан в своём собственном представлении, то для вычисления квантовой энтропии такого состояния можно пользоваться классической формулой Шеннона.
Оценка «зачтено» - высокий уровень освоения компетенции	Показать, что при унитарной эволюции квантовая энтропия остаётся неизменной.

Тема 3. Квантовые коммуникации

	Задача
Оценка «зачтено» -	Изобразить и объяснить протокол генерации секретного ключа с

низкой уровень освоения компетенции	помощью поляризованных фотонов (протокол BB-84).
Оценка «зачтено» - повышенный уровень освоения компетенции	Изобразить и объяснить протокол телепортации кубита без измерения состояний Белла.
Оценка «зачтено» - высокий уровень освоения компетенции	Изобразить и объяснить протокол телепортации с использованием базисных функций Белла.

Тема 4. Классические и квантовые логические гейты, квантовые цепи

	Задача
Оценка «зачтено» - низкой уровень освоения компетенции	Начертить и объяснить схемы полусумматора, полного сумматора и схему сложения двоичных чисел.
Оценка «зачтено» - повышенный уровень освоения компетенции	Начертить и объяснить схему квантового двоичного суммирования.
Оценка «зачтено» - высокий уровень освоения компетенции	Для двухкубитовой квантовой цепи, генерирующей состояния Белла и состоящей из однокубитового гейта Адамара и CNOT-гейта, в базисе двухкубитовых состояний |00>, |01>, |10>, |11> построить оператор Белла, описывающий результат действия этой цепи.

Тема 5. Квантовые алгоритмы

	Задача
Оценка «зачтено» - низкой уровень освоения компетенции	Начертить и объяснить схему квантового преобразования Фурье.
Оценка «зачтено» - повышенный уровень освоения компетенции	Привести пример работы алгоритма П. Шора.
Оценка «зачтено» - высокий уровень освоения компетенции	Привести пример работы алгоритма Гровера.

Тема 6. Квантовая коррекция ошибок

	Задача
Оценка «зачтено» - низкой уровень освоения компетенции	Изобразить и объяснить схему квантовой коррекции амплитудных ошибок квантовых вычислений.
Оценка «зачтено» -	Изобразить и объяснить схему квантовой коррекции фазовых

повышенный уровень освоения компетенции	ошибок квантовых вычислений.
Оценка «зачтено» - высокий уровень освоения компетенции	Изобразить и объяснить схему квантовой коррекции амплитудных и фазовых ошибок квантовых вычислений.

Примеры вопросов для устного опроса:

Тема 1. Аксиомы квантовой механики

1. Наблюдаемые и операторы.
2. Собственные значения и собственные функции операторов.
3. Состояние системы и его эволюция. Квантовое измерение. Вероятностное толкование волновой функции.
4. Средние значения физических величин.
5. Соотношение неопределённостей для физических величин.
6. Представление состояний векторами гильбертова пространства.
7. Статистический оператор и матрица плотности.
8. Спин электрона.
9. Спиновые состояния.
10. Сфера Блоха.
11. Для описания каких состояний применяется сфера Блоха?

Тема 2. Квантовая информация

1. Понятие квантовой информации.
2. Понятие меры информации.
3. Понятие бита.
4. Редуцированная матрица плотности.
5. Квантовая энтропия.
6. Эволюция измеряемой квантовой системы.
7. Понятие кубита.
8. Какое количество информации можно закодировать состояниями кубита?
9. Перепутанные состояния кубитов. ЭПР-пара. Парадокс ЭПР.
10. Теорема о неклонируемости неизвестного квантового состояния.
11. В чем принципиальное отличие квантового описания состояний кубита от описания состояний классического бита?
12. Приведите примеры реализаций кубита.
13. Приведите пример квантового состояния, которое можно клонировать.
14. Почему невозможно клонирование кубита и как это отражается на передаче квантовой информации?
15. Какой вид в обозначениях Дирака для 2-мерных кет-векторов имеет выражение для максимально перепутанных состояний двух кубитов?

Тема 3. Квантовые коммуникации

1. Криптографический ключ.
2. Проблема распространения ключа.
3. Код Вернама.
4. RSA-код.
5. Квантовые поляризационные состояния фотонов.
6. Математические модели приборов квантовой оптики.

7. Квантовая криптография, основанная на теореме Белла.
8. Квантовые криптографические протоколы BB-84, BBM -92 и их практическая реализация.
9. Протокол квантовой телепортации на основе измерения состояний Белла.
10. Протокол квантовой телепортации без измерения состояний Белла.
11. На чём основано сверхплотное кодирование?

Тема 4. Классические и квантовые логические гейты, квантовые цепи

1. Основные понятия алгебры логики.
2. Классический универсальный компьютер и логические гейты.
3. Полусумматор, сумматор.
4. Обратимые логические гейты.
5. Полусумматор и сумматор на обратимых логических гейтах.
6. Квантовые логические гейты.
7. Контролируемые квантовые гейты.
8. CNOT-гейт и невозможность клонирования неизвестного состояния.
9. Универсальные наборы квантовых логических гейтов.
10. Квантовые цепи, реализующие полусумматор и сумматор.
11. Квантовая цепь, реализующая состояния Белла.
12. NOT-гейт и гейт Адамара с помощью матриц Паули.

Тема 5. Квантовые алгоритмы

1. Понятие квантового параллельного вычисления.
2. Алгоритм Дойча.
3. Квантовое Фурье-преобразование и нахождение периода функции.
4. Факторизация чисел и алгоритм П. Шора.
5. Поиск в базе данных и алгоритм Гровера.
6. В чем состоит квантовый параллелизм вычислений?
7. Какие задачи, доступные для решения с помощью квантовых алгоритмов, практически недоступны классическим компьютерам?
8. Почему возможна абсолютно секретная квантовая генерация шифровального ключа?

Тема 6. Квантовая коррекция ошибок

1. Мажоритарная система исправления ошибок при трёхкубитовом кодировании.
2. Протокол коррекции амплитудной ошибки.
3. Квантовая схема кодирования для защиты от фазовой ошибки.
4. Какую роль в квантовой информации играет квантовая оптика?

Типовые контрольные задания:

Тема 1. Аксиомы квантовой механики

1. Изобразить условные обозначения необратимых и обратимых элементов логических цепей компьютера.
2. Показать, что произведение унитарных операторов само является унитарным оператором.
3. Записать и проанализировать соотношение неопределенностей для случая совместно измеримых величин.

Тема 2. Квантовая информация

1. Изобразить базисные и суперпозиционные состояния кубита на сфере Блоха.

2. Показать, что, если статистический оператор (матрица плотности) задан в своём собственном представлении, то для вычисления квантовой энтропии такого состояния можно пользоваться классической формулой Шеннона.
3. Показать, что при унитарной эволюции квантовая энтропия остаётся неизменной.

Тема 3. Квантовые коммуникации

1. Изобразить и объяснить протокол генерации секретного ключа с помощью поляризованных фотонов (протокол BB-84).
2. Изобразить и объяснить протокол телепортации кубита без измерения состояний Белла.
3. Изобразить и объяснить протокол телепортации с использованием базисных функций Белла.

Тема 4. Классические и квантовые логические гейты, квантовые цепи

1. Начертить и объяснить схемы полусумматора, полного сумматора и схему сложения двоичных чисел.
2. Начертить и объяснить схему квантового двоичного суммирования.
3. Для двухкубитовой квантовой цепи, генерирующей состояния Белла и состоящей из однокубитового гейта Адамара и CNOT-гейта, в базисе двухкубитовых состояний |00>, |01>, |10>, |11> построить оператор Белла, описывающий результат действия этой цепи.

Тема 5. Квантовые алгоритмы

1. Начертить и объяснить схему квантового преобразования Фурье.
2. Привести пример работы алгоритма П. Шора.
3. Привести пример работы алгоритма Гровера.

Тема 6. Квантовая коррекция ошибок

1. Изобразить и объяснить схему квантовой коррекции амплитудных ошибок квантовых вычислений.
2. Изобразить и объяснить схему квантовой коррекции фазовых ошибок квантовых вычислений.
3. Изобразить и объяснить схему квантовой коррекции амплитудных и фазовых ошибок квантовых вычислений.

8.3. Перечень вопросов и заданий для промежуточной аттестации по дисциплине

Вопросы для промежуточного контроля (зачета)

1. Наблюдаемые и операторы.
2. Собственные значения и собственные функции операторов.
3. Состояние системы и его эволюция. Квантовое измерение. Вероятностное толкование волновой функции.
4. Средние значения физических величин.
5. Соотношение неопределённостей для физических величин.
6. Представление состояний векторами гильбертова пространства.
7. Статистический оператор и матрица плотности.
8. Спин электрона.
9. Спиновые состояния.
10. Сфера Блоха.
11. Понятие квантовой информации.

12. Понятие меры информации.
13. Понятие бита.
14. Редуцированная матрица плотности.
15. Квантовая энтропия.
16. Эволюция измеряемой квантовой системы.
17. Понятие кубита.
18. Перепутанные состояния кубитов. ЭПР-пара. Парадокс ЭПР.
19. Теорема о неклонируемости неизвестного квантового состояния.
20. Приведите примеры реализаций кубита.
21. Приведите пример квантового состояния, которое можно клонировать.
22. Криптографический ключ.
23. Проблема распространения ключа.
24. Код Вернама.
25. RSA-код.
26. Квантовые поляризационные состояния фотонов.
27. Математические модели приборов квантовой оптики.
28. Квантовая криптография, основанная на теореме Белла.
29. Квантовые криптографические протоколы BB-84, BBM -92 и их практическая реализация.
30. Протокол квантовой телепортации на основе измерения состояний Белла.
31. Протокол квантовой телепортации без измерения состояний Белла.
32. Основные понятия алгебры логики.
33. Классический универсальный компьютер и логические гейты.
34. Полусумматор, сумматор.
35. Обратимые логические гейты.
36. Полусумматор и сумматор на обратимых логических гейтах.
37. Квантовые логические гейты.
38. Контролируемые квантовые гейты.
39. CNOT-гейт и невозможность клонирования неизвестного состояния.
40. Универсальные наборы квантовых логических гейтов.
41. Квантовые цепи, реализующие полусумматор и сумматор.
42. Квантовая цепь, реализующая состояния Белла.
43. Записать NOT-гейт и гейт Адамара с помощью матриц Паули.
44. Понятие квантового параллельного вычисления.
45. Алгоритм Дойча.
46. Квантовое Фурье-преобразование и нахождение периода функции.
47. Факторизация чисел и алгоритм П. Шора.
48. Поиск в базе данных и алгоритм Гровера.
49. В чем состоит квантовый параллелизм вычислений?
50. Мажоритарная система исправления ошибок при трёхкубитовом кодировании.
51. Протокол коррекции амплитудной ошибки.
52. Квантовая схема кодирования для защиты от фазовой ошибки.
53. Какую роль в квантовой информации играет квантовая оптика

8.4. Планируемые уровни сформированности компетенций обучающихся и критерии оценивания

Уровни	Содержательное описание уровня	Основные признаки выделения уровня (этапы формирования компетенции, критерии	Пятибалльная шкала (академическая)	Двухбалльная шакала, зачет	БРС, % освоения (рейтин

		оценки сформированности)	оценка		говая оценка)
Повышенный	Творческая деятельность	*Включает нижестоящий уровень.* Умение самостоятельно принимать решение, решать проблему/задачу теоретического и прикладного характера на основе изученных методов, приемов, технологий	отлично	зачтено	86-100
Базовый	Применение знаний и умений в более широких контекстах учебной и профессиональной деятельности, нежели по образцу с большей степени самостоятельности и инициативы	*Включает нижестоящий уровень.* Способность собирать, систематизировать, анализировать и грамотно использовать информацию из самостоятельно найденных теоретических источников и иллюстрировать ими теоретические положения или обосновывать практику применения	хорошо		71-85
Удовлетворительный (достаточный)	Репродуктивная деятельность	Изложение в пределах задач курса теоретически и практически контролируемого материала	удовлетворительно		55-70
Недостаточный	Отсутствие признаков удовлетворительного уровня		неудовлетворительно	не зачтено	Менее 55

9. Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины.

Основная литература

1. Физические основы защиты информации, обрабатываемой средствами вычислительной техники [Электронный ресурс]/ М-во образования и науки РФ, Балт. федер. ун-т им. И. Канта, Ин-т приклад. математики и информац. технологий; М-во образования и науки РФ, Балт. федер. ун-т им. И. Канта, Ин-т приклад. математики и информац. технологий. - Калининград: БФУ им. И. Канта, 2015. - 1 on-line, 283 с.. - Б.ц. Имеются экземпляры в отделах /There are copies in departments: ЭБС Кантиана(1)

Дополнительная литература

1. Холево, А. С. Квантовые системы, каналы, информация/ А. С. Холево. - М.: МЦНМО, 2010. - 327 с.: ил.. - Библиогр.: с. 316-324 (160 назв.). - Предм. указ.: с. 325-327. - ISBN 978-5-94057-574-0: 160.00, 402.00, 160.00, р. Имеются экземпляры в отделах /There are copies in departments: всего /all 13: УБ(11), ч.з.N3(1), НА(1)

2. Кайе, Ф. Введение в квантовые вычисления/ Ф. Кайе, Р. Лафламм, М. Моска; пер. с англ. Т. С. Никитиной, под науч. ред. А. В. Анохина. - М.; Ижевск: Регуляр. и хаот. динамика: Ин-т компьютер. исслед., 2009. - 346 с.: ил.. - Библиогр.: с. 328-339. - Предм. указ.: с. 340-346. - ISBN 978-5-93972-766-2: 150.00, 150.00, 878.00, р. Имеются экземпляры в отделах /There are copies in departments: всего /all 16: ч.з.N3(1), УБ(15)

3. Альбов, А. С. Квантовая криптография: Научно-популярное издание / Альбов А.С. - Санкт-Петербург :Страта, 2015. - 248 с. (Просто) ISBN 978-5-906150-35-6. - Текст : электронный. - URL: https://znanium.com/catalog/product/615191 (дата обращения: 27.04.2022). – Режим доступа: по подписке.

10. Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины (модуля).

- НЭБ Национальная электронная библиотека, диссертации и прочие издания
- eLIBRARY.RU Научная электронная библиотека, книги, статьи, тезисы докладов конференций
- Гребенников Электронная библиотека ИД журналы
- ЭБС Лань книги, журналы
- ЭБС Консультант студента
- ПРОСПЕКТ ЭБС
- ЭБС ZNANIUM.COM
- РГБ Информационное обслуживание по МБА
- БЕН РАН
- Электронно-библиотечная система (ЭБС) Кантитана (https://elib.kantiana.ru/)

11. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине.

Программное обеспечение обучения включает в себя:

- система электронного образовательного контента БФУ им. И. Канта – www.lms-3.kantiana.ru, обеспечивающую разработку и комплексное использование электронных образовательных ресурсов;
- серверное программное обеспечение, необходимое для функционирования сервера и связи с системой электронного обучения через Интернет;
- корпоративная платформа Microsoft Teams;

- установленное на рабочих местах обучающихся ПО: Microsoft Windows 7, Microsoft Office Standart 2010, антивирусное программное обеспечение Kaspersky Endpoint Security.
- специализированное ПО не требуется.

12. Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине.

Для проведения занятий лекционного типа, практических и семинарских занятий используются специальные помещения (учебные аудитории), оборудованные техническими средствами обучения – мультимедийной проекционной техникой. Для проведения занятий лекционного типа используются наборы демонстрационного оборудования.

Для проведения лабораторных работ, (практических занятий – при необходимости) используются специальные помещения (учебные аудитории), оснащенные специализированным лабораторным оборудованием: персональными компьютерами с возможностью выхода в интернет и с установленным программным обеспечением, заявленным в п.11.

Для проведения групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации используются специальные помещения (учебные аудитории), оборудованные специализированной мебелью (для обучающихся), меловой / маркерной доской.

Для организации самостоятельной работы обучающимся предоставляются помещения, оснащенные компьютерной техникой с возможностью подключения к сети «Интернет» и обеспечением доступа в электронную информационно-образовательную среду университета.

Для обучения инвалидов и лиц с ограниченными возможностями здоровья университетом могут быть представлены специализированные средства обучения, в том числе технические средства коллективного и индивидуального пользования.

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
федеральное государственное автономное образовательное учреждение высшего образования
«Балтийский федеральный университет имени Иммануила Канта»
Институт физико-математических наук и информационных технологий

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

«Прикладная алгебра»

Шифр: 10.05.01
Специальность: «Компьютерная безопасность»
Специализация: «Математические методы защиты информации»
Квалификация (степень) выпускника: специалист по защите информации

Калининград
2022

Лист согласования

Составитель: Малыгина Екатерина Сергеевна, к.ф.-м.н., доцент

Рабочая программа утверждена на заседании учебно-методического совета института физико-математических наук и информационных технологий

Протокол № 01/22 от «01» февраля 2022 г.

Председатель учебно-методического
совета института физико-
математических наук и информационных
технологий

Первый заместитель директора Шпилевой А. А
ИФМНиИТ, к. ф.-м. н., доцент

Ведущий менеджер Е.П.Ставицкая

Содержание

1.Наименование дисциплины: «Прикладная алгебра».

Цель дисциплины: целью освоения дисциплины «Прикладная алгебра» является расширение и углубление фундаментальной алгебраической подготовки студентов, обеспечивающей возможность овладения современными математическими методами, используемыми в криптографии, теории кодирования и общих моделях безопасности компьютерных систем, изучение дополнительных разделов алгебры, находящих непосредственные приложения в задачах защиты информации.

2. Перечень планируемых результатов обучения по дисциплине, соотнесенных с планируемыми результатами освоения образовательной программы

Код компетенции	Результаты освоения образовательной программы (ИДК)	Результаты обучения по дисциплине
ПКС-4. Способность осуществлять подбор, изучение и обобщение научно-технической информации, методических материалов отечественного и зарубежного опыта по проблемам компьютерной безопасности, а также нормативных правовых актов в сфере профессиональной деятельности.	ПКС-4.1. Осуществляет подбор, изучение и обобщение научно-технической информации, методических материалов отечественного и зарубежного опыта по проблемам компьютерной безопасности. ПКС-4.2. Знает основные руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации. ПКС-4.3. Применяет действующую законодательную базу в области обеспечения защиты информации.	- **знать** основные понятия и результаты дисциплины (группы, кольца, поля), понимать логические связи между ними; современное программное обеспечение для решения алгебраических задач; алгебраические методы для решения прикладных задач; - **уметь** производить вычисления в конкретных кольцах и алгебрах, выполнять операции над идеалами в коммутативных кольцах, осуществлять вычисления с перестановками конечного множества; использовать систему компьютерной алгебры для решения задач; - **владеть** методикой исследования свойств коммутативных колец, методикой исследования свойств групп перестановок конечного множества; навыками решения задач прикладной алгебры, в том числе, применяя системы компьютерной алгебры; способностью и готовностью применять методы прикладной алгебры к решению практических задач.

3. Место дисциплины в структуре образовательной программы

Дисциплина «Прикладная алгебра» представляет собой дисциплину части, формируемой участниками образовательных отношений, блока дисциплин подготовки обучающихся.

4. Виды учебной работы по дисциплине.

Виды учебной работы по дисциплине зафиксированы учебным планом основной профессиональной образовательной программы по указанному направлению и профилю, выражаются в академических часах. Часы контактной работы и самостоятельной работы обучающегося и часы, отводимые на процедуры контроля, могут различаться в учебных планах ОПОП по формам обучения. Объем контактной работы включает часы контактной аудиторной работы (лекции/практические занятия/ лабораторные работы), контактной внеаудиторной работы (контроль самостоятельной работы), часы контактной работы в период аттестации. Контактная работа, в том числе может проводиться посредством электронной информационно-образовательной среды университета с использованием ресурсов сети Интернет и дистанционных технологий

5. Содержание дисциплины, структурированное по темам (разделам)

Исходя из рамок, установленных учебным планом по трудоемкости и видам учебной работы по дисциплине, преподаватель самостоятельно выбирает тематику занятий по формам и количеству часов проведения контактной работы: лекции и иные учебные занятия, предусматривающие преимущественную передачу учебной информации преподавателем и (или) занятия семинарского типа (семинары, практические занятия, практикумы, лабораторные работы, коллоквиумы и иные аналогичные занятия), и (или) групповые консультации, и (или) индивидуальную работу обучающихся с преподавателем, в том числе индивидуальные консультации (по курсовым работам/проектам – при наличии курсовой работы/проекта по данной дисциплине в учебном плане). Рекомендуемая тематика занятий максимально полно реализуется в контактной работе с обучающимися очной формы обучения. В случае реализации образовательной программы в заочной / очно-заочной форме трудоемкость дисциплины сохраняется, однако объем учебного материала в значительной части осваивается обучающимися в форме самостоятельной работы. При этом требования к ожидаемым образовательным результатам обучающихся по данной дисциплине не зависят от формы реализации образовательной программы.

№	Наименование раздела	Содержание раздела
1	Введение	Свойства целых чисел. Модулярная арифметика. Метод математической индукции. Отношение эквивалентности. Функции.
2	Теория групп	Введение в теорию групп. Конечные группы. Подгруппы. Циклические группы. Группы перестановок. Изоморфизмы. Классы вычетов и теорема Лагранжа. Внешнее прямое произведение. Нормальные подгруппы и фактор-группы. Гомоморфизмы. Фундаментальная теорема конечных абелевых групп.
3	Теория колец	Введение в теорию колец. Кольца целостности. Идеалы и фактор-кольца. Гомоморфизмы. Кольца многочленов. Факторизация многочленов.

		Делимость в кольцах целых.
4	Теория полей	Векторные пространства. Расширения полей. Алгебраические расширения. Конечные поля.

6. Рекомендуемая тематика учебных занятий в форме контактной работы

Рекомендуемая тематика учебных занятий *лекционного* типа (предусматривающих преимущественную передачу учебной информации преподавателями):

№	Наименование раздела	Темы лекций
1	Введение	Лекция 1. Свойства целых чисел: Алгоритм деления. НОД. НОК. Фундаментальная теорема арифметики. Модулярная арифметика. Метод математической индукции. Лекция 2. Отношение эквивалентности. Функции, их свойства.
2	Теория групп	Лекция 3. Введение в теорию групп: Определение и примеры; Элементарные свойства. Лекция 4. Конечные группы: Основные определения; Подгруппы и их признаки; Примеры подгрупп. Лекция 5. Циклические группы: Свойства; Классификация подгрупп циклических групп. Лекция 6-7. Группы перестановок: Основные определения; Циклы; Свойства перестановок; Приложения. Лекция 8-9. Изоморфизмы групп: Основные определения и примеры; Теорема Кэли; Свойства изоморфизмов; Автоморфизмы. Лекция 10-11. Классы вычетов и теорема Лагранжа: Свойства; Теорема Лагранжа и следствия к ней; Приложения классов вычетов к группам перестановок. Лекция 12-13. Внешнее прямое произведение групп: Определения и примеры; Свойства; Группа единиц по модулю; Приложения. Лекция 14-15. Нормальные подгруппы и фактор-группы. Приложения. Внутреннее прямое произведение. Лекция 16. Гомоморфизм групп: Основные определения и примеры; Свойства; Первая теорема об изоморфизме. Лекция 17. Фундаментальная теорема конечных абелевых групп: Теорема; Классы изоморфизма абелевых групп.
3	Теория колец	Лекция 18. Введение в теорию колец: Основные определения; Примеры; Свойства; Подкольца. Лекция 19. Кольца целостности: Определения и примеры; Поля; Характеристика кольца.

		Лекция 20. Идеалы и фактор-кольца. Простые и максимальные идеалы. Лекция 21-22. Гомоморфизмы колец: Определения и примеры; Свойства; Поле частных. Лекция 23. Кольца многочленов: Основные определения; Алгоритм деления и следствия; Лекция 24-25. Факторизация многочленов: Тесты на приводимость; Тесты на неприводимость; Единственность разложения в Z[X]. Лекция 26-27. Делимость в кольцах целостности: Неприводимые и простые элементы; Единственность разложения в кольцах целеостности; Евклидовы кольца.
4	Теория полей	Лекция 28. Векторные пространства: Определения и примеры; Подпространства; Линейная независимость. Лекция 29-31. Расширения полей: Фундаментальная теорема теории полей; Поля разложений; Корни неприводимых многочленов. Лекция 32-33. Алгебраические расширения: Классификация расширений; Конечные расширения; Свойства. Лекция 34-35. Конечные поля: Классификация; Структура; Подполя.

Рекомендуемая тематика *практических* занятий:

1. Алгоритм деления целых чисел. Нахождение НОД’а и НОК’а.
2. Модулярная арифметика.
3. Метод математической индукции.
4. Отношение эквивалентности.
5. Функции.
6. Подгруппы и их признаки.
7. Циклические группы.
8. Группы перестановок.
9. Изоморфизмы групп.
10. Автоморфизмы групп.
11. Классы вычетов и теорема Лагранжа.
12. Внешнее прямое произведение групп, Группа единиц по модулю.
13. Нормальные подгруппы.
14. Фактор-группы.
15. Внутреннее прямое произведение.
16. Гомоморфизм групп.
17. Классы изоморфизма абелевых групп.
18. Кольца, подкольца.
19. Кольца целостности.
20. Идеалы и фактор-кольца.
21. Простые и максимальные идеалы.
22. Гомоморфизм колец.
23. Кольца многочленов. Алгоритм деления и следствия.
24. Факторизация многочленов.

25. Неприводимые и простые элементы в кольцах целостности. Факторизация в кольцах целостности.
26. Евклидовы кольца.
27. Векторные пространства.
28. Расширения полей.
29. Поля разложений.
30. Алгебраические расширения.
31. Конечные расширения.
32. Конечные поля. Подполя.

На практических занятиях решаются задачи по теме занятия.

Требования к самостоятельной работе обучающихся

1. Работа с лекционным материалом, предусматривающая проработку конспекта лекций и учебной литературы, по всем темам из п. 6 настоящей рабочей программы.
2. Выполнение домашнего задания, предусматривающего решение задач, выполнение упражнений, выдаваемых на практических занятиях, по всем темам из п. 6 настоящей рабочей программы.

Руководствуясь положениями статьи 47 и статьи 48 Федерального закона от 29 декабря 2012 г. N 273-ФЗ «Об образовании в Российской Федерации» научно-педагогические работники и иные лица, привлекаемые университетом к реализации данной образовательной программы, пользуются предоставленными академическими правами и свободами в части свободы преподавания, свободы от вмешательства в профессиональную деятельность; свободы выбора и использования педагогически обоснованных форм, средств, методов обучения и воспитания; права на творческую инициативу, разработку и применение авторских программ и методов обучения и воспитания в пределах реализуемой образовательной программы и отдельной дисциплины.

Исходя из рамок, установленных учебным планом по трудоемкости и видам учебной работы по дисциплине, преподаватель самостоятельно выбирает тематику занятий по формам и количеству часов проведения контактной работы: лекции и иные учебные занятия, предусматривающие преимущественную передачу учебной информации преподавателем и (или) занятия семинарского типа (семинары, практические занятия, практикумы, лабораторные работы, коллоквиумы и иные аналогичные занятия), и (или) групповые консультации, и (или) индивидуальную работу обучающихся с преподавателем, в том числе индивидуальные консультации (по курсовым работам/проектам – при наличии курсовой работы/проекта по данной дисциплине в учебном плане).

Рекомендуемая тематика занятий максимально полно реализуется в контактной работе с обучающимися очной формы обучения. В случае реализации образовательной программы в заочной / очно-заочной форме трудоемкость дисциплины сохраняется, однако объем учебного материала в значительной части осваивается обучающимися в форме самостоятельной работы. При этом требования к ожидаемым образовательным результатам обучающихся по данной дисциплине не зависят от формы реализации образовательной программы.

7. Методические рекомендации по видам занятий

Лекционные занятия.

В ходе лекционных занятий обучающимся рекомендуется выполнять следующие действия. Вести конспектирование учебного материала. Обращать внимание на категории, формулировки, раскрывающие содержание тех или иных явлений и процессов, научные выводы и практические рекомендации по их применению. Задавать преподавателю уточняющие вопросы с целью уяснения теоретических положений, разрешения спорных ситуаций.

Желательно оставить в рабочих конспектах поля, на которых во внеаудиторное время можно сделать пометки из рекомендованной литературы, дополняющие материал прослушанной лекции, а также подчеркивающие особую важность тех или иных теоретических положений.

Практические и семинарские занятия.

На практических и семинарских занятиях в зависимости от темы занятия выполняется поиск информации по решению проблем, практические упражнения, контрольные работы, выработка индивидуальных или групповых решений, итоговое обсуждение с обменом знаниями, участие в круглых столах, разбор конкретных ситуаций, командная работа, представление портфолио и т.п.

Самостоятельная работа.

Самостоятельная работа осуществляется в виде изучения литературы, эмпирических данных по публикациям и конкретных ситуаций из практики, подготовке индивидуальных работ, работа с лекционным материалом, самостоятельное изучение отдельных тем дисциплины; поиск и обзор литературы и электронных источников; чтение и изучение учебника и учебных пособий.

8. Фонд оценочных средств

8.1. Перечень компетенций с указанием этапов их формирования в процессе освоения образовательной программы в рамках учебной дисциплины

Основными этапами формирования указанных компетенций при изучении обучающимися дисциплины являются последовательное изучение содержательно связанных между собой тем учебных занятий. Изучение каждой темы предполагает овладение обучающимися необходимыми компетенциями. Результат аттестации обучающихся на различных этапах формирования компетенций показывает уровень освоения компетенций.

Контролируемые разделы (темы) дисциплины	Индекс контроли-руемой компетенции (или её части)	Оценочные средства по этапам формирования компетенций
		текущий контроль по дисциплине
1. Введение	ПКС-4	Опрос, решение задач.
2. Теория групп		Опрос, решение задач, контрольная работа.
3. Теория колец		Опрос, решение задач, контрольная работа.
4. Теория полей		Опрос, решение задач, контрольная работа.

8.2. Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений и навыков и (или) опыта деятельности процессе текущего контроля

Примеры вопросов для устного опроса:

По Теме 1. Введение

1. Перечислить основные свойства целых чисел.
2. Сформулировать основные принципы математической индукции.
3. Дать основные определения отображений двух множеств.

По Теме 2. Теория групп

1. Дать определение группе.
2. Сформулировать основные свойства групп.
3. Дать определение подгруппе.
4. Сформулировать основные свойства и признаки подгрупп.
5. Дать определение циклической группе.
6. Сформулировать основные свойства циклических групп.
7. Дать определение группе перестановок.
8. Сформулировать основные свойства групп перестановок.
9. Дать определение изоморфизму групп, сформулировать его основные свойства.
10. Дать определение автоморфизму групп.
11. Дать определение классу эквивалентности.
12. Сформулировать теорему Лагранжа.
13. Дать определение внешнему прямому произведению групп, сформулировать его основные свойства.
14. Дать определение нормальной группе и группе, факторизованной по нормальной подгруппе.
15. Дать определение гомоморфизму групп, сформулировать его основные свойства.
16. Сформулировать основную теорему конечных абелевых групп.

По Теме 3. Теория колец

1. Дать определение кольца и подкольца.
2. Дать определение кольцу целостности, характеристике кольца.
3. Дать определение идеалу.
4. Дать определение кольцу, факторизованному по идеалу.
5. Дать определения максимальному и простому идеалам.
6. Дать определение гомоморфизму колец и сформулировать его основные свойства.
7. Рассказать про алгоритм деления в кольцах многочленов.
8. Рассказать об основных тестах на приводимость/неприводимость многочленов.
9. Дать определения неприводимым и простым элементам в кольцах целостности.
10. Дать определение евклидовым кольцам.

По Теме 4. Теория полей

1. Дать определения векторного пространства и подпространства.
2. Дать определения линейной зависимости/независимости векторов.
3. Сформулировать фундаментальную теорему теории полей.
4. Дать определение полю разложений и сформулировать его основные свойства.
5. Дать определения конечным и алгебраическим расширениям.
6. Дать определение конечному полю, рассказать концепцию построения конечного поля и его подполей.

Типовые контрольные задания:

1. Является ли кольцом множество матриц вида $\begin{pmatrix} x & y \\ -3y & x \end{pmatrix}$, где x, y – целые числа. Если да, то найти обратимые элементы и делители нуля этого кольца.
2. Пусть A – множество функций $f: \mathrm{P} \to \mathrm{P}$ вида $f(x) = ax + b$, где $a, b \in \mathrm{P}$. Для $f, g \in A$, $x \in \mathrm{P}$ положим $(f + g)(x) = f(x) + g(x)$, $fg = f \circ g$ – композиция отображений. Будет ли A кольцом?
3. Доказать, что если (0) и (1) – единственные идеалы кольца A, то A – поле.
4. Построить кольцо Z/(9). Найти все идеалы $\mathfrak{a}_1, \mathfrak{a}_2, \ldots$ в этом кольце. Построить $(\mathrm{Z}/(9))/\mathfrak{a}_1$, $(\mathrm{Z}/(9))/\mathfrak{a}_2, \ldots$ Указать в построенных кольцах делители нуля, обратимые элементы, идеалы.
5. Пусть R – нётерово кольцо, $\varphi: R \to R$ – сюръективный гомоморфизм. Доказать, что φ инъективен. У к а з а н и е: Рассмотреть $\mathrm{Ker}(\varphi^j)$, $j \geq 0$.
6. Пусть S – подкольцо кольца R, S – нётерово кольцо, R – конечно порождено как модуль над S. Доказать, что R – нётерово кольцо.
7. Пусть $\lambda \in \mathrm{P}$. Является ли группой относительно умножения множество ненулевых матриц вида $\begin{pmatrix} x & y \\ \lambda y & x \end{pmatrix}$, где $x, y \in \mathrm{P}$.
8. Доказать, что если в группе G выполняется тождество $x^2 = 1$, то G - абелева.
9. Найти все гомоморфизмы аддитивных групп $\mathrm{Z}/6\mathrm{Z} \to \mathrm{Z}/6\mathrm{Z}$, $\mathrm{Z}/6\mathrm{Z} \to \mathrm{Z}/18\mathrm{Z}$.
10. Найти порядок элемента $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 1 & 5 & 4 \end{pmatrix} \in \mathrm{S}_5$.
11. Найти порядок элемента $\begin{pmatrix} 0 & i \\ 1 & 0 \end{pmatrix} \in \mathrm{GL}_2(\mathrm{X})$.
12. Найти все элементы группы S_4, коммутирующие с перестановкой (12)(34).
13. Найти фактор-группу $4\mathrm{Z}/12\mathrm{Z}$.
14. Пусть G – группа. Доказать, что множество H внутренних автоморфизмов группы G является нормальной подгруппой группы $\mathrm{Aut}(G)$ всех автоморфизмов группы G.
15. Найти минимальный многочлен числа z над полем k. Найти все гомоморфизмы поля $k(z)$ в поле X комплексных чисел.

    1) $z = \sqrt{5}$, $k = \Theta$, 2) $z = \sqrt[3]{5}$, $k = \Theta$.

16. Доказать, что $\Theta(\alpha + \beta) = \Theta(\alpha, \beta)$ и вычислить $[\Theta(\alpha + \beta) : \Theta]$.

    1) $\alpha = \sqrt{3}$, $\beta = \sqrt[3]{2}$, 2) $\alpha = \sqrt{2}$, $\beta = i$.

17. Пусть m – целое, свободное от кубов, $K = \mathbb{Q}(\sqrt[3]{m})$. Найти все гомоморфизмы из K в X.
18. Пусть θ – корень уравнения $x^3 + 2x + 2 = 0$, $K = \Theta(\theta)$ и $\alpha = \theta - \theta^2$. Найти минимальный многочлен элемента α над K.
19. Доказать, что всякое расширение полей степени 2 нормально.

20. Привести пример нормального расширения степени 2, не являющегося сепарабельным.
21. Является ли сепарабельным многочлен $f = X^3 + X + 2$ над Θ, над P, над $Ф_3$?
22. Найти все автоморфизмы полей Θ ($\sqrt{2}$), Θ($\sqrt{2}$ + $\sqrt{7}$), $\mathbb{Q}(\sqrt[3]{m})$.
23. Найти все промежуточные поля для расширения Θ($\sqrt{2}$,$\sqrt{3}$) / Θ.

8.3. Перечень вопросов и заданий для промежуточной аттестации по дисциплине

Вопросы для промежуточного контроля (зачета с оценкой)

1. Группы: определения, примеры, свойства.
2. Конечные группы и подгруппы. Признаки подгрупп. Примеры.
3. Циклические группы: определения и свойства. Классификация подгрупп циклических групп.
4. Группы перестановок: определения, свойства, примеры.
5. Изоморфизмы групп: мотивация, определения, примеры. Теорема Кэли. Свойства изоморфизмов. Автоморфизмы.
6. Классы вычетов: определения и свойства. Теорема Лагранжа и следствия к ней. Приложения к группам перестановок.
7. Внешнее прямое произведение групп: определения, примеры, свойства. Группа единиц по модулю как внешнее прямое произведение групп. Приложения.
8. Нормальные подгруппы и фактор-группы, их приложения. Внутреннее прямое произведение групп.
9. Фундаментальная теорема конечных абелевых групп. Классы изоморфизмов абелевых групп.
10. Кольца: мотивация, определения, примеры. Свойства колец. Подкольца.
11. Кольца целостности: определения и примеры. Поля. Характеристика кольца.
12. Идеалы и фактор-кольца. Простые и максимальные идеалы.
13. Гомоморфизмы колец: определения, примеры, свойства. Поля частных.
14. Кольца многочленов: определения и свойства. Алгоритм деления многочленов и следствия.
15. Тесты на приводимость/неприводимость многочленов. Единственность разложения в $Z[X]$. Приложения.
16. Неприводимые и простые элементы. Кольца с единственным разложением на множители. Евклидовы кольца.
17. Векторные пространства: определения и примеры. Подпространства. Линейная независимость.
18. Фундаментальная теорема теории полей. Поля разложения. Нули неприводимых многочленов.
19. Конечные и алгебраические расширения. Свойства и классификация расширений.
20. Классификация конечных полей. Структура конечного поля. Подполя конечных полей.

8.4. Планируемые уровни сформированности компетенций обучающихся и критерии оценивания

Уровни	Содержательн	Основные признаки	Пятибалль	Двухба	БРС, %

	ое описание уровня	выделения уровня (этапы формирования компетенции, критерии оценки сформированности)	ная шкала (академическая) оценка	лльная шакала, зачет	освоения (рейтинговая оценка)
Повышенный	Творческая деятельность	*Включает нижестоящий уровень.* Умение самостоятельно принимать решение, решать проблему/задачу теоретического и прикладного характера на основе изученных методов, приемов, технологий	отлично	зачтено	86-100
Базовый	Применение знаний и умений в более широких контекстах учебной и профессиональной деятельности, нежели по образцу с большей степени самостоятельности и инициативы	*Включает нижестоящий уровень.* Способность собирать, систематизировать, анализировать и грамотно использовать информацию из самостоятельно найденных теоретических источников и иллюстрировать ими теоретические положения или обосновывать практику применения	хорошо		71-85
Удовлетворительный (достаточный)	Репродуктивная деятельность	Изложение в пределах задач курса теоретически и практически контролируемого материала	удовлетворительно		55-70
Недостаточный	Отсутствие признаков удовлетворительного уровня		неудовлетворительно	не зачтено	Менее 55

9. Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины.

Основная литература

1. Смолин, Ю.Н. *Алгебра и теория чисел* : учеб. пособие / Ю.Н. Смолин. — 5-е изд., стер.—Москва : ФЛИНТА, 2017. — 464 с. - ISBN 978-5-9765-0050-1. - Текст : электронный. - URL: https://znanium.com/catalog/product/1034573.

2. Шевцов, Г. С. *Линейная алгебра: теория и прикладные аспекты*: Учебное пособие / Г.С. Шевцов. - 3-е изд., испр. и доп. - М.: Магистр: НИЦ ИНФРА-М, 2019. - 544 с. - ISBN 978-5-9776-0258-7. - Текст : электронный. - URL: https://znanium.com/catalog/product/1015326.

Дополнительная литература

1. Математические методы защиты информации: учеб. пособие / *С. И. Алешников, Ю. Ф. Болтнев*; Балт. гос. ун-т им. И. Канта. - Калининград: БФУ им. И. Канта. Ч.1: Алгебраические методы: учебное пособие. -2015, **on-line**, 156 с. ЭБС Кантиана
2. Математические методы защиты информации: учеб. пособие/ *С. И. Алешников, А. В. Пышкин*; Балт. федер. ун-т им. И. Канта. – Калининград. Ч.2: Методы алгебраической теории чисел: учебное пособие. – 2015, **on-line**, 121 с. ЭБС Кантиана

10. Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины (модуля).

- НЭБ Национальная электронная библиотека, диссертации и прочие издания
- eLIBRARY.RU Научная электронная библиотека, книги, статьи, тезисы докладов конференций
- Гребенников Электронная библиотека ИД журналы
- ЭБС Лань книги, журналы
- ЭБС Консультант студента
- ПРОСПЕКТ ЭБС
- ЭБС ZNANIUM.COM
- РГБ Информационное обслуживание по МБА
- БЕН РАН
- Электронно-библиотечная система (ЭБС) Кантитана (https://elib.kantiana.ru/)

11. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине.

Программное обеспечение обучения включает в себя:

- система электронного образовательного контента БФУ им. И. Канта – www.lms-3.kantiana.ru, обеспечивающую разработку и комплексное использование электронных образовательных ресурсов;
- серверное программное обеспечение, необходимое для функционирования сервера и связи с системой электронного обучения через Интернет;
- корпоративная платформа Microsoft Teams;
- установленное на рабочих местах обучающихся ПО: Microsoft Windows 7, Microsoft Office Standart 2010, антивирусное программное обеспечение Kaspersky Endpoint Security.
- специализированное ПО не требуется.

12. Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине.

Для проведения занятий лекционного типа, практических и семинарских занятий используются специальные помещения (учебные аудитории), оборудованные техническими средствами обучения – мультимедийной проекционной техникой. Для проведения занятий лекционного типа используются наборы демонстрационного оборудования.

Для проведения лабораторных работ, (практических занятий – при необходимости) используются специальные помещения (учебные аудитории), оснащенные специализированным лабораторным оборудованием: персональными компьютерами с возможностью выхода в интернет и с установленным программным обеспечением, заявленным в п.11.

Для проведения групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации используются специальные помещения (учебные аудитории), оборудованные специализированной мебелью (для обучающихся), меловой / маркерной доской.

Для организации самостоятельной работы обучающимся предоставляются помещения, оснащенные компьютерной техникой с возможностью подключения к сети «Интернет» и обеспечением доступа в электронную информационно-образовательную среду университета.

Для обучения инвалидов и лиц с ограниченными возможностями здоровья университетом могут быть представлены специализированные средства обучения, в том числе технические средства коллективного и индивидуального пользования.

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
федеральное государственное автономное образовательное учреждение высшего образования
«Балтийский федеральный университет имени Иммануила Канта»
Институт физико-математических наук и информационных технологий

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

«Вычислительная алгебра»

Шифр: 10.05.01
Специальность: «Компьютерная безопасность»
Специализация: «Математические методы защиты информации»
Квалификация (степень) выпускника: специалист по защите информации

Калининград
2022

Лист согласования

Составитель: Малыгина Екатерина Сергеевна, к.ф.-м.н., доцент

Рабочая программа утверждена на заседании учебно-методического совета института физико-математических наук и информационных технологий
Протокол № 01/22 от «01» февраля 2022 г.
Председатель учебно-методического
совета института физико-
математических наук и информационных
технологий
Первый заместитель директора Шпилевой А. А
ИФМНиИТ, к. ф.-м. н., доцент

Ведущий менеджер Е.П.Ставицкая

Содержание

1.Наименование дисциплины: «Вычислительная алгебра».

Цель дисциплины: целью освоения дисциплины «**Вычислительная алгебра**» является расширение и углубление фундаментальной алгебраической подготовки студентов, обеспечивающей возможность овладения современными математическими методами, используемыми в криптографии, теории кодирования и общих моделях безопасности компьютерных систем, изучение дополнительных разделов алгебры, находящих непосредственные приложения в задачах защиты информации.

2. Перечень планируемых результатов обучения по дисциплине, соотнесенных с планируемыми результатами освоения образовательной программы

Код компетенции	Результаты освоения образовательной программы (ИДК)	Результаты обучения по дисциплине
ПКС-4. Способность осуществлять подбор, изучение и обобщение научно-технической информации, методических материалов отечественного и зарубежного опыта по проблемам компьютерной безопасности, а также нормативных правовых актов в сфере профессиональной деятельности.	ПКС-4.1. Осуществляет подбор, изучение и обобщение научно-технической информации, методических материалов отечественного и зарубежного опыта по проблемам компьютерной безопасности. ПКС-4.2. Знает основные руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации. ПКС-4.3. Применяет действующую законодательную базу в области обеспечения защиты информации.	**Знать** типовые алгоритмы преобразования информации в компьютерных системах и оценки их эффективности; перспективные методы и алгоритмы преобразования информации в компьютерных системах и методику оценки их эффективности; российские и иностранные стандарты безопасности компьютерных систем. **Уметь** строить математические модели информационных процессов в компьютерных системах и алгоритмизировать вычислительные процедуры в этих моделях; поводить аналитическую работу по компьютерной безопасности. **Владеть** навыками построения математических моделей информационных процессов в компьютерных системах и навыками их анализа относительно безопасности.

3. Место дисциплины в структуре образовательной программы

Дисциплина «**Вычислительная алгебра**» представляет собой дисциплину части, формируемой участниками образовательных отношений, блока дисциплин подготовки обучающихся.

4. Виды учебной работы по дисциплине.

Виды учебной работы по дисциплине зафиксированы учебным планом основной профессиональной образовательной программы по указанному направлению и профилю, выражаются в академических часах. Часы контактной работы и самостоятельной работы обучающегося и часы, отводимые на процедуры контроля, могут различаться в учебных планах ОПОП по формам обучения. Объем контактной работы включает часы контактной аудиторной работы (лекции/практические занятия/ лабораторные работы), контактной внеаудиторной работы (контроль самостоятельной работы), часы контактной работы в период аттестации. Контактная работа, в том числе может проводиться посредством электронной информационно-образовательной среды университета с использованием ресурсов сети Интернет и дистанционных технологий

5. Содержание дисциплины, структурированное по темам (разделам)

Исходя из рамок, установленных учебным планом по трудоемкости и видам учебной работы по дисциплине, преподаватель самостоятельно выбирает тематику занятий по формам и количеству часов проведения контактной работы: лекции и иные учебные занятия, предусматривающие преимущественную передачу учебной информации преподавателем и (или) занятия семинарского типа (семинары, практические занятия, практикумы, лабораторные работы, коллоквиумы и иные аналогичные занятия), и (или) групповые консультации, и (или) индивидуальную работу обучающихся с преподавателем, в том числе индивидуальные консультации (по курсовым работам/проектам – при наличии курсовой работы/проекта по данной дисциплине в учебном плане). Рекомендуемая тематика занятий максимально полно реализуется в контактной работе с обучающимися очной формы обучения. В случае реализации образовательной программы в заочной / очно-заочной форме трудоемкость дисциплины сохраняется, однако объем учебного материала в значительной части осваивается обучающимися в форме самостоятельной работы. При этом требования к ожидаемым образовательным результатам обучающихся по данной дисциплине не зависят от формы реализации образовательной программы.

№ п/п	Наименование Темы	Содержание темы
1	Введение.	Обзор основных результатов элементарной теории чисел. Обзор основных свойств конечных полей. Общая задача вычисления дискретного логарифма, как задача решения системы полиномиальных уравнений над конечным полем.
2	Вычисления в кольцах и алгебрах.	Примеры колец и полей. Подкольца и подполя. Алгебры над кольцом и над полем. Алгебра многочленов от одной переменной, её свойства. Многочлены от многих переменных, его факториальность. Гомоморфизмы колец, полей и алгебр, их свойства примеры. Идеалы коммутативных колец, их свойства. Подкольца и идеалы, порождённые множеством, их свойства, их элементы. Кольца главных идеалов. Факторизация колец и гомоморфизмов по идеалам. Сумма и произведение идеалов. Свойства операций над идеалами. Максимальные и простые идеалы. Числовые кольца. Алгоритм редукции и умножения идеалов квадратичного кольца.

3	Вычисления с многочленами.	Нётеровы кольца. Эквивалентные условия нётеровости. Теорема Гильберта о базисе. Представления многочленов. Арифметика многочленов. Евклидовы алгоритмы для многочленов. Вычисление результантов и дискриминантов. Факторизация многочленов по модулю *p*. Алгоритм Берлекэмпа. Факторизация многочленов над □ и над □. Отношение порядка на множестве одночленов. Алгоритм деления в кольце многочленов от многих переменных. Мономиальные идеалы. Лемма Диксона. Базисы Грёбнера полиномиальных идеалов, их свойства. Зацепление многочленов. Алгоритм Бухбергера. Минимальный и редуцированный базисы Грёбнера, их свойства.
4	Решение систем алгебраических уравнений.	Аффинные алгебраические множеств, операции над ними. Топология Зариского. Идеал множества. Радикал идеала, его свойства. Радикальные идеалы. Свойства идеалов множеств. Понятие неприводимости. Аффинные алгебраические многообразия. Идеал многообразия. Теорема Гильберта о нулях. Соответствие между алгебраическими множествами и идеалами. Алгоритм вычисления радикалов идеалов в полиномиальных кольцах. Разложение на неприводимые компоненты. Алгоритм решения систем полиномиальных уравнений с помощью базисов Грёбнера. Алгоритм примарного разложения идеалов в полиномиальных кольцах.
5	Вычисления с группами и перестановками.	Группы. Гомоморфизмы групп, их свойства. Подгруппы. Пересечение подгрупп. Образ и прообраз группы при гомоморфизме. Образ гомоморфизма. Отношения эквивалентности в группе по подгруппе. Теорема Лагранжа. Нормальные подгруппы. Образ и прообраз нормальной подгруппы при гомоморфизме. Ядро гомоморфизма. Отношение эквивалентности в группе по нормальной подгруппе. Факторгруппа. Факторизация гомоморфизмов. Теоремы об изоморфизмах. Подгруппа, порождённая множеством. Образ с помощью гомоморфизма. Циклические группы. Обращение теоремы Лагранжа для циклических групп. Разрешимые группы, их свойства. Примеры разрешимых групп. Произведение и прямое произведение подгрупп. Прямая сумма подгрупп абелевой группы. Разложение циклической группы в прямую сумму примарных циклических подгрупп. Разложение конечной абелевой группы в прямую сумму циклических групп. Тип конечной абелевой группы. Обращение теоремы Лагранжа для конечной абелевой группы. Перестановки и шифры. Транспозиции. Разложение перестановки в произведение циклов и транспозиций. Системы образующих симметрической группы. Инверсии. Сигнатура перестановки. Четные и нечетные подстановки, теорема о декременте. Орбита и стабилизатор элемента. Сопряжённые перестановки. Критерий сопряженности подстановок. Уравнение Коши. Разрешимость и неразрешимость групп перестановок. Генерация лексикографической перестановки. Сложные замены. Простые замены. Переходы простых изменений. Общая структура. Пропуск нежелательных блоков. Лексикографические перестановки с ограниченными

		префиксами. Дуальные методы.
6	Вычисления в числовых полях и группах Галуа.	Расширения полей. Степень расширения. Конечные расширения. Теорема транзитивности конечных расширений. Алгебраические и трансцендентные элементы. Стандартные представления алгебраических чисел. Матричные представления алгебраических чисел. Алгебраические расширения полей. Минимальный многочлен алгебраического элемента. Признак алгебраического элемента. Свойства алгебраических расширений. Алгебраическое замыкание поля. Гомоморфизмы алгебраических расширений. Поля разложения многочленов и нормальные расширения. Сепарабельные элементы. Сепарабельные многочлены. Сепарабельные расширения полей. Группа автоморфизмов поля над подполем. Неподвижное поле группы автоморфизмов. Теорема Артина. Расширения Галуа. Группа Галуа расширения Галуа. Соответствие Галуа. Основная теорема теории Галуа. Группа Галуа как группа перестановок корней многочлена. Примеры. Решение кубических уравнений в радикалах. Решение уравнений четвёртой степени в радикалах. Критерий разрешимости уравнения в радикалах. Метод резольвент вычисления групп Галуа. Его применения для числовых полей степени 3, 4, 5.

6. Рекомендуемая тематика учебных занятий в форме контактной работы

Рекомендуемая тематика учебных занятий *лекционного* типа (предусматривающих преимущественную передачу учебной информации преподавателями):

№	Наименование раздела	Темы лекций
1	Введение	Лекция 1 Обзор основных свойств конечных полей. Лекция 2. Общая задача вычисления дискретного логарифма, как задача решения системы полиномиальных уравнений над конечным полем.
2	Вычисления в кольцах и алгебрах	Лекция 3. Алгебры над кольцом и над полем. Алгебра многочленов от одной переменной, её свойства. Лекция 4. Многочлены от многих переменных, его факториальность. Лекция 5. Гомоморфизмы колец, полей и алгебр, их свойства примеры. Лекция 6. Идеалы коммутативных колец, их свойства. Подкольца и идеалы, порождённые множеством, их свойства, их элементы. Лекция 7. Кольца главных идеалов. Факторизация колец и гомоморфизмов по идеалам. Лекция 8. Максимальные и простые идеалы.

		Числовые кольца. Лекция 9. Алгоритм редукции и умножения идеалов квадратичного кольца.
3	Вычисления с многочленами	Лекция 10. Нётеровы кольца. Эквивалентные условия нётеровости. Лекция 11. Теорема Гильберта о базисе. Лекция 12. Евклидовы алгоритмы для многочленов. Лекция 13. Факторизация многочленов по модулю p. Алгоритм Берлекэмпа. Лекция 14. Алгоритм деления в кольце многочленов от многих переменных. Лекция 15. Зацепление многочленов. Алгоритм Бухбергера.
4	Решение систем алгебраических уравнений	Лекция 16. Аффинные алгебраические множеств, операции над ними. Топология Зариского. Лекция 17. Радикал идеала, его свойства. Радикальные идеалы. Лекция 18. Идеал многообразия. Теорема Гильберта о нулях. Лекция 19. Алгоритм вычисления радикалов идеалов в полиномиальных кольцах. Разложение на неприводимые компоненты. Лекция 20. Алгоритм решения систем полиномиальных уравнений с помощью базисов Грёбнера.
5	Вычисления с группами перестановок	Лекция 21. Группы. Лекция 22. Теорема Лагранжа. Нормальные подгруппы. Факторгруппа. Лекция 23. Циклические группы. Лекция 24. Перестановки и шифры. Транспозиции. Лекция 25. Уравнение Коши. Лекция 26. Лексикографические перестановки с ограниченными префиксами. Дуальные методы.
6	Вычисления в числовых полях и группах Галуа	Лекция 27. Расширения полей. Степень расширения. Лекция 29. Алгебраические и трансцендентные элементы. Лекция 30. Алгебраические расширения полей. Минимальный многочлен алгебраического элемента. Лекция 31. Алгебраическое замыкание поля. Гомоморфизмы алгебраических расширений. Лекция 32. Сепарабельные многочлены. Сепарабельные расширения полей. Лекция 33. Теорема Артина. Расширения Галуа. Лекция 34. Группа Галуа расширения Галуа. Соответствие Галуа. Лекция 35. Основная теорема теории Галуа. Группа Галуа как группа перестановок корней многочлена. Лекция 36. Решение кубических уравнений в радикалах. Решение уравнений четвёртой степени в радикалах.

Рекомендуемая тематика *практических* занятий:

№ п/п	Наименование Темы	Содержание темы
1	Введение.	Решение сравнений. Построение конечных полей.
2	Вычисления в кольцах и алгебрах.	Подкольца, подалгебры, подполя. Гомоморфизмы колец. Вычисления в конечно порождённых кольцах. Вычисление идеалов факторкольца кольца многочленов от одной и многих переменных и операции над ними. Максимальные и простые идеалы.
3	Вычисления с многочленами.	Редукция и проверка свойств базисов Грёбнера полиномиальных идеалов. Отыскание базисов Грёбнера полиномиальных идеалов.
4	Решение систем алгебраических уравнений.	Вычисление аффинных алгебраических множеств и их идеалов. Радикалы идеалов и радикальные идеалы. Разложение на неприводимые компоненты.
5	Вычисления с группами и перестановками.	Подгруппы. Гомоморфизмы групп. Теорема Лагранжа. Нормальные группы и вычисления в них. Вычисления в циклических группах. Вычисления с перестановками. Разрешимые группы.
6	Вычисления в числовых полях и групп Галуа.	Вычисления в алгебраических числовых полях. Исследование полей разложений многочленов. Вычисление групп Галуа многочленов. Исследование разрешимости конкретных уравнений в радикалах.

Требования к самостоятельной работе обучающихся

1. Работа с лекционным материалом, предусматривающая проработку конспекта лекций и учебной литературы, по всем темам из п. 6 настоящей рабочей программы.
2. Выполнение домашнего задания, предусматривающего решение задач, выполнение упражнений, выдаваемых на практических занятиях, по всем темам из п. 6 настоящей рабочей программы.

Руководствуясь положениями статьи 47 и статьи 48 Федерального закона от 29 декабря 2012 г. N 273-ФЗ «Об образовании в Российской Федерации» научно-педагогические работники и иные лица, привлекаемые университетом к реализации данной образовательной программы, пользуются предоставленными академическими правами и свободами в части свободы преподавания, свободы от вмешательства в профессиональную деятельность; свободы выбора и использования педагогически обоснованных форм, средств, методов обучения и воспитания; права на творческую инициативу, разработку и применение авторских программ и методов обучения и воспитания в пределах реализуемой образовательной программы и отдельной дисциплины.

Исходя из рамок, установленных учебным планом по трудоемкости и видам учебной работы по дисциплине, преподаватель самостоятельно выбирает тематику занятий по формам и количеству часов проведения контактной работы: лекции и иные учебные занятия, предусматривающие преимущественную передачу учебной информации

преподавателем и (или) занятия семинарского типа (семинары, практические занятия, практикумы, лабораторные работы, коллоквиумы и иные аналогичные занятия), и (или) групповые консультации, и (или) индивидуальную работу обучающихся с преподавателем, в том числе индивидуальные консультации (по курсовым работам/проектам – при наличии курсовой работы/проекта по данной дисциплине в учебном плане).

Рекомендуемая тематика занятий максимально полно реализуется в контактной работе с обучающимися очной формы обучения. В случае реализации образовательной программы в заочной / очно-заочной форме трудоемкость дисциплины сохраняется, однако объем учебного материала в значительной части осваивается обучающимися в форме самостоятельной работы. При этом требования к ожидаемым образовательным результатам обучающихся по данной дисциплине не зависят от формы реализации образовательной программы.

7. Методические рекомендации по видам занятий

Лекционные занятия.

В ходе лекционных занятий обучающимся рекомендуется выполнять следующие действия. Вести конспектирование учебного материала. Обращать внимание на категории, формулировки, раскрывающие содержание тех или иных явлений и процессов, научные выводы и практические рекомендации по их применению. Задавать преподавателю уточняющие вопросы с целью уяснения теоретических положений, разрешения спорных ситуаций.

Желательно оставить в рабочих конспектах поля, на которых во внеаудиторное время можно сделать пометки из рекомендованной литературы, дополняющие материал прослушанной лекции, а также подчеркивающие особую важность тех или иных теоретических положений.

Практические и семинарские занятия.

На практических и семинарских занятиях в зависимости от темы занятия выполняется поиск информации по решению проблем, практические упражнения, контрольные работы, выработка индивидуальных или групповых решений, итоговое обсуждение с обменом знаниями, участие в круглых столах, разбор конкретных ситуаций, командная работа, представление портфолио и т.п.

Самостоятельная работа.

Самостоятельная работа осуществляется в виде изучения литературы, эмпирических данных по публикациям и конкретных ситуаций из практики, подготовке индивидуальных работ, работа с лекционным материалом, самостоятельное изучение отдельных тем дисциплины; поиск и обзор литературы и электронных источников; чтение и изучение учебника и учебных пособий.

8. Фонд оценочных средств

8.1. Перечень компетенций с указанием этапов их формирования в процессе освоения образовательной программы в рамках учебной дисциплины

Основными этапами формирования указанных компетенций при изучении обучающимися дисциплины являются последовательное изучение содержательно связанных между собой тем учебных занятий. Изучение каждой темы предполагает овладение обучающимися необходимыми компетенциями. Результат аттестации

обучающихся на различных этапах формирования компетенций показывает уровень освоения компетенций.

Контролируемые разделы (темы) дисциплины	Индекс контроли-руемой компетенции (или её части)	Оценочные средства по этапам формирования компетенций
		текущий контроль по дисциплине
Введение	ПКС-4	Опрос, решение задач.
Вычисления в кольцах и алгебрах		Опрос, решение задач, контрольная работа.
Вычисления с многочленами		Опрос, решение задач, контрольная работа.
Решение систем алгебраических уравнений		Опрос, решение задач, контрольная работа.
Вычисления с группами перестановок		Опрос, решение задач, контрольная работа.
Вычисления в числовых полях и группах Галуа		Опрос, решение задач, контрольная работа.

8.2. Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений и навыков и (или) опыта деятельности процессе текущего контроля

Примеры вопросов для устного опроса:

Тема 1. Введение

	Вопрос
Оценка «удовлетворительно» (зачтено) или низкой уровень освоения компетенции	Перечислить основные алгоритмы теории чисел и конечных полей, встречающиеся в задаче дискретного логарифмирования.
Оценка «хорошо» (зачтено) или повышенный уровень освоения компетенции	Доказать основные свойства колец классов вычетов.
Оценка «отлично» (зачтено) или высокий уровень освоения компетенции	Доказать основные свойства конечных полей.

Тема 2. Вычисления в кольцах и алгебрах

	Вопрос
Оценка «удовлетворительно» (зачтено) или низкой уровень освоения компетенции	Дать определения кольца, подкольца, алгебры. Сформулировать Критерий неприводимости Эйзенштейна. Дать определение гомоморфизма колец, подкольца, порождённого множеством, идеала кольца, идеала, порождённого множеством, главного идеала. Как устроено отношение сравнения в кольце по идеалу. Дать определение максимального идеала, простого идеала.

Оценка «хорошо» (зачтено) или повышенный уровень освоения компетенции	Доказать критерий неприводимости Эйзенштейна. Дать определение полиномиальной функции. Привести примеры гомоморфизмов подстановки и редукции. Обосновать, что есть образ и прообраз подкольца при гомоморфизме. Доказать простейшие свойства идеалов. Обосновать, что есть образ и прообраз идеала при гомоморфизме. Доказать основные свойства произведения идеалов. Доказать признак максимального и простого идеалов.
Оценка «отлично» (зачтено) или высокий уровень освоения компетенции	Доказать основные свойства подкольца, порождённого множеством. Доказать основные свойства результата факторизации гомоморфизма. Теорема об изоморфизме. Доказать основные свойства результата факторизация гомоморфизма по двум идеалам. Доказать теорему относительно максимальных и простых идеалов в кольце главных идеалов.

Тема 3. Вычисления с многочленами

	Вопрос
Оценка «удовлетворительно» (зачтено) или низкой уровень освоения компетенции	Дать определение нётерова кольца. Сформулировать теорему Гильберта о базисе. Как определить отношение порядка на множестве одночленов. Дать определение базиса Грёбнера полиномиальных идеалов. В чем заключается минимальность и редукция базиса Грёбнера.
Оценка «хорошо» (зачтено) или повышенный уровень освоения компетенции	Воспроизвести алгоритм деления в кольце многочленов от многих переменных. Что есть базисы Грёбнера полиномиальных идеалов, доказать их свойства.
Оценка «отлично» (зачтено) или высокий уровень освоения компетенции	Воспроизвести алгоритм Бухбергера. Доказать соответствующие теоремы о минимальном и редуцированном базисе Грёбнера.

Тема 4. Решение систем алгебраических уравнений

	Вопрос
Оценка «удовлетворительно» (зачтено) или низкой уровень освоения компетенции	Дать определение аффинного алгебраического множества, сформулировать его основные свойства. Дать определение идеала множества, сформулировать его основные свойства. Дать определение радикала идеала. Дать определение аффинного алгебраического многообразия. Сформулировать слабую сильную теоремы Гильберта о нулях. Сильная теорема Гильберта о нулях.
Оценка «хорошо» (зачтено) или повышенный уровень освоения компетенции	Доказать основные свойства алгебраических множеств. Доказать основные свойства идеала множества. В чем заключается разложение алгебраического множества на неприводимые компоненты.
Оценка «отлично» (зачтено) или высокий уровень освоения компетенции	Доказать слабую и сильную теоремы Гильберта о нулях. Вывести соответствие между алгебраическими множествами и идеалами. В чем заключаются приложения базисов Грёбнера к решению систем

	полиномиальных уравнений.

Тема 5. Вычисления с группами и перестановками

	Вопрос
Оценка «удовлетворительно» (зачтено) или низкой уровень освоения компетенции	Дать определение группы, гомоморфизма групп. Сформулировать основные свойства гомоморфизмов. Сформулировать признак подгруппы. Что есть отношение эквивалентности в группе по подгруппе и смежные классы. Перечислить свойства смежных классов. Сформулировать теорему Лагранжа. Дать определение и привести примеры нормальных подгрупп, циклических групп, симметрических групп.
Оценка «хорошо» (зачтено) или повышенный уровень освоения компетенции	Доказать основные свойства гомоморфизмов групп. Обосновать, что есть образ и прообраз подгруппы при помощи гомоморфизма. Доказать теорему Лагранжа. Обосновать, что есть образ и прообраз нормальной подгруппы при гомоморфизме. Доказать признак инъективности гомоморфизма. Доказать основные свойства смежных классов по нормальной подгруппе. Обосновать, что есть образ циклической группы при гомоморфизме. Доказать основные свойства группы перестановок.
Оценка «отлично» (зачтено) или высокий уровень освоения компетенции	Доказать теорему о факторизации гомоморфизма по нормальной подгруппе и свойства результата факторизации. Обосновать, что есть образ подгруппы, порождённой множеством, с помощью гомоморфизма. Провести классификацию циклических групп с точностью до изоморфизма. Сформулировать понятие разрешимой группы, доказать основные свойства.

Тема 6. Вычисления в числовых полях и групп Галуа

	Вопрос
Оценка «удовлетворительно» (зачтено) или низкой уровень освоения компетенции	Дать определение расширения полей, степени расширения, конечного расширения. Сформулировать теорему транзитивности конечных расширений. Что есть алгебраические и трансцендентные элементы? Дать определение минимального многочлена алгебраического элемента. Сформулировать признак алгебраического элемента. Дать определение гомоморфизма простого алгебраического расширения в алгебраически замкнутое поле. Что есть поле разложения многочлена? Дать определения нормальных и сепарабельных расширений полей. Что есть группа Галуа расширения полей? Дать определение расширения Галуа. Сформулировать основную теорему теории Галуа.
Оценка «хорошо» (зачтено) или повышенный уровень освоения компетенции	Доказать теорему транзитивности конечных расширений. Доказать свойства минимального многочлена алгебраического элемента. Доказать теорему транзитивности алгебраических расширений. Что есть сопряжённые элементы поля над подполем?

	Сформулировать теорему о примитивном элементе. Как действую автоморфизмы поля над подполем? Что есть стабилизатор группы автоморфизмов, перечислить его свойства. Дать понятие разрешимости уравнения в радикалах.
Оценка «отлично» (зачтено) или высокий уровень освоения компетенции	Оценить порядок группы Галуа конечного сепарабельного расширения. Доказать свойство расширения неподвижного поля группы автоморфизмов и свойство стабилизатора группы автоморфизмов. Доказать основную теорему теории Галуа. В чем заключается проблема разрешимости алгебраических уравнений в радикалах.

Типовые задачи для решения:

Тема 1. Введение

	Задача
Оценка «удовлетворительно» (зачтено) или низкой уровень освоения компетенции	Решить сравнение: $3x \equiv 1 \pmod 5$.
Оценка «хорошо» (зачтено) или повышенный уровень освоения компетенции	Записать таблицы сложения и умножения для кольца $\mathbb{Z}/(9)$. Найти делители нуля, обратимые элементы и обратные к ним.
Оценка «отлично» (зачтено) или высокий уровень освоения компетенции	Построить поле $\mathbb{F}_8$. Подобрать подходящие неприводимые многочлены, найти базис поля $\mathbb{F}_q$ над простым подполем $\mathbb{F}_p$, найти примитивный корень поля, построить таблицу индексов, найти все примитивные корни степени $q-1$ из единицы в $\mathbb{F}_q$, найти группу Галуа $G(\mathbb{F}_q/\mathbb{F}_p)$, найти все подполя поля $\mathbb{F}_q$.

Тема 2. Вычисления в кольцах и алгебрах

	Задача
Оценка «удовлетворительно» (зачтено) или низкой уровень освоения компетенции	Является ли кольцом множество матриц вида $\begin{pmatrix} x & y \\ -3y & x \end{pmatrix}$, где x, y – целые числа. Если да, то найти обратимые элементы и делители нуля этого кольца.
Оценка «хорошо» (зачтено) или повышенный уровень освоения компетенции	Доказать, что если (0) и (1) – единственные идеалы кольца A, то A – поле.
Оценка «отлично» (зачтено) или высокий уровень освоения компетенции	Построить кольцо $\mathbb{Z}/(9)$. Найти все идеалы $a_1, a_2, \ldots$ в этом кольце. Построить $(\mathbb{Z}/(9))/a_1$, $(\mathbb{Z}/(9))/a_2, \ldots$ Указать в построенных кольцах делители нуля, обратимые элементы, идеалы.

Тема 3. Вычисления с многочленами

	Задача
Оценка «удовлетворительно»	Построить минимальный редуцированный базис Грёбнера для идеала $(X^2-1, (X-1)Y, (X+1)Z)$.

(зачтено) или низкой уровень освоения компетенции	
Оценка «хорошо» (зачтено) или повышенный уровень освоения компетенции	Доказать, что гомоморфный образ нётерова кольца есть нётерово кольцо.
Оценка «отлично» (зачтено) или высокий уровень освоения компетенции	Пусть S – подкольцо кольца R, S – нётерово кольцо, R – конечно порождено как модуль над S. Доказать, что R – нётерово кольцо.

Тема 4. Решение систем алгебраических уравнений

	Задача
Оценка «удовлетворительно» (зачтено) или низкой уровень освоения компетенции	Нарисовать следующие аффинные алгебраические множества в $\mathbb{C}^2$: $Z(X^2 + 4Y^2 + 2X - 16Y + 1)$; $Z(X^2 - Y^2)$.
Оценка «хорошо» (зачтено) или повышенный уровень освоения компетенции	Пусть $\mathfrak{a} = (X^2 - YZ, XZ - X)$ – идеал в $k[X, Y, Z]$. Разложить $V = Z(\mathfrak{a})$ в объединение неприводимых компонент.
Оценка «отлично» (зачтено) или высокий уровень освоения компетенции	Применяя базис Грёбнера, решить систему уравнений: $\begin{cases} X^2 = 1, \\ (X-1)Y = 0, \\ (X+1)Z = 0. \end{cases}$

Тема 5. Вычисления с группами и перестановками

	Задача
Оценка «удовлетворительно» (зачтено) или низкой уровень освоения компетенции	Пусть $\lambda \in \mathbb{C}$. Является ли группой относительно умножения множество ненулевых матриц вида $\begin{pmatrix} x & y \\ \lambda y & x \end{pmatrix}$, где $x, y \in \mathbb{C}$.
Оценка «хорошо» (зачтено) или повышенный уровень освоения компетенции	Найти факторгруппу $4\mathbb{Z} / 12\mathbb{Z}$.
Оценка «отлично» (зачтено) или высокий уровень освоения компетенции	Найти все гомоморфизмы аддитивных групп $\mathbb{Z} / 6\mathbb{Z} \to \mathbb{Z} / 6\mathbb{Z}$, $\mathbb{Z} / 6\mathbb{Z} \to \mathbb{Z} / 18\mathbb{Z}$, $\mathbb{Z} / 18\mathbb{Z} \to \mathbb{Z} / 6\mathbb{Z}$.

Тема 6. Вычисления в числовых полях и группах Галуа

	Задача
Оценка «удовлетворительно» (зачтено) или низкой уровень освоения компетенции	Найти минимальный многочлен числа z над полем k. Найти все гомоморфизмы поля $k(z)$ в поле $\mathbb{C}$ комплексных чисел. $z = \sqrt{5}$, $k = \mathbb{Q}$.

Оценка «хорошо» (зачтено) или повышенный уровень освоения компетенции	Найти степень алгебраического числового поля K, порождённого корнями многочлена $f(X)$, указать базис K над $\square$. $f(X) = X^2 - 7$.
Оценка «отлично» (зачтено) или высокий уровень освоения компетенции	Доказать, что всякое расширение полей степени 2 нормально.

Типовые контрольные задания:

1. Решить сравнения:
   1) $3x \equiv 1 \pmod 5$, 2) $3x \equiv 8 \pmod{13}$.
2. Решить системы сравнений:
   1) $\begin{cases} x \equiv 2 \pmod 5, \\ x \equiv 8 \pmod{11}. \end{cases}$ 2) $\begin{cases} x \equiv 1 \pmod{25}, \\ x \equiv 2 \pmod 4, \\ x \equiv 3 \pmod 7, \\ x \equiv 4 \pmod 9. \end{cases}$
3. Является ли кольцом множество матриц вида $\begin{pmatrix} x & y \\ -3y & x \end{pmatrix}$, где x, y – целые числа. Если да, то найти обратимые элементы и делители нуля этого кольца.
4. Пусть A – множество функций $f: \square \to \square$ вида $f(x) = ax + b$, где $a, b \in \square$. Для $f, g \in A$, $x \in \square$ положим $(f + g)(x) = f(x) + g(x)$, $fg = f \circ g$ – композиция отображений. Будет ли A кольцом?
5. Доказать, что если (0) и (1) – единственные идеалы кольца A, то A – поле.
6. Построить кольцо $\square / (9)$. Найти все идеалы a_1, a_2,… в этом кольце. Построить $(\square / (9)) / a_1$, $(\square / (9)) / a_2$,… Указать в построенных кольцах делители нуля, обратимые элементы, идеалы.
7. Пусть R – нётерово кольцо, $\varphi: R \to R$ – сюръективный гомоморфизм. Доказать, что φ инъективен. У к а з а н и е: Рассмотреть $\mathrm{Ker}(\varphi^j)$, $j \geq 0$.
8. Пусть S – подкольцо кольца R, S – нётерово кольцо, R – конечно порождено как модуль над S. Доказать, что R – нётерово кольцо.
9. Построить минимальный редуцированный базис Грёбнера для идеалов
   a. $(X^2 - 1, (X - 1)Y, (X + 1)Z)$;
   b. $(X^2 - 1, (X - 1)Y, (X - 1)Z)$.
10. Нарисовать следующие аффинные алгебраические множества в $\square^2$:
    1) $Z(X^2 + 4Y^2 + 2X - 16Y + 1)$; 2). $Z(X^2 - Y^2)$.
    Будут ли эти множества многообразиями? Ответ обосновать.
11. Найти идеалы $I(V)$ следующих множеств:
    1) $V = Z(X - Y, X - Z) \subset \square^3$; 2). $V = Z(X^4 - Y^2) \subset \square^2$;
12. Найти идеалы $I(V)$ следующих множеств:
    1) $V = \{2, 3, 4, 5\} \subset \square^1$; 2). $V = Z(X^2 - 2XY + Y^2) \subset \square^2$.
13. Найти радикал $\sqrt{a}$ идеала a для
    1) $a = (X^2, Y) \subset k[X, Y]$; 2). $a = (X - Y, Y) \subset k[X, Y]$;
14. Пусть $a = (X^2 + Y^2 - 1, Y - 1)$. Найти многочлен $f \in I(Z(a))$, такой, что $f \notin a$.
15. Пусть k – бесконечное поле. Доказать, что прямые в $\square^2(k)$ и $\square^3(k)$ являются аффинными алгебраическими многообразиями.

16. Пусть a = $(X^2 - YZ,\ XZ - X)$ – идеал в $k[X, Y, Z]$. Разложить $V = Z(\text{a})$ в объединение неприводимых компонент.
17. Применяя базис Грёбнера, решить систему уравнений: $\begin{cases} X^2 = 1, \\ (X-1)Y = 0, \\ (X+1)Z = 0. \end{cases}$
18. Пусть $\lambda \in \square$. Является ли группой относительно умножения множество ненулевых матриц вида $\begin{pmatrix} x & y \\ \lambda y & x \end{pmatrix}$, где $x, y \in \square$.
19. Доказать, что если в группе G выполняется тождество $x^2 = 1$, то G - абелева.
20. Найти все гомоморфизмы аддитивных групп $\square/6\square \to \square/6\square$, $\square/6\square \to \square/18\square$.
21. Найти порядок элемента $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 1 & 5 & 4 \end{pmatrix} \in S_5$.
22. Найти порядок элемента $\begin{pmatrix} 0 & i \\ 1 & 0 \end{pmatrix} \in GL_2(\square)$.
23. Найти все элементы группы S_4, коммутирующие с перестановкой (12)(34).
24. Найти факторгруппу $4\square/12\square$.
25. Пусть G – группа. Доказать, что множество H внутренних автоморфизмов группы G является нормальной подгруппой группы $\mathrm{Aut}(G)$ всех автоморфизмов группы G.
26. Найти минимальный многочлен числа z над полем k. Найти все гомоморфизмы поля $k(z)$ в поле $\square$ комплексных чисел.

    1) $z = \sqrt{5}$, $k = \square$, 2) $z = \sqrt[3]{5}$, $k = \square$.
27. Доказать, что $\square(\alpha + \beta) = \square(\alpha, \beta)$ и вычислить $[\square(\alpha + \beta) : \square]$.

    1) $\alpha = \sqrt{3}$, $\beta = \sqrt[3]{2}$, 2) $\alpha = \sqrt{2}$, $\beta = i$.
28. Пусть m – целое, свободное от кубов, $K = \mathrm{Q}(\sqrt[3]{m})$. Найти все гомоморфизмы из K в $\square$.
29. Пусть θ – корень уравнения $x^3 + 2x + 2 = 0$, $K = \square(\theta)$ и $\alpha = \theta - \theta^2$. Найти минимальный многочлен элемента α над K.
30. Доказать, что всякое расширение полей степени 2 нормально.
31. Привести пример нормального расширения степени 2, не являющегося сепарабельным.
32. Является ли сепарабельным многочлен $f = X^3 + X + 2$ над $\square$, над $\square$, над $\square_3$?
33. Найти все автоморфизмы полей $\square(\sqrt{2})$, $\square(\sqrt{2} + \sqrt{7})$, $\mathrm{Q}(\sqrt[3]{m})$.
34. Вычислить группу Галуа поля разложения многочлена $X^p - 1$ над $\square$, где p – простое число.
35. Найти группы Галуа многочленов над $\square$:
    1) $X^3 - 12X + 8$;
    2) $X^3 - 3X + 1$.
36. Вычислить группу Галуа поля разложения многочлена $X^3 - 1$ над $\square$.
37. Вычислить группу Галуа поля разложения многочлена $X^2 - 2$ над $\square$.
38. Вычислить группу Галуа поля разложения многочлена $X^2 + X + 1$ над $\square$.
39. Вычислить группу Галуа расширения $\mathrm{Q}(\sqrt{2} + \sqrt{3})/\mathrm{Q}$.
40. С помощью основной теоремы теории Галуа найти все промежуточные поля для расширения $\square(\sqrt{2}, \sqrt{3})/\square$.
41. Решить в радикалах уравнение $X^3 - 19X + 30$.

42. Решить в радикалах уравнение $X^4 + 4X + 2$.

8.3. Перечень вопросов и заданий для промежуточной аттестации по дисциплине

Вопросы для промежуточного контроля (зачета с оценкой)

1. Примеры колец и полей. Подкольца и подполя. Алгебры над кольцом и над полем.
2. Алгебра многочленов от одной переменной, её свойства. Многочлены от многих переменных, его факториальность.
3. Гомоморфизмы колец, полей и алгебр, их свойства примеры.
4. Идеалы коммутативных колец, их свойства.
5. Подкольца и идеалы, порождённые множеством, их свойства, их элементы. Кольца главных идеалов.
6. Факторизация колец и гомоморфизмов по идеалам.
7. Присоединение корней многочлена. Алгебраически замкнутое поле.
8. Сумма и произведение идеалов. Деление идеалов. Свойства операций над идеалами.
9. Максимальные и простые идеалы, их свойства.
10. Нётеровы кольца. Эквивалентные условия нётеровости. Теорема Гильберта о базисе.
11. Представление многочленов. Арифметика многочленов. Евклидовы алгоритмы для многочленов.
12. Алгоритм факторизации многочленов по модулю p.
13. Алгоритмы факторизации многочленов над конечными полями. Алгоритм Берлекэмпа.
14. Алгоритмы факторизации многочленов над и над .
15. Отношение порядка на множестве одночленов. Алгоритм деления в кольце многочленов от многих переменных. Мономиальные идеалы. Лемма Диксона.
16. Базисы Грёбнера полиномиальных идеалов, их свойства.
17. Зацепление многочленов. Алгоритм Бухбергера.
18. Минимальный и редуцированный базисы Грёбнера, их свойства.
19. Аффинные алгебраические множеств, операции над ними. Топология Зарискогo. Идеал множества.
20. Радикал идеала, его свойства. Радикальные идеалы. Свойства идеалов множеств.
21. Понятие неприводимости. Аффинные алгебраические многообразия. Идеал многообразия.
22. Теорема Гильберта о нулях. Соответствие между алгебраическими множествами и идеалами.
23. Алгоритм вычисления радикалов идеалов в полиномиальных кольцах.
24. Разложение алгебраических множеств на неприводимые компоненты.
25. Алгоритм решения систем полиномиальных уравнений с помощью базисов Грёбнера.
26. Группы. Гомоморфизмы групп, их свойства. Подгруппы. Пересечение подгрупп. Образ и прообраз группы при гомоморфизме. Образ гомоморфизма.
27. Отношения эквивалентности в группе по подгруппе. Смежные классы. Индекс подгруппы в группе. Теорема Лагранжа.
28. Нормальные подгруппы. Образ и прообраз нормальной подгруппы при гомоморфизме. Ядро гомоморфизма.
29. Отношение эквивалентности в группе по нормальной подгруппе. Факторгруппа. Факторизация гомоморфизмов. Теоремы об изоморфизмах.
30. Подгруппа, порождённая множеством. Образ с помощью гомоморфизма.
31. Циклические группы. Обращение теоремы Лагранжа для циклических групп.
32. Разрешимые группы, их свойства. Примеры разрешимых групп.

33. Алгоритмы возведения матрицы в степень. Быстрое умножение матриц. Обращение матриц.
34. Перестановки и шифры. Транспозиции. Разложение перестановки в произведение циклов и транспозиций. Системы образующих симметрической группы.
35. Разрешимость и неразрешимость групп перестановок.
36. Генерация лексикографической перестановки.
37. Генерация перестановок методом сложные замены. Простые замены. Переходы простых изменений.
38. Генерация перестановок методом общей структуры. Пропуск нежелательных блоков.
39. Лексикографические перестановки с ограниченными префиксами.
40. Дуальные методы генерирования перестановок.
41. Расширения полей. Степень расширения. Конечные расширения. Теорема транзитивности конечных расширений.
42. Алгебраические и трансцендентные элементы. Стандартные представления алгебраических чисел. Матричные представления алгебраических чисел.
43. Минимальный многочлен алгебраического элемента и его вычисление. Признак алгебраического элемента.
44. Алгебраические расширения полей. Свойства алгебраических расширений. Алгебраическое замыкание поля.
45. Гомоморфизмы алгебраических расширений.
46. Поля разложения многочленов и нормальные расширения.
47. Сепарабельные элементы. Сепарабельные многочлены. Сепарабельные расширения полей. Сепарабельная степень.
48. Группа автоморфизмов поля над подполем. Неподвижное поле группы автоморфизмов. Теорема Артина.
49. Расширения Галуа, их свойства. Группа Галуа расширения Галуа.
50. Соответствие Галуа. Основная теорема теории Галуа.
51. Группа Галуа как группа перестановок корней многочлена. Примеры. Критерий разрешимости уравнения в радикалах.
52. Решение кубических уравнений в радикалах.
53. Решение уравнений четвёртой степени в радикалах.
54. Метод резольвент вычисления групп Галуа для числовых полей степени 3, 4 и 5.

8.4. Планируемые уровни сформированности компетенций обучающихся и критерии оценивания

Уровни	Содержательное описание уровня	Основные признаки выделения уровня (этапы формирования компетенции, критерии оценки сформированности)	Пятибалльная шкала (академическая) оценка	Двухбалльная шакала, зачет	БРС, % освоения (рейтинговая оценка)
Повышенный	Творческая деятельность	*Включает нижестоящий уровень.* Умение самостоятельно принимать решение, решать проблему/задачу теоретического и прикладного характера на основе изученных	отлично	зачтено	86-100

		методов, приемов, технологий			
Базовый	Применение знаний и умений в более широких контекстах учебной и профессиональной деятельности, нежели по образцу с большей степени самостоятельности и инициативы	*Включает нижестоящий уровень.* Способность собирать, систематизировать, анализировать и грамотно использовать информацию из самостоятельно найденных теоретических источников и иллюстрировать ими теоретические положения или обосновывать практику применения	хорошо		71-85
Удовлетворительный (достаточный)	Репродуктивная деятельность	Изложение в пределах задач курса теоретически и практически контролируемого материала	удовлетворительно		55-70
Недостаточный	Отсутствие признаков удовлетворительного уровня		неудовлетворительно	не зачтено	Менее 55

9. Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины.

Основная литература

1. Смолин, Ю.Н. *Алгебра и теория чисел* : учеб. пособие / Ю.Н. Смолин. — 5-е изд., стер.—Москва : ФЛИНТА, 2017. — 464 с. - ISBN 978-5-9765-0050-1. - Текст : электронный. - URL: https://znanium.com/catalog/product/1034573.
2. Шевцов, Г. С. *Линейная алгебра: теория и прикладные аспекты*: Учебное пособие / Г.С. Шевцов. - 3-е изд., испр. и доп. - М.: Магистр: НИЦ ИНФРА-М, 2019. - 544 с. - ISBN 978-5-9776-0258-7. - Текст : электронный. - URL: https://znanium.com/catalog/product/1015326.

Дополнительная литература

1. Математические методы защиты информации: учеб. пособие / *С. И. Алешников, Ю. Ф. Болтнев*; Балт. гос. ун-т им. И. Канта. - Калининград: БФУ им. И. Канта. Ч.1: Алгебраические методы: учебное пособие. -2015, **on-line**, 156 с. ЭБС Кантиана
2. Математические методы защиты информации: учеб. пособие/ *С. И. Алешников, А. В. Пышкин*; Балт. федер. ун-т им. И. Канта. – Калининград. Ч.2: Методы алгебраической теории чисел: учебное пособие. – 2015, **on-line**, 121 с. ЭБС Кантиана

10. Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины (модуля).

- НЭБ Национальная электронная библиотека, диссертации и прочие издания
- eLIBRARY.RU Научная электронная библиотека, книги, статьи, тезисы докладов конференций
- Гребенников Электронная библиотека ИД журналы
- ЭБС Лань книги, журналы
- ЭБС Консультант студента
- ПРОСПЕКТ ЭБС
- ЭБС ZNANIUM.COM
- РГБ Информационное обслуживание по МБА
- БЕН РАН
- Электронно-библиотечная система (ЭБС) Кантитана (https://elib.kantiana.ru/)

11. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине.

Программное обеспечение обучения включает в себя:

- система электронного образовательного контента БФУ им. И. Канта – www.lms-3.kantiana.ru, обеспечивающую разработку и комплексное использование электронных образовательных ресурсов;
- серверное программное обеспечение, необходимое для функционирования сервера и связи с системой электронного обучения через Интернет;
- корпоративная платформа Microsoft Teams;
- установленное на рабочих местах обучающихся ПО: Microsoft Windows 7, Microsoft Office Standart 2010, антивирусное программное обеспечение Kaspersky Endpoint Security.
- специализированное ПО не требуется.

12. Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине.

Для проведения занятий лекционного типа, практических и семинарских занятий используются специальные помещения (учебные аудитории), оборудованные техническими средствами обучения – мультимедийной проекционной техникой. Для проведения занятий лекционного типа используются наборы демонстрационного оборудования.

Для проведения лабораторных работ, (практических занятий – при необходимости) используются специальные помещения (учебные аудитории), оснащенные специализированным лабораторным оборудованием: персональными компьютерами с возможностью выхода в интернет и с установленным программным обеспечением, заявленным в п.11.

Для проведения групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации используются специальные помещения (учебные аудитории), оборудованные специализированной мебелью (для обучающихся), меловой / маркерной доской.

Для организации самостоятельной работы обучающимся предоставляются помещения, оснащенные компьютерной техникой с возможностью подключения к сети «Интернет» и обеспечением доступа в электронную информационно-образовательную среду университета.

Для обучения инвалидов и лиц с ограниченными возможностями здоровья университетом могут быть представлены специализированные средства обучения, в том числе технические средства коллективного и индивидуального пользования.

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
федеральное государственное автономное образовательное учреждение высшего образования «Балтийский федеральный университет имени Иммануила Канта»
Институт физико-математических наук и информационных технологий

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

«ТЕОРИЯ АВТОМАТОВ»

Шифр: 10.05.01
Специальность: «Компьютерная безопасность»
Специализация: «Математические методы защиты информации»
Квалификация (степень) выпускника: специалист по защите информации

Калининград
2022

Лист согласования

Составитель: БОЛТНЕВ ЮРИЙ ФЕДОРОВИЧ. старший преподаватель

Рабочая программа утверждена на заседании учебно-методического совета института физико-математических наук и информационных технологий
Протокол № 01/22 от «01» февраля 2022 г.

Председатель учебно-методического совета института физико-математических наук и информационных технологий
Первый заместитель директора ИФМНиИТ, к. ф.-м. н., доцент — Шпилевой А. А

Ведущий менеджер — Е.П.Ставицкая

СОДЕРЖАНИЕ

1. **Наименование дисциплины:** «ТЕОРИЯ АВТОМАТОВ»

Целью освоения дисциплины «Теория автоматов» является овладение основами теории формальных языков, грамматик и автоматов, что заложит фундамент понимания принципов построения современных информационных систем.

2. **<u>Перечень планируемых результатов обучения по дисциплине, соотнесенных с планируемыми результатами освоения образовательной программы</u>**

Код компетенции	Результаты освоения образовательной программы (ИДК)	Результаты обучения по дисциплине
ПКС-7 Способность проводить анализ и участвовать в разработке математических моделей безопасности компьютерных систем	ПКС-7.1. Знает математические методы моделирования безопасных компьютерных систем ПКС-7.2. Осуществляет анализ математических моделей безопасности компьютерных систем ПКС-7.3. Участвует в разработке математических моделей безопасности компьютерных систем	• **Знать** основы теории формальных языков, грамматик и автоматов, принципы построения конечных, магазинных автоматов и машин Тьюринга; основные алгоритмически неразрешимые проблемы информатики, связанные с формальными языками • **Уметь** использовать полученные теоретические знания для решения конкретных прикладных задач, производить математические расчеты в стандартных постановках, производить содержательный анализ результатов вычислений, строить контекстно-свободную грамматику, порождающую указанный язык; строить конечный автомат, принимающий регулярный язык и детерминировать его; строить магазинный автомат, принимающий указанный контекстно-свободный язык; строить грамматику, порождающую указанный контекстно-зависимый язык; строить машину Тьюринга, принимающую указанный перечислимый язык или вычисляющую заданную функцию • **Владеть** навыками применения понятий и методов дисциплины для решения различных задач, используемых в дальнейшей учебной и профессиональной деятельности; навыками моделирования перечисленных грамматик и автоматов на компьютере

3. **<u>Место дисциплины в структуре ООП ВО</u>**

Дисциплина «*Теория автоматов»* представляет собой дисциплину части, формируемой участниками образовательных отношений, блока дисциплин подготовки обучающихся.

4. Виды учебной работы по дисциплине.

Виды учебной работы по дисциплине зафиксированы учебным планом основной профессиональной образовательной программы по указанному направлению и профилю, выражаются в академических часах. Часы контактной работы и самостоятельной работы студента и часы, отводимые на процедуры контроля, могут различаться в учебных планах ОПОП по формам обучения. Объем контактной работы включает часы контактной аудиторной работы (лекции/практические занятия/ лабораторные работы), контактной внеаудиторной работы (контроль самостоятельной работы), часы контактной работы в период аттестации. Контактная работа, в том числе может проводиться посредством электронной информационно-образовательной среды университета с использованием ресурсов сети Интернет и дистанционных технологий

5. Содержание дисциплины, структурированное по темам (разделам)

Исходя из рамок, установленных учебным планом по трудоемкости и видам учебной работы по дисциплине, преподаватель самостоятельно выбирает тематику занятий по формам и количеству часов проведения контактной работы: лекции и иные учебные занятия, предусматривающие преимущественную передачу учебной информации преподавателем и (или) занятия семинарского типа (семинары, практические занятия, практикумы, лабораторные работы, коллоквиумы и иные аналогичные занятия), и (или) групповые консультации, и (или) индивидуальную работу обучающихся с преподавателем, в том числе индивидуальные консультации (по курсовым работам/проектам – при наличии курсовой работы/проекта по данной дисциплине в учебном плане). Рекомендуемая тематика занятий максимально полно реализуется в контактной работе со студентами очной формы обучения. В случае реализации образовательной программы в заочной / очно-заочной форме трудоемкость дисциплины сохраняется, однако объем учебного материала в значительной части осваивается студентами в форме самостоятельной работы. При этом требования к ожидаемым образовательным результатам студентов по данной дисциплине не зависят от формы реализации образовательной программы.

Содержание основных разделов и тем курса

1. ФОРМАЛЬНЫЕ ЯЗЫКИ. КОНТЕКСТНО-СВОБОДНЫЕ ГРАММАТИКИ.

Алфавиты и языки. Формальное определение грамматики. Типы грамматик. Деревья вывода в контекстно-свободных грамматиках. Операторы регулярных выражений. Построение регулярных выражений. Применение регулярных выражений. Регулярные языки.

2. КОНЕЧНЫЕ И МАГАЗИННЫЕ АВТОМАТЫ.

Формальное определение конечного автомата. Недетерминированные конечные автоматы. Конечные автоматы и языки типа 3. Конечные автоматы и регулярные выражения. Формальное определение магазинного автомата. Представление контекстно-свободных языков магазинными автоматами

3. КОНТЕКСТНО-ЗАВИСИМЫЕ ГРАММАТИКИ. МАШИНЫ ТЬЮРИНГА

Иерархия грамматик по Хомскому. Контекстно-зависимые грамматики. Системы Линденмайера. Основные понятия и принципы действия. Примеры машин Тьюринга для

принятия перечислимого языка и для вычисления функции. Модификации машин Тьюринга. Односторонние и многоленточные машины. Недетерминированные машины Тьюринга.

6. Рекомендуемая тематика учебных занятий в форме контактной работы

Рекомендуемая тематика учебных занятий лекционного типа (предусматривающих преимущественную передачу учебной информации преподавателями):

№	Наименование раздела	Темы лекций
1	Формальные языки. Контекстно-свободные грамматики	Лекции 1 - 2. Формальные языки и грамматики Лекции 3 - 4. Контекстно-свободные грамматики и регулярные выражения
2	Конечные и магазинные автоматы	Лекции 5 - 6. Детерминированные и недетерминированные конечные автоматы. Лекции 7 - 8. Магазинные автоматы. Представление контекстно-свободных языков магазинными автоматами
3	.Контекстно-зависимые грамматики. Машины Тьюринга	Лекции 9 – 10. Иерархия грамматик по Хомскому. Контекстно-зависимые грамматики Лекции 11 – 12. Машины Тьюринга. Модификации машин Тьюринга Лекции 13 – 14. Недетерминированные машины Тьюринга Труднорешаемые задачи.

Тематика практических занятий

1. Формальные языки. Контекстно-свободные грамматики.
2. Регулярные языки. Регулярные выражения.
3. Системы Линденмайера
4. Детерминированные и недетерминированные конечные автоматы.
5. Конечные автоматы и регулярные выражения.
6. Конечные автоматы Мили и Мура
7. Магазинные автоматы.
8. Контекстно-зависимые грамматики.
9. Машины Тьюринга
10. Построение машин Тьюринга для принятия перечислимого языка и для вычисления функции
11. Недетерминированные машины Тьюринга

Требования к самостоятельной работе обучающихся

1. Работа с лекционным материалом, предусматривающая проработку конспекта лекций и учебной литературы, по всем темам из п. 6 настоящей рабочей программы.

2. Выполнение домашнего задания, предусматривающего решение задач, выполнение упражнений, выдаваемых на практических занятиях, по всем темам из п. 6 настоящей рабочей программы.

Руководствуясь положениями статьи 47 и статьи 48 Федерального закона от 29 декабря 2012 г. N 273-ФЗ «Об образовании в Российской Федерации» научно-педагогические работники и иные лица, привлекаемые университетом к реализации данной образовательной программы, пользуются предоставленными академическими правами и свободами в части свободы преподавания, свободы от вмешательства в профессиональную деятельность; свободы выбора и использования педагогически обоснованных форм, средств, методов обучения и воспитания; права на творческую инициативу, разработку и применение авторских программ и методов обучения и воспитания в пределах реализуемой образовательной программы и отдельной дисциплины.

Исходя из рамок, установленных учебным планом по трудоемкости и видам учебной работы по дисциплине, преподаватель самостоятельно выбирает тематику занятий по формам и количеству часов проведения контактной работы: лекции и иные учебные занятия, предусматривающие преимущественную передачу учебной информации преподавателем и (или) занятия семинарского типа (семинары, практические занятия, практикумы, лабораторные работы, коллоквиумы и иные аналогичные занятия), и (или) групповые консультации, и (или) индивидуальную работу обучающихся с преподавателем, в том числе индивидуальные консультации (по курсовым работам/проектам – при наличии курсовой работы/проекта по данной дисциплине в учебном плане).

Рекомендуемая тематика занятий максимально полно реализуется в контактной работе с обучающимися очной формы обучения. В случае реализации образовательной программы в заочной / очно-заочной форме трудоемкость дисциплины сохраняется, однако объем учебного материала в значительной части осваивается обучающимися в форме самостоятельной работы. При этом требования к ожидаемым образовательным результатам обучающихся по данной дисциплине не зависят от формы реализации образовательной программы.

7. Методические рекомендации по видам занятий

Лекционные занятия.

В ходе лекционных занятий обучающимся рекомендуется выполнять следующие действия. Вести конспектирование учебного материала. Обращать внимание на категории, формулировки, раскрывающие содержание тех или иных явлений и процессов, научные выводы и практические рекомендации по их применению. Задавать преподавателю уточняющие вопросы с целью уяснения теоретических положений, разрешения спорных ситуаций.

Желательно оставить в рабочих конспектах поля, на которых во внеаудиторное время можно сделать пометки из рекомендованной литературы, дополняющие материал прослушанной лекции, а также подчеркивающие особую важность тех или иных теоретических положений.

Практические и семинарские занятия.

На практических и семинарских занятиях в зависимости от темы занятия выполняется поиск информации по решению проблем, практические упражнения, контрольные работы, выработка индивидуальных или групповых решений, итоговое обсуждение с обменом знаниями, участие в круглых столах, разбор конкретных ситуаций, командная работа, представление портфолио и т.п.

Самостоятельная работа.

Самостоятельная работа осуществляется в виде изучения литературы, эмпирических данных по публикациям и конкретных ситуаций из практики, подготовке индивидуальных работ, работа с лекционным материалом, самостоятельное изучение отдельных тем

дисциплины; поиск и обзор литературы и электронных источников; чтение и изучение учебника и учебных пособий.

8. Фонд оценочных средств

8.1 Перечень компетенций с указанием этапов их формирования в процессе освоения образовательной программы

Основными этапами формирования указанных компетенций при изучении студентами дисциплины являются последовательное изучение содержательно связанных между собой *разделов* (*тем*) учебных занятий. Изучение каждого раздела (темы) предполагает овладение студентами необходимыми компетенциями. Результат аттестации студентов на различных этапах формирования компетенций показывает уровень освоения компетенций студентами.

Контролируемые модули, разделы (темы) дисциплины	Индекс контролируемой компетенции (или её части)	Оценочные средства по этапам формирования компетенций
1. Формальные языки. Контекстно-свободные грамматики	ПКС-7	Решение задач. Защита индивид. работ
2. Конечные и магазинные автоматы	ПКС-7	Решение задач. Защита индивид. работ
3. Контекстно-зависимые грамматики. Машины Тьюринга	ПКС-7	Решение задач. Защита индивид. работ

8.2. Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений и навыков и (или) опыта деятельности процессе текущего контроля

Типовые контрольные задания

Предусматривается выполнение студентами шести индивидуальных самостоятельных заданий следующего содержания:

1. Построить контекстно-свободную грамматику, порождающую указанный язык.
2. Построить конечный автомат, принимающий регулярный язык и детерминизировать его.
3. Построить конечный автомат по данному регулярному выражению.
4. Построить магазинный автомат, принимающий указанный контекстно-свободный язык.
5. Построить одноленточную машину Тьюринга, принимающую указанный перечислимый язык.
6. Построить машину Тьюринга, вычисляющую заданную функцию.

Варианты заданий выбираются из пособия [4] или выдаются преподавателем. Все построенные грамматики и автоматы должны быть реализованы на компьютере средствами программы *JFLAP*.

Примеры типовых задач

1. Укажите контекстно-свободную грамматику G с алфавитом терминальных символов $\Sigma = \{a, b\}$, такую, что $L(G) = \{a^n b^{2n} | n > 3\}$.
2. Постройте для входного алфавита $\Sigma = \{0,1\}$ конечный автомат , который принимает язык $L = \| \ \| = \{w | \ w \in \{0,1\}^*$, w – двоичное представление натурального числа, делящегося на 3$\}$. Для простоты можно положить, что ε представляет 0 и что разрешены ведущие нули.
3. (a) Постройте наименьший недетерминированный конечный автомат с входным алфавитом $\Sigma = \{a,b,c\}$, такой, что $\| \| = \{a,b,c\}^* abc \{a,b,c\}^*$.
   (b) Детерминируйте этот автомат.
4. Построить конечный автомат, который допускает язык, заданный следующими выражениями:
   1)$\mathbf{aa^*bb^*cc^*}$
   2)$\mathbf{(a^*ba^*ba^*b)^*}$
5. Постройте машину Тьюринга, которая для входного слова a^n, $n \geq 0$ вычисляет двоичное представление числа n как слово над $\{0, 1\}$.
6. Постройте машину Тьюринга T, которая принимает формальный язык $\{a^n b^n c^n \mid n \geq 1\}$:
7. (a) Постройте для языка $L = \{waw^R | \ w \in \{a, b\}^*\}$ контекстно-свободную грамматику в нормальной форме Грайбах. ($w = a_1 a_2 ... a_n$, $a_i \in \Sigma \Rightarrow w^R = a_n a_{n-1} ... a_1$)
   (b) Укажите магазинный автомат , который принимает язык L через конечное состояние и пустую магазинную ленту.
8. Постройте машину Тьюринга, которая вычисляет следующую функцию: f: $(\{a\}^*)^2 \rightarrow \{a\}^*$, $f(a^n, a^m) = a^{n \cdot m}$, $n, m \in \infty$.
9. Постройте машину Тьюринга, которая вычисляет следующую функцию f: $\{a, b\}^* \rightarrow \{a, b\}^*$, $f(w) = w^R$, $w \in \{a, b\}^*$ (w^R обозначает зеркальное отражение w).
10. Постройте машину Тьюринга, которая принимает следующий язык L:$L = \{a^n b^{2n} c^{3n} \mid n \in \infty\}$ ($L \subseteq \{a, b, c\}^*$).
11. Постройте машину Тьюринга, которая принимает следующий язык L:$L = \{a^n b^{n^2} \mid n \in \infty\}$ ($L \subseteq \{a, b\}^*$).
12. Постройте машину Тьюринга, которая принимает следующий язык L:$L = \{ww \mid w \in \{a, b\}^*\}$.

8.3. Перечень вопросов и заданий для промежуточной аттестации по дисциплине

Вопросы для промежуточного контроля (зачета)

1. Формальное определение грамматики.
2. Операторы регулярных выражений.
3. Свойства регулярных выражений.
4. Формальное определение конечного автомата
5. Недетерминированный конечный автомат.
6. Эквивалентность недетерминированных и детерминированных конечных автоматов.
7. Формальное определение магазинного автомата.
8. Эквивалентность магазинных автоматов и контекстно-свободных грамматик.
9. Иерархия грамматик по Хомскому.
10. Контекстно-зависимая грамматика.
11. Системы Линденмайера.
12. Одноленточная двусторонняя машина Тьюринга.
13. Односторонняя машина Тьюринга.
14. Многоленточная машина Тьюринга.
15. Недетерминированная машина Тьюринга.

8.4. Планируемые уровни сформированности компетенций обучающихся и критерии оценивания

Уровни	Содержательное описание уровня	Основные признаки выделения уровня (этапы формирования компетенции, критерии оценки сформированности)	Пятибалльная шкала (академическая) оценка	Двухбалльная шакала, зачет	БРС, % освоения (рейтинговая оценка)
Повышенный	Творческая деятельность	*Включает нижестоящий уровень.* Умение самостоятельно принимать решение, решать проблему/задачу теоретического и прикладного характера на основе изученных методов, приемов, технологий	отлично	зачтено	86-100
Базовый	Применение знаний и умений в более широких контекстах учебной и профессиональной деятельности,	*Включает нижестоящий уровень.* Способность собирать, систематизировать, анализировать и грамотно использовать информацию из самостоятельно найденных теоретических	хорошо		71-85

	нежели по образцу с большей степени самостоятельности и инициативы	источников и иллюстрировать ими теоретические положения или обосновывать практику применения			
Удовлетворительный (достаточный)	Репродуктивная деятельность	Изложение в пределах задач курса теоретически и практически контролируемого материала	удовлетворительно		55-70
Недостаточный	Отсутствие признаков удовлетворительного уровня		неудовлетворительно	не зачтено	Менее 55

9. Перечень основной и дополнительной литературы, необходимой для освоения дисциплины

Основная литература.

1. *Алымова, Е. В.* Конечные автоматы и формальные языки: учебник / Е. В. Алымова. В. М. Деундяк. А. М. Пеленицын ; Южный федеральный университет. - Ростов-на-Дону: Таганрог : Издательство Южного федерального университета. 2018 https://znanium.com/catalog/product/1020503

Дополнительная литература

1. *Мартыненко Б. К.* Языки и трансляции [Электронный ресурс] [Электронный учебник] : учеб. пособие / Б. К. Мартыненко. - Изд-во С.-Петерб. гос. ун-та, 2013 on-line, 265 с.Режим доступа: https://elib.kantiana.ru/viewer/books/pdf/MartinenkoYzikiITranckzcii.pdf/reading
2. *Куих В*. Введение в теорию информатики [Электронный ресурс] [Электронный учебник] : учеб. пособие / В. Куих, Ю. Ф. Болтнев. - БФУ им. И. Канта, 2015 on-line, 91 с. Режим доступа: https://elib.kantiana.ru/viewer/books/pdf/KuihBoltnevTeoriyInformatiki.pdf/reading

10. Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины

- НЭБ Национальная электронная библиотека, диссертации и прочие издания
- eLIBRARY.RU Научная электронная библиотека, книги, статьи, тезисы докладов конференций
- Гребенников Электронная библиотека ИД журналы

- ЭБС Лань книги, журналы
- ЭБС Консультант студента
- ПРОСПЕКТ ЭБС
- ЭБС ZNANIUM.COM
- РГБ Информационное обслуживание по МБА
- БЕН РАН
- Электронно-библиотечная система (ЭБС) Кантиана (https://lib.kantiana.ru/jirbis2/

11. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине

Программное обеспечение обучения включает в себя:

- система электронного образовательного контента БФУ им. И. Канта – www.lms-3.kantiana.ru, обеспечивающую разработку и комплексное использование электронных образовательных ресурсов;
- серверное программное обеспечение, необходимое для функционирования сервера и связи с системой электронного обучения через Интернет;
- корпоративная платформа Microsoft Teams;
- установленное на рабочих местах обучающихся ПО: Microsoft Windows 7, Microsoft Office Standart 2010, антивирусное программное обеспечение Kaspersky Endpoint Security.
- специализированное ПО - свободно распространяемая программа эмуляции грамматик и автоматов JFLAP (jflap.org**).** Работает на установленной платформе Java.

12. Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине

Для проведения занятий лекционного типа, практических и семинарских занятий используются специальные помещения (учебные аудитории), оборудованные техническими средствами обучения – мультимедийной проекционной техникой. Для проведения занятий лекционного типа используются наборы демонстрационного оборудования.

Для проведения лабораторных работ, (практических занятий – при необходимости) используются специальные помещения (учебные аудитории), оснащенные специализированным лабораторным оборудованием: персональными компьютерами с возможностью выхода в интернет и с установленным программным обеспечением, заявленным в п.11.

Для проведения групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации используются специальные помещения (учебные аудитории), оборудованные специализированной мебелью (для обучающихся), меловой / маркерной доской.

Для организации самостоятельной работы обучающимся предоставляются помещения, оснащенные компьютерной техникой с возможностью подключения к сети «Интернет» и обеспечением доступа в электронную информационно-образовательную среду университета.

Для обучения инвалидов и лиц с ограниченными возможностями здоровья университетом могут быть представлены специализированные средства обучения, в том числе технические средства коллективного и индивидуального пользования.

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
федеральное государственное автономное образовательное учреждение высшего образования «Балтийский федеральный университет имени Иммануила Канта»
Институт физико-математических наук и информационных технологий

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

«ФОРМАЛЬНЫЕ ЯЗЫКИ»

Шифр: 10.05.01
Специальность: «Компьютерная безопасность»
Специализация: «Математические методы защиты информации»
Квалификация (степень) выпускника: специалист по защите информации

Калининград
2022

Лист согласования

Составитель: БОЛТНЕВ ЮРИЙ ФЕДОРОВИЧ. старший преподаватель

Рабочая программа утверждена на заседании учебно-методического совета института физико-математических наук и информационных технологий
Протокол № 01/22 от «01» февраля 2022 г.

Председатель учебно-методического совета института физико-математических наук и информационных технологий
Первый заместитель директора ИФМНиИТ, к. ф.-м. н., доцент — Шпилевой А. А

Ведущий менеджер — Е.П.Ставицкая

СОДЕРЖАНИЕ

1. Наименование дисциплины: «ФОРМАЛЬНЫЕ ЯЗЫКИ»

Целью освоения дисциплины «Формальные языки» является овладение основами теории формальных языков, грамматик и автоматов, что заложит фундамент понимания принципов построения современных информационных систем

2. Перечень планируемых результатов обучения по дисциплине, соотнесенных с планируемыми результатами освоения образовательной программы

Код компетенции	Результаты освоения образовательной программы (ИДК)	Результаты обучения по дисциплине
ПКС-7 Способность проводить анализ и участвовать в разработке математических моделей безопасности компьютерных систем	ПКС-7.1. Знает математические методы моделирования безопасных компьютерных систем ПКС-7.2. Осуществляет анализ математических моделей безопасности компьютерных систем ПКС-7.3. Участвует в разработке математических моделей безопасности компьютерных систем	• **Знать** основы теории формальных языков, грамматик и автоматов, принципы построения конечных, магазинных автоматов и машин Тьюринга; основные алгоритмически неразрешимые проблемы информатики, связанные с формальными языками • **Уметь** использовать полученные теоретические знания для решения конкретных прикладных задач, производить математические расчеты в стандартных постановках, производить содержательный анализ результатов вычислений, строить контекстно-свободную грамматику, порождающую указанный язык; строить конечный автомат, принимающий регулярный язык и детерминировать его; строить магазинный автомат, принимающий указанный контекстно-свободный язык; строить грамматику, порождающую указанный контекстно-зависимый язык; строить машину Тьюринга, принимающую указанный перечислимый язык или вычисляющую заданную функцию • **Владеть** навыками применения понятий и методов дисциплины для решения различных задач, используемых в дальнейшей учебной и профессиональной деятельности; навыками моделирования перечисленных грамматик и автоматов на компьютере

3. Место дисциплины в структуре ООП ВО

Дисциплина «*Формальные языки»* представляет собой дисциплину части, формируемой участниками образовательных отношений, блока дисциплин подготовки обучающихся.

4. Виды учебной работы по дисциплине.

Виды учебной работы по дисциплине зафиксированы учебным планом основной профессиональной образовательной программы по указанному направлению и профилю, выражаются в академических часах. Часы контактной работы и самостоятельной работы студента и часы, отводимые на процедуры контроля, могут различаться в учебных планах ОПОП по формам обучения. Объем контактной работы включает часы контактной аудиторной работы (лекции/практические занятия/ лабораторные работы), контактной внеаудиторной работы (контроль самостоятельной работы), часы контактной работы в период аттестации. Контактная работа, в том числе может проводиться посредством электронной информационно-образовательной среды университета с использованием ресурсов сети Интернет и дистанционных технологий

5. Содержание дисциплины, структурированное по темам (разделам)

Исходя из рамок, установленных учебным планом по трудоемкости и видам учебной работы по дисциплине, преподаватель самостоятельно выбирает тематику занятий по формам и количеству часов проведения контактной работы: лекции и иные учебные занятия, предусматривающие преимущественную передачу учебной информации преподавателем и (или) занятия семинарского типа (семинары, практические занятия, практикумы, лабораторные работы, коллоквиумы и иные аналогичные занятия), и (или) групповые консультации, и (или) индивидуальную работу обучающихся с преподавателем, в том числе индивидуальные консультации (по курсовым работам/проектам – при наличии курсовой работы/проекта по данной дисциплине в учебном плане). Рекомендуемая тематика занятий максимально полно реализуется в контактной работе со студентами очной формы обучения. В случае реализации образовательной программы в заочной / очно-заочной форме трудоемкость дисциплины сохраняется, однако объем учебного материала в значительной части осваивается студентами в форме самостоятельной работы. При этом требования к ожидаемым образовательным результатам студентов по данной дисциплине не зависят от формы реализации образовательной программы.

Содержание основных разделов и тем курса

1. ЯЗЫКИ И ИХ ПРЕДСТАВЛЕНИЕ. ГРАММАТИКИ

Алфавиты и языки. Представление языков. Мотивировка. Формальное определение грамматики. Типы грамматик. Пустое предложение. Рекурсивность контекстно-зависимых грамматик. Деревья вывода в контекстно-свободных грамматиках

.

2. КОНЕЧНЫЕ АВТОМАТЫ И РЕГУЛЯРНЫЕ ГРАММАТИКИ. КОНТЕКСТНО-СВОБОДНЫЕ ГРАММАТИКИ.

Конечный автомат. Отношения эквивалентности и конечные автоматы. Недетерминированные конечные автоматы. Конечные автоматы и языки типа 3. Свойства языков типа 3. Алгоритмически разрешимые проблемы, касающиеся конечных автоматов. Упрощение контекстно-свободных грамматик. Нормальная форма Хомского. Нормальная форма Грейбах. Разрешимость конечности КС-языков. Свойство самовставленности. е-правила в контекстно-свободных грамматиках. Специальные типы контекстно-свободных языков и грамматик

3. МАГАЗИННЫЕ АВТОМАТЫ. МАШИНЫ ТЬЮРИНГА

Неформальное описание магазинного автомата. Формальное описание. Недетерминированные магазинные автоматы и контекстно-свободные языки. Неформальное описание машин Тьюринга. Определения и обозначения. Методы построения машин Тьюринга. Память в конечном управлении. Многодорожечные ленты. Отметка символов. Сдвиг. Моделирование. Диагонализация. Подпрограммы. Машина Тьюринга как процедура. Модификации машин Тьюринга. Ограниченные машины Тьюринга, эквивалентные основной модели

6. Рекомендуемая тематика учебных занятий в форме контактной работы

Рекомендуемая тематика учебных занятий лекционного типа (предусматривающих преимущественную передачу учебной информации преподавателями):

№	Наименование раздела	Темы лекций
1	Языки и их представление. Грамматики	Лекции 1 - 2. Формальные языки и грамматики. Лекции 3 - 4. Классификация грамматик и языков.
2	Конечные автоматы и регулярные грамматики. Контекстно-свободные грамматики	Лекции 5 - 6. Детерминированные и недетерминированные конечные автоматы. Лекции 7 - 8. Нормальная форма Хомского. Нормальная форма Грейбах
3	Магазинные автоматы. Машины Тьюринга	Лекции 9 – 10. Детерминированные и недетерминированные магазинные автоматы и контекстно-свободные языки. Лекции 11 – 12. Машины Тьюринга. Модификации машин Тьюринга Лекции 13 – 14. Недетерминированные машины Тьюринга

Тематика практических занятий

1. Формальные языки. Контекстно-свободные грамматики.
2. Регулярные языки. Регулярные выражения.
3. Детерминированные и недетерминированные конечные автоматы.
4. Конечные автоматы и регулярные выражения.
5. Системы Линденмайера
6. Граммматики Ван Вайнгаардена
7. Магазинные автоматы.
8. Контекстно-зависимые грамматики.

9. Машины Тьюринга
10. Построение машин Тьюринга для принятия перечислимого языка и для вычисления функции
11. Недетерминированные машины Тьюринга

Требования к самостоятельной работе обучающихся

1. Работа с лекционным материалом, предусматривающая проработку конспекта лекций и учебной литературы, по всем темам из п. 6 настоящей рабочей программы.

2. Выполнение домашнего задания, предусматривающего решение задач, выполнение упражнений, выдаваемых на практических занятиях, по всем темам из п. 6 настоящей рабочей программы.

Руководствуясь положениями статьи 47 и статьи 48 Федерального закона от 29 декабря 2012 г. N 273-ФЗ «Об образовании в Российской Федерации» научно-педагогические работники и иные лица, привлекаемые университетом к реализации данной образовательной программы, пользуются предоставленными академическими правами и свободами в части свободы преподавания, свободы от вмешательства в профессиональную деятельность; свободы выбора и использования педагогически обоснованных форм, средств, методов обучения и воспитания; права на творческую инициативу, разработку и применение авторских программ и методов обучения и воспитания в пределах реализуемой образовательной программы и отдельной дисциплины.

Исходя из рамок, установленных учебным планом по трудоемкости и видам учебной работы по дисциплине, преподаватель самостоятельно выбирает тематику занятий по формам и количеству часов проведения контактной работы: лекции и иные учебные занятия, предусматривающие преимущественную передачу учебной информации преподавателем и (или) занятия семинарского типа (семинары, практические занятия, практикумы, лабораторные работы, коллоквиумы и иные аналогичные занятия), и (или) групповые консультации, и (или) индивидуальную работу обучающихся с преподавателем, в том числе индивидуальные консультации (по курсовым работам/проектам – при наличии курсовой работы/проекта по данной дисциплине в учебном плане).

Рекомендуемая тематика занятий максимально полно реализуется в контактной работе с обучающимися очной формы обучения. В случае реализации образовательной программы в заочной / очно-заочной форме трудоемкость дисциплины сохраняется, однако объем учебного материала в значительной части осваивается обучающимися в форме самостоятельной работы. При этом требования к ожидаемым образовательным результатам обучающихся по данной дисциплине не зависят от формы реализации образовательной программы.

7. Методические рекомендации по видам занятий

Лекционные занятия.

В ходе лекционных занятий обучающимся рекомендуется выполнять следующие действия. Вести конспектирование учебного материала. Обращать внимание на категории, формулировки, раскрывающие содержание тех или иных явлений и процессов, научные выводы и практические рекомендации по их применению. Задавать преподавателю уточняющие вопросы с целью уяснения теоретических положений, разрешения спорных ситуаций.

Желательно оставить в рабочих конспектах поля, на которых во внеаудиторное время можно сделать пометки из рекомендованной литературы, дополняющие материал прослушанной лекции, а также подчеркивающие особую важность тех или иных теоретических положений.

Практические и семинарские занятия.

На практических и семинарских занятиях в зависимости от темы занятия выполняется поиск информации по решению проблем, практические упражнения, контрольные работы, выработка индивидуальных или групповых решений, итоговое обсуждение с обменом знаниями, участие в круглых столах, разбор конкретных ситуаций, командная работа, представление портфолио и т.п.

Самостоятельная работа.

Самостоятельная работа осуществляется в виде изучения литературы, эмпирических данных по публикациям и конкретных ситуаций из практики, подготовке индивидуальных работ, работа с лекционным материалом, самостоятельное изучение отдельных тем дисциплины; поиск и обзор литературы и электронных источников; чтение и изучение учебника и учебных пособий.

8. Фонд оценочных средств

8.1 Перечень компетенций с указанием этапов их формирования в процессе освоения образовательной программы

Основными этапами формирования указанных компетенций при изучении студентами дисциплины являются последовательное изучение содержательно связанных между собой *разделов* (*тем*) учебных занятий. Изучение каждого раздела (темы) предполагает овладение студентами необходимыми компетенциями. Результат аттестации студентов на различных этапах формирования компетенций показывает уровень освоения компетенций студентами.

Контролируемые модули, разделы (темы) дисциплины	Индекс контролируемой компетенции (или её части)	Оценочные средства по этапам формирования компетенций
1. Формальные языки. Контекстно-свободные грамматики	ПКС-7	Решение задач. Защита индивид. работ
2. Конечные и магазинные автоматы	ПКС-7	Решение задач. Защита индивид. работ
3. Контекстно-зависимые грамматики. Машины Тьюринга	ПКС-7	Решение задач. Защита индивид. работ

8.2. Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений и навыков и (или) опыта деятельности процессе текущего контроля

Типовые контрольные задания

Предусматривается выполнение студентами шести индивидуальных самостоятельных заданий следующего содержания:

1. Построить контекстно-свободную грамматику, порождающую указанный язык.
2. Построить конечный автомат, принимающий регулярный язык и детерминизировать его.
3. Построить конечный автомат по данному регулярному выражению.
4. Построить магазинный автомат, принимающий указанный контекстно-свободный язык.
5. Построить одноленточную машину Тьюринга, принимающую указанный перечислимый язык.
6. Построить машину Тьюринга, вычисляющую заданную функцию.

Варианты заданий выбираются из пособия [1] или выдаются преподавателем. Все построенные грамматики и автоматы должны быть реализованы на компьютере средствами программы *JFLAP*.

Примеры типовых задач

1. Укажите контекстно-свободную грамматику G с алфавитом терминальных символов $\Sigma = \{a, b\}$, такую, что $L(G) = \{a^n b^{2n} | n > 3\}$.
2. Укажите контекстно-свободную грамматику G над $\Sigma = \{a, b, c\}$, которая порождает язык $L = \{a^i b^j c^k | k \le i + j, i, j, k \in \mathbb{N}\}$.
3. Покажите, что если $L \subseteq \Sigma^*$ контекстно-свободный и $a \in \Sigma$, то и $:= LL^R a$ также контекстно-свободный ($L^R = \{w^R \mid w \in L\}$, w^R - зеркальное отражение w).
4. (а) Постройте для языка $L = \{waw^R \mid w \in \{a, b\}^*\}$ контекстно-свободную грамматику в нормальной форме Грайбаха. ($w = a_1 a_2 ... a_n$, $a_i \in \sum \Rightarrow w^R = a_n a_{n-1} ... a_1$)
   (б) Укажите магазинный автомат, который принимает язык L через конечное состояние и пустую магазинную ленту.
5. (а) Постройте наименьший недетерминированный конечный автомат с входным алфавитом $\Sigma = \{a,b,c\}$, такой, что $\| \| = \{a,b,c\}^* abc \{a,b,c\}^*$.
   (b) Детерминируйте этот автомат.
6. Постройте машину Тьюринга T, которая принимает формальный язык $\{a^n b^n c^n \mid n \ge 1\}$:

8.3. Перечень вопросов и заданий для промежуточной аттестации по дисциплине

Вопросы для промежуточного контроля (зачета)

1. Формальное определение грамматики.
2. Операторы регулярных выражений.
3. Свойства регулярных выражений.
4. Формальное определение конечного автомата
5. Недетерминированный конечный автомат.
6. Эквивалентность недетерминированных и детерминированных конечных автоматов.
7. Формальное определение магазинного автомата.
8. Эквивалентность магазинных автоматов и контекстно-свободных грамматик.

9. Иерархия грамматик по Хомскому.
10. Контекстно-зависимая грамматика.
11. Системы Линденмайера.
12. Однолентоная двусторонняя машина Тьюринга.
13. Односторонняя машина Тьюринга.
14. Многоленточная машина Тьюринга.
15. Недетерминированная машина Тьюринга.

8.4. Планируемые уровни сформированности компетенций обучающихся и критерии оценивания

Уровни	Содержательное описание уровня	Основные признаки выделения уровня (этапы формирования компетенции, критерии оценки сформированности)	Пятибалльная шкала (академическая) оценка	Двухбалльная шакала, зачет	БРС, % освоения (рейтинговая оценка)
Повышенный	Творческая деятельность	*Включает нижестоящий уровень.* Умение самостоятельно принимать решение, решать проблему/задачу теоретического и прикладного характера на основе изученных методов, приемов, технологий	отлично	зачтено	86-100
Базовый	Применение знаний и умений в более широких контекстах учебной и профессиональной деятельности, нежели по образцу с большей степени самостоятельности и инициативы	*Включает нижестоящий уровень.* Способность собирать, систематизировать, анализировать и грамотно использовать информацию из самостоятельно найденных теоретических источников и иллюстрировать ими теоретические положения или обосновывать практику применения	хорошо		71-85
Удовлетворительный (достаточный)	Репродуктивная деятельность	Изложение в пределах задач курса теоретически и практически контролируемого	удовлетворительно		55-70

		материала			
Недостаточный	Отсутствие признаков удовлетворительного уровня		неудовлетворительно	не зачтено	Менее 55

9. Перечень основной и дополнительной литературы, необходимой для освоения дисциплины

Основная литература.

1. *Алымова, Е. В.* Конечные автоматы и формальные языки: учебник / Е. В. Алымова. В. М. Деундяк. А. М. Пеленицын ; Южный федеральный университет. - Ростов-на-Дону: Таганрог : Издательство Южного федерального университета. 2018 https://znanium.com/catalog/product/1020503

Дополнительная литература

1. *Мартыненко Б. К.* Языки и трансляции [Электронный ресурс] [Электронный учебник] : учеб. пособие / Б. К. Мартыненко. - Изд-во С.-Петерб. гос. ун-та, 2013 on-line, 265 с.Режим доступа: https://elib.kantiana.ru/viewer/books/pdf/MartinenkoYzikiITranckzcii.pdf/reading

2. *Куих В*. Введение в теорию информатики [Электронный ресурс] [Электронный учебник] : учеб. пособие / В. Куих, Ю. Ф. Болтнев. - БФУ им. И. Канта, 2015 on-line, 91 с. Режим доступа: https://elib.kantiana.ru/viewer/books/pdf/KuihBoltnevTeoriyInformatiki.pdf/reading

10. Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины

- НЭБ Национальная электронная библиотека, диссертации и прочие издания
- eLIBRARY.RU Научная электронная библиотека, книги, статьи, тезисы докладов конференций
- Гребенников Электронная библиотека ИД журналы
- ЭБС Лань книги, журналы
- ЭБС Консультант студента
- ПРОСПЕКТ ЭБС
- ЭБС ZNANIUM.COM
- РГБ Информационное обслуживание по МБА
- БЕН РАН
- Электронно-библиотечная система (ЭБС) Кантиана (https://elib.kantiana.ru/)

11. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине

Программное обеспечение обучения включает в себя:

- система электронного образовательного контента БФУ им. И. Канта – www.lms-3.kantiana.ru, обеспечивающую разработку и комплексное использование электронных образовательных ресурсов;
- серверное программное обеспечение, необходимое для функционирования сервера и связи с системой электронного обучения через Интернет;
- корпоративная платформа Microsoft Teams;
- установленное на рабочих местах обучающихся ПО: Microsoft Windows 7, Microsoft Office Standart 2010, антивирусное программное обеспечение Kaspersky Endpoint Security.
- специализированное ПО - свободно распространяемая программа эмуляции грамматик и автоматов JFLAP (jflap.org). Работает на установленной платформе Java.

12. Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине

Для проведения занятий лекционного типа, практических и семинарских занятий используются специальные помещения (учебные аудитории), оборудованные техническими средствами обучения – мультимедийной проекционной техникой. Для проведения занятий лекционного типа используются наборы демонстрационного оборудования.

Для проведения лабораторных работ, (практических занятий – при необходимости) используются специальные помещения (учебные аудитории), оснащенные специализированным лабораторным оборудованием: персональными компьютерами с возможностью выхода в интернет и с установленным программным обеспечением, заявленным в п.11.

Для проведения групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации используются специальные помещения (учебные аудитории), оборудованные специализированной мебелью (для обучающихся), меловой / маркерной доской.

Для организации самостоятельной работы обучающимся предоставляются помещения, оснащенные компьютерной техникой с возможностью подключения к сети «Интернет» и обеспечением доступа в электронную информационно-образовательную среду университета.

Для обучения инвалидов и лиц с ограниченными возможностями здоровья университетом могут быть представлены специализированные средства обучения, в том числе технические средства коллективного и индивидуального пользования.

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
федеральное государственное автономное образовательное учреждение высшего образования «Балтийский федеральный университет имени Иммануила Канта»
Институт физико-математических наук и информационных технологий

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

«Функциональные поля и их приложения»

Шифр: 10.05.01
Специальность: «Компьютерная безопасность»
Специализация: «Математические методы защиты информации»
Квалификация (степень) выпускника: специалист по защите информации

Калининград
2022

Лист согласования

Составитель: Мельничук Евгений Михайлович, ассистент Института физико-математических наук и информационных технологий

Рабочая программа утверждена на заседании учебно-методического совета института физико-математических наук и информационных технологий
Протокол № 01/22 от «01» февраля 2022 г.

Председатель учебно-методического
совета института физико-
математических наук и
информационных технологий
Первый заместитель директора Шпилевой А. А
ИФМНиИТ, к. ф.-м. н., доцент

Ведущий менеджер Е.П.Ставицкая

Содержание

1.Наименование дисциплины: «Функциональные поля и их приложения».

Цель дисциплины: целью освоения дисциплины «Функциональные поля и их приложения» является расширение и углубление фундаментальной подготовки студентов в области алгебры и теории чисел до уровня, необходимого для анализа и формализации задач в области защиты информации и разработки математических моделей защищаемых информационных потоков; овладение основными принципами и результатами теории алгеброгеометрических кодов, вычислительными процедурами кодирования и декодирования и методикой оценки эффективности соответствующих кодов.

2. Перечень планируемых результатов обучения по дисциплине, соотнесенных с планируемыми результатами освоения образовательной программы

Код компетенции	Результаты освоения образовательной программы (ИДК)	Результаты обучения по дисциплине
ПКС-7. Способность проводить анализ и участвовать в разработке математических моделей безопасности компьютерных систем	ПКС-7.1. Знает математические методы моделирования безопасных компьютерных систем. ПКС-7.2. Осуществляет анализ математических моделей безопасности компьютерных систем ПКС-7.3. Участвует в разработке математических моделей безопасности компьютерных систем	• ***знать*** перспективные методы криптографической защиты информации и помехоустойчивого кодирования, принципы функционирования и возможности перспективных инструментальных средств и компьютерных технологий для реализации вычислительных алгоритмов, структуры данных и методы построения вычислительных алгоритмов в алгебраических структурах, специфичных для перспективных систем защиты информации • ***уметь*** грамотно применять изученные математические методы, математические пакеты для обработки, детального анализа и систематизации криптографической информации, строить схемы и модели подсистем информационной безопасности компьютерной системы, анализировать корректность и быстродействие вычислительных алгоритмов,

		специфичных для перспективных систем защиты информации; • ***владеть*** практическими навыками построения вычислительных алгоритмов в алгебраических структурах, используемых в системах криптографической защиты и помехоустойчивого кодирования, навыками сравнительного анализа эффективности различных моделей, методов, алгоритмов, реализованных в средствах защиты информации, анализа их технических характеристик.

3. Место дисциплины в структуре образовательной программы

Дисциплина «Функциональные поля и их приложения» представляет собой дисциплину части, формируемой участниками образовательных отношений блока дисциплин подготовки обучающихся.

4. Виды учебной работы по дисциплине.

Виды учебной работы по дисциплине зафиксированы учебным планом основной профессиональной образовательной программы по указанному направлению и профилю, выражаются в академических часах. Часы контактной работы и самостоятельной работы обучающегося и часы, отводимые на процедуры контроля, могут различаться в учебных планах ОПОП по формам обучения. Объем контактной работы включает часы контактной аудиторной работы (лекции/практические занятия/ лабораторные работы), контактной внеаудиторной работы (контроль самостоятельной работы), часы контактной работы в период аттестации. Контактная работа, в том числе может проводиться посредством электронной информационно-образовательной среды университета с использованием ресурсов сети Интернет и дистанционных технологий

5. Содержание дисциплины, структурированное по темам (разделам)

Исходя из рамок, установленных учебным планом по трудоемкости и видам учебной работы по дисциплине, преподаватель самостоятельно выбирает тематику занятий по формам и количеству часов проведения контактной работы: лекции и иные учебные занятия, предусматривающие преимущественную передачу учебной информации преподавателем и (или) занятия семинарского типа (семинары, практические занятия, практикумы, лабораторные работы, коллоквиумы и иные аналогичные занятия), и (или) групповые консультации, и (или) индивидуальную работу обучающихся с преподавателем, в том числе индивидуальные консультации (по

курсовым работам/проектам – при наличии курсовой работы/проекта по данной дисциплине в учебном плане). Рекомендуемая тематика занятий максимально полно реализуется в контактной работе с обучающимися очной формы обучения. В случае реализации образовательной программы в заочной / очно-заочной форме трудоемкость дисциплины сохраняется, однако объем учебного материала в значительной части осваивается обучающимися в форме самостоятельной работы. При этом требования к ожидаемым образовательным результатам обучающихся по данной дисциплине не зависят от формы реализации образовательной программы.

№	Наименование раздела	Содержание раздела
1	Функциональные поля.	Задачи и программа курса. Место теории функциональных полей в ряду других математических и прикладных дисциплин. Источники её развития и области приложения. Роль теории функциональных полей в задачах защиты информации. Формы самостоятельной работы студентов по изучению курса. Основная литература к курсу. Сепарабельные расширения полей. Теорема о примитивном элементе. Совершенные поля. Локальные кольца. Кольца нормирования. Кольца дискретного нормирования. Функциональное поле. Поле констант. Рациональное поле. Сепарирующий элемент поля. Дискретные нормирования. Кольца нормирования. Точки поля. Локальный параметр точки. Поле классов вычетов. Отображение классов вычетов. Нули и полюсы. Пример рационального поля. Дивизоры. Сложение дивизоров. Степень дивизора. Дивизоры нулей и полюсов элемента функционального поля. Главный дивизор. Теорема о степени главного дивизора. Линейно эквивалентные дивизоры. Группа классов дивизоров. Якобиан функционального поля. Пример рационального поля. Пространство Римана-Роха, ассоциированное с дивизором. Размерность дивизора. Род функционального поля. Пример рационального поля.
2	Дифференциалы и теорема Римана – Роха	Дифференцирования функционального поля, их свойства. Дифференцирование по сепарирующему элементу. Размерность пространства дифференцирований. Обобщение понятия дифференцирования. Дифференциалы функционального поля. Полные дифференциалы элементов функционального поля. Свойства полных дифференциалов. Размерность пространства дифференциалов. Базис пространства дифференциалов. Канонический дивизор и канонический класс. Пространство дифференциалов, ассоциированное с дивизором. Индекс специальности дивизора. Теорема Римана-Роха. Следствия из теоремы Римана-Роха. Пример рационального поля.

3	*P*-адические разложения и вычеты	*P*-адические разложения элементов функционального поля. Дифференцирование *P*-адических разложений. Пополнение функционального поля в точке. Вычет дифференциала в точке. Свойства вычетов. Теорема о вычетах. Примеры.
4	Алгеброгеометрические коды	Коды Рида-Соломона, их свойства. Алгеброгеометрические коды $C_L(D, G)$, их свойства. Алгеброгеометрические коды $C_\Omega(D, G)$, их свойства. Двойственность алгеброгеометрических кодов. Рациональные алгеброгеометрические коды, их свойства. Дальнейшие примеры алгеброгеометрических кодов. Декодирование алгеброгеометрических кодов. Синдром сообщения. Функция локаторов ошибок. Алгоритм декодирования. Примеры.
5	Расширения функциональных полей	Алгебраические (сепарабельные, конечные) расширения функциональных полей. Продолжение нормирований. Индекс ветвления. Расширение колец нормирования и точек. Типы расширений точки. Типы расширений функционального поля. Расширение поля классов вычетов. Относительная степень точки. Основное тождество. Конорма точки. Конорма дивизора. Степень конормы. Критерий неприводимости Эйзенштейна для функционального поля. Целое замыкание кольца нормирования. Целый базис расширения функционального поля. Теорема Куммера. Следствие из теоремы Куммера. Дифферента. Теорема Дедекинда. Вычисление показателей дифференты. Формула Гурвица для Рода. Неравенство Римана. Вычисление канонического дивизора. Расширения Галуа функциональных полей. Циклические расширения.
6	Примеры расширений	Расширение поля констант, его свойства. Расширение Куммера, его свойства. Расширение Артина-Шрайера, его свойства.
7	Дзета-функция	Функциональные поля с конечным полем констант. Число классов поля. Определение дзета-функции. *L*-многочлен функционального поля. Свойства коэффициентов *L*-многочлена. Теорема Хассе-Вейля. Представление дзета-функции в виде произведения. Максимальные поля. Граница Серра. Метод Вейля вычисления числа рациональных точек в случае расширения поля констант. Формула числа точек произвольной степени.
8	Эллиптические функциональные поля.	Различные виды уравнений эллиптических полей. Степени точек. Индексы ветвления. Дифферента. Род эллиптического поля. Канонический дивизор. Пример вычисления числа рациональных точек эллиптического поля.

6. Рекомендуемая тематика учебных занятий в форме контактной работы

Рекомендуемая тематика учебных занятий *лекционного* типа (предусматривающих преимущественную передачу учебной информации преподавателями):

№	Наименование раздела	Темы лекций
1	Функциональные поля.	Лекция 1. Понятие ункционального поля Лекция 2. Нормирования и их свойства Лекция 3. Дивизоры
2	Дифференциалы и теорема Римана – Роха	Лекция 4. Дифференцирования функционального поля. Лекция 5. Дифференциалы функционального поля. Лекция 6. Теорема Римана-Роха
3	*P*-адические разложения и вычеты	Лекция 7. *P*-адические разложения элементов функционального поля.
4	Алгеброгеометрические коды	Лекция 8. Коды Рида-Соломона, их свойства. Алгеброгеометрические коды $C_L(D, G)$, их свойства. Алгеброгеометрические коды $C_\Omega(D, G)$, их свойства. Лекция 9. Рациональные алгеброгеометрические коды, их свойства. Дальнейшие примеры алгеброгеометрических кодов. Лекции 10. Декодирование алгеброгеометрических кодов.
5	Расширения функциональных полей	Лекция 11. Алгебраические (сепарабельные, конечные) расширения функциональных полей.
6	Примеры расширений	Лекция 12. Примеры расширений функциональных полей.
7	Дзета-функция	Лекция 13. Функциональные поля с конечным полем констант. Число классов поля. Определение дзета-функции. *L*-многочлен функционального поля. Свойства коэффициентов *L*-многочлена. Лекция 14. Теорема Хассе-Вейля. Представление дзета-функции в виде произведения. Максимальные поля. Граница Серра. Метод Вейля вычисления числа рациональных точек в случае расширения поля констант. Формула числа точек произвольной степени
8	Эллиптические функциональные поля.	Лекции 15. Различные виды уравнений эллиптических полей.

Рекомендуемая тематика *практических* занятий:

1. Рациональное функциональное поле и его свойства.
2. Свойства и примеры дифференциалов. Примеры применения теоремы Римана-Роха.
3. *P*-адические разложения.
4. Построение и свойства рациональных кодов.
5. Примеры применения теоремы Куммера.
6. Исследование свойств расширений функциональных полей.

7. Примеры вычисления L-многочленов функциональных полей.
8. Исследование свойств эллиптических и некоторых неэллиптических функциональных полей.

На практических занятиях решаются задачи по теме занятия.

Требования к самостоятельной работе обучающихся

1. Работа с лекционным материалом, предусматривающая проработку конспекта лекций и учебной литературы, по всем темам из п. 6 настоящей рабочей программы.

2. Выполнение домашнего задания, предусматривающего решение задач, выполнение упражнений, выдаваемых на практических занятиях, по всем темам из п. 6 настоящей рабочей программы.

Руководствуясь положениями статьи 47 и статьи 48 Федерального закона от 29 декабря 2012 г. N 273-ФЗ «Об образовании в Российской Федерации» научно-педагогические работники и иные лица, привлекаемые университетом к реализации данной образовательной программы, пользуются предоставленными академическими правами и свободами в части свободы преподавания, свободы от вмешательства в профессиональную деятельность; свободы выбора и использования педагогически обоснованных форм, средств, методов обучения и воспитания; права на творческую инициативу, разработку и применение авторских программ и методов обучения и воспитания в пределах реализуемой образовательной программы и отдельной дисциплины.

Исходя из рамок, установленных учебным планом по трудоемкости и видам учебной работы по дисциплине, преподаватель самостоятельно выбирает тематику занятий по формам и количеству часов проведения контактной работы: лекции и иные учебные занятия, предусматривающие преимущественную передачу учебной информации преподавателем и (или) занятия семинарского типа (семинары, практические занятия, практикумы, лабораторные работы, коллоквиумы и иные аналогичные занятия), и (или) групповые консультации, и (или) индивидуальную работу обучающихся с преподавателем, в том числе индивидуальные консультации (по курсовым работам/проектам – при наличии курсовой работы/проекта по данной дисциплине в учебном плане).

Рекомендуемая тематика занятий максимально полно реализуется в контактной работе с обучающимися очной формы обучения. В случае реализации образовательной программы в заочной / очно-заочной форме трудоемкость дисциплины сохраняется, однако объем учебного материала в значительной части осваивается обучающимися в форме самостоятельной работы. При этом требования к ожидаемым образовательным результатам обучающихся по данной дисциплине не зависят от формы реализации образовательной программы.

7. Методические рекомендации по видам занятий

Лекционные занятия.

В ходе лекционных занятий обучающимся рекомендуется выполнять следующие действия. Вести конспектирование учебного материала. Обращать внимание на категории, формулировки, раскрывающие содержание тех или иных

явлений и процессов, научные выводы и практические рекомендации по их применению. Задавать преподавателю уточняющие вопросы с целью уяснения теоретических положений, разрешения спорных ситуаций.

Желательно оставить в рабочих конспектах поля, на которых во внеаудиторное время можно сделать пометки из рекомендованной литературы, дополняющие материал прослушанной лекции, а также подчеркивающие особую важность тех или иных теоретических положений.

Практические и семинарские занятия.

На практических и семинарских занятиях в зависимости от темы занятия выполняется поиск информации по решению проблем, практические упражнения, контрольные работы, выработка индивидуальных или групповых решений, итоговое обсуждение с обменом знаниями, участие в круглых столах, разбор конкретных ситуаций, командная работа, представление портфолио и т.п.

Самостоятельная работа.

Самостоятельная работа осуществляется в виде изучения литературы, эмпирических данных по публикациям и конкретных ситуаций из практики, подготовке индивидуальных работ, работа с лекционным материалом, самостоятельное изучение отдельных тем дисциплины; поиск и обзор литературы и электронных источников; чтение и изучение учебника и учебных пособий.

8. Фонд оценочных средств

8.1. Перечень компетенций с указанием этапов их формирования в процессе освоения образовательной программы в рамках учебной дисциплины

Основными этапами формирования указанных компетенций при изучении обучающимися дисциплины являются последовательное изучение содержательно связанных между собой тем учебных занятий. Изучение каждой темы предполагает овладение обучающимися необходимыми компетенциями. Результат аттестации обучающихся на различных этапах формирования компетенций показывает уровень освоения компетенций.

Контролируемые разделы (темы) дисциплины	Индекс контроли-руемой компетенции (или её части)	Оценочные средства по этапам формирования компетенций
		текущий контроль по дисциплине
1. Функциональные поля.	ПКС-7	Опрос, решение задач.
2. Дифференциалы и теорема Римана – Роха	ПКС-7	Опрос, решение задач
3. Р-адические разложения и вычеты	ПКС-7	Опрос, решение задач
4. Алгеброгеометрические коды	ПКС-7	Опрос, решение задач, контрольная работа
5. Расширения функциональных полей	ПКС-7	Опрос, решение задач
6. Примеры расширений	ПКС-7	Опрос, решение задач
7. Дзета-функция	ПКС-7	Опрос, решение задач,

Контролируемые разделы (темы) дисциплины	Индекс контроли-руемой компетенции (или её части)	Оценочные средства по этапам формирования компетенций
		текущий контроль по дисциплине
8. Эллиптические функциональные поля.	ПКС-7	Опрос, решение задач

8.2. Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений и навыков и (или) опыта деятельности процессе текущего контроля

Примеры вопросов для устного опроса:

По Теме 1. Функциональные поля.

1. Что такое сепарабельные расширения полей?
2. Теорема о примитивном элементе.
3. Что такое совершенные поля?
4. Что такое локальное кольцо?.
5. Что такое кольцо нормирования, кольцо дискретного нормирования?
6. Что такое функциональное поле, поле констант.
7. Что такое рациональное поле?
8. Что такое сепарирующий элемент поля?
9. Что такое дискретное нормирования?
10. Что локальный параметр точки?
11. Что такое поле классов вычетов, отображение классов вычетов?
12. Что такое дивизор и степень дивизора?
13. Что такое линейно эквивалентные дивизоры?
14 Что такое группа классов дивизоров?
15. Что такое род функционального поля?

Типовые контрольные задания:

Тема 1. Функциональные поля

	Задача
Оценка «зачтено» - низкой уровень освоения компетенции	Пусть p – простое число. Всякое $x \in \square$, $x \neq 0$, единственным образом записывается в виде $x = = p^n \frac{a}{b}$, где $a, b \in \square$, $b \neq 0$, p не делит ни a, ни b, $n \in \square$. Положим $v_p(x) = n$. Дополнительно положим $v_p(0) = \infty$. Доказать, что v_p – дискретное нормирование на $\square$.
Оценка «зачтено» -	Пусть $A = 2/5$, $B = 1/5$, $C = 7/15$. Вычислить длины сторон

повышенный уровень освоения компетенции	треугольника ΔABC в 5-адической топологии.
Оценка «зачтено» - высокий уровень освоения компетенции	Пусть $k(x)$ – рациональное поле, p – неприводимый многочлен из $k[x]$, $\alpha \in k$, r – целое ≥ 0. Найти базисы пространств $L(rP_\alpha)$ и $L(rP_{p(x)})$.

Тема 2. Дифференциалы и теорема Римана – Роха

	Задача
Оценка «зачтено» - низкой уровень освоения компетенции	Пусть D – дифференцирование функционального поля F. Доказать, что для любого $x \in F$ и $n \in$ □ выполняется $nx^{n-1}D(x)$.
Оценка «зачтено» - повышенный уровень освоения компетенции	Пусть F/k – функциональное поле с совершенным полем констант k, x, y – сепарирующие элементы поля, то 1) $dy = \delta_x(y)dx$. 2) Если $\omega = udx = vdy \in \Omega_F$, то $u = vdy/dx$.
Оценка «зачтено» - высокий уровень освоения компетенции	Пусть $F = k(x)$ – рациональное поле с совершенным полем констант k, p – неприводимый многочлен из $k[x]$, $\alpha \in k$, δ – целое ≥ 0. Найти базисы пространств $\Omega_{k(x)}(-\delta P_\alpha)$ и $\Omega_{k(x)}(-\delta P_p)$.

Тема 3. *P*-адические разложения и вычеты

	Задача
Оценка «зачтено» - низкой уровень освоения компетенции	Пусть F – функциональное поле с совершенным полем констант k, P – его точка степени 1, t – локальный параметр точки P, $z = \sum_{i=m}^{\infty} \alpha_n t^n \in F$. Доказать, что $\frac{dz}{dt} = \sum_{i=m}^{\infty} n\alpha_n t^{n-1}$.
Оценка «зачтено» - повышенный уровень освоения компетенции	Пусть $F = k(x)$ – рациональное поле с совершенным полем констант k. Найти P-адические разложения дифференциалов dx и dx/x в рациональных точках поля $k(x)$.
Оценка «зачтено» - высокий уровень освоения компетенции	Пусть $k(x)$ – рациональное поле. Найти P-адическое разложение элемента $z \in k(x)$ в точках P для $z = \frac{x^3+x}{x^2+x+1} \in$ □$_2(x)$, $P = P_\infty$ и $P = P_\alpha$, где $\alpha \in$ □$_2$,

Тема 4. Алгеброгеометрические коды

	Задача
Оценка «зачтено» - низкой уровень освоения компетенции	Пусть □$_q(x)$ – рациональное функциональное поле, $G = \delta P$, $P_1,\ldots, P_n$ – рациональные точки поля F, не лежащие в supp G. Построить порождающую матрицу рационального кода $C_L(D, G)$.
Оценка «зачтено» - повышенный уровень освоения компетенции	Пусть □$_q(x)$ – рациональное функциональное поле, $G = \delta P$, $P_1,\ldots, P_n$ – рациональные точки поля F, не лежащие в supp G. Определить его размерность k, конструктивное расстояние d^*, минимальное расстояние

	d и число t исправляемых ошибок кода $C_L(D, G)$.
Оценка «зачтено» - высокий уровень освоения компетенции	Пусть $\square_q(x)$ – рациональное функциональное поле, $G = \delta P$, $P_1,\ldots, P_n$ – рациональные точки поля F, не лежащие в $\mathrm{supp}\, G$. Построить алгоритм декодирования кода $C_L(D, G)$.

8.3. Перечень вопросов и заданий для промежуточной аттестации по дисциплине

Вопросы для промежуточного контроля (зачёта)

1. Определение и общая структура функционального поля.
2. Дискретные нормирования. Кольца нормирования. Точки. Локальные параметры.
3. Поле классов вычетов точки. Отображение классов вычетов. Нули и полюсы элемента функционального поля.
4. Рациональное функциональное поле. Дискретные нормирования, кольца нормирования и точки, определяемые неприводимыми многочленами.
5. Рациональное функциональное поле. Дискретное нормирование, кольцо нормирование, определяемое бесконечной точкой.
6. Дивизоры функционального поля. Главный дивизор элемента функционального поля. Линейная эквивалентность дивизоров. Якобиан функционального поля.
7. Дивизоры рационального функционального поля.
8. Пространство Римана-Роха, ассоциированное с дивизором, его свойства. Род функционального поля. Теорема Римана.
9. Пространство Римана-Роха, ассоциированное с дивизором рационального функционального поля.
10. Дифференцирования функционального поля.
11. Дифференциалы функционального поля. Полные дифференциалы.
12. Канонический дивизор, ассоциированный с дифференциалом. Пространство дифференциалов, ассоциированное с дивизором, его свойства. Индекс специальности дивизора.
13. Теорема Римана-Роха, следствия из неё.
14. Канонические дивизоры рационального поля. Пространство дифференциалов, ассоциированное с дивизором рационального поля.
15. P-адические разложения элементов функционального поля. Дифференцирование P-адических разложений.
16. Вычет элемента функционального поля в точке. Вычет дифференциал в точке. Свойства вычетов. Теорема о вычетах.
17. Методика отыскания P-адических разложений в рациональных точках поля. Примеры.
18. Коды Рида-Соломона и их свойства.
19. AG-коды CL(D, G). Их структура и основные свойства.
20. AG-коды CΩ(D, G). Их структура и основные свойства.
21. Двойственность AG-кодов.
22. Представление кода CΩ(D, G) как CL(D, H).
23. Рациональные AG-коды. Их основные свойства.
24. Порождающая матрица рационального AG-кода.
25. Вычисление канонического дивизора рационального поля.
26. Предпосылки декодирования AG-кода. Синдром.
27. Отыскание функции локаторов ошибок.

28. Отыскание вектора ошибок.
29. Общий алгоритм декодирования AG-кодов.
30. Расширение функционального поля. Индекс ветвления. Типы расширений точки. Типы расширений функционального поля.
31. Расширение поля классов вычетов точки. Относительная степень расширения точки. Основное соотношение для степени.
32. Основное тождество для расширения точки. Конорма. Степень конормы.
33. Критерий неприводимости Эйзенштейна для многочленов над функциональным полем. Примеры.
34. Целое замыкание кольца нормирования в расширении функциональных полей. Целый базис расширения.
35. Теорема Куммера.
36. Следствие из теоремы Куммера.
37. Дифферента расширения функциональных полей. Теорема Дедекинда. Вычисление показателей дифференты.
38. Формула Гурвица для рода. Неравенство Римана. Вычисление канонического дивизора.
39. Группа автоморфизмов функционального поля. Расширения Галуа функциональных полей. Циклические расширения.
40. Расширение поля констант, его свойства.
41. Расширение Куммера, его свойства.
42. Расширение Артина-Шрайера, его свойства.
43. Вычисление базиса пространства $L(rQ\infty)$ в элементарном абелевом расширении.
44. Дзета-функция и L-многочлен функционального поля. Соотношения для коэффициентов L-многочлена.
45. Теорема Хассе-Вейля. Следствия. Граница Хассе-Вейля. Максимальные поля. Граница Серра.
46. Оценка числа точек произвольной степени.
47. Эллиптические функциональные поля. Их уравнения и основные свойства для характеристики $p \neq 2$.
48. Эллиптические функциональные поля. Их уравнения и основные свойства для характеристики $p = 2$.
49. Вычисление канонического дивизора эллиптического функционального поля.
50. Пример вычисления числа точек эллиптического функционального поля.

8.4. Планируемые уровни сформированности компетенций обучающихся и критерии оценивания

Уровни	Содержательное описание уровня	Основные признаки выделения уровня (этапы формирования компетенции, критерии оценки сформированности)	Пятибалльная шкала (академическая) оценка	Двухбалльная шакала, зачет	БРС, % освоения (рейтинговая оценка)

Повышенный	Творческая деятельность	*Включает нижестоящий уровень.* Умение самостоятельно принимать решение, решать проблему/задачу теоретического и прикладного характера на основе изученных методов, приемов, технологий	отлично	зачтено	86-100
Базовый	Применение знаний и умений в более широких контекстах учебной и профессиональной деятельности, нежели по образцу с большей степени самостоятельности и инициативы	*Включает нижестоящий уровень.* Способность собирать, систематизировать, анализировать и грамотно использовать информацию из самостоятельно найденных теоретических источников и иллюстрировать ими теоретические положения или обосновывать практику применения	хорошо		71-85
Удовлетворительный (достаточный)	Репродуктивная деятельность	Изложение в пределах задач курса теоретически и практически контролируемого материала	удовлетворительно		55-70
Недостаточный	Отсутствие признаков удовлетворительного уровня		неудовлетворительно	не зачтено	Менее 55

9. Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины.

Основная литература

1. Алешников С.И., Болтнев Ю.Ф. Математические методы защиты информации. Часть 5. Методы алгебраических кривых: Учебное пособие. – Калининград: БФУ им. И. Канта, 2015. – 166 с. on-line. ЭБС Кантиана

Дополнительная литература

1. Кнауб, Л. В. *Теоретико-численные методы в криптографии* [Электронный ресурс] : Учеб. пособие / Л. В. Кнауб, Е. А. Новиков, Ю. А. Шитов. - Красноярск : Сибирский федеральный университет, 2011. - 160 с. - ISBN 978-5-7638-2113-7. - Текст : электронный. - URL: https://znanium.com/catalog/product/441493
2. Романьков, В. А. Введение в криптографию : курс лекций / В.А. Романьков. — 2-е изд., испр. и доп. — Москва : ФОРУМ : ИНФРА-М, 2021. — 240 с. — (Высшее образование: Бакалавриат). - ISBN 978-5-00091-493-9. - Текст : электронный. - URL: https://znanium.com/catalog/product/1514566
3. Ященко, В. В. *Введение в криптографию*: Учебное пособие / Ященко В.В., - 4-е изд. - Москва :МЦНМО, 2014. - 352 с.: ISBN 978-5-4439-2162-4. - Текст : электронный. - URL: https://znanium.com/catalog/product/958585

10. Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины (модуля).

- ЭБС Кантиана (http://lib.kantiana.ru/irbis/standart/ELIB).
- Электронная библиотечная система «Znanium» (https://znanium.com/)
- Препринты института экспериментальной математики университета Дуйсбурга-Эссена (https://www.uni-due.de/mathematik/preprints.php).
- Форум «Функциональные поля и АГ-коды» (http://dxdy.ru/post925934.html).
- Лекторий «Арифметика алгебраических многообразий» (https://www.lektorium.tv/course/22986).
- Сайт книг по всем разделам теории чисел и её приложениям (http://www.numbertheory.org/ntw/N12.html).

11. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине.

Программное обеспечение обучения включает в себя:

- система электронного образовательного контента БФУ им. И. Канта – www.lms-3.kantiana.ru, обеспечивающую разработку и комплексное использование электронных образовательных ресурсов;
- серверное программное обеспечение, необходимое для функционирования сервера и связи с системой электронного обучения через Интернет;
- корпоративная платформа Microsoft Teams;
- установленное на рабочих местах обучающихся ПО: Microsoft Windows 7, Microsoft Office Standart 2010, антивирусное программное обеспечение Kaspersky Endpoint Security.
- специализированное ПО не требуется.

12. Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине.

Для проведения занятий лекционного типа, практических и семинарских занятий используются специальные помещения (учебные аудитории), оборудованные техническими средствами обучения – мультимедийной проекционной техникой. Для проведения занятий лекционного типа используются наборы демонстрационного оборудования.

Для проведения лабораторных работ, (практических занятий – при необходимости) используются специальные помещения (учебные аудитории), оснащенные специализированным лабораторным оборудованием: персональными компьютерами с возможностью выхода в интернет и с установленным программным обеспечением, заявленным в п.11.

Для проведения групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации используются специальные помещения (учебные аудитории), оборудованные специализированной мебелью (для обучающихся), меловой / маркерной доской.

Для организации самостоятельной работы обучающимся предоставляются помещения, оснащенные компьютерной техникой с возможностью подключения к сети «Интернет» и обеспечением доступа в электронную информационно-образовательную среду университета.

Для обучения инвалидов и лиц с ограниченными возможностями здоровья университетом могут быть представлены специализированные средства обучения, в том числе технические средства коллективного и индивидуального пользования.

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
федеральное государственное автономное образовательное учреждение высшего образования «Балтийский федеральный университет имени Иммануила Канта»
Институт физико-математических наук и информационных технологий

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

«Локальные поля и их приложения»

Шифр: 10.05.01
Специальность: «Компьютерная безопасность»
Специализация: «Математические методы защиты информации»
Квалификация (степень) выпускника: специалист по защите информации

Калининград
2022

Лист согласования

Составитель: Мельничук Евгений Михайлович, ассистент Института физико-математических наук и информационных технологий

Рабочая программа утверждена на заседании учебно-методического совета института физико-математических наук и информационных технологий
Протокол № 01/22 от «01» февраля 2022 г.
Председатель учебно-методического
совета института физико-
математических наук и
информационных технологий
Первый заместитель директора Шпилевой А. А
ИФМНиИТ, к. ф.-м. н., доцент

Ведущий менеджер Е.П.Ставицкая

Содержание

1.Наименование дисциплины: «Локальные поля и их приложения».

Цель дисциплины: целью освоения дисциплины «Локальные поля и их приложения» расширение и углубление специализированной алгебраической подготовки и подготовки студентов в области теории чисел до уровня, необходимого для анализа и формализации задач в области защиты информации и разработки математических моделей защищаемых информационных потоков; овладение методикой использования групп Брауэра в задачах анализа стойкости и эффективности криптосистем, изучение вычислительных процедур в локальных полях и подготовка к написанию теоретической части выпускной квалификационной работы.

2. Перечень планируемых результатов обучения по дисциплине, соотнесенных с планируемыми результатами освоения образовательной программы

Код компетенции	Результаты освоения образовательной программы (ИДК)	Результаты обучения по дисциплине
ПКС-7. Способность проводить анализ и участвовать в разработке математических моделей безопасности компьютерных систем	ПКС-7.1. Знает математические методы моделирования безопасных компьютерных систем. ПКС-7.2. Осуществляет анализ математических моделей безопасности компьютерных систем ПКС-7.3. Участвует в разработке математических моделей безопасности компьютерных систем	● ***знать*:** номенклатуру и основные характеристики сертифицированных программно-аппаратных средств защиты информации, выпускаемых российской промышленностью; математические методы и алгоритмы, применяемые в программно-аппаратных средствах защиты информации; перспективные математические методы защиты информации; ● ***уметь*:** осуществлять самостоятельную проектно-аналитическую работу; проводить сравнительный анализ эффективности математических методов и алгоритмов; ● ***владеть*:** навыками сравнительного анализа эффективности различных моделей, методов, алгоритмов, реализованных в средствах защиты информации, анализа их технических характеристик.

3. Место дисциплины в структуре образовательной программы

Дисциплина «Локальные поля и их приложения» представляет собой дисциплину части, формируемой участниками образовательных отношений блока дисциплин подготовки обучающихся.

4. Виды учебной работы по дисциплине.

Виды учебной работы по дисциплине зафиксированы учебным планом основной профессиональной образовательной программы по указанному направлению и профилю, выражаются в академических часах. Часы контактной работы и самостоятельной работы обчающегося и часы, отводимые на процедуры контроля, могут различаться в учебных планах ОПОП по формам обучения. Объем контактной работы включает часы контактной аудиторной работы (лекции/практические занятия/ лабораторные работы), контактной внеаудиторной работы (контроль самостоятельной работы), часы контактной работы в период аттестации. Контактная работа, в том числе может проводиться посредством электронной информационно-образовательной среды университета с использованием ресурсов сети Интернет и дистанционных технологий

5. Содержание дисциплины, структурированное по темам (разделам)

Исходя из рамок, установленных учебным планом по трудоемкости и видам учебной работы по дисциплине, преподаватель самостоятельно выбирает тематику занятий по формам и количеству часов проведения контактной работы: лекции и иные учебные занятия, предусматривающие преимущественную передачу учебной информации преподавателем и (или) занятия семинарского типа (семинары, практические занятия, практикумы, лабораторные работы, коллоквиумы и иные аналогичные занятия), и (или) групповые консультации, и (или) индивидуальную работу обучающихся с преподавателем, в том числе индивидуальные консультации (по курсовым работам/проектам – при наличии курсовой работы/проекта по данной дисциплине в учебном плане). Рекомендуемая тематика занятий максимально полно реализуется в контактной работе с обучающимися очной формы обучения. В случае реализации образовательной программы в заочной / очно-заочной форме трудоемкость дисциплины сохраняется, однако объем учебного материала в значительной части осваивается обучающимися в форме самостоятельной работы. При этом требования к ожидаемым образовательным результатам обучающихся по данной дисциплине не зависят от формы реализации образовательной программы.

№ п/п	Наименование темы	Содержание темы
1	Предварительные сведения.	Задачи и программа курса. Место теории локальных полей и групп Брауэра в ряду других математических и прикладных дисциплин. Источники её развития и направления развития. Роль теории локальных полей в задачах защиты информации. Формы самостоятельной работы студентов по изучению курса. Основная литература к курсу. Тензорное произведение модулей. Тензорное произведение алгебр. Проективные пределы топологических групп. Проконечные группы, их топологическая характеристика. Построение проконечных групп из абстрактных групп.

		Проконечные группы в теории полей. Когомологии Галуа. Точная когомологическая последовательность. Ограничение и инфляция. Индуктивные пределы абелевых групп. Дискретные модули. Когомологии проконечных групп. Примеры.
2	Локальные поля.	Абсолютные значения и нормирования. Неархимедово нормирование. Кольцо и идеал нормирования. Поле классов вычетов. n-группы единиц. Полные поля. Процедура пополнения. Теорема Островского. Свойства пополнения. Представление элементов пополнения. Лемма Гензеля. Нормирование расширения. Локальные поля. Логарифмическая и показательная функции. Структура группы единиц локального поля. Неразветвлённые и слаборазветвлённые расширения. Продолжение нормирований. Расширения Галуа локальных полей.
3	Группы Брауэра.	Центрально-простые алгебры над полем. Теорема Веддербёрна. Теорема Сколема – Нётер. Отношение подобия. Группы Брауэра. Отображение ограничения. Поле расщепления алгебры. Относительные группы Брауэра. Примеры. Скрещенное произведение. Связь группы Брауэра с когомологиями Галуа. Случай циклического расширения Галуа. Связь относительной группы Брауэра с отображением нормы.
4	Группы Брауэра локального и глобального поля, применение в криптографии.	Отображение нормы групп единиц локального поля. Вычисление группы Брауэра локального поля. Отображение инвариантов. Группа Брауэра глобального поля. Теорема Хассе – Брауэра – Нётер. Дискретный логарифм в группе единиц конечного поля. Описание подходящей группы Брауэра. Перевод проблемы дискретного логарифмирования в подходящую группу Брауэра.
5	Локальные вычисления инвариантов.	Вычисление отображений инвариантов в неразветвлённых расширениях. Вывод соотношений для инвариантов. Вычисление инвариантов в слаборазветвлённых расширениях. Свойства отображения θ. Вычисление инвариантов в локальном поле, являющемся расширением Куммера.
6	Локально-глобальные методы.	Постановка задачи явного вычисления инвариантов. Сведение задачи явного вычисления инвариантов к задаче явного построения глобальной алгебры. Свойства расширения Куммера. Подъём локальной алгебры до глобальной. Эффективные методы вычисления инвариантов. Примеры. Анализ экспериментальных результатов.

6. Рекомендуемая тематика учебных занятий в форме контактной работы

Рекомендуемая тематика учебных занятий *лекционного* типа (предусматривающих преимущественную передачу учебной информации преподавателями):

№	Наименование раздела	Темы лекций
1	Предварительные сведения.	Лекция 1. Тензорное произведение модулей. Тензорное произведение алгебр. Лекция 2. Когомологии Галуа.
2	Локальные поля.	Лекция 4. Кольцо и идеал нормирования. Поле классов вычетов Лекция 5. Теорема Островского. Лемма Гензеля. Лекция 6. Локальные поля. Логарифмическая и показательная функции.
3	Группы Брауэра.	Лекция 7. Центрально-простые алгебры над полем. Лекция 8. Группы Брауэра. Лекция 9. Связь группы Брауэра с когомологиями Галуа.
4	Группы Брауэра локального и глобального поля, применение в криптографии.	Лекция 10. Вычисление группы Брауэра локального поля. Лекция 11 Теорема Хассе – Брауэра – Нётер. Лекции 12. Перевод проблемы дискретного логарифмирования в подходящую группу Брауэра.
5	Локальные вычисления инвариантов.	Лекция 13. Вычисление отображений инвариантов в неразветвлённых расширениях. Лекция 14. Вычисление инвариантов в слаборазветвлённых расширениях. Лекция 15. Вычисление инвариантов в локальном поле, являющемся расширением Куммера.
6	Локально-глобальные методы.	Лекция 16. Постановка задачи явного вычисления инвариантов.

Рекомендуемая тематика *практических* занятий:

№ п/п	Наименование Темы	Содержание темы
1	Предварительные сведения.	Вычисление первых и вторых групп когомологий конечных и проконечных групп.
2	Локальные поля.	Вычисления в локальных полях.
3	Группы Брауэра.	Когомологическое описание групп Брауэра циклических расширений локальных полей.
4	Группы Брауэра локального и глобального поля, применение в криптографии.	По данной теме практических занятий не предусмотрено.
5	Локальные вычисления инвариантов.	Вычисление отображений инвариантов в неразветвлённых и слаборазветвлённых расширениях локальных полей.
6	Локально-глобальные методы.	Явное вычисление инвариантов циклических расширений локальных полей и дискретное логарифмирование в группах Брауэра.

Требования к самостоятельной работе обучающихся

1. Работа с лекционным материалом, предусматривающая проработку конспекта лекций и учебной литературы, по всем темам из п. 6 настоящей рабочей программы.

2. Выполнение домашнего задания, предусматривающего решение задач, выполнение упражнений, выдаваемых на практических занятиях, по всем темам из п. 6 настоящей рабочей программы.

Руководствуясь положениями статьи 47 и статьи 48 Федерального закона от 29 декабря 2012 г. N 273-ФЗ «Об образовании в Российской Федерации» научно-педагогические работники и иные лица, привлекаемые университетом к реализации данной образовательной программы, пользуются предоставленными академическими правами и свободами в части свободы преподавания, свободы от вмешательства в профессиональную деятельность; свободы выбора и использования педагогически обоснованных форм, средств, методов обучения и воспитания; права на творческую инициативу, разработку и применение авторских программ и методов обучения и воспитания в пределах реализуемой образовательной программы и отдельной дисциплины.

Исходя из рамок, установленных учебным планом по трудоемкости и видам учебной работы по дисциплине, преподаватель самостоятельно выбирает тематику занятий по формам и количеству часов проведения контактной работы: лекции и иные учебные занятия, предусматривающие преимущественную передачу учебной информации преподавателем и (или) занятия семинарского типа (семинары, практические занятия, практикумы, лабораторные работы, коллоквиумы и иные аналогичные занятия), и (или) групповые консультации, и (или) индивидуальную работу обучающихся с преподавателем, в том числе индивидуальные консультации (по курсовым работам/проектам – при наличии курсовой работы/проекта по данной дисциплине в учебном плане).

Рекомендуемая тематика занятий максимально полно реализуется в контактной работе с обучающимися очной формы обучения. В случае реализации образовательной программы в заочной / очно-заочной форме трудоемкость дисциплины сохраняется, однако объем учебного материала в значительной части осваивается обучающимися в форме самостоятельной работы. При этом требования к ожидаемым образовательным результатам обучающихся по данной дисциплине не зависят от формы реализации образовательной программы.

7. Методические рекомендации по видам занятий

Лекционные занятия.

В ходе лекционных занятий обучающимся рекомендуется выполнять следующие действия. Вести конспектирование учебного материала. Обращать внимание на категории, формулировки, раскрывающие содержание тех или иных явлений и процессов, научные выводы и практические рекомендации по их применению. Задавать преподавателю уточняющие вопросы с целью уяснения теоретических положений, разрешения спорных ситуаций.

Желательно оставить в рабочих конспектах поля, на которых во внеаудиторное время можно сделать пометки из рекомендованной литературы, дополняющие

материал прослушанной лекции, а также подчеркивающие особую важность тех или иных теоретических положений.

Практические и семинарские занятия.

На практических и семинарских занятиях в зависимости от темы занятия выполняется поиск информации по решению проблем, практические упражнения, контрольные работы, выработка индивидуальных или групповых решений, итоговое обсуждение с обменом знаниями, участие в круглых столах, разбор конкретных ситуаций, командная работа, представление портфолио и т.п.

Самостоятельная работа.

Самостоятельная работа осуществляется в виде изучения литературы, эмпирических данных по публикациям и конкретных ситуаций из практики, подготовке индивидуальных работ, работа с лекционным материалом, самостоятельное изучение отдельных тем дисциплины; поиск и обзор литературы и электронных источников; чтение и изучение учебника и учебных пособий.

8. Фонд оценочных средств

8.1. Перечень компетенций с указанием этапов их формирования в процессе освоения образовательной программы в рамках учебной дисциплины

Основными этапами формирования указанных компетенций при изучении обучающимися дисциплины являются последовательное изучение содержательно связанных между собой тем учебных занятий. Изучение каждой темы предполагает овладение обучающимися необходимыми компетенциями. Результат аттестации обучающихся на различных этапах формирования компетенций показывает уровень освоения компетенций.

Контролируемые разделы (темы) дисциплины	Индекс контроли-руемой компетенции (или её части)	Оценочные средства по этапам формирования компетенций
		текущий контроль по дисциплине
Тема 1. Предварительные сведения.	ПКС-7	Опрос, решение задач.
Тема 2. Локальные поля.	ПКС-7	Опрос, решение задач
Тема 3. Группы Брауэра.	ПКС-7	Опрос, решение задач
Тема 4. Группы Брауэра локального и глобального поля, применение в криптографии.	ПКС-7	Опрос, письменный опрос
Тема 5. Локальные вычисления инвариантов.	ПКС-7	Опрос, решение задач
Тема 6. Локально-глобальные методы.	ПКС-7	Опрос, решение задач

8.2. Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений и навыков и (или) опыта деятельности процессе текущего контроля

Примеры задач для решения:

Тема 1. Предварительные сведения

	Задача
Оценка «зачтено» - низкой уровень освоения компетенции	Пусть E – алгебра над коммутативным кольцом A, а – идеал в A. Доказать, что имеет место изоморфизм $E \otimes_A (A/\mathfrak{a}) \cong E/\mathfrak{a}E$, где $\mathfrak{a}E$ – идеал в E, порожденный элементами вида αx, $\alpha \in \mathfrak{a}$, $x \in E$.
Оценка «зачтено» - повышенный уровень освоения компетенции	Проверить свойства граничного гомоморфизма $\partial_q : C^{q-1} \to C^q$.
Оценка «зачтено» - высокий уровень освоения компетенции	Вычислить нулевую и первую группы когомологий конечного поля $\mathbb{F}_q$ для его группы автоморфизмов.

Тема 2. Локальные поля

	Задача
Оценка «зачтено» - низкой уровень освоения компетенции	Для заданного локального поля $\mathbb{Q}_2(\zeta_5)$ найти поле классов вычетов.
Оценка «зачтено» - повышенный уровень освоения компетенции	Для заданного локального поля $\mathbb{Q}_2(\zeta_5)$ найти простой элемент π.
Оценка «зачтено» - высокий уровень освоения компетенции	Для заданного локального поля $\mathbb{Q}_2(\zeta_5)$ найти индекс ветвления e относительную степень f над $\mathbb{Q}_2$.

Тема 3. Группа Брауэра

	Задача
Оценка «зачтено» - низкой уровень освоения компетенции	Для заданного циклического расширения $\mathbb{Q}_5(\sqrt[3]{2})$ локального поля $\mathbb{Q}_5$ найти простой элемент поля $\mathbb{Q}_5$.
Оценка «зачтено» - повышенный уровень освоения компетенции	Для заданного циклического расширения $\mathbb{Q}_5(\sqrt[3]{2})$ локального поля $\mathbb{Q}_5$ найти образующую группы $\mathrm{Gal}(\mathbb{Q}_5(\sqrt[3]{2})/\mathbb{Q}_5)$.
Оценка «зачтено» - высокий уровень освоения компетенции	Для заданного циклического расширения $\mathbb{Q}_5(\sqrt[3]{2})$ локального поля $\mathbb{Q}_5$ вычислить норму $N((\mathbb{Q}_5(\sqrt[3]{2}))^*)$.

Тема 5. Локальные вычисления инвариантов

	Задача
Оценка «зачтено» - низкой уровень освоения компетенции	Пусть $K = \mathbb{Q}_3(\sqrt{2})$, $L = K(\zeta_5)$. Найти тип расширения L/K.
Оценка «зачтено» - повышенный уровень освоения компетенции	Пусть $K = \mathbb{Q}_3(\sqrt{2})$, $L = K(\zeta_5)$. Найти простой элемент π поля K,
Оценка «зачтено» - высокий уровень освоения компетенции	Пусть $K = \mathbb{Q}_3(\sqrt{2})$, $L = K(\zeta_5)$. Найти элемент Фробениуса для идеала $\mathfrak{p} = (\pi) \subset K$.

Примеры вопросов для устного опроса:

Тема 1. Предварительные сведения

1. Сформулировать универсальное свойство тензорного произведения.
1. Сформулировать определение проконечной группы.
2. Описать построение проконечных групп из абстрактных групп.
3. Как вычисляется группа Галуа бесконечного расширения полей?
4. Описать структуру проконечных групп, возникающих из теории полей.
5. Охарактеризовать группы когомологий малой размерности.
6. Что такое связывающий гомоморфизм?
7. Как вычислить группы когомологий проконечных групп?
8. Сформулировать «теорему Гильберта 90».

Тема 2. Локальные поля

1. Доказать в качестве упражнения строгое неравенство треугольника.
2. Что такое экспоненциальное нормирование поля?
3. Что такое кольцо нормирования и идеал нормирования?
4. Что такое локальный параметр дискретного нормирования?
5. Какими свойствами обладает кольцо дискретного нормирования?
6. Описать структуру высших групп единиц.
7. В чём состоит идея пополнения?
8. В чём смысл теоремы Островского?
9. Как соотносятся локальные кольца и их максимальный идеалы с соответствующими пополнениями?
10. Какова процедура пополнения с помощью проективных пределов?
11. Сформулировать лемму Гензеля.
12. Дать определение локального поля.
13. Логарифмическая и показательная функции.
14. Сформулировать основные свойства локальных полей.
15. Описать свойства высших групп единиц локального поля.
16. Описать структуру мультипликативной группы локального поля.
17. Описать структуру неразветвлённого расширения локального поля.
18. Что такое максимальное неразветвлённое расширение локального поля?

19. Что такое слабо разветвлённое расширение локального поля?
20. Описать структуру слабо разветвлённого расширения локального поля.
21. Что такое максимальное слабо разветвлённое расширение локального поля?
22. Свойства циклических расширений поля p-адических чисел.
23. Как строится продолжение нормирования на алгебраическое расширение поля?
24. Какова связь продолжений нормирований и вложений полей?

Тема 3. Группа Брауэра

1. Сформулировать теорему Веддербёрна.
2. Сформулировать теорему Сколема – Нётер.
3. Описать соотношение подобия центральных простых алгебр.
4. Дать общее определение группы Брауэра поля K.
5. Отображение ограничения. Поле расщепления алгебры.
6. Что такое относительная группа Брауэра? Какова её связь с общей группой Брауэра?
7. Чему равна группа Брауэра конечного поля?
8. Чему равна группа Брауэра алгебраически замкнутого поля?
9. Чему равна группа Брауэра вещественно замкнутого поля?
10. Дать определение скрещенного произведения.
11. Описать изоморфизм группы Брауэра и 2-й группы когомологий.
12. Описать структуру скрещенного произведения в случае циклического расширения Галуа.
13. Связь относительной группы Брауэра с отображением нормы.
14. Отображение нормы групп единиц локального поля.
15. Описать группу Брауэра в терминах основного поля.

Тема 4. Группы Брауэра локального и глобального поля, применение в криптографии

1. Основное свойство нормы циклического неразветвлённого расширения локального поля.
2. Чему равна группа Брауэра неразветвлённого расширения степени n поля K?
3. Сформулировать фундаментальную теорему о группах Брауэра локальных полей.
4. Описать группу Брауэра локального поля.
5. Описать связь группы Брауэра с группой корней из единицы.
6. Чему равна группа Брауэра неразветвлённого расширения степени n поля K?
7. Дать определение отображения инвариантов.
8. Свойства локальных групп Брауэра числового поля.
9. Прокомментировать точную последовательность Хассе – Брауэра – Нётер.
10. Связь группы Брауэра с группой корней из единицы.
11. Решение проблемы дискретного логарифма в группе корней из единицы с помощью группы Брауэра.
12. Описать свойства нормы циклического неразветвлённого расширения локального поля.
13. Дискретный логарифм в группе единиц конечного поля.
14. Перевод проблемы дискретного логарифмирования в подходящую группу Брауэра.

Тема 5. Локальные вычисления инвариантов

1. Как с помощью коциклов задаются элементы группы Брауэра неразветвлённого расширения локального поля?
2. Как вычисляются значения отображений инвариантов в неразветвлённых расширениях локального поля?
3. Как с помощью коциклов задаются элементы группы Брауэра слабо разветвлённых расширений локального поля?
4. Как задаются инфляции коциклов?
5. Как вычисляются значения отображений инвариантов в слабо разветвлённых расширениях локального поля?
6. Каковы свойства фундаментального отображения θ?
7. Как вычисляются значения отображений инвариантов в локальных полях в общем?
8. Свойства расширения Куммера как слаборазветвлённого расширения.

Тема 6. Локально-глобальные методы

1. Описать постановку задачи явного описания инвариантов.
2. Какова структура основной короткой точной последовательности для групп Брауэра?
3. Интерпретация локальных инвариантов с точки зрения теоремы Хассе – Брауэра – Нётер.
4. Описать подход к явному вычислению инвариантов с помощью сведение задачи явного вычисления инвариантов к задаче явного построения глобальной алгебры.
5. Описать процедуру подъёма локальной алгебры до глобальной.
6. Привести пример явного вычисления инвариантов.
7. Прокомментировать экспериментальные результаты по дискретному логарифмированию с помощью групп Брауэра.

Вопросы для письменного опроса:

Тема 4. Группы Брауэра локального и глобального поля, применение в криптографии

1. В чём заключается основное свойство нормы циклического неразветвлённого расширения локального поля?
2. Описать изоморфизм для группы Брауэра неразветвлённого расширения степени n поля K.
3. Описать изоморфизм для группы Брауэра локального поля.
4. Какова связь группы Брауэра с группой корней из единицы.
5. Как определяется отображение инвариантов?
6. Какова структура группы Брауэра числового поля?
7. Что такое точная последовательность Хассе – Брауэра – Нётер.
8. Описать изоморфизм, позволяющий перенести проблему дискретного логарифма из группы корней из единицы в группу Брауэра?

Тема 5. Локальные вычисления инвариантов

Пусть $K = \mathbb{Q}_p(\zeta)$, где ζ – примитивный корень степени n из единицы, $(n, p) = 1$.

1. Описать картину ветвления в $K / \mathbb{Q}_p$.
2. Найти группу Галуа $Gal(K / \mathbb{Q}_p)$.
3. Указать кольцо нормирования $\mathbb{Q}$.

4. Описать группу Брауэра $Br(K / \mathbb{Q}_p)$.
5. Указать поле классов вычетов k поля K и описать перенос проблемы дискретного логарифмирования из конечного поля k в группу Брауэра $Br(K / \mathbb{Q}_p)$.
6. Указать соотношения, используемые для вычисления инвариантов.

Тема 6. Локально-глобальные методы

Для заданного простого числа l и конечного поля $\mathbb{Q}_q$, такого, что $l \mid q - 1$, и $p = \mathrm{char}\, \mathbb{Q}_q$, построить:

1. расширение K поля $\mathbb{Q}_p$ с полем классов вычетов $k = \mathbb{Q}_q$,
2. циклическое разветвлённое расширение Галуа L / K степени l с группой Галуа $Gal(L / K) = \langle \sigma \rangle$.

Для заданных элементов $\zeta_0, \zeta_1 \in \mu_l \subset \mathbb{F}_q^{\times}$:

3. взять циклические алгебры $A_0 = (L / K, \sigma, \zeta_0)$, $A_1 = (L / K, \sigma, \zeta_1)$,
4. вычислить $inv(A_0)$ и $inv(A_1) = n \cdot inv(A_0)$,
5. вычислить дискретный логарифм $n = \dfrac{inv(A_1)}{inv(A_0)} \pmod{l}$.

8.3. Перечень вопросов и заданий для промежуточной аттестации по дисциплине

Вопросы для промежуточного контроля (зачёта)

1. Тензорное произведение модулей. Тензорное произведение алгебр.
2. Проективные пределы топологических групп. Проконечные группы, их топологическая характеристика. Построение проконечных групп из абстрактных групп.
3. Проконечные группы в теории полей.
4. Когомологии Галуа. Точная когомологическая последовательность.
5. Ограничение и инфляция. Построение и свойства.
6. Индуктивные пределы абелевых групп.
7. Дискретные модули. Когомологии проконечных групп.
8. Примеры когомологий проконечных групп.
9. Абсолютные значения и нормирования. Неархимедово нормирование.
10. Кольцо и идеал нормирования. Поле классов вычетов.
11. *n*-группы единиц.
12. Полные поля. Процедура пополнения. Теорема Островского.
13. Свойства пополнения.
14. Представление элементов пополнения.
15. Лемма Гензеля.
16. Нормирование расширения.
17. Локальные поля.
18. Логарифмическая и показательная функции.
19. Структура группы единиц локального поля.
20. Неразветвлённые расширения локальных полей.
21. Слаборазветвлённые расширения локальных полей.

22. Примеры неразветвленных и слаборазветвлённых расширений.
23. Продолжение нормирований.
24. Продолжение нормирований и вложения полей.
25. Центрально-простые алгебры над полем. Теорема Веддербёрна. Теорема Сколема – Нётер.
26. Центр тензорного произведения. Отношение подобия.
27. Группы Брауэра. Алгебраическая операция в группе Брауэра.
28. Отображение ограничения. Поле расщепления алгебры. Относительные группы Брауэра.
29. Примеры групп Брауэра.
30. Скрещенное произведение. Связь группы Брауэра с когомологиями Галуа.
31. Группа Брауэра циклического расширения Галуа.
32. Изоморфизм для скрещенного произведения.
33. Связь относительной группы Брауэра с отображением нормы.
34. Отображение нормы групп единиц локального поля.
35. Вычисление группы Брауэра локального поля.
36. Отображение инвариантов.
37. Группа Брауэра глобального поля.
38. Теорема Хассе – Брауэра – Нётер.
39. Дискретный логарифм в группе единиц конечного поля. Описание подходящей группы Брауэра.
40. Перевод проблемы дискретного логарифмирования в подходящую группу Брауэра.
41. Вычисление отображений инвариантов в неразветвлённых расширениях.
42. Вывод соотношений для инвариантов.
43. Вычисление инвариантов в слаборазветвлённых расширениях.
44. Свойства отображения θ.
45. Свойства расширения Куммера как слаборазветвлённого расширения.
46. Постановка задачи явного вычисления инвариантов. Сведение задачи явного вычисления инвариантов к задаче явного построения глобальной алгебры.
47. Свойства расширения Куммера.
48. Подъем локальной алгебры до глобальной.
49. Эффективные методы вычисления инвариантов.
50. Описание исходных данных для экспериментов. Анализ экспериментальных результатов.

8.4. Планируемые уровни сформированности компетенций обучающихся и критерии оценивания

Уровни	Содержательное описание уровня	Основные признаки выделения уровня (этапы формирования компетенции, критерии оценки сформированности)	Пятибалльная шкала (академическая) оценка	Двухбалльная шакала, зачет	БРС, % освоения (рейтинговая оценка)
Повышенный	Творческая деятельность	*Включает нижестоящий уровень.* Умение самостоятельно	отлично	зачтено	86-100

		принимать решение, решать проблему/задачу теоретического и прикладного характера на основе изученных методов, приемов, технологий			
Базовый	Применение знаний и умений в более широких контекстах учебной и профессиональной деятельности, нежели по образцу с большей степени самостоятельности и инициативы	*Включает нижестоящий уровень.* Способность собирать, систематизировать, анализировать и грамотно использовать информацию из самостоятельно найденных теоретических источников и иллюстрировать ими теоретические положения или обосновывать практику применения	хорошо		71-85
Удовлетворительный (достаточный)	Репродуктивная деятельность	Изложение в пределах задач курса теоретически и практически контролируемого материала	удовлетворительно		55-70
Недостаточный	Отсутствие признаков удовлетворительного уровня		неудовлетворительно	не зачтено	Менее 55

9. Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины.

Основная литература

1. Алешников С.И., Болтнев Ю.Ф. Математические методы защиты информации. Часть 5. Методы алгебраических кривых: Учебное пособие. – Калининград: БФУ им. И. Канта, 2015. – 166 с. on-line. ЭБС Кантиана

Дополнительная литература

1. Кнауб, Л. В. *Теоретико-численные методы в криптографии* [Электронный ресурс] : Учеб. пособие / Л. В. Кнауб, Е. А. Новиков, Ю. А. Шитов. - Красноярск : Сибирский федеральный университет, 2011. - 160 с. - ISBN 978-5-7638-2113-7. - Текст : электронный. - URL: https://znanium.com/catalog/product/441493

2. Локальные поля и их приложения [Электронный ресурс]: учеб.-метод. комплекс/ М-во образования и науки РФ, Балт. федер. ун-т им. И. Канта, Ин-т приклад. математики и информац. технологий; сост. С. И. Алешников. - Калининград: БФУ им. И. Канта, 2015. - 1 on-line, 128 с.. - Бессрочная лицензия. - Б.ц. Имеются экземпляры в отделах /There are copies in departments: ЭБС Кантиана(1)

10. Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины (модуля).

- ЭБС Кантиана (http://lib.kantiana.ru/irbis/standart/ELIB).
- Электронная библиотечная система «Znanium» (https://znanium.com/)
- Препринты института экспериментальной математики университета Дуйсбурга-Эссена (https://www.uni-due.de/mathematik/preprints.php).
- Форум «Функциональные поля и АГ-коды» (http://dxdy.ru/post925934.html).
- Лекторий «Арифметика алгебраических многообразий» (https://www.lektorium.tv/course/22986).
- Сайт книг по всем разделам теории чисел и её приложениям (http://www.numbertheory.org/ntw/N12.html).

11. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине.

Программное обеспечение обучения включает в себя:

- система электронного образовательного контента БФУ им. И. Канта – www.lms-3.kantiana.ru, обеспечивающую разработку и комплексное использование электронных образовательных ресурсов;
- серверное программное обеспечение, необходимое для функционирования сервера и связи с системой электронного обучения через Интернет;
- корпоративная платформа Microsoft Teams;
- установленное на рабочих местах обучающихся ПО: Microsoft Windows 7, Microsoft Office Standart 2010, антивирусное программное обеспечение Kaspersky Endpoint Security.
- специализированное ПО не требуется.

12. Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине.

Для проведения занятий лекционного типа, практических и семинарских занятий используются специальные помещения (учебные аудитории), оборудованные техническими средствами обучения – мультимедийной проекционной техникой. Для проведения занятий лекционного типа используются наборы демонстрационного оборудования.

Для проведения лабораторных работ, (практических занятий – при необходимости) используются специальные помещения (учебные аудитории), оснащенные специализированным лабораторным оборудованием: персональными компьютерами с возможностью выхода в интернет и с установленным программным обеспечением, заявленным в п.11.

Для проведения групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации используются специальные помещения (учебные аудитории), оборудованные специализированной мебелью (для обучающихся), меловой / маркерной доской.

Для организации самостоятельной работы обучающимся предоставляются помещения, оснащенные компьютерной техникой с возможностью подключения к сети «Интернет» и обеспечением доступа в электронную информационно-образовательную среду университета.

Для обучения инвалидов и лиц с ограниченными возможностями здоровья университетом могут быть представлены специализированные средства обучения, в том числе технические средства коллективного и индивидуального пользования.

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
федеральное государственное автономное образовательное учреждение высшего образования «Балтийский федеральный университет имени Иммануила Канта»
Институт физико-математических наук и информационных технологий

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

«Криптографические протоколы для защиты банковской информации»

Шифр: 10.05.01
Специальность: «Компьютерная безопасность»
Специализация: «Математические методы защиты информации»
Квалификация (степень) выпускника: специалист по защите информации

Калининград
2022

Лист согласования

Составитель: Белова Ольга Олеговна, к.ф.-м.н., доцент

Рабочая программа утверждена на заседании учебно-методического совета института физико-математических наук и информационных технологий

Протокол № 01/22 от «01» февраля 2022 г.

Председатель учебно-методического совета института физико-математических наук и информационных технологий

Первый заместитель директора ИФМНиИТ, к. ф.-м. н., доцент — Шпилевой А. А

Ведущий менеджер — Е.П.Ставицкая

Содержание

1.Наименование дисциплины: «*Криптографические протоколы для защиты банковской информации*».

Цель дисциплины: целью изучения дисциплины «*Криптографические протоколы для защиты банковской информации*» является формирование знаний об основополагающих принципах защиты информации с помощью криптографических методов и примеров реализации этих методов на практике.

2. Перечень планируемых результатов обучения по дисциплине, соотнесенных с планируемыми результатами освоения образовательной программы

Код компетенции	Результаты освоения образовательной программы (ИДК)	Результаты обучения по дисциплине
ПКС-2. Способен разрабатывать требования по защите, формировать политики безопасности компьютерных систем и сетей.	ПКС-2.1. Выполняет анализ безопасности компьютерных систем и разрабатывает рекомендации по эксплуатации системы защиты информации. ПКС-2.2. Разработка модели угроз безопасности информации. ПКС-2.3. Формирует политики безопасности компьютерных систем и сетей.	• **знать** основы построения системы защиты компьютерных систем, базовые криптографические протоколы, применяемые в электронной коммерции и в электронном документообороте; виды атак на протоколы; • **уметь:** проводить аналитическую работу в области информационной безопасности компьютерных систем, проводить сравнительный анализ криптографических протоколов, решающих сходные задачи; • **владеть:** навыками работы с ПК, криптографической терминологией; навыками построения моделей криптографических протоколов, которые используются на практике

3. Место дисциплины в структуре образовательной программы

Дисциплина «*Криптографические протоколы для защиты банковской информации*» относится к части, формируемой участниками образовательных отношений блока Дисциплины подготовки обучающихся, представляет собой дисциплину по выбору раздела «Дисциплины», Б1.В.ДВ.04.01.

4. Виды учебной работы по дисциплине.

Виды учебной работы по дисциплине зафиксированы учебным планом основной профессиональной образовательной программы по указанному направлению и профилю, выражаются в академических часах. Часы контактной работы и самостоятельной работы обчающегося и часы, отводимые на процедуры контроля, могут различаться в учебных планах ОПОП по формам обучения. Объем контактной работы включает часы контактной аудиторной работы (лекции/практические занятия/ лабораторные работы), контактной внеаудиторной работы (контроль самостоятельной работы), часы контактной работы в период аттестации. Контактная работа, в том числе может проводиться посредством электронной информационно-образовательной среды университета с использованием ресурсов сети Интернет и дистанционных технологий

5. Содержание дисциплины, структурированное по темам (разделам)

Исходя из рамок, установленных учебным планом по трудоемкости и видам учебной работы по дисциплине, преподаватель самостоятельно выбирает тематику занятий по формам и количеству часов проведения контактной работы: лекции и иные учебные занятия, предусматривающие преимущественную передачу учебной информации преподавателем и (или) занятия семинарского типа (семинары, практические занятия, практикумы, лабораторные работы, коллоквиумы и иные аналогичные занятия), и (или) групповые консультации, и (или) индивидуальную работу обучающихся с преподавателем, в том числе индивидуальные консультации (по курсовым работам/проектам – при наличии курсовой работы/проекта по данной дисциплине в учебном плане). Рекомендуемая тематика занятий максимально полно реализуется в контактной работе с обучающимися очной формы обучения. В случае реализации образовательной программы в заочной / очно-заочной форме трудоемкость дисциплины сохраняется, однако объем учебного материала в значительной части осваивается обучающимися в форме самостоятельной работы. При этом требования к ожидаемым образовательным результатам обучающихся по данной дисциплине не зависят от формы реализации образовательной программы.

№	Наименование раздела	Содержание раздела
1	Введение	Роль криптографических протоколов для банковских операций.
2	Основные виды криптографических протоколов. Роль криптографических протоколов в системах защиты информации.	Протоколы аутентификации. Алгоритм разложения на множители.
3	Протокол электронной подписи	Электронная подпись. Стираемые подписи.
4	Криптографические протоколы в электронной коммерции и в электронном документообороте	Электронные деньги. Аутентификация и электронные платежи.

6. Рекомендуемая тематика учебных занятий в форме контактной работы

Рекомендуемая тематика учебных занятий *лекционного* типа (предусматривающих преимущественную передачу учебной информации преподавателем):

№	Наименование раздела	Темы лекций
1	Введение.	Задачи и программа дисциплины.
2	Основные виды криптографических протоколов. Роль криптографических протоколов в системах защиты информации.	Понятие криптографического протокола. Подходы к классификации криптографических протоколов. Подходы к моделированию криптографических протоколов. Свойства протоколов, характеризующие их безопасность. Основные виды уязвимостей. Виды атак на криптографические протоколы. Подходы к моделированию криптографических протоколов.
3	Протокол электронной подписи.	Схема Эль-Гамаля. Схема RSA. Хэш-функции. Криптостойкость и особенности.
4	Криптографические протоколы в электронной коммерции и в электронном документообороте.	Классификация и структура СЭП. Неанонимные СЭП, работающие в реальном масштабе времени. Неанонимные автономные СЭП. Анонимные СЭП, работающие в реальном масштабе времени. Анонимные автономные СЭП. Основные задачи защиты информации в электронной коммерции. Классификация задач электронной коммерции. Честный обмен цифровыми подписями и его приложения. Многосторонние транзакции, коммерческие сделки.

Рекомендуемая тематика *практических* занятий:

1. Схема аутентификации Фиата и Шамира.

2. Схема аутентификации Шнорра.

3. Схема аутентификации Брикелла и МакКарли.

4. Схема Эль Гамаля.

5. Схемы RSA и Рабина.

6. Хэш-функции.

7. Протоколы типа Диффи – Хеллмана.

8. Схема Брандса.

На практических занятиях решаются задачи по теме занятия.

Требования к самостоятельной работе обучающихся

1. Работа с лекционным материалом, предусматривающая проработку конспекта лекций и учебной литературы, по всем темам из п. 6 настоящей рабочей программы.

2. Выполнение домашнего задания, предусматривающего решение задач, выполнение упражнений, выдаваемых на практических занятиях, по всем темам из п. 6 настоящей рабочей программы.

Руководствуясь положениями статьи 47 и статьи 48 Федерального закона от 29 декабря 2012 г. N 273-ФЗ «Об образовании в Российской Федерации» научно-педагогические работники и иные лица, привлекаемые университетом к реализации данной образовательной программы, пользуются предоставленными академическими правами и свободами в части свободы преподавания, свободы от вмешательства в профессиональную деятельность; свободы выбора и использования педагогически обоснованных форм, средств, методов обучения и воспитания; права на творческую инициативу, разработку и применение авторских программ и методов обучения и воспитания в пределах реализуемой образовательной программы и отдельной дисциплины.

Исходя из рамок, установленных учебным планом по трудоемкости и видам учебной работы по дисциплине, преподаватель самостоятельно выбирает тематику занятий по формам и количеству часов проведения контактной работы: лекции и иные учебные занятия, предусматривающие преимущественную передачу учебной информации преподавателем и (или) занятия семинарского типа (семинары, практические занятия, практикумы, лабораторные работы, коллоквиумы и иные аналогичные занятия), и (или) групповые консультации, и (или) индивидуальную работу обучающихся с преподавателем, в том числе индивидуальные консультации (по курсовым работам/проектам – при наличии курсовой работы/проекта по данной дисциплине в учебном плане).

Рекомендуемая тематика занятий максимально полно реализуется в контактной работе с обучающимися очной формы обучения. В случае реализации образовательной программы в заочной / очно-заочной форме трудоемкость дисциплины сохраняется, однако объем учебного материала в значительной части осваивается обучающимися в форме самостоятельной работы. При этом требования к ожидаемым образовательным результатам обучающихся по данной дисциплине не зависят от формы реализации образовательной программы.

7. Методические рекомендации по видам занятий

Лекционные занятия.

В ходе лекционных занятий обучающимся рекомендуется выполнять следующие действия. Вести конспектирование учебного материала. Обращать внимание на категории, формулировки, раскрывающие содержание тех или иных явлений и процессов, научные выводы и практические рекомендации по их применению. Задавать преподавателю уточняющие вопросы с целью уяснения теоретических положений, разрешения спорных ситуаций.

Желательно оставить в рабочих конспектах поля, на которых во внеаудиторное время можно сделать пометки из рекомендованной литературы, дополняющие материал прослушанной лекции, а также подчеркивающие особую важность тех или иных теоретических положений.

Практические и семинарские занятия.

На практических и семинарских занятиях в зависимости от темы занятия выполняется поиск информации по решению проблем, практические упражнения, контрольные работы, выработка индивидуальных или групповых решений, итоговое обсуждение с обменом знаниями, участие в круглых столах, разбор конкретных ситуаций, командная работа, представление портфолио и т.п.

Самостоятельная работа.

Самостоятельная работа осуществляется в виде изучения литературы, эмпирических данных по публикациям и конкретных ситуаций из практики, подготовке индивидуальных

работ, работа с лекционным материалом, самостоятельное изучение отдельных тем дисциплины; поиск и обзор литературы и электронных источников; чтение и изучение учебника и учебных пособий.

8. Фонд оценочных средств

8.1. Перечень компетенций с указанием этапов их формирования в процессе освоения образовательной программы в рамках учебной дисциплины

Основными этапами формирования указанных компетенций при изучении обучающимися дисциплины являются последовательное изучение содержательно связанных между собой тем учебных занятий. Изучение каждой темы предполагает овладение обучающимися необходимыми компетенциями. Результат аттестации обучающихся на различных этапах формирования компетенций показывает уровень освоения компетенций.

Контролируемые разделы (темы) дисциплины	Индекс контроли-руемой компетенции (или её части)	Оценочные средства по этапам формирования компетенций
		текущий контроль по дисциплине
Введение.	ПКС-2	Опрос.
Основные виды криптографических протоколов. Роль криптографических протоколов в системах защиты информации.	ПКС-2	Опрос, написание кода программы.
Протокол электронной подписи.	ПКС-2	Опрос, написание кода программы.
Криптографические протоколы в электронной коммерции и в электронном документообороте.	ПКС-2	Опрос, написание кода программы.

8.2. Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений и навыков и (или) опыта деятельности процессе текущего контроля

Примеры вопросов для устного опроса:

1. Суть схемы Эль-Гамаля.
2. Схема аутентификации Шамира
3. Схема аутентификации Шнорра.
4. Схема аутентификации Брикелла и МакКарли.

Типовые контрольные задания:

1. Построить систему электронной подписи по схеме RSA, если

$$P = 19, \quad Q = 37,$$
$$p = 23, \quad q = 13,$$
$$E = 43, \ e = 47.$$

В ответ записать значение D

2. Найти a^{-1} по модулю m $\quad a = 19, m = 93.$

3. В системе электронной подписи

$$P = 19, \quad Q = 37,$$
$$p = 23, \quad q = 13,$$
$$E = 43, \quad e = 47$$

банк получает от клиента сообщение $(m, s) = (39, 57)$. Принять подпись или нет? (В ответ записать да или нет).

8.3. Перечень вопросов и заданий для промежуточной аттестации по дисциплине

Вопросы для промежуточного контроля (зачета)

1. Определение криптографического протокола. Виды протоколов.

2. Протоколы аутентификации.

3. Протоколы электронной подписи.

4. Системы электронных платежей. Классификация и структура.

5. Основные задачи защиты информации в электронной коммерции.

6. Банковские криптографические протоколы.

7. Честный обмен цифровыми подписями и его приложения.

8. Многосторонние транзакции, коммерческие сделки.

8.4. Планируемые уровни сформированности компетенций обучающихся и критерии оценивания

Уровни	Содержательное описание уровня	Основные признаки выделения уровня (этапы формирования компетенции, критерии оценки сформированности)	Пятибалльная шкала (академическая) оценка	Двухбалльная шакала, зачет	БРС, % освоения (рейтинговая оценка)
Повышенный	Творческая деятельность	*Включает нижестоящий уровень.* Умение самостоятельно принимать решение, решать	отлично	зачтено	86-100

		проблему/задачу теоретического и прикладного характера на основе изученных методов, приемов, технологий			
Базовый	Применение знаний и умений в более широких контекстах учебной и профессиональной деятельности, нежели по образцу с большей степени самостоятельности и инициативы	*Включает нижестоящий уровень.* Способность собирать, систематизировать, анализировать и грамотно использовать информацию из самостоятельно найденных теоретических источников и иллюстрировать ими теоретические положения или обосновывать практику применения	хорошо		71-85
Удовлетворительный (достаточный)	Репродуктивная деятельность	Изложение в пределах задач курса теоретически и практически контролируемого материала	удовлетворительно		55-70
Недостаточный	Отсутствие признаков удовлетворительного уровня		неудовлетворительно	не зачтено	Менее 55

9. Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины.

Основная литература

1. Бабаш, А. В. Криптографические методы защиты информации. Том 1 : учебно-методическое пособие / А. В. Бабаш. — 2-е изд., перераб. и доп. — Москва : РИОР : ИНФРА-М, 2021. — 413 с. — (Высшее образование: Бакалавриат). - ISBN 978-5-369-01267-3. - Текст : электронный. - URL: https://znanium.com/catalog/product/1215714 (дата обращения: 25.04.2022). – Режим доступа: по подписке.

Дополнительная литература

1. Костин, В. Н. Методы и средства защиты компьютерной информации : криптографические методы для защиты информации : учебное пособие / В. Н. Костин. - Москва : Изд. Дом НИТУ «МИСиС», 2018. - 40 с. - ISBN 978-5-90695-334-6. - Текст : электронный. - URL: https://znanium.com/catalog/product/1232230 (дата обращения: 25.04.2022). – Режим доступа: по подписке.

Интернет-ресурсы:

1. Криптографические методы защиты банковской информации (http://cryptowiki.net/images/3/32/Part3-CryptoProtocols.pdf)
2. *Запечников С.В.* Криптографические протоколы и их применение в финансовой и коммерческой деятельности: Учебное пособие для вузов. — М.: Горячая линия-Телеком, 2007 (http://www.dut.edu.ua/uploads/l_1066_65357958.pdf)

10. Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины (модуля).

- НЭБ Национальная электронная библиотека, диссертации и прочие издания
- eLIBRARY.RU Научная электронная библиотека, книги, статьи, тезисы докладов конференций
- Гребенников Электронная библиотека ИД журналы
- ЭБС Лань книги, журналы
- ЭБС Консультант студента
- ПРОСПЕКТ ЭБС
- ЭБС ZNANIUM.COM
- РГБ Информационное обслуживание по МБА
- БЕН РАН
- Электронно-библиотечная система (ЭБС) Кантитана (https://elib.kantiana.ru/)

11. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине.

Программное обеспечение обучения включает в себя:

- система электронного образовательного контента БФУ им. И. Канта – www.lms-3.kantiana.ru, обеспечивающую разработку и комплексное использование электронных образовательных ресурсов;
- серверное программное обеспечение, необходимое для функционирования сервера и связи с системой электронного обучения через Интернет;
- корпоративная платформа Microsoft Teams;
- специализированное ПО не требуется.

12. Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине.

Для проведения занятий лекционного типа, практических и семинарских занятий используются специальные помещения (учебные аудитории), оборудованные техническими средствами обучения – мультимедийной проекционной техникой. Для проведения занятий лекционного типа используются наборы демонстрационного оборудования.

Для проведения лабораторных работ, (практических занятий – при необходимости) используются специальные помещения (учебные аудитории), оснащенные специализированным лабораторным оборудованием: персональными компьютерами с возможностью выхода в интернет и с установленным программным обеспечением, заявленным в п.11.

Для проведения групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации используются специальные помещения (учебные аудитории), оборудованные специализированной мебелью (для обучающихся), меловой / маркерной доской.

Для организации самостоятельной работы обучающимся предоставляются помещения, оснащенные компьютерной техникой с возможностью подключения к сети «Интернет» и обеспечением доступа в электронную информационно-образовательную среду университета.

Для обучения инвалидов и лиц с ограниченными возможностями здоровья университетом могут быть представлены специализированные средства обучения, в том числе технические средства коллективного и индивидуального пользования.

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
федеральное государственное автономное образовательное учреждение высшего образования «Балтийский федеральный университет имени Иммануила Канта»
Институт физико-математических наук и информационных технологий

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

«Анализ стойкости финансовых протоколов»

Шифр: 10.05.01
Специальность: «Компьютерная безопасность»
Специализация: «Математические методы защиты информации»
Квалификация (степень) выпускника: специалист по защите информации

Калининград
2022

Лист согласования

Составитель: Белова Ольга Олеговна, к.ф.-м.н., доцент

Рабочая программа утверждена на заседании учебно-методического совета института физико-математических наук и информационных технологий
Протокол № 01/22 от «01» февраля 2022 г.

Председатель учебно-методического совета института физико-математических наук и информационных технологий
Первый заместитель директора ИФМНиИТ, к. ф.-м. н., доцент — Шпилевой А. А

Ведущий менеджер — Е.П.Ставицкая

Содержание

1.Наименование дисциплины: «*Анализ стойкости финансовых протоколов*».

Цель дисциплины: целью изучения дисциплины «*Анализ стойкости финансовых протоколов*» формирование знаний об основополагающих принципах защиты информации с помощью криптографических методов и примеров реализации этих методов на практике.

2. Перечень планируемых результатов обучения по дисциплине, соотнесенных с планируемыми результатами освоения образовательной программы

Код компетенции	Результаты освоения образовательной программы (ИДК)	Результаты обучения по дисциплине
ПКС-2. Способен разрабатывать требования по защите, формировать политики безопасности компьютерных систем и сетей.	ПКС-2.1. Выполняет анализ безопасности компьютерных систем и разрабатывает рекомендации по эксплуатации системы защиты информации. ПКС-2.2. Разработка модели угроз безопасности информации. ПКС-2.3. Формирует политики безопасности компьютерных систем и сетей.	• **знать** базовые криптографические протоколы, применяемые в электронной коммерции и в электронном документообороте; виды атак на протоколы; • **уметь:** проводить сравнительный анализ криптографических протоколов, решающих сходные задачи; • **владеть:** криптографической терминологией; навыками построения моделей криптографических протоколов, которые используются на практике

3. Место дисциплины в структуре образовательной программы

Дисциплина «*Анализ стойкости финансовых протоколов*» относится к части, формируемой участниками образовательных отношений блока Дисциплины подготовки обучающихся, представляет собой дисциплину по выбору раздела «Дисциплины», Б1.В.ДВ.04.02.

4. Виды учебной работы по дисциплине.

Виды учебной работы по дисциплине зафиксированы учебным планом основной профессиональной образовательной программы по указанному направлению и профилю, выражаются в академических часах. Часы контактной работы и самостоятельной работы обучающегося и часы, отводимые на процедуры контроля, могут различаться в учебных планах ОПОП по формам обучения. Объем контактной работы включает часы контактной аудиторной работы (лекции/практические занятия/ лабораторные работы), контактной внеаудиторной работы (контроль самостоятельной работы), часы контактной работы в период аттестации. Контактная работа, в том числе может проводиться посредством электронной информационно-образовательной среды университета с использованием ресурсов сети Интернет и дистанционных технологий

5. Содержание дисциплины, структурированное по темам (разделам)

Исходя из рамок, установленных учебным планом по трудоемкости и видам учебной работы по дисциплине, преподаватель самостоятельно выбирает тематику занятий по формам и количеству часов проведения контактной работы: лекции и иные учебные занятия, предусматривающие преимущественную передачу учебной информации преподавателем и (или) занятия семинарского типа (семинары, практические занятия, практикумы, лабораторные работы, коллоквиумы и иные аналогичные занятия), и (или) групповые консультации, и (или) индивидуальную работу обучающихся с преподавателем, в том числе индивидуальные консультации (по курсовым работам/проектам – при наличии курсовой работы/проекта по данной дисциплине в учебном плане). Рекомендуемая тематика занятий максимально полно реализуется в контактной работе с обучающимися очной формы обучения. В случае реализации образовательной программы в заочной / очно-заочной форме трудоемкость дисциплины сохраняется, однако объем учебного материала в значительной части осваивается обучающимися в форме самостоятельной работы. При этом требования к ожидаемым образовательным результатам обучающихся по данной дисциплине не зависят от формы реализации образовательной программы.

№	Наименование раздела	Содержание раздела
1	Введение	Задачи и программа дисциплины.
2	Основные виды криптографических протоколов. Роль криптографических протоколов в системах защиты информации.	Понятие криптографического протокола. Подходы к классификации криптографических протоколов. Подходы к моделированию криптографических протоколов. Свойства протоколов, характеризующие их безопасность. Основные виды уязвимостей. Виды атак на криптографические протоколы. Подходы к моделированию криптографических протоколов.
3	Протокол электронной подписи	Схема Эль-Гамаля. Схема RSA. Хэш-функции. Криптостойкость и особенности.
4	Криптографические протоколы в электронной коммерции и в электронном документообороте	Классификация и структура СЭП. Неанонимные СЭП, работающие в реальном масштабе времени. Неанонимные автономные СЭП. Анонимные СЭП, работающие в реальном масштабе времени. Анонимные автономные СЭП. Основные задачи защиты информации в электронной коммерции. Классификация задач электронной коммерции. Честный обмен цифровыми подписями и его приложения. Многосторонние транзакции, коммерческие сделки.
5	Заключение	Обзор государственных стандартов и стандартов организаций в области криптографических протоколов. Итоги изучения дисциплины.

6. Рекомендуемая тематика учебных занятий в форме контактной работы

Рекомендуемая тематика учебных занятий *лекционного* типа (предусматривающих преимущественную передачу учебной информации преподавателем):

№	Наименование раздела	Содержание раздела
1	Введение	Лекция 1. Задачи и программа дисциплины.
2	Основные виды криптографических протоколов. Роль криптографических протоколов в системах защиты информации.	Лекция 1. Понятие криптографического протокола. Лекция 2. Подходы к классификации криптографических протоколов. Лекция 3. Подходы к моделированию криптографических протоколов. Лекция 4. Свойства протоколов, характеризующие их безопасность. Лекция 5. Основные виды уязвимостей. Виды атак на криптографические протоколы. Лекция 6. Подходы к моделированию криптографических протоколов.
3	Протокол электронной подписи	Лекция 7. Схема Эль-Гамаля. Лекция 8. Схема RSA. Лекция 9. Хэш-функции. Лекция 10. Криптостойкость и особенности.
4	Криптографические протоколы в электронной коммерции и в электронном документообороте	Лекция 11. Классификация и структура СЭП. Неанонимные СЭП, работающие в реальном масштабе времени. Неанонимные автономные СЭП. Лекция 12. Анонимные СЭП, работающие в реальном масштабе времени. Анонимные автономные СЭП. Лекция 13. Основные задачи защиты информации в электронной коммерции. Классификация задач электронной коммерции. Лекция 14. Честный обмен цифровыми подписями и его приложения. Лекция 15. Многосторонние транзакции, коммерческие сделки.
5	Заключение	Лекция 16. Обзор государственных стандартов и стандартов организаций в области криптографических протоколов. Итоги изучения дисциплины.

Рекомендуемая тематика *практических* занятий:

1. Схема аутентификации Фиата и Шамира.
2. Схема аутентификации Шнорра.
3. Схема аутентификации Брикелла и МакКарли.
4. Схема Эль Гамаля.
5. Схемы RSA и Рабина.
6. Хэш-функции.
7. Протоколы типа Диффи – Хеллмана.
8. Схема Брандса.

На практических занятиях решаются задачи по теме занятия.

Требования к самостоятельной работе обучающихся

1. Работа с лекционным материалом, предусматривающая проработку конспекта лекций и учебной литературы, по всем темам из п. 6 настоящей рабочей программы.
2. Выполнение домашнего задания, предусматривающего решение задач, выполнение упражнений, выдаваемых на практических занятиях, по всем темам из п. 6 настоящей рабочей программы.

Руководствуясь положениями статьи 47 и статьи 48 Федерального закона от 29 декабря 2012 г. N 273-ФЗ «Об образовании в Российской Федерации» научно-педагогические работники и иные лица, привлекаемые университетом к реализации данной образовательной программы, пользуются предоставленными академическими правами и свободами в части свободы преподавания, свободы от вмешательства в профессиональную деятельность; свободы выбора и использования педагогически обоснованных форм, средств, методов обучения и воспитания; права на творческую инициативу, разработку и применение авторских программ и методов обучения и воспитания в пределах реализуемой образовательной программы и отдельной дисциплины.

Исходя из рамок, установленных учебным планом по трудоемкости и видам учебной работы по дисциплине, преподаватель самостоятельно выбирает тематику занятий по формам и количеству часов проведения контактной работы: лекции и иные учебные занятия, предусматривающие преимущественную передачу учебной информации преподавателем и (или) занятия семинарского типа (семинары, практические занятия, практикумы, лабораторные работы, коллоквиумы и иные аналогичные занятия), и (или) групповые консультации, и (или) индивидуальную работу обучающихся с преподавателем, в том числе индивидуальные консультации (по курсовым работам/проектам – при наличии курсовой работы/проекта по данной дисциплине в учебном плане).

Рекомендуемая тематика занятий максимально полно реализуется в контактной работе с обучающимися очной формы обучения. В случае реализации образовательной программы в заочной / очно-заочной форме трудоемкость дисциплины сохраняется, однако объем учебного материала в значительной части осваивается обучающимися в форме самостоятельной работы. При этом требования к ожидаемым образовательным результатам обучающихся по данной дисциплине не зависят от формы реализации образовательной программы.

7. Методические рекомендации по видам занятий

Лекционные занятия.

В ходе лекционных занятий обучающимся рекомендуется выполнять следующие действия. Вести конспектирование учебного материала. Обращать внимание на категории, формулировки, раскрывающие содержание тех или иных явлений и процессов, научные выводы и практические рекомендации по их применению. Задавать преподавателю уточняющие вопросы с целью уяснения теоретических положений, разрешения спорных ситуаций.

Желательно оставить в рабочих конспектах поля, на которых во внеаудиторное время можно сделать пометки из рекомендованной литературы, дополняющие материал прослушанной лекции, а также подчеркивающие особую важность тех или иных теоретических положений.

Практические и семинарские занятия.

На практических и семинарских занятиях в зависимости от темы занятия выполняется поиск информации по решению проблем, практические упражнения, контрольные работы, выработка индивидуальных или групповых решений, итоговое обсуждение с обменом знаниями, участие в круглых столах, разбор конкретных ситуаций, командная работа, представление портфолио и т.п.

Самостоятельная работа.

Самостоятельная работа осуществляется в виде изучения литературы, эмпирических данных по публикациям и конкретных ситуаций из практики, подготовке индивидуальных работ, работа с лекционным материалом, самостоятельное изучение отдельных тем дисциплины; поиск и обзор литературы и электронных источников; чтение и изучение учебника и учебных пособий.

8. Фонд оценочных средств

8.1. Перечень компетенций с указанием этапов их формирования в процессе освоения образовательной программы в рамках учебной дисциплины

Основными этапами формирования указанных компетенций при изучении обучающимися дисциплины являются последовательное изучение содержательно связанных между собой тем учебных занятий. Изучение каждой темы предполагает овладение обучающимися необходимыми компетенциями. Результат аттестации обучающихся на различных этапах формирования компетенций показывает уровень освоения компетенций.

Контролируемые разделы (темы) дисциплины	Индекс контроли-руемой компетенции (или её части)	Оценочные средства по этапам формирования компетенций
		текущий контроль по дисциплине
1 Введение	ПКС-2	Устный опрос
2. Основные виды криптографических протоколов. Роль криптографических протоколов в системах защиты информации.	ПКС-2	Тестирование, выполнение практической работы
3. Протокол электронной подписи	ПКС-2	Тестирование, выполнение практической работы
4. Криптографические протоколы в электронной коммерции и в электронном документообороте	ПКС-2	Тестирование, выполнение практической работы
5. Заключение	ПКС-2	Устный опрос

8.2. Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений и навыков и (или) опыта деятельности процессе текущего контроля

Тема 1. Основные виды криптографических протоколов. Роль криптографических протоколов в системах защиты информации.

	Вопрос теста	Варианты ответов

Оценка «удовлетворительно» (зачтено) или низкой уровень освоения компетенции	Что используется для создания цифровой подписи?	A. Закрытый ключ получателя B. Открытый ключ отправителя C. Закрытый ключ отправителя Д. Открытый ключ получателя
Оценка «хорошо» (зачтено) или повышенный уровень освоения компетенции	Какова эффективная длина ключа в DES?	A. 56 B. 64 C. 32 Д. 16
Оценка «отлично» (зачтено) или высокий уровень освоения компетенции	Кто участвовал в разработке первого алгоритма с открытым ключом?	A. Ади Шамир B. Росс Андерсон C. Брюс Шнайер Д. Мартин Хеллман

Тема 2. Протокол электронной подписи.

	Вопрос теста	Варианты ответов
Оценка «удовлетворительно» (зачтено) или низкой уровень освоения компетенции	Найти НОД чисел 217 и 413	
Оценка «хорошо» (зачтено) или повышенный уровень освоения компетенции	Правильное ли утверждение $2^{17} \equiv 2 \pmod{17}$? В ответ записать да или нет	
Оценка «отлично» (зачтено) или высокий уровень освоения компетенции	Построить систему электронной подписи по схеме RSA, если $P = 19, \quad Q = 37,$ $p = 23, \quad q = 13,$ $E = 43, \ e = 47.$ В ответ записать значение D	

Тема 3. Криптографические протоколы в электронной коммерции и в электронном документообороте.

	Вопрос теста	Варианты ответов
Оценка «удовлетворительно» (зачтено) или низкой уровень освоения компетенции	Найти a^{-1} по модулю m $a = 19, m = 93$	
Оценка «хорошо» (зачтено) или повышенный уровень освоения компетенции	В системе электронной подписи $P = 19, \quad Q = 37,$ $p = 23, \quad q = 13,$ $E = 43, \quad e = 47$ банк получает от клиента сообщение $(m, s) = (39, 57)$. Принять подпись	

	или нет? (В ответ записать да или нет).	
Оценка «отлично» (зачтено) или высокий уровень освоения компетенции	В криптосистеме обмена ключами Диффи — Хеллмана вычислить общий ключ k, если $n = 107,\ g = 7,\ x = 65,$ $y = 41.$	

8.3. Перечень вопросов и заданий для промежуточной аттестации по дисциплине

Вопросы для промежуточного контроля (зачета)

1. Определение криптографического протокола. Виды протоколов.
2. Протоколы аутентификации.
3. Протоколы электронной подписи.
4. Системы электронных платежей. Классификация и структура.
5. Основные задачи защиты информации в электронной коммерции.
6. Банковские криптографические протоколы.
7. Честный обмен цифровыми подписями и его приложения.
8. Многосторонние транзакции, коммерческие сделки.

8.4. Планируемые уровни сформированности компетенций обучающихся и критерии оценивания

Уровни	Содержательное описание уровня	Основные признаки выделения уровня (этапы формирования компетенции, критерии оценки сформированности)	Пятибалльная шкала (академическая) оценка	Двухбалльная шакала, зачет	БРС, % освоения (рейтинговая оценка)
Повышенный	Творческая деятельность	*Включает нижестоящий уровень.* Умение самостоятельно принимать решение, решать проблему/задачу теоретического и прикладного характера на основе изученных методов, приемов, технологий	отлично	зачтено	86-100
Базовый	Применение знаний и умений в более широких контекстах учебной и профессиональной	*Включает нижестоящий уровень.* Способность собирать, систематизировать, анализировать и грамотно использовать информацию из самостоятельно найденных	хорошо		71-85

	деятельности, нежели по образцу с большей степени самостоятельности и инициативы	теоретических источников и иллюстрировать ими теоретические положения или обосновывать практику применения			
Удовлетворительный (достаточный)	Репродуктивная деятельность	Изложение в пределах задач курса теоретически и практически контролируемого материала	удовлетворительно		55-70
Недостаточный	Отсутствие признаков удовлетворительного уровня		неудовлетворительно	не зачтено	Менее 55

9. Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины.

Основная литература

1. Бабаш, А. В. Криптографические методы защиты информации. Том 1 : учебно-методическое пособие / А. В. Бабаш. — 2-е изд., перераб. и доп. — Москва : РИОР : ИНФРА-М, 2021. — 413 с. — (Высшее образование: Бакалавриат). - ISBN 978-5-369-01267-3. - Текст : электронный. - URL: https://znanium.com/catalog/product/1215714 (дата обращения: 25.04.2022). – Режим доступа: по подписке.

Дополнительная литература

1. Костин, В. Н. Методы и средства защиты компьютерной информации : криптографические методы для защиты информации : учебное пособие / В. Н. Костин. - Москва : Изд. Дом НИТУ «МИСиС», 2018. - 40 с. - ISBN 978-5-90695-334-6. - Текст : электронный. - URL: https://znanium.com/catalog/product/1232230 (дата обращения: 25.04.2022). – Режим доступа: по подписке.

Интернет-ресурсы:

1. Криптографические методы защиты банковской информации (http://cryptowiki.net/images/3/32/Part3-CryptoProtocols.pdf)
2. *Запечников С.В.* Криптографические протоколы и их применение в финансовой и коммерческой деятельности: Учебное пособие для вузов. — М.: Горячая линия-Телеком, 2007 (http://www.dut.edu.ua/uploads/l_1066_65357958.pdf)

10. Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины (модуля).

– НЭБ Национальная электронная библиотека, диссертации и прочие издания

- eLIBRARY.RU Научная электронная библиотека, книги, статьи, тезисы докладов конференций
- Гребенников Электронная библиотека ИД журналы
- ЭБС Лань книги, журналы
- ЭБС Консультант студента
- ПРОСПЕКТ ЭБС
- ЭБС ZNANIUM.COM
- РГБ Информационное обслуживание по МБА
- БЕН РАН
- Электронно-библиотечная система (ЭБС) Кантитана (https://elib.kantiana.ru/)

11. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине.

Программное обеспечение обучения включает в себя:

- система электронного образовательного контента БФУ им. И. Канта – www.lms-3.kantiana.ru, обеспечивающую разработку и комплексное использование электронных образовательных ресурсов;
- серверное программное обеспечение, необходимое для функционирования сервера и связи с системой электронного обучения через Интернет;
- корпоративная платформа Microsoft Teams;
- специализированное ПО не требуется.

12. Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине.

Для проведения занятий лекционного типа, практических и семинарских занятий используются специальные помещения (учебные аудитории), оборудованные техническими средствами обучения – мультимедийной проекционной техникой. Для проведения занятий лекционного типа используются наборы демонстрационного оборудования.

Для проведения лабораторных работ, (практических занятий – при необходимости) используются специальные помещения (учебные аудитории), оснащенные специализированным лабораторным оборудованием: персональными компьютерами с возможностью выхода в интернет и с установленным программным обеспечением, заявленным в п.11.

Для проведения групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации используются специальные помещения (учебные аудитории), оборудованные специализированной мебелью (для обучающихся), меловой / маркерной доской.

Для организации самостоятельной работы обучающимся предоставляются помещения, оснащенные компьютерной техникой с возможностью подключения к сети «Интернет» и обеспечением доступа в электронную информационно-образовательную среду университета.

Для обучения инвалидов и лиц с ограниченными возможностями здоровья университетом могут быть представлены специализированные средства обучения, в том числе технические средства коллективного и индивидуального пользования.

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
федеральное государственное автономное образовательное учреждение высшего образования «Балтийский федеральный университет имени Иммануила Канта»
Институт физико-математических наук и информационных технологий

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

«Программирование микроконтроллеров»

Шифр: 10.05.01
Специальность: «Компьютерная безопасность»
Специализация: «Математические методы защиты информации»
Квалификация (степень) выпускника: специалист по защите информации

Калининград
2022

Лист согласования

Составители:

Колесников Никита Сергеевич, мл. науч. сотрудник лаборатории «Математические методы защиты и обработки информации»;

Рабочая программа утверждена на заседании учебно-методического совета института физико-математических наук и информационных технологий

Протокол № 01/22 от «01» февраля 2022 г.

Председатель учебно-методического
совета института физико-
математических наук и информационных
технологий

Первый заместитель директора Шпилевой А. А
ИФМНиИТ, к. ф.-м. н., доцент

Ведущий менеджер Е.П.Ставицкая

Содержание

1. Наименование дисциплины: «Программирование микроконтроллеров».

Цель дисциплины: формирование у обучающихся понимания основных принципов проектирования современных цифровых электрических схем общего назначения, а также развитие навыков интеграции в такие схемы микроконтроллерной и микропроцессорной техники, написания для них программ на языках программирования высокого и низкого уровня.

2. Перечень планируемых результатов обучения по дисциплине, соотнесенных с планируемыми результатами освоения образовательной программы

Код компетенции	Результаты освоения образовательной программы (ИДК)	Результаты обучения по дисциплине
ПКС-1. Способен разрабатывать программно-аппаратные средства защиты информации компьютерных систем и сетей	ПКС-1.1. Проводит анализ существующих методов и средств, применяемых для контроля и защиты информации. ПКС-1.2. Разрабатывает проекты программных и аппаратных средств защиты информации в соответствии с техническим заданием. ПКС-1.3. Проводит аттестацию программ и алгоритмов на предмет соответствия требованиям защиты информации.	- **знать** структуру и принцип работы 8-битных микроконтроллеров (архитектура, технология производства, электрические характеристики, порядок выполнения машинного кода, назначение периферийных устройств), инструкции ассемблера, интерфейсы (I2C, SPI), задачи интеграции микроконтроллеров в различных системах защиты информации; - **уметь** разрабатывать электрические схемы электронно-вычислительных устройств общего назначения, основанные на микроконтроллерах, выполнять программирование и отладку программ на микроконтроллерах; - **владеть** методами разработки эффективного программного кода с помощью использования регистров памяти специального назначения и машинных команд (команд ассемблера); методами оптимизации программ для микроконтроллеров.

3. Место дисциплины в структуре образовательной программы

«*Программирование микроконтроллеров*» представляет собой дисциплину части, формируемой участниками образовательных отношений блока 1 «Дисциплины (модули)», является дисциплиной по выбору Б1.В.ДВ.05 «Дисциплины по выбору Б1.В.ДВ.5» дисциплин специальности 10.05.01 «Компьютерная безопасность», специализация «Математические методы защиты информации».

4. Виды учебной работы по дисциплине.

Виды учебной работы по дисциплине зафиксированы учебным планом основной профессиональной образовательной программы по указанному направлению и профилю, выражаются в академических часах. Часы контактной работы и самостоятельной работы обучающегося и часы, отводимые на процедуры контроля, могут различаться в учебных планах ОПОП по формам обучения. Объем контактной работы включает часы контактной аудиторной работы (лекции/практические занятия/ лабораторные работы), контактной внеаудиторной работы (контроль самостоятельной работы), часы контактной работы в период аттестации. Контактная работа, в том числе может проводиться посредством электронной информационно-образовательной среды университета с использованием ресурсов сети Интернет и дистанционных технологий

5. Содержание дисциплины, структурированное по темам (разделам)

Исходя из рамок, установленных учебным планом по трудоемкости и видам учебной работы по дисциплине, преподаватель самостоятельно выбирает тематику занятий по формам и количеству часов проведения контактной работы: лекции и иные учебные занятия, предусматривающие преимущественную передачу учебной информации преподавателем и (или) занятия семинарского типа (семинары, практические занятия, практикумы, лабораторные работы, коллоквиумы и иные аналогичные занятия), и (или) групповые консультации, и (или) индивидуальную работу обучающихся с преподавателем, в том числе индивидуальные консультации (по курсовым работам/проектам – при наличии курсовой работы/проекта по данной дисциплине в учебном плане). Рекомендуемая тематика занятий максимально полно реализуется в контактной работе с обучающимися очной формы обучения. В случае реализации образовательной программы в заочной / очно-заочной форме трудоемкость дисциплины сохраняется, однако объем учебного материала в значительной части осваивается обучающимися в форме самостоятельной работы. При этом требования к ожидаемым образовательным результатам обучающихся по данной дисциплине не зависят от формы реализации образовательной программы.

№	Наименование раздела	Содержание раздела
1	Схемотехника цифровых устройств	Задачи и программа курса. Общие принципы проектирования встраиваемых и автономных электронно-вычислительных устройств. Место микроконтроллеров и микропроцессоров в цифровой электронике. Их назначение и функциональные возможности. Интегральные микросхемы (ИМС). Классификация интегральных микросхем по функциональному назначению (цифровые и аналоговые). Классификация цифровых ИМС по технологии производства (ТТЛ, ТТЛШ, КМОП). Электрические характеристики цифровых ИМС разных серий — диапазон допустимого напряжения питания, потребления тока, напряжения логических уровней, рабочая частота. Конструкция источников питания цифровых ИМС

		и микроконтроллеров. Линейные и LDO стабилизаторы. Обозначение источников питания на принципиальной схеме.
2	Устройство и функциональные возможности 8-битных микроконтроллеров	Обзор функциональных возможностей 8-битных микроконтроллеров различных производителей. Обзор средств программирования и отладки (IDE), аппаратных программаторов.
2.1	Архитектура микроконтроллеров PIC16. Порты ввода-вывода.	Архитектура 8-битных микроконтроллеров на примере PIC16F887. Структура памяти и ее адресация — области памяти программ, оперативной памяти и EEPROM. Набор инструкций микроконтроллера PIC16F887 (команды ассемблера). Регистры специального назначения, слово конфигурации (Configuration Word). Тактирование микроконтроллера от внешнего или встроенного RC-генератора, тактирование от внешнего кварцевого резонатора. Тактовая частота и скорость обработки команд (машинные циклы). Периферийные модули микроконтроллеров: таймеры, АЦП (аналого-цифровой преобразователь) и ЦАП, обзор встроенных интерфейсов (i2c, spi, uart). Модули управления питанием (режимы SLEEP пониженного энергопотребления), повышения отказоустойчивости (сторожевой таймер Watchdog, Brown-out detect). Команды сброса Reset и периферийный модуль Power-on Reset.
2.2	Прерывания и таймеры	Последовательность выполнения машинного кода микроконтроллером. Адресация памяти программ. Вектор сброса, таблица векторов прерываний. Уровни аппаратного стека. Настройка аппаратного таймера TIMER0 в составе микроконтроллера с помощью соответствующих регистров специального назначения (TMR0, INTCON, OPTION_REG, TRISA). Работа таймера в режиме счетчика. Предделитель частоты и его установка. Обработка прерывания, вызываемого таймером. Внешние прерывания и их обработка.
2.3	ШИМ управление	Понятие ШИМ модуляции. Примеры устройств, управляемых с помощью широтно-модулированного сигнала. Программный и аппаратный ШИМ. Формирование задержек в работе программы. Задержки с помощью периферии (таймеров) и с помощью циклов. Расчет времени задержки по количеству машинных операций в циклах.
2.4	Шина I2C, внутренняя и	Примеры устройств, управляемых по шине I2C.

	внешняя память EEPROM	Особенности ее аппаратной реализации — электрические соединения, уровни сигналов, задержки, адресация устройств (при одновременном подключении к шине нескольких устройств). Назначение памяти EEPROM, ее адресное пространство. Считывание и запись данных во встроенную память EEPROM микроконтроллера с помощью управляющих регистров специального назначения (EEDATA, EEADR, EECON). Внешняя память EEPROM — семейство микросхем 24CXX. Их подключение к микроконтроллеру по шине I2C и программирование.
3	Реализация протоколов обмена данными. Протокол 1-Wire.	Программная реализация на микроконтроллере протоколов передачи данных физического и канального уровней модели OSI. Пример — структура протокола передачи данных по одному проводу One-Wire: временные задержки, алгоритм приема и передачи данных. Реализация нестандартных протоколов, имеющих формальное описание в соответствующей документации (datasheet).
4	Реализация криптографических алгоритмов на микроконтроллерах	Примеры задач обработки данных на микроконтроллерах, требующих реализации криптографических алгоритмов. Встроенные симметрические алгоритмы блочного шифрования на некоторых микроконтроллерах. Поточный шифр Crypto-1, используемый в бесконтактных (RFID) картах доступа стандарта Mifare производителя NXP.

6. Рекомендуемая тематика учебных занятий в форме контактной работы

Рекомендуемая тематика учебных занятий *лекционного* типа (предусматривающих преимущественную передачу учебной информации преподавателями):

№	Наименование раздела	Темы лекций
1	Схемотехника цифровых устройств	Лекция 1. Цели и задачи курса. Схемотехника цифровых устройств. Микроконтроллеры.
2	Устройство и функциональные	Лекция 2. Микроконтроллер PIC16F84A и его периферия. Программирование на Assembler и C++.

	возможности 8-битных микроконтроллеров	
2.1	Архитектура микроконтроллеров PIC16. Порты ввода-вывода.	Лекция 3. Порты ввода-вывода микроконтроллера. Время выполнения микропрограммы. Задержки и таймер.
2.2	Прерывания и таймеры	Лекция 4. Индикация на 7-сегментном индикаторе.
2.3	ШИМ управление	Лекция 5. ШИМ модуляция сигнала, управление мощностью.
2.4	Шина I2C, внутренняя и внешняя память EEPROM	Лекция 6. Схема шины I2C — уровни сигнала, адресация. Лекция 7. Внешняя память 24C64 EEPROM — подключение к микроконтроллеру по шине I2C, операции чтения и записи.
3	Реализация протоколов обмена данными. Протокол 1-Wire.	Лекция 8. Схема протокола обмена данными 1-Wire.
4	Реализация криптографических алгоритмов на микроконтроллерах	Лекция 9. Алгоритмы шифрования, используемые в бесконтактных (RFID) картах доступа стандарта Mifare производителя NXP. Поточный шифр Crypto-1.

Рекомендуемая тематика *практических* занятий:

№	Наименование раздела	Описание практических занятий
1	Схемотехника цифровых устройств	Составление принципиальных схем, их расчет и сборка устройств, состоящих из элементарных электронных компонентов — светодиод, резистор, кнопка тактовая, транзистор, пьезоэлектрический звукоизлучатель, трехцветный светодиод. Перечисленные компоненты управляются цифровыми микросхемами семейства 74HC00 или микроконтроллером. Исследование алгоритмов работы и электрических параметров стандартных цифровых микросхем серии 74HC00.
2	Устройство и функциональные возможности 8-битных микроконтроллеров	Установка и настройка среды программирования микроконтроллера — редактора кода программ, компилятора и отладчика (например, MPLab IDE для микроконтроллеров семейства PIC16). Написание пробной программы, исследование машинного кода, подготовленного компилятором (дизассемблирование). Изучение особенностей синтаксиса компилятора языка

		программирования высокого уровня C++ (XC8). Ассемблерные вставки в коде программы, инструкции #pragma, описание битов конфигурации в коде программы.
2.1	Архитектура микроконтроллеров PIC16. Порты ввода-вывода	Написание программы для микроконтроллера PIC16F84A, использующей порты ввода-вывода PORTA, PORTB для управления светодиодами с помощью кнопки. Изучение машинного кода скомпилированной программы, оптимизация кода программы с помощью ассемблерных вставок.
2.2	Прерывания и таймеры	1. Добавление задержек в код программы управления светодиодами с помощью кнопки. Формирование электрических сигналов на выходе микроконтроллера с заданными временными характеристиками, проверка длины задержек с помощью осциллографа. Программирование задержки с помощью циклов и с помощью периферии микроконтроллера (таймера TIMER0 для PIC16F84A), сравнение занимаемого объема RAM и ROM памяти в обоих случаях. 2. Обработка сигнала управления, поступающего с кнопки с помощью инструкции условного перехода и с помощью генерации соответствующего прерывания. Сравнение занимаемого объема RAM и ROM памяти в обоих случаях. Изучение машинного кода скомпилированных программ.
2.3	ШИМ управление	Формирование ШИМ-сигнала на одном из выходов микроконтроллера с помощью программных задержек и с помощью периферии микроконтроллера (периферийный модуль ШИМ PIC16F887). Использование ШИМ-сигнала для плавного регулирования яркости свечения светодиода, для управления трехцветным светодиодом. Сравнение эффективности обоих программ. Проверка временных характеристик выходного сигнала с помощью осциллографа.
2.4	Шина I2C, внутренняя и внешняя память EEPROM	Сохранение параметров выходного сигнала в энергонезависимой памяти EEPROM и извлечение сохраненных данных при включении питания микроконтроллера (доработать одну из программ, написанных в ходе предыдущих практических занятий). Подключение к микроконтроллеру PIC16F887 микросхемы памяти 24C16 по шине I2C. Программирование интерфейса обмена данными. Контроль передаваемых по шине данных с помощью осциллографа.

3	Реализация протоколов обмена данными. Протокол 1-Wire	Программирование протокола передачи данных 1-Wire. Подключение считывателя карт доступа Mifare 13,56 Мгц к микроконтроллеру, обмен данными между картой и микроконтроллером по протоколу 1-Wire. Альтернативное задание: подключение к микроконтроллеру датчика температуры DS18B20 по протоколу 1-Wire, считывание значений, сбор и сохранение статистических данных в энергонезависимую память EEPROM. Контроль передаваемых данных с помощью осциллографа.
4	Реализация криптографических алгоритмов на микроконтроллерах	Изучение алгоритма поточного шифрования данных Crypto-1, используемого в RFID-картах доступа стандарта Mifare. Генерация ключей и запись данных с помощью микроконтроллера в защищенную область карты доступа Mifare Classic 1K. Чтение данных с защищенной карты с помощью считывателя, подключенного к ПК.

Тематика самостоятельных работ

№	Наименование раздела	Тематика самостоятельных работ
1	Схемотехника цифровых устройств	Повторение теоретического материала к практическим занятиям. Решение задач домашнего задания по теме. Ознакомление с литературой по курсу. Выбор темы групповой практической работы. Подготовка к контрольной работе.
2	Устройство и функциональные возможности 8-битных микроконтроллеров	Повторение теоретического материала к практическим занятиям. Решение задач домашнего задания по теме. Чтение литературы по теме групповой практической работы. Подготовка к контрольной работе.
2.1	Архитектура микроконтроллеров PIC16. Порты ввода-вывода	Сравнение особенностей архитектуры 8-битных микроконтроллеров разных серий и разных производителей. Изучение битов конфигурации микроконтроллера PIC16F887. Повторение примера программы, разобранной на практическом занятии, подключение дополнительных периферийных модулей микроконтроллера, повышающих отказоустойчивость программы — сторожевого таймера (Watchdog), Brown-out detector, Power-on Reset. Изучение дополнительной литературы по теме.

2.2	Прерывания и таймеры	Повторение примера программы, разобранной на практическом занятии, программирование дополнительных таймеров — TIMER1, TIMER2 (PIC16F887), описание задач, для программирования которых использование указанных таймеров оптимально. Обработка прерываний с помощью отдельных процедур-обработчиков для каждого из источников прерывания (PIC16F887). Изучение дополнительной литературы по теме.
2.3	ШИМ управление	Повторение примера программы, разобранной на практическом занятии. Изучение дополнительной литературы по теме.
2.4	Шина I2C, внутренняя и внешняя память EEPROM	Повторение примера программы, разобранной на практическом занятии. Подключение микросхемы памяти 24C512, доработка программы для обмена данными с указанной микросхемой. Изучение дополнительной литературы по теме.
3	Реализация протоколов обмена данными. Протокол 1-Wire	Повторение примера программы, разобранной на практическом занятии. Изучение документации карты доступа Mifare Classic 1K. Изучение дополнительной литературы по теме.
4	Реализация криптографических алгоритмов на микроконтроллерах	Повторение примера программы, разобранной на практическом занятии. Выбор одной из известных (описанных в технической литературе) уязвимостей криптографического протокола, реализованного в карте доступа Mifare Classic 1K. Подготовка доклада с описанием этой уязвимости и примером ее реализации. Изучение дополнительной литературы по теме. Подготовка к зачёту.

Требования к самостоятельной работе обучающихся

1. Работа с лекционным материалом, предусматривающая проработку конспекта лекций и учебной литературы, по всем темам из п. 6 настоящей рабочей программы.
2. Выполнение домашнего задания, предусматривающего выполнение упражнений, выдаваемых на практических занятиях, по всем темам из п. 6 настоящей рабочей программы.

Руководствуясь положениями статьи 47 и статьи 48 Федерального закона от 29 декабря 2012 г. N 273-ФЗ «Об образовании в Российской Федерации» научно-педагогические работники и иные лица, привлекаемые университетом к реализации данной образовательной программы, пользуются предоставленными академическими правами и свободами в части свободы преподавания, свободы от вмешательства в профессиональную деятельность; свободы выбора и использования педагогически обоснованных форм, средств, методов обучения и воспитания; права на творческую инициативу, разработку и применение авторских программ и методов обучения и

воспитания в пределах реализуемой образовательной программы и отдельной дисциплины.

Исходя из рамок, установленных учебным планом по трудоемкости и видам учебной работы по дисциплине, преподаватель самостоятельно выбирает тематику занятий по формам и количеству часов проведения контактной работы: лекции и иные учебные занятия, предусматривающие преимущественную передачу учебной информации преподавателем и (или) занятия семинарского типа (семинары, практические занятия, практикумы, лабораторные работы, коллоквиумы и иные аналогичные занятия), и (или) групповые консультации, и (или) индивидуальную работу обучающихся с преподавателем, в том числе индивидуальные консультации (по курсовым работам/проектам – при наличии курсовой работы/проекта по данной дисциплине в учебном плане).

Рекомендуемая тематика занятий максимально полно реализуется в контактной работе с обучающимися очной формы обучения. В случае реализации образовательной программы в заочной / очно-заочной форме трудоемкость дисциплины сохраняется, однако объем учебного материала в значительной части осваивается обучающимися в форме самостоятельной работы. При этом требования к ожидаемым образовательным результатам обучающихся по данной дисциплине не зависят от формы реализации образовательной программы.

7. Методические рекомендации по видам занятий

Лекционные занятия.

В ходе лекционных занятий обучающимся рекомендуется выполнять следующие действия. Вести конспектирование учебного материала. Обращать внимание на категории, формулировки, раскрывающие содержание тех или иных явлений и процессов, научные выводы и практические рекомендации по их применению. Задавать преподавателю уточняющие вопросы с целью уяснения теоретических положений, разрешения спорных ситуаций.

Желательно оставить в рабочих конспектах поля, на которых во внеаудиторное время можно сделать пометки из рекомендованной литературы, дополняющие материал прослушанной лекции, а также подчеркивающие особую важность тех или иных теоретических положений.

Практические и семинарские занятия.

На практических и семинарских занятиях в зависимости от темы занятия выполняется поиск информации по решению проблем, практические упражнения, контрольные работы, выработка индивидуальных или групповых решений, итоговое обсуждение с обменом знаниями, участие в круглых столах, разбор конкретных ситуаций, командная работа, представление портфолио и т.п.

Самостоятельная работа.

Самостоятельная работа осуществляется в виде изучения литературы, эмпирических данных по публикациям и конкретных ситуаций из практики, подготовке индивидуальных работ, работа с лекционным материалом, самостоятельное изучение отдельных тем дисциплины; поиск и обзор литературы и электронных источников; чтение и изучение учебника и учебных пособий.

8. Фонд оценочных средств

8.1. Перечень компетенций с указанием этапов их формирования в процессе освоения образовательной программы в рамках учебной дисциплины

Основными этапами формирования указанных компетенций при изучении обучающимися дисциплины являются последовательное изучение содержательно связанных между собой тем учебных занятий. Изучение каждой темы предполагает овладение обучающимися необходимыми компетенциями. Результат аттестации обучающихся на различных этапах формирования компетенций показывает уровень освоения компетенций.

Контролируемые разделы (темы) дисциплины	Индекс контроли-руемой компетенции (или её части)	Оценочные средства по этапам формирования компетенций
		текущий контроль по дисциплине
Тема 1. Схемотехника цифровых устройств	ПКС-1	Опрос, решение задач
Тема 2. Устройство и функциональные возможности 8-битных микроконтроллеров	ПКС-1	Опрос, выполнение практических заданий, контрольная работа
Тема 2.1. Архитектура микроконтроллеров PIC16. Порты ввода-вывода	ПКС-1	Опрос, выполнение практических заданий
Тема 2.2. Прерывания и таймеры	ПКС-1	Опрос, выполнение практических заданий
Тема 2.3. ШИМ управление.	ПКС-1	Опрос, выполнение практических заданий
Тема 2.4. Шина I2C, внутренняя и внешняя память EEPROM	ПКС-1	Опрос, выполнение практических заданий
Тема 3. Реализация протоколов обмена данными. Протокол 1-Wire	ПКС-1	Опрос, выполнение практических заданий
Тема 4. Реализация криптографических алгоритмов на микроконтроллерах	ПКС-1	Опрос, выполнение практических заданий

8.2. Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений и навыков и (или) опыта деятельности процессе текущего контроля

Примеры вопросов для устного опроса:

По Теме 1. Схемотехника цифровых устройств

1. Какие бывают аналоговые и цифровые интегральные микросхемы (ИМС)?
2. Какие напряжения соответствуют уровням логического нуля и единицы в цифровых ИМС?
3. В чем заключается отличие между линейным и LDO стабилизатором напряжения?
4. Чем различаются микросхемы логики КМОП и ТТЛ?
5. Какие функции в электронных схемах способен выполнять микроконтроллер?
6. Чем микроконтроллер отличается от микропроцессора?
7. Что такое операционный усилитель?

8. Что такое компаратор?
9. Что такое кварцевый резонатор?

По Теме 2. Устройства и функциональные возможности 8-битных микроконтроллеров

1. Чем отличается Гарвардская архитектура ЭВМ от фон Неймановской? Какую архитектуру имеют имеют 8-битные микроконтроллеры PIC Microchip?
2. В чем заключаются особенности архитектуры RISC?
3. Назовите виды встроенной памяти микроконтроллеров PIC16.
4. Для чего используется память EEPROM?
5. Какие периферийные устройства могут находиться на кристалле микроконтроллера?
6. Что называют сигналом тактирования? Какую форму имеет этот сигнал?
7. С какой скоростью микроконтроллер выполняет машинные инструкции?
8. С помощью каких схем можно сгенерировать тактовый сигнал для микроконтроллера?
9. Для чего нужны регистры специального назначения микроконтроллера? В каком адресном пространстве они находятся?
10. Для чего нужно слово конфигурации микроконтроллеров PIC? В каком адресном пространстве оно расположено?
11. Что такое меандр?

Типовые контрольные задания:

Задание 1. Имеется источник не стабилизированного постоянного напряжения, находящегося в диапазоне от U_{min}=9В до U_{max}=21В. Требуется разработать устройство, осуществляющего индикацию уровня входного (нестабильного) напряжения на экране, представляющем собой сборку из пяти светодиодов. Нарисовать схему обвязки микроконтроллера PIC16F688 для решения поставленной задачи.

Pin Diagram (PDIP, SOIC, TSSOP)

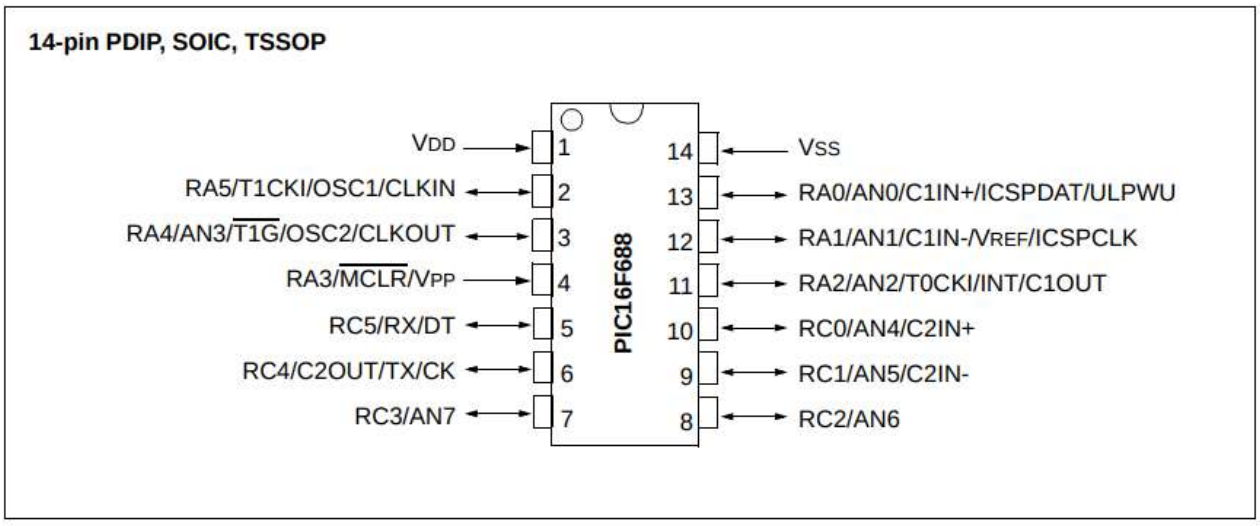


Рисунок 1: Назначение выводов микроконтроллера PIC16F688

FIGURE 7-4: ANALOG INPUT MODEL

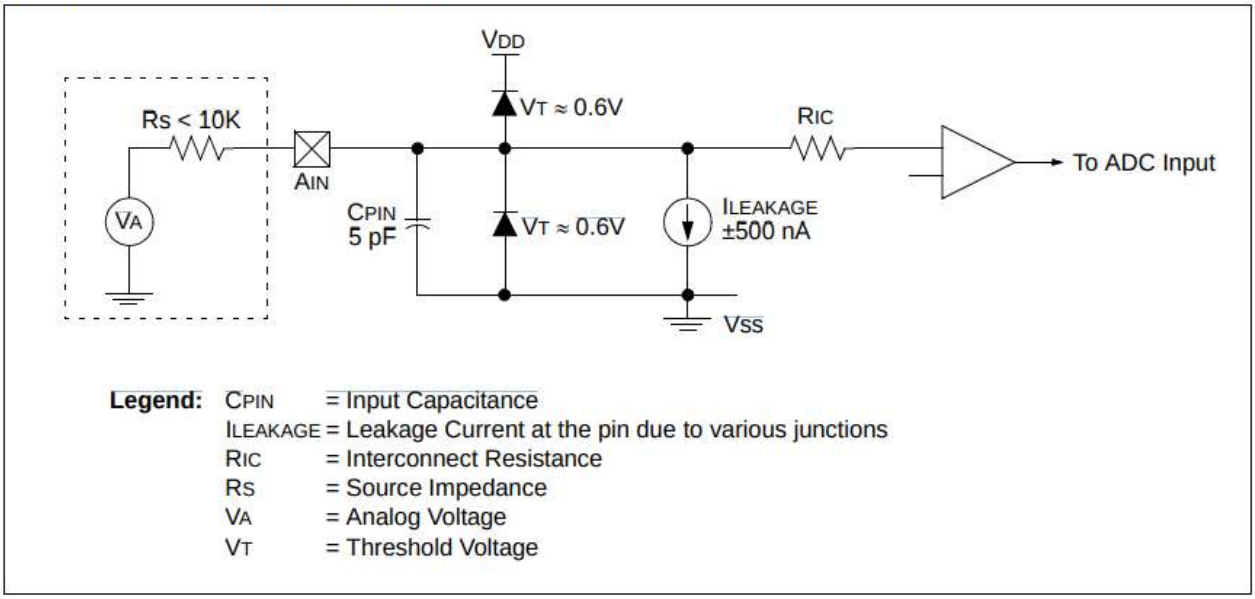


Рисунок 2: Структурная схема АЦП микроконтроллера PIC16F688 (для справки)

Задание 2. Опишите алгоритм работы программы, позволяющей выполнить поставленную задачу. Составьте блок-схемы для всех необходимых подпрограмм.

Задание 3* (дополнительное). Можно ли собрать устройство, выполняющее ту же самую функцию, без использования микроконтроллера? Предложите электрическую схему.

8.3. Перечень вопросов и заданий для промежуточной аттестации по дисциплине

Вопросы для промежуточного контроля (зачета)

1. Интегральные микросхемы - классификация и технология производства.
2. Источники питания цифровых электрических схем. Выпрямители напряжения, стабилизаторы (линейные и LDO). Расчет источников питания.
3. Виды логики — КМОП, ТТЛ, ТТЛШ, ДТЛ. Согласование логических уровней.
4. Функции микроконтроллера и микропроцессора в электрических схемах. Подбор микроконтроллера для поставленной задачи.
5. Архитектура микроконтроллера. Виды внутренней памяти — их назначение и особенности.
6. Архитектура микроконтроллера. Наборы инструкций.
7. Архитектура микроконтроллера. Внутренние периферийные устройства (модули).
8. Схемы внутреннего и внешнего тактирования микроконтроллера.
9. Регистры специального назначения микроконтроллеров PIC16. Назначение, адресация. Слово конфигурации.

10. Подключение и программирование портов ввода-вывода микроконтроллера.

11. Таймеры микроконтроллера — назначение, программирование, обработка прерываний. Режим счетчика. Предделитель частоты.

12. Сторожевой таймер — назначение, программирование.

13. Понятие широтно-импульсной модуляции сигнала. Аналоговая и цифровая ШИМ.

14. Составить схему устройства, управляемого с помощью ШИМ-сигнала, сформированного микроконтроллером. Описать блок-схему алгоритма микропрограммы.

15. Составить схему устройства на микроконтроллере со светодиодной индикацией. Описать блок-схему алгоритма микропрограммы.

16. Составить схему устройства на микроконтроллере с управлением кнопкой. Описать блок-схему алгоритма микропрограммы.

17. Составить схему устройства на микроконтроллере для считывания данных с датчика температуры DS18B20 по протоколу 1-Wire. Описать блок-схему алгоритма микропрограммы.

18. Составить схему устройства на микроконтроллере с отображением данных на дисплее из 4-х семисегментных индикаторов. Описать блок-схему алгоритма микропрограммы.

19. Составить схему устройства на микроконтроллере с отображением данных на ЖК-дисплее HD44780, включенного по 8-битной шине данных. Описать блок-схему алгоритма микропрограммы.

20. Составить схему устройства на микроконтроллере с сохранением переменных величин во внешнюю память EEPROM 24C64. Описать блок-схему алгоритма микропрограммы.

21. Составить схему устройства на микроконтроллере с управлением кнопкой. Описать блок-схему алгоритма микропрограммы.

22. Протокол 1-Wire. Применение и особенности реализации.

23. Асинхронный приемопередатчик UART и его применение в микроконтроллерах.

24. Встроенные криптографические алгоритмы в микроконтроллерах — назначение, порядок работы.

25. Уязвимости алгоритмов шифрования, применяемых в бесконтактных картах Mifare.

26. Составить схему устройства на микроконтроллере с применением АЦП (пример: цветомузыкальная приставка). Описать блок-схему алгоритма микропрограммы.

27. Составить схему устройства на микроконтроллере с применением встроенного таймера. Описать блок-схему алгоритма микропрограммы.

28. Составить схему устройства на микроконтроллере с применением сторожевого таймера. Описать блок-схему алгоритма микропрограммы.

8.4. Планируемые уровни сформированности компетенций обучающихся и критерии оценивания

Уровни	Содержательное описание уровня	Основные признаки выделения уровня (этапы формирования компетенции, критерии оценки сформированности)	Пятибалльная шкала (академическая) оценка	Двухбалльная шакала, зачет	БРС, % освоения (рейтинговая оценка)
Повышенный	Творческая деятельность	*Включает нижестоящий уровень.* Умение самостоятельно принимать решение, решать проблему/задачу теоретического и прикладного характера на основе изученных методов, приемов, технологий	отлично	зачтено	86-100
Базовый	Применение знаний и умений в более широких контекстах учебной и профессиональной деятельности, нежели по образцу с большей степени самостоятельности и инициативы	*Включает нижестоящий уровень.* Способность собирать, систематизировать, анализировать и грамотно использовать информацию из самостоятельно найденных теоретических источников и иллюстрировать ими теоретические	хорошо		71-85

		положения или обосновывать практику применения			
Удовлетворительный (достаточный)	Репродуктивная деятельность	Изложение в пределах задач курса теоретически и практически контролируемого материала	удовлетворительно		55-70
Недостаточный	Отсутствие признаков удовлетворительного уровня		неудовлетворительно	не зачтено	Менее 55

9. Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины.

Основная литература

1. *Кистрин А.В., Костров Б.В., Никифоров М.Б., Устюков Д.И.* Проектирование цифровых устройств. Учебник, изд-во КУРС, 2019 г. - 352с. Имеются экземпляры в отделах / There are copies in departments: ЭБС «Znanium» (https://znanium.com/catalog/document?id=333699)

Дополнительная литература

1. *Гуров В.В.* Микропроцессорные системы. Учебное пособие, изд-во НИЦ Инфра-М, 2022г. -336с.Имеются экземпляры в отделах / There are copies in departments: ЭБС «Znanium» (https://znanium.com/catalog/document?id=379994)

10. Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины (модуля).

- План занятий и конспекты лекций по настоящему курсу «Программирование микроконтроллеров» (https://crypto-kantiana.com/nikita.kolesnikov/teaching/microchip_2022.html);
- ЭБС Кантиана (https://lib.kantiana.ru/);
- Научная электронная библиотека eLIBRARY.RU (https://elibrary.ru/defaultx.asp);
- Электронно-библиотечная система «Знаниум» (https://znanium.com/);
- Учебно-методический комплекс по теории информации, размещенный на портале БФУ им. И.Канта (https://kantiana.ru/).

11. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине.

Программное обеспечение обучения включает в себя:

- система электронного образовательного контента БФУ им. И. Канта – www.lms-3.kantiana.ru, обеспечивающую разработку и комплексное использование электронных образовательных ресурсов;
- серверное программное обеспечение, необходимое для функционирования сервера и связи с системой электронного обучения через Интернет;
- корпоративная платформа Microsoft Teams;
- установленное на рабочих местах обучающихся ПО: Microsoft Windows 7, Microsoft Office Standart 2010, антивирусное программное обеспечение Kaspersky Endpoint Security.
- специализированное ПО: MPLAB X IDE Windows v6.00 (среда разработки), компилятор C++ для микроконтроллеров Microchip XC8 v2.20.

12. Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине.

Для проведения занятий лекционного типа, практических и семинарских занятий используются специальные помещения (учебные аудитории), оборудованные техническими средствами обучения – мультимедийной проекционной техникой. Для проведения занятий лекционного типа используются наборы демонстрационного оборудования.

Для проведения лабораторных работ, (практических занятий) используются специальные помещения (учебные аудитории), оснащенные специализированным лабораторным оборудованием: персональными компьютерами с возможностью выхода в интернет и с установленным программным обеспечением, заявленным в п. 11.

Для проведения групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации используются специальные помещения (учебные аудитории), оборудованные специализированной мебелью (для обучающихся), меловой / маркерной доской.

Для организации самостоятельной работы обучающимся предоставляются помещения, оснащенные компьютерной техникой с возможностью подключения к сети «Интернет» и обеспечением доступа в электронную информационно-образовательную среду университета.

Для обучения инвалидов и лиц с ограниченными возможностями здоровья университетом могут быть представлены специализированные средства обучения, в том числе технические средства коллективного и индивидуального пользования.

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
федеральное государственное автономное образовательное учреждение высшего образования «Балтийский федеральный университет имени Иммануила Канта»
Институт физико-математических наук и информационных технологий

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

«Технология инфраструктуры открытых ключей»

Шифр: 10.05.01
Специальность: «Компьютерная безопасность»
Специализация: «Математические методы защиты информации»
Квалификация (степень) выпускника: специалист по защите информации

Калининград
2022

Лист согласования

Составители:

Колесников Никита Сергеевич, мл. науч. сотрудник лаборатории «Математические методы защиты и обработки информации»;

Рабочая программа утверждена на заседании учебно-методического совета института физико-математических наук и информационных технологий
Протокол № 01/22 от «01» февраля 2022 г.
Председатель учебно-методического
совета института физико-
математических наук и информационных
технологий
Первый заместитель директора Шпилевой А. А
ИФМНиИТ, к. ф.-м. н., доцент

Ведущий менеджер Е.П.Ставицкая

Содержание

1. Наименование дисциплины: «Технология инфраструктуры открытых ключей».

Цель дисциплины: освоение студентами основ теоретических знаний о технологии PKI, необходимые будущим специалистам в области информационной безопасности; сформировать представление о современных подходах к развертыванию инфраструктур открытых ключей.

2. Перечень планируемых результатов обучения по дисциплине, соотнесенных с планируемыми результатами освоения образовательной программы

Код компетенции	Результаты освоения образовательной программы (ИДК)	Результаты обучения по дисциплине
ПКС-1. Способен разрабатывать программно-аппаратные средства защиты информации компьютерных систем и сетей	ПКС-1.1. Проводит анализ существующих методов и средств, применяемых для контроля и защиты информации. ПКС-1.2. Разрабатывает проекты программных и аппаратных средств защиты информации в соответствии с техническим заданием. ПКС-1.3. Проводит аттестацию программ и алгоритмов на предмет соответствия требованиям защиты информации.	• ***знать*:** номенклатуру и основные характеристики сертифицированных программно-аппаратных средств защиты информации, выпускаемых российской промышленностью; математические методы и алгоритмы, применяемые в программно-аппаратных средствах защиты информации; перспективные методы обработки информации в компьютерных системах; методы алгебры, теории чисел, алгебраической геометрии и дискретной математики и их применение в моделях информационных процессов; • ***уметь*:** строить математические модели информационных процессов, возникающих при работе программно-аппаратных средств; проводить анализ адекватности существующих математических моделей на основе сравнения их показателей эффективности с перспективными моделями; проводить анализ адекватности существующих математических моделей на основе компьютерного моделирования и получения статистических оценок эффективности; • ***владеть*:** методикой разработки математических моделей информационных процессов в компьютерных

		системах, используя методы алгебры, теории чисел, алгебраической геометрии и дискретной математики; навыками оценки адекватности моделей информационных процессов в программно-аппаратных средствах.

3. Место дисциплины в структуре образовательной программы

«*Технология инфраструктуры открытых ключей*» представляет собой дисциплину части, формируемой участниками образовательных отношений блока 1 «Дисциплины (модули)», является дисциплиной по выбору Б1.В.ДВ.05 «Дисциплины по выбору Б1.В.ДВ.5» дисциплин специальности 10.05.01 «Компьютерная безопасность», специализация «Математические методы защиты информации».

4. Виды учебной работы по дисциплине.

Виды учебной работы по дисциплине зафиксированы учебным планом основной профессиональной образовательной программы по указанному направлению и профилю, выражаются в академических часах. Часы контактной работы и самостоятельной работы обучающегося и часы, отводимые на процедуры контроля, могут различаться в учебных планах ОПОП по формам обучения. Объем контактной работы включает часы контактной аудиторной работы (лекции/практические занятия/ лабораторные работы), контактной внеаудиторной работы (контроль самостоятельной работы), часы контактной работы в период аттестации. Контактная работа, в том числе может проводиться посредством электронной информационно-образовательной среды университета с использованием ресурсов сети Интернет и дистанционных технологий

5. Содержание дисциплины, структурированное по темам (разделам)

Исходя из рамок, установленных учебным планом по трудоемкости и видам учебной работы по дисциплине, преподаватель самостоятельно выбирает тематику занятий по формам и количеству часов проведения контактной работы: лекции и иные учебные занятия, предусматривающие преимущественную передачу учебной информации преподавателем и (или) занятия семинарского типа (семинары, практические занятия, практикумы, лабораторные работы, коллоквиумы и иные аналогичные занятия), и (или) групповые консультации, и (или) индивидуальную работу обучающихся с преподавателем, в том числе индивидуальные консультации (по курсовым работам/проектам – при наличии курсовой работы/проекта по данной дисциплине в учебном плане). Рекомендуемая тематика занятий максимально полно реализуется в контактной работе с обучающимися очной формы обучения. В случае реализации образовательной программы в заочной / очно-заочной форме трудоемкость дисциплины сохраняется, однако объем учебного материала в значительной части осваивается обучающимися в форме самостоятельной работы. При этом требования к ожидаемым образовательным результатам обучающихся по данной дисциплине не зависят от формы реализации образовательной программы.

№	Наименование раздела	Содержание раздела
1	Тема 1. Введение	Понятие доверия в контексте электронных коммуникаций, характеристика ключевых элементов и механизмов доверия, политики доверия, понятие инфраструктуры безопасности, сервисы инфраструктуры безопасности. Механизмы аутентификации: аутентификация на основе паролей, механизмы одноразовой аутентификации, механизм аутентификации Kerberos, возможности инфраструктуры открытых ключей PKI как технологии аутентификации.
2	Тема 2. Основные компоненты и сервисы PKI.	Функции удостоверяющего и регистрационного центров, репозитория, архива сертификатов, серверных компонентов PKI. Характеристика сервисов PKI и сервисов, базирующихся на PKI: криптографические и вспомогательные сервисы, сервисы управления сертификатами. Сервисы идентификации и аутентификации, целостности и конфиденциальности.
3	Тема 3. Модели удостоверяющих центров.	Модели строгой и нестрогой иерархии удостоверяющих центров, модель распределенного доверия, четырехсторонняя модель доверия, web-модель доверия, модель доверия, сконцентрированного вокруг пользователя. Сетевая и мостовая конфигурации PKI. Механизм кросс-сертификации и виды кросс-сертификатов.
4	Тема 4. Сертификаты открытых ключей.	Формат сертификата открытого ключа. Классификация сертификатов открытых ключей. Характеристика классов и видов сертификатов. Жизненный цикл сертификатов и ключей. Примерные сценарии управления жизненным циклом сертификатов и ключей. Способы проверки статуса сертификата. Основные типы списков аннулированных сертификатов.
5	Тема 5. Типы архитектуры PKI.	Понятия архитектуры PKI: путь сертификации, пункты доверия PKI, доверенный ключ. Простая, иерархическая, сетевая и гибридная архитектура PKI. Способы построения пути сертификации для каждого типа архитектуры.
6	Тема 6. Описание политики PKI.	Определение политики безопасности. Способы реализации политики безопасности. Основные требования к политике PKI. Способы отображения политики в сертификатах. Структура набора положений политики PKI. Характеристика общих положений политики. Основные проблемы разработки политики и регламента. Этапы разработки политики применения сертификатов.
7	Тема 7. Проблемы реализации PKI.	Основные правовые документы PKI. Соглашения между участниками PKI. Рекомендации по выбору основных средств и оборудования. Требования к

		персоналу обслуживающему PKI. Управление сертификатами и ключами. Подходы к решению проблем интеграции и обеспечения работы приложений.

6. Рекомендуемая тематика учебных занятий в форме контактной работы

Рекомендуемая тематика учебных занятий *лекционного* типа (предусматривающих преимущественную передачу учебной информации преподавателями):

№	Наименование раздела	Темы лекций
1	Тема 1. Введение	Лекция 1. Механизмы аутентификации.
2	Тема 2. Основные компоненты и сервисы PKI.	Лекция 2. Характеристика сервисов PKI и сервисов, базирующихся на PKI.
3	Тема 3. Модели удостоверяющих центров.	Лекция 3. Модели удостоверяющих центров. Сетевая и мостовая конфигурации PKI.
4	Тема 4. Сертификаты открытых ключей.	Лекция 4. Классификация сертификатов открытых ключей. Способы проверки статуса сертификата.
5	Тема 5. Типы архитектуры PKI.	Лекция 5. Понятия архитектуры PKI: путь сертификации, пункты доверия PKI, доверенный ключ.
6	Тема 6. Описание политики PKI.	Лекция 6. Способы реализации политики безопасности. Основные требования к политике PKI. Лекция 7. Структура набора положений политики PKI.
7	Тема 7. Проблемы реализации PKI.	Лекции 8. Основные правовые документы PKI. Лекция 9. Управление сертификатами и ключами.

Рекомендуемая тематика *лабораторных* занятий:

№ п/п	Наименование Темы	Содержание темы
1	Введение	Электронно-цифровая подпись в системах защищенного электронного документооборота.
2	Основные компоненты и сервисы PKI.	Исследование отечественных стандартов хэш-функции (ГОСТ Р 34.11-94) и электронной цифровой подписи (ЭЦП ГОСТ Р 34.10-2001).
3	Модели удостоверяющих центров.	Развертывание инфраструктуры открытых ключей с использованием средств Microsoft Windows.
4	Сертификаты открытых ключей.	Развертывание инфраструктуры открытых ключей с использованием специального программного средства криптографической защиты КриптоПРО.
5	Типы архитектуры PKI.	Разработка политики PKI.

6	Описание политики PKI.	Организационно-правовые вопросы функционирования УЦ.
7	Проблемы реализации PKI.	Лабораторных работ по теме не предусмотрено.

Тематика самостоятельных работ

№ п/п	Наименование темы	Тематика самостоятельных работ
1	Введение	Повторение теоретического материала к лабораторным работам. Ознакомление с литературой по курсу. Выбор темы реферата.
2	Основные компоненты и сервисы PKI.	Повторение теоретического материала к лабораторным работам. Чтение литературы по теме реферата.
3	Модели удостоверяющих центров.	Повторение теоретического материала к лабораторным работам. Подготовка краткой сводки предварительных результатов для реферата.
4	Сертификаты открытых ключей.	Повторение теоретического материала к лабораторным работам. Подготовка основной части реферата. Подготовка к письменному опросу.
5	Типы архитектуры PKI.	Повторение теоретического материала к лабораторным работам. Подготовка основной части реферата.
6	Описание политики PKI.	Повторение теоретического материала к лабораторным работам. Завершение основной части реферата.
7	Проблемы реализации PKI.	Подготовка презентации реферата. Подготовка к письменному опросу. Подготовка к промежуточной аттестации – зачёту.

Требования к самостоятельной работе обучающихся

1. Работа с лекционным материалом, предусматривающая проработку конспекта лекций и учебной литературы, по всем темам из п. 6 настоящей рабочей программы.

2. Выполнение домашнего задания, предусматривающего выполнение упражнений, выдаваемых на практических занятиях, по всем темам из п. 6 настоящей рабочей программы.

Руководствуясь положениями статьи 47 и статьи 48 Федерального закона от 29 декабря 2012 г. N 273-ФЗ «Об образовании в Российской Федерации» научно-педагогические работники и иные лица, привлекаемые университетом к реализации данной образовательной программы, пользуются предоставленными академическими правами и свободами в части свободы преподавания, свободы от вмешательства в профессиональную деятельность; свободы выбора и использования педагогически обоснованных форм, средств, методов обучения и воспитания; права на творческую инициативу, разработку и применение авторских программ и методов обучения и воспитания в пределах реализуемой образовательной программы и отдельной дисциплины.

Исходя из рамок, установленных учебным планом по трудоемкости и видам учебной работы по дисциплине, преподаватель самостоятельно выбирает тематику занятий по формам и количеству часов проведения контактной работы: лекции и иные

учебные занятия, предусматривающие преимущественную передачу учебной информации преподавателем и (или) занятия семинарского типа (семинары, практические занятия, практикумы, лабораторные работы, коллоквиумы и иные аналогичные занятия), и (или) групповые консультации, и (или) индивидуальную работу обучающихся с преподавателем, в том числе индивидуальные консультации (по курсовым работам/проектам – при наличии курсовой работы/проекта по данной дисциплине в учебном плане).

Рекомендуемая тематика занятий максимально полно реализуется в контактной работе с обучающимися очной формы обучения. В случае реализации образовательной программы в заочной / очно-заочной форме трудоемкость дисциплины сохраняется, однако объем учебного материала в значительной части осваивается обучающимися в форме самостоятельной работы. При этом требования к ожидаемым образовательным результатам обучающихся по данной дисциплине не зависят от формы реализации образовательной программы.

7. Методические рекомендации по видам занятий

Лекционные занятия.

В ходе лекционных занятий обучающимся рекомендуется выполнять следующие действия. Вести конспектирование учебного материала. Обращать внимание на категории, формулировки, раскрывающие содержание тех или иных явлений и процессов, научные выводы и практические рекомендации по их применению. Задавать преподавателю уточняющие вопросы с целью уяснения теоретических положений, разрешения спорных ситуаций.

Желательно оставить в рабочих конспектах поля, на которых во внеаудиторное время можно сделать пометки из рекомендованной литературы, дополняющие материал прослушанной лекции, а также подчеркивающие особую важность тех или иных теоретических положений.

Практические и семинарские занятия.

На практических и семинарских занятиях в зависимости от темы занятия выполняется поиск информации по решению проблем, практические упражнения, контрольные работы, выработка индивидуальных или групповых решений, итоговое обсуждение с обменом знаниями, участие в круглых столах, разбор конкретных ситуаций, командная работа, представление портфолио и т.п.

Самостоятельная работа.

Самостоятельная работа осуществляется в виде изучения литературы, эмпирических данных по публикациям и конкретных ситуаций из практики, подготовке индивидуальных работ, работа с лекционным материалом, самостоятельное изучение отдельных тем дисциплины; поиск и обзор литературы и электронных источников; чтение и изучение учебника и учебных пособий.

8. Фонд оценочных средств

8.1. Перечень компетенций с указанием этапов их формирования в процессе освоения образовательной программы в рамках учебной дисциплины

Основными этапами формирования указанных компетенций при изучении обучающимися дисциплины являются последовательное изучение содержательно связанных между собой тем учебных занятий. Изучение каждой темы предполагает овладение обучающимися необходимыми компетенциями. Результат аттестации обучающихся на различных этапах формирования компетенций показывает уровень освоения компетенций.

Контролируемые разделы (темы) дисциплины	Индекс контроли-руемой компетенции (или её части)	Оценочные средства по этапам формирования компетенций
		текущий контроль по дисциплине
Тема 1. Введение	ПКС-1	Устный опрос, лабораторные работы
Тема 2. Основные компоненты и сервисы PKI.	ПКС-1	Устный опрос, лабораторные работы
Тема 3. Модели удостоверяющих центров.	ПКС-1	Устный опрос, лабораторные работы
Тема 4. Сертификаты открытых ключей.	ПКС-1	Письменный опрос, лабораторные работы
Тема 5. Типы архитектуры PKI.	ПКС-1	Устный опрос, лабораторные работы
Тема 6. Описание политики PKI.	ПКС-1	Устный опрос, лабораторные работы
Тема 7. Проблемы реализации PKI.	ПКС-1	Письменный опрос.

8.2. Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений и навыков и (или) опыта деятельности процессе текущего контроля

Примеры вопросов для устного опроса:

Тема 1. Введение

1. Цель и сфера применения Федерального Закона Российской Федерации ФЗ №63 от 6 апреля 2011 года «Об электронной подписи».
2. Особенности юридического определения ЭЦП в РФ.
3. Организационно-штатные мероприятия обеспечения деятельности удостоверяющего центра.
4. Что общего между собственноручной и цифровой подписями?
5. Какие задачи информационной безопасности решает ЭЦП?

Тема 2. Основные компоненты и сервисы PKI

1. Дайте определения основных понятий: электронная цифровая подпись, владелец сертификата, средства электронной цифровой подписи, закрытый ключ электронной цифровой подписи, сертификат ключа подписи, подтверждение подлинности электронной цифровой подписи в электронном документе, условия использования электронной цифровой подписи, обязательства удостоверяющего центра по отношению к владельцу сертификата ключа подписи.
2. Основные компоненты PKI.
3. Основные сервисы PKI.
4. Методика применения программного обеспечения в технологии PKI на примере «КриптоПРО» или «КриптоАРМ».
5. Цифровая подпись Фиата-Шамира.
6. Цифровые подписи семейства Эль-Гамаля.

Тема 3. Модели удостоверяющих центров

1. Дайте определения основных понятий: электронный документ, владелец сертификата ключа подписи, сертификат средств электронной цифровой подписи, закрытый ключ электронной цифровой подписи, открытый ключ электронной

цифровой подписи, сертификат ключа подписи, пользователь сертификата ключа подписи, статус удостоверяющего центра.
2. Должностные обязанности системного оператора УЦ.
3. Должностные обязанности системного администратора УЦ.

Тема 5. Типы архитектуры PKI

1. Public Key Infrastructure (PKI) определение, компоненты и их функции, пользователи PKI).
2. Цели применения PKI.
3. Компоненты PKI и их функции, пользователи PKI.

Тема 6. Описание политики PKI

1. Модели доверительных отношений PKI.
2. Набор положений политики PKI.
3. Проблемы формирования политики PKI.

Письменные опросы

Тема 4. Сертификаты открытых ключей

1. Дайте определения основных понятий: владелец сертификата ключа подписи, сертификат средств электронной цифровой подписи, закрытый ключ электронной цифровой подписи, открытый ключ электронной цифровой подписи, сертификат ключа подписи, пользователь сертификата ключа подписи.
2. Сертификаты открытых ключей X.509.
3. Почему в криптографических системах, основанных на открытых ключах, нельзя использовать одинаковые ключи для шифрования и ЭЦП?
4. Набор положений политики PKI.
5. Проблемы и этапы формирования политики PKI.

Тема 7. Проблемы реализации PKI

1. Проверка подлинности цифровых сертификатов в инфраструктуре Windows PKI - процедуры сличения.
2. Построение и обработка цепочки сертификатов Windows PKI.
3. Проверка подлинности цепочки сертификатов Windows PKI, списки аннулированных сертификатов CLR; риск, связанный с технологией CLR.
4. Перечислите должностные обязанности системного оператора УЦ.

Перечислите должностные обязанности системного администратора УЦ

8.3. Перечень вопросов и заданий для промежуточной аттестации по дисциплине

Вопросы для промежуточного контроля (зачета)

1. Федеральный закон Российской Федерации от 6 апреля 2011 г. N 63-ФЗ "Об электронной подписи".
2. Особенности юридического определения ЭЦП в РФ.
3. Положение о лицензировании отдельных видов деятельности, связанных с шифровальными (криптографическими) средствами.
4. Положение ПЗК-2005 «о разработке, производстве, реализации и использовании шифровальных (криптографических) средств защиты информации».

5. Организационно-штатные мероприятия обеспечения деятельности удостоверяющего центра.
6. Регламент удостоверяющего центра (типы регламентов УЦ, основные положения типового регламента УЦ, дополнительные положения и документы).
7. Традиционные бумажные и электронные документы (аутентификация и корректность восприятия информации в бумажных и электронных документах, угрозы безопасности субъектам ЭД).
8. Схема ЭЦП построенная на симметричной криптосистеме, схема ЭЦП построенная на асимметричной криптосистеме.
9. Доверие к открытому ключу и цифровые сертификаты (основные определения, стандарт X.509, сравнение версий сертификатов стандарта X.509, классы сертификатов, хранилище сертификатов в ОС Windows).
10. Криптопровайдеры, входящие в стандартный состав Windows 2007 Server. КриптоПро CSP.
11. Внешнее устройство хранения ключевой информации eToken (линейка моделей, функциональная модель, составляющие безопасности eToken PRO, жизненный цикл eToken PRO, уровни доступа).
12. Public Key Infrastructure (PKI) (Основные определения, цели применения, компоненты и их функции, пользователи PKI).
13. Принципы доверия в PKI (модели доверительных отношений, регулируемые доверительные отношения, настройка регулируемых доверительных отношений).
14. Проверка подлинности цифровых сертификатов в инфраструктуре Windows PKI (процедуры сличения, построение и обработка цепочки сертификатов, проверка подлинности цепочки сертификатов, списки аннулированных сертификатов CLR; риск, связанный с технологией CLR).
15. КриптоПро OCSP Server и КриптоПро Revocation Provider (основные определения, назначение, характеристики).
16. КриптоПро TSP Server (основные определения, назначение, характеристики) и усовершенствованная подпись КриптоПро (схема и формат усовершенствованной подписи, архивное хранение, технологические процедуры создания и проверки усовершенствованной ЭЦП).
17. ЭЦП на основе удостоверяющего центра КриптоПро (структура, состав и основные возможности УЦ КриптоПро, взаимодействие компонентов УЦ КриптоПро, режим работы удостоверяющего центра).

8.4. Планируемые уровни сформированности компетенций обучающихся и критерии оценивания

Уровни	Содержательное описание уровня	Основные признаки выделения уровня (этапы формирования компетенции, критерии оценки сформированности)	Пятибалльная шкала (академическая) оценка	Двухбалльная шакала, зачет	БРС, % освоения (рейтинговая оценка)
Повышенный	Творческая деятельность	*Включает нижестоящий уровень.*	отлично	зачтено	86-100

		Умение самостоятельно принимать решение, решать проблему/задачу теоретического и прикладного характера на основе изученных методов, приемов, технологий			
Базовый	Применение знаний и умений в более широких контекстах учебной и профессиональной деятельности, нежели по образцу с большей степени самостоятельности и инициативы	*Включает нижестоящий уровень.* Способность собирать, систематизировать, анализировать и грамотно использовать информацию из самостоятельно найденных теоретических источников и иллюстрировать ими теоретические положения или обосновывать практику применения	хорошо		71-85
Удовлетворительный (достаточный)	Репродуктивная деятельность	Изложение в пределах задач курса теоретически и практически контролируемого материала	удовлетворительно		55-70
Недостаточный	Отсутствие признаков удовлетворительного уровня		неудовлетворительно	не зачтено	Менее 55

9. Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины.

Основная литература

1. Алешников, С. И. Математические методы защиты информации [Электронный ресурс]: учеб. пособие/ С. И. Алешников, Ю. Ф. Болтнев ; Балт. федер. ун-т им. И. Канта. - Калининград: БФУ им. И. Канта, 2015 - 2015. Ч. 3: Вычислительный практикум по числовым полям и криптографии в квадратичных полях on-line, 93 с.. - Библиогр. в конце кн.. - ISBN 978-5-9971-0388-0: Б.ц. Имеются экземпляры в отделах /There are copies in departments: ЭБС Кантиана(1)

Дополнительная литература

1. Алешников, С. И. Математические методы защиты информации [Электронный ресурс]: учеб. пособие/ С. И. Алешников, Ю. Ф. Болтнев ; Балт. федер. ун-т им. И. Канта. - Калининград: БФУ им. И. Канта, 2015 - 2015. Ч. 2: Методы алгебраической теории чисел on-line, 121 с.. - Библиогр.: с. 119-120. - ISBN 978-5-9971-0386-6: Б.ц. Имеются экземпляры в отделах /There are copies in departments: ЭБС Кантиана(1)
2. Алешников, С. И. Математические методы защиты информации [Электронный ресурс]: учеб. пособие/ С. И. Алешников, Ю. Ф. Болтнев ; Балт. федер. ун-т им. И. Канта. - Калининград: БФУ им. И. Канта, 2015 - 2015. - Ч. 4: Вычислительный практикум по эллиптическим кривым и криптографии на эллиптических кривых on-line, 60 с.. - Библиогр.: с. 58-59. - ISBN 978-5-9971-0389-7: Б.ц. Имеются экземпляры в отделах /There are copies in departments: ЭБС Кантиана(1)

10. Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины (модуля).

- План занятий и конспекты лекций по настоящему курсу «Программирование микроконтроллеров» (https://crypto-kantiana.com/nikita.kolesnikov/teaching/microchip_2022.html);
- ЭБС Кантиана (https://lib.kantiana.ru/);
- Научная электронная библиотека eLIBRARY.RU (https://elibrary.ru/defaultx.asp);
- Электронно-библиотечная система «Знаниум» (https://znanium.com/);
- Учебно-методический комплекс по теории информации, размещенный на портале БФУ им. И.Канта (https://kantiana.ru/).

11. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине.

Программное обеспечение обучения включает в себя:

- система электронного образовательного контента БФУ им. И. Канта – www.lms-3.kantiana.ru, обеспечивающую разработку и комплексное использование электронных образовательных ресурсов;
- серверное программное обеспечение, необходимое для функционирования сервера и связи с системой электронного обучения через Интернет;
- корпоративная платформа Microsoft Teams;
- установленное на рабочих местах обучающихся ПО: Microsoft Windows 7, Microsoft Office Standart 2010, антивирусное программное обеспечение Kaspersky Endpoint Security.
- специализированное ПО: MPLAB X IDE Windows v6.00 (среда разработки), компилятор C++ для микроконтроллеров Microchip XC8 v2.20.

12. Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине.

Для проведения занятий лекционного типа, практических и семинарских занятий используются специальные помещения (учебные аудитории), оборудованные техническими средствами обучения – мультимедийной проекционной техникой. Для проведения занятий лекционного типа используются наборы демонстрационного оборудования.

Для проведения лабораторных работ, (практических занятий) используются специальные помещения (учебные аудитории), оснащенные специализированным лабораторным оборудованием: персональными компьютерами с возможностью выхода в интернет и с установленным программным обеспечением, заявленным в п. 11.

Для проведения групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации используются специальные помещения (учебные аудитории), оборудованные специализированной мебелью (для обучающихся), меловой / маркерной доской.

Для организации самостоятельной работы обучающимся предоставляются помещения, оснащенные компьютерной техникой с возможностью подключения к сети «Интернет» и обеспечением доступа в электронную информационно-образовательную среду университета.

Для обучения инвалидов и лиц с ограниченными возможностями здоровья университетом могут быть представлены специализированные средства обучения, в том числе технические средства коллективного и индивидуального пользования.

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
федеральное государственное автономное образовательное учреждение высшего образования «Балтийский федеральный университет имени Иммануила Канта»
Институт физико-математических наук и информационных технологий

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

«Внешний аудит безопасности корпоративных сетей»

Шифр: 10.05.01
Специальность: «Компьютерная безопасность»
Специализация: «Математические методы защиты информации»
Квалификация (степень) выпускника: Специалист по защите информации

Калининград
2022

Лист согласования

Составитель: Новоселов Семен Александрович, старший преподаватель.

Рабочая программа утверждена на заседании учебно-методического совета института физико-математических наук и информационных технологий

Протокол № 01/22 от «01» февраля 2022 г.

Председатель учебно-методического совета института физико-математических наук и информационных технологий

Первый заместитель директора ИФМНиИТ, к. ф.-м. н., доцент — Шпилевой А. А

Ведущий менеджер — Е.П.Ставицкая

Содержание

1.Наименование дисциплины: «Внешний аудит безопасности корпоративных сетей».

Целью освоения дисциплины «**Внешний аудит безопасности корпоративных сетей**» является расширение и углубление фундаментальной и практической подготовки студентов, обеспечивающей возможность овладения современными методами выявления уязвимостей компьютерных сетей, овладение практическими навыками проведения тестовых вторжений для практической оценки безопасности корпоративных сетей; изучение методологии тестового вторжения и составления отчетности о выявленных уязвимостях.

Необходимость изучения дисциплины продиктована требованиям к защите корпоративных сетей от растущего числа хакерских атак. Внешний аудит сетей позволяет протестировать сети на уязвимости и соответствие стандартам защищенности и своевременно закрыть все найденные уязвимости, препятствуя доступу хакеров в сеть.

Задачами освоения дисциплины «Внешний аудит безопасности корпоративных сетей» являются:

- овладение методами сканирования компьютерных сетей;
- овладение методами выявления уязвимостей;
- овладение методами обнаружения атаки на компьютерные сети.
- практическое освоение систем тестового вторжения Metasploit и Kali Linux.

2. Перечень планируемых результатов обучения по дисциплине, соотнесенных с планируемыми результатами освоения образовательной программы

Код компетенции	Результаты освоения образовательной программы (ИДК)	Результаты обучения по дисциплине
ПКС-2 Способен разрабатывать требования по защите, формировать политики безопасности компьютерных систем и сетей	ПКС-2.1. Выполняет анализ безопасности компьютерных систем и разрабатывает рекомендации по эксплуатации системы защиты информации. ПКС-2.2. Разработка модели угроз безопасности информации. ПКС-2.3. Формирует политики безопасности компьютерных систем и сетей.	**Знать:** • общие принципы экспериментального и теоретического исследования безопасности компьютерных сетей; • основные современные отечественные и зарубежные стандарты в области компьютерной безопасности и проведения аудита безопасности; • современные методики и технологии проведения аудита безопасности сетей • основные виды уязвимостей компьютерных сетей и программ; • механизмы реализации атак в сетях TCP/IP и защиты от них. **Уметь:**

		• проводить аудит безопасности сети и анализ найденных уязвимостей; • пользоваться системами анализа сетевого трафика, сканерами безопасности и сетевыми сканерами; • составлять рекомендации по устранению уязвимостей, настройке средств защиты и улучшению политики безопасности **Владеть:** • практическими навыками проведения аудита безопасности сетей, инструментами систем тестового вторжения Metasploit и Kali Linux, сканерами безопасности навыками аудита исходного кода для нахождения уязвимостей

3. Место дисциплины в структуре образовательной программы

Дисциплина «Внешний аудит безопасности корпоративных сетей» представляет собой дисциплину по выбору части, формируемой участниками образовательных отношений Блока 1 Дисциплины (модули) подготовки студентов.

4. Виды учебной работы по дисциплине.

Виды учебной работы по дисциплине зафиксированы учебным планом основной профессиональной образовательной программы по указанному направлению и профилю, выражаются в академических часах. Часы контактной работы и самостоятельной работы студента и часы, отводимые на процедуры контроля, могут различаться в учебных планах ОПОП по формам обучения. Объем контактной работы включает часы контактной аудиторной работы (лекции/практические занятия/ лабораторные работы), контактной внеаудиторной работы (контроль самостоятельной работы), часы контактной работы в период аттестации. Контактная работа, в том числе может проводиться посредством электронной информационно-образовательной среды университета с использованием ресурсов сети Интернет и дистанционных технологий

5. Содержание дисциплины, структурированное по темам (разделам)

Исходя из рамок, установленных учебным планом по трудоемкости и видам учебной работы по дисциплине, преподаватель самостоятельно выбирает тематику занятий по формам и количеству часов проведения контактной работы: лекции и иные учебные занятия, предусматривающие преимущественную передачу учебной информации преподавателем и (или) занятия семинарского типа (семинары, практические занятия, практикумы, лабораторные работы, коллоквиумы и иные аналогичные занятия), и (или) групповые консультации, и (или) индивидуальную работу обучающихся с преподавателем, в том числе индивидуальные консультации (по курсовым работам/проектам – при наличии

курсовой работы/проекта по данной дисциплине в учебном плане). Рекомендуемая тематика занятий максимально полно реализуется в контактной работе со студентами очной формы обучения. В случае реализации образовательной программы в заочной / очно-заочной форме трудоемкость дисциплины сохраняется, однако объем учебного материала в значительной части осваивается студентами в форме самостоятельной работы. При этом требования к ожидаемым образовательным результатам студентов по данной дисциплине не зависят от формы реализации образовательной программы.

№	Наименование раздела	Содержание раздела
1	Введение	Задачи и программа курса. Место курса «***Внешний аудит безопасности корпоративных сетей***» в ряду других дисциплин. Формы самостоятельной работы студентов по изучению курса. Литература к курсу. Понятие уязвимости и эксплоита. Локальные и удаленные эксплоиты. Эскалация привилегий. Примеры сетевых атак. Краткая история возникновения хакеров. Интернет-черви и вирусы. Необходимость классификации эксплоитов. Базы уязвимостей и эксплойтов. Стандарты проведения тестовых вторжений. Фазы тестового вторжения. Базовые сетевые протоколы и их безопасность: TCP/IP, HTTP(S). Механизмы реализации атак на разных уровнях модели OSI.
2	Основные виды уязвимостей программ и веб-приложений	Удалённое выполнение кода. Уязвимость Shellshock. SQL-инъекции (SQLi). Межсайтовый скриптинг (XSS). Уязвимости, возникающие при работе с памятью: утечки, переполнения буфера. Примеры: уязвимость Heartbleed, эксплойт EternalBlue и шифровальщик WannaCry. Методы обнаружения уязвимостей. Методы защиты от эксплуатации уязвимостей.
3	Сетевой сканер nmap	Определение сетевого сканирования. Методики сетевого сканирования: составление карты сети, сканирование портов, обнаружение сервисов и определение их версий, определение версии операционной системы. Составления карты сети (обнаружение активных хостов):

		ICMP эхо запрос, ICMP запрос временной метки, запрос сетевой маски. UDP ping запрос. Влияние сетевого экрана на процесс обнаружения активных хостов. Способы сканирования портов, доступные в nmap: сканирование с помощью подключения, полуоткрытое сканирование, idle-сканирование. Сравнительные достоинства и достоверность различных методов сканирования. Влияние межсетевого экрана при фильтрации открытых портов. TCP и UDP сканирование. Идентификация сервисов и определение их версий. Важность этой стадии для процесса тестового вторжения. Сбор и анализ баннеров активных сервисов. Способы сокрытия баннеров. Определение активных сервисов на нестандартных портах. Определение версии операционной системы. Определение версии по особенностям реализации стека TCP/IP. Достоверность этого метода. Определение версии по набору открытых сервисов и их баннерам.
4	Скриптовый движок Nmap	Программирования скриптов. Язык Lua. Категории скриптов. Структура скрипта. Доступные библиотеки. Функции для работы с различными протоколами. Пример: разработка фаззера.
5	Анализ сетевого трафика с целью выявления атак	Определение термина «сетевые снифферы». Принципы перехвата трафика на канальном уровне. Методы перехвата сетевого трафика. Возможности сетевых снифферов. Категории сетевых снифферов. Основы сетевого сниффера wireshark. Сферы применения wireshark. Возможности wireshark. Основные части и назначение графического интерфейса. Способы перехвата сетевого трафика в wireshark. Фильтрация пакетов. Задание фильтрации на уровне операционной системы. Фильтры захвата пакетов

		wireshark. Фильтры отображения пакетов. Рекомендации для использования различных типов фильтров для практического применения.
6	Сканеры безопасности	Необходимость появления и назначение сканеров безопасности. Коммерческие и некоммерческие сканеры безопасности. Сканер безопасности Nessus/OpenVAS. Общие принципы функционирования сканеров безопасности. Сканирование активных хостов. Сканирование открытых портов. Анализ баннеров активных сервисов для выявления уязвимостей. Ограничения сканеров безопасности. Отличия сканеров безопасности от систем тестового вторжения.
7	Система тестового вторжения METASPLOIT	История создания Metasploit. Лицензирование и условия распространения. Поддерживаемые платформы. Архитектура среды MSF. Модульность и возможность расширения MSF. Взаимодействие с ядром MSF. Типы интерфейсов. Интерфейс msfconsole. Запуск интерфейса в Windows и Linux. Команды общего назначения version, quit и show. Среда окружения MSF. Команды локальной и временной среды MSF. Выбор и конфигурация эксплоитов. Выбор и конфигурация шелл-кода. Работа с генератором NOP дорожки в интерфейсе msfconsole. Запуск эксплоита и динамическая обработка обратного соединения с атакованным хостом
8	Система тестового вторжения Kali Linux.	История развития, версии, условия распространения и поддерживаемые платформы. Категории инструментов, включенных в Kali Linux: сбор информации, карта сети, идентификация уязвимостей, анализ веб-приложений, анализ WiFi сетей, вторжение, эскалация привилегий, удержание удаленного доступа, аудит VoIP. Методологии тестового вторжения. Тестирование методом белого ящика, черного ящика и серого ящика. Сравнение различных методологий

		тестирования, их достоинства, недостатки и сфера применения. Категории фазы сбора информации. Инструменты для получения информация из DNS: dnswalk, dnsenum, dnsmap и dnsrecon. Запуск, параметры и сохранение результатов. Инструменты для сбора информации о маршрутизации: 0trace, dmitry, itrace, tcptraceroute и tcptrace. Методы обхода блокировки сетевого экрана, реализованные в данных инструментах. Универсальный инструмент для сбора информации mantego. Фаза сканирования портов – назначение и категории инструментов. Сканеры портов nmap, zenmap. Функциональные возможности и особенности перечисленных сканеров. Анализаторы открытых сервисов: amap, httpprint, httsquash. Сканирование виртуальных частных сетей программой ike-scan. Проведение тестовой атаки в Kali Linux. Интеграция Metasploit и Kali Linux. Фаза эскалации привилегий. Методы эскалации привилегий, реализованные в Kali Linux: взлом паролей, сетевое прослушивание (сниффинг) и сетевой спуфинг. Инструменты взлома паролей при атаке оффлайн: rainbowcrack, samdump2, john-the-ripper, ophcrack, crunch, wyd. Принципы работы радужных таблиц. Инструменты взлома паролей при атаке онлайн: BruteSSH и Hydra. Сетевые снифферы dsniff, hamster, tcpdump, tcpick и wireshark. Средства подделки сетевых пакетов (спуфинг) ARPspoof и Ettercap. Удержание активного доступа. Категории этой фазы: средства туннелирования протокола, прокси-сервера, средства коммуникации точка-точка. средства туннелирования протокола DNS2tcp, ptunnel, stunnel4. Прокси-серверы 3proxy и proxychains. Средства

		коммуникации точка-точка: CryptCat, sbd и socat.

6. Рекомендуемая тематика учебных занятий в форме контактной работы

Рекомендуемая тематика учебных занятий *лекционного* типа (предусматривающих преимущественную передачу учебной информации преподавателями):

№	**Наименование раздела**	**Темы лекций**
1	Введение	Лекция 1. Основные понятия Лекция 2. Базовые сетевые протоколы и их безопасность: TCP/IP, HTTP(S). Лекция 3. Механизмы реализации атак на различных уровнях модели OSI Лекция 4. Источники уязвимостей в веб-приложениях
2	Основные виды уязвимостей программ и веб-приложений	Лекция 5. Удалённое выполнение кода. Пример: уязвимость Shellshock. Лекция 6. SQL-инъекции (SQLi) I. Классические Лекция 7. SQL-инъекции (SQLi) II. Слепые Лекция 8. Межсайтовый скриптинг (XSS). Лекция 9. Утечки данных из памяти Лекция 10. Переполнения буфера I. Основы Лекция 11. Переполнения буфера II. Разработка шелкодов. Лекция 12. Переполнения буфера III. Примеры. Эксплойт EternalBlue и шифровальщик WannaCry. Лекция 13. Методы обнаружения уязвимостей. Лекция 14. Методы защиты от эксплуатации уязвимостей.
3	Сетевой сканер nmap	Лекция 15. Методы сетевого сканирования. Лекция 16. Сетевая разведка с помощью Nmap
4	Скриптовый движок Nmap	Лекция 17. Введение в программирование скриптов Nmap. Пример: поиск уязвимых серверов.
5	Анализ сетевого трафика с целью выявления атак	Лекция 18. Методы перехвата сетевого трафика. Основы сетевого сниффера wireshark.
6	Сканеры безопасности	Лекция 19. Общие принципы функционирования сканеров безопасности. Сканер безопасности Nessus/OpenVAS.
7	Система тестового вторжения METASPLOIT	Лекция 20. Введение в проведение тестовых вторжений с помощью Metasploit.

		Лекция 21. Разработка простых модулей для Metasploit: разработка эксплойта для веб-приложения и сканера уязвимых серверов.
8	Система тестового вторжения Kali Linux.	Лекция 22. Kali Linux. Введение Лекция 23. Kali Linux. Сбор информации. Лекция 24. Kali Linux. Проведение тестовой атаки. Лекция 25. Kali Linux. Анализ безопасности WiFi сетей

Рекомендуемая тематика *практических* занятий:

№ п/п	**Наименование Темы**	**Содержание темы**
1	Введение	Организация соединения между двумя машинами по TCP с помощью netcat, перехват передаваемых данных. Подключение к HTTP-серверу и передача данных вручную. Простой поиск уязвимостей с помощью сканирования портов и поиска по базам уязвимостей и эксплойтов.
2	Основные виды уязвимостей программ и веб-приложений	Нахождение и использование уязвимостей классов: удалённое выполнение кода (инъекция команд ОС, Shellshock), SQL-инъекция, XSS, утечки памяти (Heartbleed), переполнение буфера (разработка шелкода, обход ASLR через утечки памяти, перебор StackCanary, использование ROP)
3	Сетевой сканер nmap	Спецификация цели. Определение активных хостов в сети. Сканирование портов. Определение активных сервисов и их версий. Определение версии операционной системы. Обход системы обнаружения вторжений. Idle-сканирование
4	Скриптовый движок Nmap	Разработка фаззера. Разработка сканера для заданной уязвимости.
5	Анализ сетевого трафика с целью выявления атак	Определение активных хостов с помощью ARP протокола. Определение источника сканирования портов. Определение попыток применения эксплойтов.
6	Сканеры безопасности	Использование сканера безопасности Nessus/OpenVAS для выявления уязвимостей в сети.
7	Система тестового вторжения METASPLOIT	Проведение тестовых вторжений на уязвимые виртуальные машины.
8	Система тестового вторжения Kali Linux	Использовать систему тестового вторжения Kali Linux для нахождения уязвимостей на виртуальной машине. Использование инструментов оффлайн атаки для анализа хэш-кодов. Создать туннель между атакованной машиной и машиной аудитора.

Требования к самостоятельной работе студентов.

1. Работа с лекционным материалом, предусматривающая проработку конспекта лекций и учебной литературы, по всем темам из п. 6 настоящей рабочей программы.

2. Выполнение домашнего задания, предусматривающего решение задач, выполнение упражнений, выдаваемых на практических занятиях, по всем темам из п. 6 настоящей рабочей программы.

Руководствуясь положениями статьи 47 и статьи 48 Федерального закона от 29 декабря 2012 г. N 273-ФЗ «Об образовании в Российской Федерации» научно-педагогические работники и иные лица, привлекаемые университетом к реализации данной образовательной программы, пользуются предоставленными академическими правами и свободами в части свободы преподавания, свободы от вмешательства в профессиональную деятельность; свободы выбора и использования педагогически обоснованных форм, средств, методов обучения и воспитания; права на творческую инициативу, разработку и применение авторских программ и методов обучения и воспитания в пределах реализуемой образовательной программы и отдельной дисциплины.

Исходя из рамок, установленных учебным планом по трудоемкости и видам учебной работы по дисциплине, преподаватель самостоятельно выбирает тематику занятий по формам и количеству часов проведения контактной работы: лекции и иные учебные занятия, предусматривающие преимущественную передачу учебной информации преподавателем и (или) занятия семинарского типа (семинары, практические занятия, практикумы, лабораторные работы, коллоквиумы и иные аналогичные занятия), и (или) групповые консультации, и (или) индивидуальную работу обучающихся с преподавателем, в том числе индивидуальные консультации (по курсовым работам/проектам – при наличии курсовой работы/проекта по данной дисциплине в учебном плане).

Рекомендуемая тематика занятий максимально полно реализуется в контактной работе со студентами очной формы обучения. В случае реализации образовательной программы в заочной / очно-заочной форме трудоемкость дисциплины сохраняется, однако объем учебного материала в значительной части осваивается студентами в форме самостоятельной работы. При этом требования к ожидаемым образовательным результатам студентов по данной дисциплине не зависят от формы реализации образовательной программы.

7. Методические рекомендации по видам занятий

Лекционные занятия.

В ходе лекционных занятий обучающимся рекомендуется выполнять следующие действия. Вести конспектирование учебного материала. Обращать внимание на категории, формулировки, раскрывающие содержание тех или иных явлений и процессов, научные выводы и практические рекомендации по их применению. Задавать преподавателю уточняющие вопросы с целью уяснения теоретических положений, разрешения спорных ситуаций.

Желательно оставить в рабочих конспектах поля, на которых во внеаудиторное время можно сделать пометки из рекомендованной литературы, дополняющие материал прослушанной лекции, а также подчеркивающие особую важность тех или иных теоретических положений.

Практические и семинарские занятия.

На практических и семинарских занятиях в зависимости от темы занятия выполняется поиск информации по решению проблем, практические упражнения, контрольные работы, выработка индивидуальных или групповых решений, итоговое обсуждение с обменом знаниями, участие в круглых столах, разбор конкретных ситуаций, командная работа, представление портфолио и т.п.

Самостоятельная работа.

Самостоятельная работа осуществляется в виде изучения литературы, эмпирических данных по публикациям и конкретных ситуаций из практики, подготовке индивидуальных работ, работа с лекционным материалом, самостоятельное изучение отдельных тем дисциплины; поиск и обзор литературы и электронных источников; чтение и изучение учебника и учебных пособий.

8. Фонд оценочных средств

8.1. Перечень компетенций с указанием этапов их формирования в процессе освоения образовательной программы в рамках учебной дисциплины

Основными этапами формирования указанных компетенций при изучении обучающимися дисциплины являются последовательное изучение содержательно связанных между собой тем учебных занятий. Изучение каждой темы предполагает овладение обучающимися необходимыми компетенциями. Результат аттестации обучающихся на различных этапах формирования компетенций показывает уровень освоения компетенций.

Контролируемые разделы (темы) дисциплины	Индекс контроли-руемой компетенции (или её части)	Оценочные средства по этапам формирования компетенций
		текущий контроль по дисциплине
Тема 1. Введение.	ПКС-2	Решение задач, устный опрос
Тема 2. Основные виды уязвимостей программ и веб-приложений	ПКС-2	Решение задач
Тема 3. Сетевой сканер nmap.	ПКС-2	Решение задач
Тема 4. Скриптовый движок Nmap	ПКС-2	Решение задач
Тема 5. Анализ сетевого трафика с цель выявления атак.	ПКС-2	Решение задач
Тема 6. Сканеры безопасности.	ПКС-2	Решение задач
Тема 7. Система тестового вторжения METASPLOIT.	ПКС-2	Решение задач Реферат или групповое задание
Тема 8. Система тестового вторжения Kali Linux.	ПКС-2	Решение задач Контрольная работа Реферат или групповое задание

8.2. Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений и навыков и (или) опыта деятельности процессе текущего контроля

Примеры вопросов для устного опроса:
Тема 1. Введение

1. Понятие уязвимости и эксплоита. Локальные и удаленные эксплоиты.
2. Эскалация привилегий.
3. Примеры сетевых атак.

4. Основные классификаторы уязвимостей. База уязвимостей CVE/NVD.
5. Стандарт проведения тестового вторжения PTES.
6. Фазы тестового вторжения.

Типовые задания практических работ:

Тема 1. Введение

1. С помощью инструмента netcat организовать чат между двумя компьютерами. Найти пакеты TCP-пакеты с сообщениями в Wireshark.
2. С помощью nmap просканировать машину Metasploitable 2 с определением версий сервисов. Найти уязвимый сервис, определить список его уязвимостей по базам. Подобрать эксплойт и с помощью него получить доступ к машине.
3. Написать сканер для перебора DNS-поддоменов.

Тема 2. Основные виды уязвимостей программ и веб-приложений

1. Используя уязвимость Shellshock получить удалённый доступ к виртуальной машине.
2. Используя уязвимость XSS и Heartbleed получить cookie с сессией другого пользователя (студента) уязвимого сервиса.
3. Разработать шелкод для загрузки на сервер заданной картинки с помощью запуска wget системным вызовом execve.

Тема 3. Сетевой сканер Nmap.

1. Найти активные хосты в сети kantiana с использованием:
    a. ping сканирования (-sP)
    b. ARP-сканирования (-PR)
    c. TCP SYN сканирования (-PS).
2. Определить открытые порты и сервисы одного из компьютеров в сети kantiana, используя:
    a. TCP SYN сканирование (-sS);
    b. Сканирование методом подключения по TCP (-sT);
    c. UDP сканирование (-sU);
    d. Сканирование версий (-sV) для определения дополнительной информации;
3. Используя встроенные сценарии Nmap найти уязвимости на учебной машине Metasploitable 3.

Тема 4. Скриптовый движок Nmap

1. Используя встроенные сценарии Nmap найти уязвимости на учебной машине Metasploitable 2/3 и использовать их для получения удалённого доступа
2. Разработать скрипт для поиска уязвимости в сервере Nginx или Apache (использовать определение версий и информацию о последних уязвимостях из CVE/NVD).
3. Разработать фазер для поиска уязвимостей в HTTP-сервера.

Тема 5. Анализ сетевого трафика с целью выявления атак

1. Собрать сетевой трафик в сети в течение 10 минут.
2. Отфильтровать трафик по протоколам TCP/IP, ARP, SMTP, HTTP, DNS.
3. Определить активные хосты с использованием ARP протокола
4. Определить какие хосты являются рабочими станциями, а какие серверами.
5. Определить наличие DNS и HTTP серверов с локальной сети
6. Выявить сканирование портов с помощью TCP SYN и TCP Xmas

Тема 6. Сканеры безопасности.

1. Использовать сканер уязвимости OpenVAS для поиска уязвимых хостов в виртуальной сети-лаборатории.

Тема 7. Система тестового вторжения METASPLOIT

1. Провести тестовое вторжение на учебную систему Metasploitable 2/3.
2. Написать модуль для сканирования сети на наличие уязвимых серверов Nginx.

Тема 8. Система тестового вторжения Kali Linux

1. Провести тестовое вторжение на заданную виртуальную машину с уязвимыми севрисами.

Типовые контрольные задания:

Проверочная работа по теме «Система тестового вторжения METASPLOIT».

Вариант 1

1. Используя систему Metasploit провести тестовое вторжение на учебную виртуальную машину с системой Metasploitable 2/3.
2. Составить список уязвимостей кратким описанием.
3. Классифицировать найденные уязвимости (CVE, CWE, NVD, CVSS).
4. Отсортировать найденные уязвимости по степени опасности.
5. Описать принцип работы используемых эксплоитов.
6. Какие меры защиты закрывают данную уязвимость?
7. Составить отчет.

Проверочная работа по теме «Система тестового вторжения Kali Linux»

Вариант 1

Используя инструменты системы Kali Linux исследовать уязвимость в веб-сервере Nginx версий 1.3.9-1.4.0 (CVE-2013-2028):

1. Дать описание уязвимости, классификацию, описать технику эксплуатации.
2. Воспроизвести уязвимость на тестовой виртуальной машине.
3. Существуют ли эксплоиты? Если есть, опишите принцип работы одного из них.
4. Насколько распространена данная уязвимость?
5. Какие меры защиты закрывают уязвимость?

6. Составить правила к Snort для детектирования атаки.
7. Составить отчет.

Темы рефератов и практических групповых заданий:

1. Обнаружение сетевого сниффера, работающего в полностью пассивном режиме.
2. Разработка модулей Metasploit.
3. Анализ безопасности мобильных устройств и приложений
4. Интеграция системы тестового вторжения Metasploit и Meterpreter.
5. Анализ уязвимости беспроводных сетей.

8.3. Перечень вопросов и заданий для промежуточной аттестации по дисциплине

Вопросы для промежуточного контроля (зачёта):

Тема 1. Введение

1. Понятие уязвимости и эксплоита. Локальные и удаленные эксплоиты.
2. Эскалация привилегий.
3. Примеры сетевых атак.
4. Базы уязвимостей NVD и CVE.
5. Стандарт проведения тестового вторжения PTES. Фазы тестового вторжения.

Тема 2. Основные виды уязвимостей программ и веб-приложений

6. Удалённое выполнение кода. Уязвимость Shellshock.
7. SQL-инъекции (SQLi).
8. Межсайтовый скриптинг (XSS).
9. Уязвимости памяти: утечки. Уязвимость Heartbleed
10. Уязвимости памяти: переполнения буфера. Эксплойт EternalBlue и шифровальщик WannaCry.
11. Методы обнаружения уязвимостей.
12. Методы защиты от уязвимостей.

Тема 3. Сетевой сканер nmap

13. Определение сетевого сканирования.
14. Методики сетевого сканирования
15. Составления карты сети
16. Способы сканирования портов. Сравнительные достоинства и недостатки различных методов сканирования.
17. Идентификация сервисов и определение их версий
18. Способы определения типа и версии операционной системы на целевом хосте. Сравнительные достоинства и недостатки различных способов.
19. Средства обхода межсетевого экрана при сканировании портов.
20. Способы маскировки сканирования портов, реализованные в сетевом сканере nmap.

Тема 4. Скриптовый движок Nmap

21. Программирования скриптов. Язык Lua.
22. Категории скриптов. Структура скрипта. Доступные библиотеки. Функции для работы с различными протоколами.
23. Пример: разработка фаззера.

Тема 5. Анализ сетевого трафика с целью выявления атак

24. Определение термина «сетевые снифферы». Возможности и категории сетевых снифферов.
25. Принципы перехвата трафика на канальном уровне.
26. Методы перехвата сетевого трафика.
27. Возможности сетевых снифферов.
28. Категории сетевых снифферов.
29. Фильтрация пакетов. Пакетные фильтры в wireshark.

Тема 6. Сканеры безопасности

30. Необходимость появления и назначение сканеров безопасности.
31. Общие принципы функционирования сканеров безопасности.
32. Сканирование активных хостов.
33. Сканирование открытых портов.
34. Анализ баннеров активных сервисов для выявления уязвимостей.
35. Ограничения сканеров безопасности.
36. Отличия сканеров безопасности от систем тестового вторжения.

Тема 7. Система тестового вторжения METASPLOIT

37. Архитектура среды MSF. Модульность и возможность расширения MSF. Взаимодействие с ядром MSF. Типы интерфейсов.
38. Обязательные и необязательные параметры в MSF. Параметры RHOST и RPORT. Завершающая функция и параметр LPORT. Выбор и генерация шелл-кода.
39. Шифрование шелл-кодов и создание полиморфных эксплоитов в MSF. Генераторы NOP дорожки.
40. Запуск эксплоита в MSF и динамическая обработка обратного соединения с атакованным хостом.

Тема 8. Система тестового вторжения Kali Linux.

41. Методологии тестового вторжения. Тестирование методом белого ящика, черного ящика и серого ящика. Сравнение различных методологий тестирования, их достоинства, недостатки и сфера применения.
42. Категории фазы сбора информации. Сбор информации о DNS. Уязвимость зонного трансфера DNS.
43. Инструменты для сбора информации о маршрутизации
44. Методы обхода блокировки сетевого экрана, реализованные в инструментах системы.
45. Сканирование виртуальных частных сетей программой.
46. Проведение тестовой атаки в Kali Linux.
47. Фаза эскалации привилегий. Методы эскалации привилегий, реализованные в системе тестового вторжения Kali Linux. Принципы работы радужных таблиц.
48. Методы взлома паролей при атаке оффлайн.
49. Методы взлома паролей при атаке онлайн.
50. Средства подделки сетевых пакетов (спуфинг).
51. Удержание активного доступа.

8.4. Планируемые уровни сформированности компетенций обучающихся и критерии оценивания

Уровни	Содержательное описание уровня	Основные признаки выделения уровня (этапы формирования компетенции, критерии оценки сформированности)	Пятибалльная шкала (академическая) оценка	Двухбалльная шакала, зачет	БРС, % освоения (рейтинговая оценка)
Повышенный	Творческая деятельность	*Включает нижестоящий уровень.* Умение самостоятельно принимать решение, решать проблему/задачу теоретического и прикладного характера на основе изученных методов, приемов, технологий	отлично	зачтено	86-100
Базовый	Применение знаний и умений в более широких контекстах учебной и профессиональной деятельности, нежели по образцу с большей степени самостоятельности и инициативы	*Включает нижестоящий уровень.* Способность собирать, систематизировать, анализировать и грамотно использовать информацию из самостоятельно найденных теоретических источников и иллюстрировать ими теоретические положения или обосновывать практику применения	хорошо		71-85
Удовлетворительный (достаточный)	Репродуктивная деятельность	Изложение в пределах задач курса теоретически и практически контролируемого материала	удовлетворительно		55-70
Недостаточный	Отсутствие признаков удовлетворительного уровня		неудовлетворительно	не зачтено	Менее 55

9. Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины.

Основная литература

1. Шаньгин, В. Ф. Комплексная защита информации в корпоративных системах : учеб. пособие / В.Ф. Шаньгин. — Москва : ИД «ФОРУМ» : ИНФРА-М, 2019. — 592 с. - ISBN 978-5-8199-0730-6. - Текст : электронный. - URL: https://znanium.com/catalog/product/996789 **(online)**

2. Шаньгин, В. Ф. Информационная безопасность компьютерных систем и сетей : учеб. пособие / В.Ф. Шаньгин. — Москва : ИД «ФОРУМ» : ИНФРА-М, 2019. — 416 с. - ISBN 978-5-8199-0754-2. - Текст : электронный. - URL: https://znanium.com/catalog/product/1009605 **(online)**

Дополнительная литература

1. Бирюков, А. А. Информационная безопасность: защита и нападение / А.А. Бирюков. - 2-е изд., перераб. и доп. - Москва : ДМК Пресс, 2017. - 434 с. - ISBN 978-5-97060-435-9. - Текст : электронный. - URL: https://znanium.com/catalog/product/1028060 **(online)**
2. Платонов, В.В. Программно-аппаратные средства обеспечения информационной безопасности вычислительных сетей/В.В. Платонов. 2-е изд. – М: Издательский центр «Академия», 2014. – 336 с. **(10 экз.)**

10. Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины (модуля).

- НЭБ Национальная электронная библиотека, диссертации и прочие издания
- eLIBRARY.RU Научная электронная библиотека, книги, статьи, тезисы докладов конференций
- Гребенников Электронная библиотека ИД журналы
- ЭБС Лань книги, журналы
- ЭБС Консультант студента
- ПРОСПЕКТ ЭБС
- ЭБС ZNANIUM.COM
- РГБ Информационное обслуживание по МБА
- БЕН РАН
- Электронно-библиотечная система (ЭБС) Кантитана (https://elib.kantiana.ru/)
- База эксплоитов (http://www.exploit-db.com)
- База уязвимостей NVD (http://nvd.nist.gov)
- База уязвимостей CVE (http://cve.mitre.org)

11. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине.

Программное обеспечение обучения включает в себя:

- система электронного образовательного контента БФУ им. И. Канта – www.lms-3.kantiana.ru, обеспечивающую разработку и комплексное использование электронных образовательных ресурсов;
- серверное программное обеспечение, необходимое для функционирования сервера и связи с системой электронного обучения через Интернет;
- корпоративная платформа Microsoft Teams;
- установленное на рабочих местах студентов ПО: Microsoft Windows 7-11 или Linux.
- специализированное ПО (при наличии):
    - Kali Linux (Свободное ПО, лицензия GPL).
    - Nmap (Свободное ПО, лицензия GPL).
    - VirtualBox (Свободное ПО, лицензия GPL).
    - Wireshark (Свободное ПО, лицензия GPL).
    - OpenVAS (Свободное ПО, лицензия GPL)
    - Metasploit Framework (Свободное ПО, лицензия BSD).

12. Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине.

Для проведения занятий лекционного типа, практических и семинарских занятий используются специальные помещения (учебные аудитории), оборудованные техническими средствами обучения – мультимедийной проекционной техникой. Для проведения занятий лекционного типа используются наборы демонстрационного оборудования.

Для проведения лабораторных работ, (практических занятий – при необходимости) используются специальные помещения (учебные аудитории), оснащенные специализированным лабораторным оборудованием: персональными компьютерами с возможностью выхода в интернет и с установленным программным обеспечением, заявленным в п.11.

Для проведения групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации используются специальные помещения (учебные аудитории), оборудованные специализированной мебелью (для обучающихся), меловой / маркерной доской.

Для организации самостоятельной работы обучающимся предоставляются помещения, оснащенные компьютерной техникой с возможностью подключения к сети «Интернет» и обеспечением доступа в электронную информационно-образовательную среду университета.

Для обучения инвалидов и лиц с ограниченными возможностями здоровья университетом могут быть представлены специализированные средства обучения, в том числе технические средства коллективного и индивидуального пользования.

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
федеральное государственное автономное образовательное учреждение высшего образования «Балтийский федеральный университет имени Иммануила Канта»
Институт физико-математических наук и информационных технологий

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

«Системы тестового вторжения»

Шифр: 10.05.01
Специальность: «Компьютерная безопасность»
Специализация: «Математические методы защиты информации»
Квалификация (степень) выпускника: Специалист по защите информации

Калининград
2022

Лист согласования

Составитель: Новоселов Семен Александрович, старший преподаватель.

Рабочая программа утверждена на заседании учебно-методического совета института физико-математических наук и информационных технологий
Протокол № 01/22 от «01» февраля 2022 г.

Председатель учебно-методического совета института физико-математических наук и информационных технологий
Первый заместитель директора ИФМНиИТ, к. ф.-м. н., доцент — Шпилевой А. А

Ведущий менеджер — Е.П.Ставицкая

Содержание

1.Наименование дисциплины: «Системы тестового вторжения».

Целью освоения дисциплины «**Системы тестового вторжения**» является расширение и углубление фундаментальной и практической подготовки студентов, обеспечивающей возможность овладения современными методами выявления уязвимостей компьютерных сетей, а также овладение практическими навыками проведения тестовых вторжений для последующей ликвидации выявленных уязвимостей; изучение методологии тестового вторжения и составления отчетности о выявленных уязвимостях.

Необходимость изучения дисциплины продиктована требованиям к защите компьютерных сетей от растущего числа хакерских атак. Исследователи безопасности постоянно находят всё новые и новые уязвимости сетевом программном обеспечении. Системы тестового вторжения позволяют протестировать сети на уязвимости и соответствие стандартам защищенности и своевременно закрыть все найденные уязвимости, препятствуя доступу хакеров в сеть.

Задачами освоения дисциплины «Системы тестового вторжения» являются:

- овладение методами сканирования компьютерных сетей;
- овладение методами выявления уязвимостей;
- овладение методами обнаружения атаки на компьютерные сети.
- практическое освоение систем тестового вторжения Metasploit и Kali Linux.

2. Перечень планируемых результатов обучения по дисциплине, соотнесенных с планируемыми результатами освоения образовательной программы

Код компетенции	Результаты освоения образовательной программы (ИДК)	Результаты обучения по дисциплине
ПКС-2 Способен разрабатывать требования по защите, формировать политики безопасности компьютерных систем и сетей	ПКС-2.1. Выполняет анализ безопасности компьютерных систем и разрабатывает рекомендации по эксплуатации системы защиты информации. ПКС-2.2. Разработка модели угроз безопасности информации. ПКС-2.3. Формирует политики безопасности компьютерных систем и сетей.	**Знать:** • **знать:** основные современные отечественные и зарубежные стандарты в области компьютерной безопасности и проведения аудита безопасности. • **уметь:** грамотно проводить анализ безопасности систем на соответствие стандартам, уметь выявлять уязвимости компьютерных систем и проводить их классификацию. • **владеть:** практическими навыками проведения аудита безопасности сетей и составления отчета.

3. Место дисциплины в структуре образовательной программы

Дисциплина «Системы тестового вторжения» представляет собой дисциплину по выбору части, формируемой участниками образовательных отношений Блока 1 Дисциплины (модули) подготовки студентов.

4. Виды учебной работы по дисциплине.

Виды учебной работы по дисциплине зафиксированы учебным планом основной профессиональной образовательной программы по указанному направлению и профилю, выражаются в академических часах. Часы контактной работы и самостоятельной работы студента и часы, отводимые на процедуры контроля, могут различаться в учебных планах ОПОП по формам обучения. Объем контактной работы включает часы контактной аудиторной работы (лекции/практические занятия/ лабораторные работы), контактной внеаудиторной работы (контроль самостоятельной работы), часы контактной работы в период аттестации. Контактная работа, в том числе может проводиться посредством электронной информационно-образовательной среды университета с использованием ресурсов сети Интернет и дистанционных технологий

5. Содержание дисциплины, структурированное по темам (разделам)

Исходя из рамок, установленных учебным планом по трудоемкости и видам учебной работы по дисциплине, преподаватель самостоятельно выбирает тематику занятий по формам и количеству часов проведения контактной работы: лекции и иные учебные занятия, предусматривающие преимущественную передачу учебной информации преподавателем и (или) занятия семинарского типа (семинары, практические занятия, практикумы, лабораторные работы, коллоквиумы и иные аналогичные занятия), и (или) групповые консультации, и (или) индивидуальную работу обучающихся с преподавателем, в том числе индивидуальные консультации (по курсовым работам/проектам – при наличии курсовой работы/проекта по данной дисциплине в учебном плане). Рекомендуемая тематика занятий максимально полно реализуется в контактной работе со студентами очной формы обучения. В случае реализации образовательной программы в заочной / очно-заочной форме трудоемкость дисциплины сохраняется, однако объем учебного материала в значительной части осваивается студентами в форме самостоятельной работы. При этом требования к ожидаемым образовательным результатам студентов по данной дисциплине не зависят от формы реализации образовательной программы.

№	Наименование раздела	Содержание раздела
1	Тема 1. Введение	Задачи и программа курса. Место курса «*Системы тестового вторжения*» в ряду других математических дисциплин. Формы самостоятельной работы студентов по изучению курса. Литература к курсу. Понятие уязвимости и эксплоита. Локальные и удаленные эксплоиты. Эскалация привилегий. Примеры сетевых атак. Краткая история возникновения хакеров. Журнал phrack. Червь Морриса, первые эксплоиты. Интернет черви и вирусы. Необходимость классификации эксплоитов. Базы уязвимостей Backtrack, CVE и NVD. Стандарт проведения тестового вторжения PTES. Фазы тестового вторжения.
2	Тема 2. Сетевой сканер nmap	Определение сетевого сканирования. Методики сетевого сканирования: составление карты сети, сканирование портов, обнаружение сервисов и определение их версий, определение версии операционной системы.

		Составления карты сети (обнаружение активных хостов): ICMP эхо запрос, ICMP запрос временной метки, запрос сетевой маски. UDP ping запрос. Влияние сетевого экрана на процесс обнаружения активных хостов. Способы сканирования портов, доступные в nmap: сканирование с помощью подключения, полуоткрытое сканирование, невидимое сканирование. Сравнительные достоинства и достоверность различных методов сканирования. Влияние межсетевого экрана при фильтрации открытых портов. TCP и UDP сканирование. Идентификация сервисов и определение их версий. Важность этой стадии для процесса тестового вторжения. Сбор и анализ баннеров активных сервисов. Способы сокрытия баннеров. Определение активных сервисов на нестандартных портах. Определение версии операционной системы. Определение версии по особенностям реализации стека TCP/IP. Достоверность этого метода. Определение версии по набору открытых сервисов и их баннерам. Язык скриптов NSE (Nmap Scripting Engine). Разработка скриптов для поиска уязвимостей.
3	Тема 3. Анализ сетевого трафика с целью выявления атак	Определение термина «сетевые снифферы». Принципы перехвата трафика на канальном уровне. Методы перехвата сетевого трафика. Возможности сетевых снифферов. Категории сетевых снифферов. Основы сетевого сниффера wireshark. Сферы применения wireshark. Возможности wireshark. Основные части и назначение графического интерфейса. Способы перехвата сетевого трафика в wireshark. Фильтрация пакетов. Задание фильтрации на уровне операционной системы. Фильтры захвата пакетов wireshark. Фильтры отображения пакетов. Рекомендации для использования различных типов фильтров для практического применения.
4	Тема 4. Сканеры безопасности XSpider, Nessus, OpenVAS	Необходимость появления и назначение сканеров безопасности. SATAN – первый сканер безопасности с открытым кодом. Коммерческие сканеры безопасности – GFI LAN Guard, XSpider, ISS Internet Scanner. Сканер безопасности Nessus. Сканер безопасности OpenVAS. Сканеры веб-приложений – BurpSuite, OWASP ZAP, w3af, Sqlmap, Nikto. Общие принципы функционирования сканеров безопасности. Сканирование активных хостов. Сканирование открытых портов. Анализ баннеров активных сервисов для выявления уязвимостей.

		Анализ уязвимостей веб-приложений: sql-инъекций и XSS. Ограничения сканеров безопасности. Отличия сканеров безопасности от систем тестового вторжения.
5	Тема 5. Система тестового вторжения METASPLOIT	История создания Metasploit. Лицензирование и условия распространения. Поддерживаемые платформы. Архитектура среды MSF. Модульность и возможность расширения MSF. Взаимодействие с ядром MSF. Типы интерфейсов. Интерфейс msfweb. Навигационная панель интерфейса. Страница выбора эксплоитов. Страница выбора шелл-кодов. Страница активных сессий. Фильтры и категории эксплоитов. Обязательные и необязательные параметры. Параметры RHOST и RPORT. Завершающая функция и параметр LPORT. Выбор и генерация шелл-кода. Шифрование шелл-кодов и создание полиморфных эксплоитов. Генераторы NOP дорожки. Генератор Msf::Nop::Opty2. Получение доступа к командной оболочке в интерфейсе msfweb. Интерфейс msfconsole. Запуск интерфейса в Windows и Linux. Команды общего назначения version, quit и show. Среда окружения MSF. Команды локальной и временной среды MSF. Выбор и конфигурация эксплоитов. Выбор и конфигурация шелл-кода. Работа с генератором NOP дорожки в интерфейсе msfconsole. Запуск эксплоита и динамическая обработка обратного соединения с атакованным хостом. Интерфейс msfcli. Запуск интерфейса msfcli и опции командной строки. Отличия msfcli от интерфейсов msfweb и msfconsole. Выбор и конфигурация эксплоита, шелл-кода и генератора NOP дорожки в интерфейса msfcli. Обновление и загрузка дополнительных эксплоитов и шелл-кодов в Metasploit.
6	Тема 6. Разработка модулей к Metasploit	Введение в язык программирования Ruby. Подмешивание и примеси (mixins). Типы модулей Metasploit. Примеси Metasploit. Создание сканера уязвимостей для поиска старых уязвимых версий веб-серверов Nginx/Apache.
7	Тема 7. Система тестового вторжения Kali Linux	История развития, версии, условия распространения и поддерживаемые платформы. Категории инструментов, включенных в Backtrack: сбор информации, карта сети, идентификация уязвимостей, анализ веб-приложений, анализ WiFi сетей, вторжение, эскалация привилегий, удержание удаленного доступа, аудит VoIP.

		Методологии тестового вторжения. Тестирование методом белого ящика, черного ящика и серого ящика. Сравнение различных методологий тестирования, их достоинства, недостатки и сфера применения. Категории фазы сбора информации. Информация DNS: инструменты dnswalk, dnsenum, dnsmap и dnsrecon. Запуск, параметры и сохранение результатов. Уязвимость зонного трансфера DNS. Инструменты для сбора информации о маршрутизации: 0trace, dmitry, itrace, tcptraceroute и tcptrace. Методы обхода блокировки сетевого экрана, реализованные в данных инструментах. Универсальный инструмент для сбора информации mantego. Фаза сканирования портов – назначение и категории инструментов. Сканеры портов AutoScan, netifera, nmap. Unicornscan, zenmap. Функциональные возможности и особенности перечисленных сканеров. Анализаторы открытых сервисов: amap, httpprint, httsquash. Сканирование виртуальных частных сетей программой ike-scan. Проведение тестовой атаки в Backtrack. Интеграция Metasploit и Backtrack. Фаза эскалации привилегий. Методы эскалации привилегий, реализованные в Backtrack: взлом паролей, сетевое прослушивание (сниффинг) и сетевой спуфинг. Инструменты взлома паролей при атаке оффлайн: rainbowcrack, samdump2, john-the-ripper,ophcrack, crunch, wyd. Принципы работы радужных таблиц. Инструменты взлома паролей при атаке онлайн: BruteSSH и Hydra. Сетевые снифферы dsniff, hamster, tcpdump, tcpick и wireshark. Средства подделки сетевых пакетов (спуфинг) ARPspoof и Etthercap. Удержание активного доступа. Категории этой фазы: средства туннелирования протокола, прокси-сервера, средства коммуникации точка-точка. средства туннелирования протокола DNS2tcp, ptunnel, stunnel4. Прокси-серверы 3proxy и proxychains. Средства коммуникации точка-точка: CryptCat, sbd и socat.

6. Рекомендуемая тематика учебных занятий в форме контактной работы

Рекомендуемая тематика учебных занятий *лекционного* типа (предусматривающих преимущественную передачу учебной информации преподавателями):

№	**Наименование раздела**	**Темы лекций**
1	Тема 1. Введение	Лекция 1. Понятие уязвимости и эксплоита. Базы уязвимостей Backtrack, CVE и NVD.

2	Тема 2. Сетевой сканер nmap	Лекция 2. Методики сетевого сканирования Лекция 3. Способы сканирования портов, доступные в nmap Лекция 4. Идентификация сервисов и определение их версий
3	Тема 3. Анализ сетевого трафика с целью выявления атак	Лекция 5. Определение термина «сетевые снифферы». Лекция 6. Основы сетевого сниффера wireshark Лекция 7. Фильтрация пакетов
4	Тема 4. Сканеры безопасности XSpider, Nessus, OpenVAS	Лекция 8. Сканер безопасности XSpider Лекция 9. Сканер безопасности Nessus Лекция 10. Сканер безопасности OpenVAS
5	Тема 5. Система тестового вторжения METASPLOIT	Лекция 11. Архитектура среды MSF. Лекция 12. Интерфейс msfconsole. Лекция 13. Интерфейс msfcli.
6	Тема 6. Разработка модулей к Metasploit	Лекция 14. Введение в язык программирования Ruby. Лекция 15. Примеси Metasploit.
7	Тема 7. Система тестового вторжения Kali Linux	Лекция 16. Методологии тестового вторжения Лекция 17. Категории фазы сбора информации Лекция 18. Проведение тестовой атаки в Backtrack. Интеграция Metasploit и Backtrack.

Рекомендуемая тематика *практических* занятий:

№ п/п	**Наименование Темы**	**Содержание темы**
1	Использование сетевого сканера nmap	Спецификация цели. Определение активных хостов в сети kantiana. Сканирование портов. Определение активных сервисов и их версий. Определение версии операционной системы. Обход системы обнаружения вторжений.
2	Анализ сетевого трафика с целью выявления атак.	Определение активных хостов с помощью ARP протокола. Определить наличие сетевого сканера nmap при проведении атак TCP SYN и TCP Xmas.
3	Сканеры безопасности XSpider, Nessus, OpenVAS	Использование сканера безопасности XSpider для анализа уязвимостей виртуальных машин Net BSD 1.52 и Open BSD 8.3. Использование сканера безопасности Nessus/OpenVAS для выявления уязвимостей в сети kantiana.
4	Система тестового вторжения METASPLOIT	Проведение тестового вторжения с использованием уязвимости веб-сервера Apache при обработке запросов, разбитых на куски (классификация BID-5033) на виртуальной машине Open BSD 3.0 с использованием интерфейса msfconsole. Использовать генератор NOP дорожки Msf::Nop::Opty2 и шифратор для создания полиморфного шелл-кода.
5	Разработка модулей к Metasploit	Разработка модуля к Metasploit для выявления уязвимости численного переполнения при аутентификации OpenSSH (классификация CVE-2002-0649, BID-5093). Разработка модуля для поиска уязвимых версий Nginx/Apache.
6	Система тестового вторжения Kali Linux	Использовать систему тестового вторжения Kali Linux для определения списка активных хостов и работающих сервисов в сети kantiana. Классифицировать хосты по типу

		операционной системы. Провести тестовое вторжение на виртуальную машину Free BSD 3.0 с использованием возможностей Metasploit Framework. Использовать инструменты оффлайн атаки для анализа хэш-кодов. Создать туннель между атакованной машиной и машиной аудитора.

Требования к самостоятельной работе студентов.

1. Работа с лекционным материалом, предусматривающая проработку конспекта лекций и учебной литературы, по всем темам из п. 6 настоящей рабочей программы.
2. Выполнение домашнего задания, предусматривающего решение задач, выполнение упражнений, выдаваемых на практических занятиях, по всем темам из п. 6 настоящей рабочей программы.

Руководствуясь положениями статьи 47 и статьи 48 Федерального закона от 29 декабря 2012 г. N 273-ФЗ «Об образовании в Российской Федерации» научно-педагогические работники и иные лица, привлекаемые университетом к реализации данной образовательной программы, пользуются предоставленными академическими правами и свободами в части свободы преподавания, свободы от вмешательства в профессиональную деятельность; свободы выбора и использования педагогически обоснованных форм, средств, методов обучения и воспитания; права на творческую инициативу, разработку и применение авторских программ и методов обучения и воспитания в пределах реализуемой образовательной программы и отдельной дисциплины.

Исходя из рамок, установленных учебным планом по трудоемкости и видам учебной работы по дисциплине, преподаватель самостоятельно выбирает тематику занятий по формам и количеству часов проведения контактной работы: лекции и иные учебные занятия, предусматривающие преимущественную передачу учебной информации преподавателем и (или) занятия семинарского типа (семинары, практические занятия, практикумы, лабораторные работы, коллоквиумы и иные аналогичные занятия), и (или) групповые консультации, и (или) индивидуальную работу обучающихся с преподавателем, в том числе индивидуальные консультации (по курсовым работам/проектам – при наличии курсовой работы/проекта по данной дисциплине в учебном плане).

Рекомендуемая тематика занятий максимально полно реализуется в контактной работе со студентами очной формы обучения. В случае реализации образовательной программы в заочной / очно-заочной форме трудоемкость дисциплины сохраняется, однако объем учебного материала в значительной части осваивается студентами в форме самостоятельной работы. При этом требования к ожидаемым образовательным результатам студентов по данной дисциплине не зависят от формы реализации образовательной программы.

7. Методические рекомендации по видам занятий

Лекционные занятия.

В ходе лекционных занятий обучающимся рекомендуется выполнять следующие действия. Вести конспектирование учебного материала. Обращать внимание на категории, формулировки, раскрывающие содержание тех или иных явлений и процессов, научные выводы и практические рекомендации по их применению. Задавать преподавателю

уточняющие вопросы с целью уяснения теоретических положений, разрешения спорных ситуаций.

Желательно оставить в рабочих конспектах поля, на которых во внеаудиторное время можно сделать пометки из рекомендованной литературы, дополняющие материал прослушанной лекции, а также подчеркивающие особую важность тех или иных теоретических положений.

Практические и семинарские занятия.

На практических и семинарских занятиях в зависимости от темы занятия выполняется поиск информации по решению проблем, практические упражнения, контрольные работы, выработка индивидуальных или групповых решений, итоговое обсуждение с обменом знаниями, участие в круглых столах, разбор конкретных ситуаций, командная работа, представление портфолио и т.п.

Самостоятельная работа.

Самостоятельная работа осуществляется в виде изучения литературы, эмпирических данных по публикациям и конкретных ситуаций из практики, подготовке индивидуальных работ, работа с лекционным материалом, самостоятельное изучение отдельных тем дисциплины; поиск и обзор литературы и электронных источников; чтение и изучение учебника и учебных пособий.

8. Фонд оценочных средств

8.1. Перечень компетенций с указанием этапов их формирования в процессе освоения образовательной программы в рамках учебной дисциплины

Основными этапами формирования указанных компетенций при изучении обучающимися дисциплины являются последовательное изучение содержательно связанных между собой тем учебных занятий. Изучение каждой темы предполагает овладение обучающимися необходимыми компетенциями. Результат аттестации обучающихся на различных этапах формирования компетенций показывает уровень освоения компетенций.

Контролируемые разделы (темы) дисциплины	Индекс контроли-руемой компетенции (или её части)	Оценочные средства по этапам формирования компетенций
		текущий контроль по дисциплине
Тема 1. Введение	ПКС-2	Устный опрос
Тема 2. Сетевой сканер nmap	ПКС-2	Решение задач
Тема 3. Анализ сетевого трафика с целью выявления атак	ПКС-2	Решение задач
Тема 4. Сканеры безопасности XSpider, Nessus, OpenVAS	ПКС-2	Решение задач
Тема 5. Система тестового вторжения METASPLOIT	ПКС-2	Решение задач
Тема 6. Разработка модулей к Metasploit	ПКС-2	Решение задач
Тема 7. Система тестового вторжения Kali Linux	ПКС-2	Решение задач Проверочная работа

8.2. Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений и навыков и (или) опыта деятельности процессе текущего контроля

Примеры вопросов для устного опроса:

Тема 1. Введение

1. Понятие уязвимости и эксплоита. Локальные и удаленные эксплоиты.
2. Эскалация привилегий.
3. Примеры сетевых атак.
4. Основные классификаторы уязвимостей. Базы уязвимостей Backtrack и CVE.
5. Стандарт проведения тестового вторжения PTES.
6. Фазы тестового вторжения.

Типовые задания практических работ:

Тема 5. Система тестового вторжения METASPLOIT.

	Задача
Оценка «зачтено» - низкий уровень освоения компетенции	Найти уязвимости в учебной системе Metasploitable 2.
Оценка «зачтено» - повышенный уровень освоения компетенции	Провести тестовое вторжение на учебную систему Metasploitable 2.
Оценка «зачтено» - высокий уровень освоения компетенции	Написать модуль для сканирования сети на наличие уязвимых серверов Nginx.

Тема 7. Система тестового вторжения Kali Linux»

	Задача
Оценка «зачтено» - низкий уровень освоения компетенции	1. Составить список активных хостов в сети kantiana.ru с использованием инструментов сбора информации по протоколу DNS. Определить разрешен ли в сети kantiana.ru механизм зонного трансфера DNS и объяснить почему. 2. Выбрать целевой хост в сети kantiana.ru и определить на нем открытые порты с использованием инструментов AutoScan, Netifera, nmap и Unicornmap.
Оценка «зачтено» - повышенный уровень освоения компетенции	1. Выбрать целевой хост в сети kantiana.ru и определить типы и номера версий работающих на хосте сервисов с использованием amap, httpprint, httsquash. Сравнить эти результаты с результатами ‘nmap -sV’. 2. Определить, есть ли в сети kantiana.ru виртуальные частные сети с помощью инструмента ike-scan.
Оценка «зачтено» - высокий уровень	1. Провести тестовое вторжение на виртуальную машину Free BSD 3.0 с использованием возможностей Metasploit

освоения компетенции	Framework, интегрированного с Backtrack. Получив права суперпользователя, скопировать файл паролей /etc/shadow и htpasswd из-под DOCROOT веб-сервера Apache для их последующего анализа. 2. Использовать файлы паролей shadow и htpasswd для взлома хэш-значений с использованием инструментов оффлайн атаки john, crunch, ophcrack. Использовать для тех же целей анализ хэш-значений с использованием rainbowcrack и радужных таблиц. Сравнить результативность и время выполнения. Определить время работы для криптографически нестойких паролей для всех указанных инструментов.

Тема 3. Анализ сетевого трафика с целью выявления атак.

	Задача
Оценка «зачтено» - низкий уровень освоения компетенции	1. Собрать сетевой трафик в сети kantiana в течение 10 минут. 2. Отфильтровать трафик по протоколам TCP/IP, ARP, SMTP, HTTP, DNS. 3. Определить активные хосты с использованием ARP протокола 4. Определить какие хосты являются рабочими станциями, а какие серверами.
Оценка «зачтено» - повышенный уровень освоения компетенции	1. Определить наличие DNS и HTTP серверов с локальной сети 2. Протрассировать HTTP сессии 3. Использовать возможности трассировки для выявления уязвимости протоколов HTTP, telnet и FTP 4. Показать, что протокол HTTPS безопасен
Оценка «зачтено» - высокий уровень освоения компетенции	Выявить наличие сетевого сканера nmap при проведении атак TCP SYN и TCP Xmas

Тема 6. Разработка модулей к Metasploit.

	Задача
Оценка «зачтено» - низкий уровень освоения компетенции	Написать модуль Metasploit для определения активных хостов и сервисов в сети kantiana.ru
Оценка «зачтено» - повышенный уровень освоения компетенции	Написать модуль Metasploit для определения DNS серверов в сети kantiana.ru
Оценка «зачтено» - высокий уровень освоения компетенции	Написать модуль Metasploit для выявления уязвимости численного переполнения при аутентификации OpenSSH (классификация CVE-2002-0649, BID-5093).

Тема 2. Сетевой сканер nmap.

	Задача

Оценка «зачтено» - низкий уровень освоения компетенции	Найти активные хосты в сети kantiana с использованием: 1. ping сканирования (-sP) 2. ARP-сканирования (-PR) 3. TCP SYN сканирования (-PS).
Оценка «зачтено» - повышенный уровень освоения компетенции	Определить открытые порты и сервисы одного из компьютеров в сети kantiana, используя: 1. TCP SYN сканирование (-sS); 2. Сканирование методом подключения по TCP (-sT); 3. UDP сканирование (-sU); 4. Сканирование версий (-sV) для определения дополнительной информации;
Оценка «зачтено» - высокий уровень освоения компетенции	Используя встроенные сценарии Nmap найти уязвимости на учебной машине Metasploitable 2.

Тема 4. Сканеры безопасности.

	Задача
Оценка «зачтено» - низкий уровень освоения компетенции	1. Использовать сканер безопасности XSpider для анализа уязвимостей виртуальной машины Net BSD 1.52 2. Дать пояснения по каждой найденной уязвимости с использованием баз данных Bugtraq и CVE. Ответ обосновать.
Оценка «зачтено» - повышенный уровень освоения компетенции	1. Использовать сканер безопасности XSpider для анализа уязвимостей виртуальной машины OpenBSD 8.3. 2. Являются ли все найденные уязвимости реальными? Ответ обосновать.
Оценка «зачтено» - высокий уровень освоения компетенции	Использовать сканер уязвимости OpenVAS для поиска уязвимых хостов в сети kantiana.ru.

Типовые проверочные задания:

Проверочная работа по теме «Система тестового вторжения METASPLOIT».
Вариант 1

1. Используя систему Metasploit провести тестовое вторжение на учебную виртуальную машину с системой Metasploitable 2.
2. Составить список уязвимостей кратким описанием.
3. Классифицировать найденные уязвимости (CVE, CWE, NVD, CVSS).
4. Отсортировать найденные уязвимости по степени опасности.
5. Описать принцип работы используемых эксплоитов.
6. Какие меры защиты закрывают данную уязвимость?
7. Составить отчет.

Проверочная работа по теме «Система тестового вторжения Kali Linux»
Вариант 1

Используя инструменты системы Kali Linux исследовать уязвимость в веб-сервере Nginx версий 1.3.9-1.4.0 (CVE-2013-2028):

1. Дать описание уязвимости, классификацию, описать технику эксплуатации.
2. Воспроизвести уязвимость на тестовой виртуальной машине.
3. Существуют ли эксплоиты? Если есть, опишите принцип работы одного из них.
4. Насколько распространена данная уязвимость?
5. Какие меры защиты закрывают уязвимость?
6. Составить правила к Snort для детектирования атаки.
7. Составить отчет.

Проверочная работа по теме «Анализ сетевого трафика с целью выявления атак»

Вариант 1

Собрать сетевой трафик в сети kantiana в течение 10 минут.

1. Отфильтровать трафик по протоколам TCP/IP, ARP, SMTP, HTTP, DNS
2. Составить список активных хостов по данным ARP-протокола
3. Определить какие хосты являются рабочими станциями, а какие серверами
4. Определить наличие DNS и HTTP серверов в локальной сети
5. По данным SSDP-протокола определить наличие и тип устройств в сети (принтеров,
6. сканеров и т.п.)
7. Протрассировать HTTP сессии и авторизацию
8. Использовать возможности трассировки для выявления уязвимости протоколов
9. HTTP, telnet и FTP
10. Показать, что протокол HTTPS безопасен

Проверочная работа по теме «Разработка модулей к Metasploit»
Вариант 1

Написать модуль для Metasploit для выявления уязвимости численного переполнения при аутентификации OpenSSH (классификация CVE-2002-0649, BID-5093).

Проверочная работа по теме «Сетевой сканер nmap»
Вариант 1

1. Провести сканирование портов учебной машины методом «невидимого» idle-сканирования.
2. С помощью скриптов из состава Nmap найти уязвимости сервисов целевой машины.
3. Составить отчет.

Проверочная работа по теме «Сканеры безопасности»
Вариант 1

1. С помощью сканера OpenVAS найти уязвимости на учебной машине.
2. Разработать рекомендации по их устранению.
3. Составить отчет.

8.3. Перечень вопросов и заданий для промежуточной аттестации по дисциплине

Вопросы для промежуточного контроля (зачёта):

Тема 1. Введение

1. Понятие уязвимости и эксплоита. Локальные и удаленные эксплоиты.
2. Эскалация привилегий.
3. Примеры сетевых атак.
4. Базы уязвимостей Backtrack, CVE, NVD.
5. Стандарт проведения тестового вторжения PTES. Фазы тестового вторжения.

Тема 2. Сетевой сканер nmap

6. Определение сетевого сканирования.
7. Методики сетевого сканирования
8. Составления карты сети
9. Способы сканирования портов. Сравнительные достоинства и недостатки различных методов сканирования.
10. Идентификация сервисов и определение их версий
11. Способы определения типа и версии операционной системы на целевом хосте. Сравнительные достоинства и недостатки различных способов.
12. Средства обхода межсетевого экрана при сканировании портов.
13. Способы маскировки сканирования портов, реализованные в сетевом сканере nmap.

Тема 3. Анализ сетевого трафика с целью выявления атак

14. Определение термина «сетевые снифферы». Возможности и категории сетевых снифферов.
15. Принципы перехвата трафика на канальном уровне.
16. Методы перехвата сетевого трафика.
17. Возможности сетевых снифферов.
18. Категории сетевых снифферов.
19. Фильтрация пакетов. Пакетные фильтры в wireshark.

Тема 4. Сканеры безопасности

20. Необходимость появления и назначение сканеров безопасности.
21. Общие принципы функционирования сканеров безопасности.
22. Сканирование активных хостов.
23. Сканирование открытых портов.
24. Анализ баннеров активных сервисов для выявления уязвимостей.
25. Ограничения сканеров безопасности.
26. Отличия сканеров безопасности от систем тестового вторжения.

Тема 5. Система тестового вторжения METASPLOIT

27. Архитектура среды MSF. Модульность и возможность расширения MSF. Взаимодействие с ядром MSF. Типы интерфейсов.
28. Обязательные и необязательные параметры в MSF. Параметры RHOST и RPORT. Завершающая функция и параметр LPORT. Выбор и генерация шелл-кода.
29. Шифрование шелл-кодов и создание полиморфных эксплоитов в MSF. Генераторы NOP дорожки.
30. Запуск эксплоита в MSF и динамическая обработка обратного соединения с атакованным хостом.

Тема 6. Разработка модулей к METASPLOIT

31. Язык программирования Ruby. Подмешивание и примеси (mixins).
32. Типы модулей Metasploit.
33. Примеси Metasploit.

34. Создание сканера уязвимостей для поиска старых уязвимых версий веб-серверов Nginx/Apache.

Тема 7. Система тестового вторжения Kali Linux.

35. Методологии тестового вторжения. Тестирование методом белого ящика, черного ящика и серого ящика. Сравнение различных методологий тестирования, их достоинства, недостатки и сфера применения.
36. Категории фазы сбора информации. Сбор информации о DNS. Уязвимость зонного трансфера DNS.
37. Инструменты для сбора информации о маршрутизации
38. Методы обхода блокировки сетевого экрана, реализованные в инструментах системы.
39. Сканирование виртуальных частных сетей программой.
40. Проведение тестовой атаки в Kali Linux.
41. Фаза эскалации привилегий. Методы эскалации привилегий, реализованные в системе тестового вторжения Kali Linux. Принципы работы радужных таблиц.
42. Методы взлома паролей при атаке оффлайн.
43. Методы взлома паролей при атаке онлайн.
44. Средства подделки сетевых пакетов (спуфинг).
45. Удержание активного доступа.

8.4. Планируемые уровни сформированности компетенций обучающихся и критерии оценивания

Уровни	Содержательное описание уровня	Основные признаки выделения уровня (этапы формирования компетенции, критерии оценки сформированности)	Пятибалльная шкала (академическая) оценка	Двухбалльная шакала, зачет	БРС, % освоения (рейтинговая оценка)
Повышенный	Творческая деятельность	*Включает нижестоящий уровень.* Умение самостоятельно принимать решение, решать проблему/задачу теоретического и прикладного характера на основе изученных методов, приемов, технологий	отлично	зачтено	86-100
Базовый	Применение знаний и умений в более широких контекстах учебной и профессиональной деятельности,	*Включает нижестоящий уровень.* Способность собирать, систематизировать, анализировать и грамотно использовать информацию из самостоятельно найденных теоретических	хорошо		71-85

	нежели по образцу с большей степени самостоятельности и инициативы	источников и иллюстрировать ими теоретические положения или обосновывать практику применения			
Удовлетворительный (достаточный)	Репродуктивная деятельность	Изложение в пределах задач курса теоретически и практически контролируемого материала	удовлетворительно		55-70
Недостаточный	Отсутствие признаков удовлетворительного уровня		неудовлетворительно	не зачтено	Менее 55

9. Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины.

Основная литература

1. Шаньгин, В. Ф. Комплексная защита информации в корпоративных системах : учеб. пособие / В.Ф. Шаньгин. — Москва : ИД «ФОРУМ» : ИНФРА-М, 2019. — 592 с. - ISBN 978-5-8199-0730-6. - Текст : электронный. - URL: https://znanium.com/catalog/product/996789 **(online)**
2. Шаньгин, В. Ф. Информационная безопасность компьютерных систем и сетей : учеб. пособие / В.Ф. Шаньгин. — Москва : ИД «ФОРУМ» : ИНФРА-М, 2019. — 416 с. - ISBN 978-5-8199-0754-2. - Текст : электронный. - URL: https://znanium.com/catalog/product/1009605 **(online)**

Дополнительная литература

1. Бирюков, А. А. Информационная безопасность: защита и нападение / А.А. Бирюков. - 2-е изд., перераб. и доп. - Москва : ДМК Пресс, 2017. - 434 с. - ISBN 978-5-97060-435-9. - Текст : электронный. - URL: https://znanium.com/catalog/product/1028060 **(online)**
2. Платонов, В.В. Программно-аппаратные средства обеспечения информационной безопасности вычислительных сетей/В.В. Платонов. 2-е изд. – М: Издательский центр «Академия», 2014. – 336 с. **(10 экз.)**

10. Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины (модуля).

- НЭБ Национальная электронная библиотека, диссертации и прочие издания
- eLIBRARY.RU Научная электронная библиотека, книги, статьи, тезисы докладов конференций
- Гребенников Электронная библиотека ИД журналы
- ЭБС Лань книги, журналы
- ЭБС Консультант студента
- ПРОСПЕКТ ЭБС
- ЭБС ZNANIUM.COM
- РГБ Информационное обслуживание по МБА
- БЕН РАН

- Электронно-библиотечная система (ЭБС) Кантитана (https://elib.kantiana.ru/)
- База эксплоитов (http://www.exploit-db.com)
- База уязвимостей NVD (http://nvd.nist.gov)
- База уязвимостей CVE (http://cve.mitre.org)

11. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине.

Программное обеспечение обучения включает в себя:

- система электронного образовательного контента БФУ им. И. Канта – www.lms-3.kantiana.ru, обеспечивающую разработку и комплексное использование электронных образовательных ресурсов;
- серверное программное обеспечение, необходимое для функционирования сервера и связи с системой электронного обучения через Интернет;
- корпоративная платформа Microsoft Teams;
- установленное на рабочих местах студентов ПО: Microsoft Windows 7-11 или Linux.
- специализированное ПО (при наличии):
    - Kali Linux (Свободное ПО, лицензия GPL).
    - Nmap (Свободное ПО, лицензия GPL).
    - VirtualBox (Свободное ПО, лицензия GPL).
    - Wireshark (Свободное ПО, лицензия GPL).
    - OpenVAS (Свободное ПО, лицензия GPL)
    - Metasploit Framework (Свободное ПО, лицензия BSD).

12. Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине.

Для проведения занятий лекционного типа, практических и семинарских занятий используются специальные помещения (учебные аудитории), оборудованные техническими средствами обучения – мультимедийной проекционной техникой. Для проведения занятий лекционного типа используются наборы демонстрационного оборудования.

Для проведения лабораторных работ, (практических занятий – при необходимости) используются специальные помещения (учебные аудитории), оснащенные специализированным лабораторным оборудованием: персональными компьютерами с возможностью выхода в интернет и с установленным программным обеспечением, заявленным в п.11.

Для проведения групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации используются специальные помещения (учебные аудитории), оборудованные специализированной мебелью (для обучающихся), меловой / маркерной доской.

Для организации самостоятельной работы обучающимся предоставляются помещения, оснащенные компьютерной техникой с возможностью подключения к сети «Интернет» и обеспечением доступа в электронную информационно-образовательную среду университета.

Для обучения инвалидов и лиц с ограниченными возможностями здоровья университетом могут быть представлены специализированные средства обучения, в том числе технические средства коллективного и индивидуального пользования.

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ
федеральное государственное автономное образовательное учреждение
высшего образования
«Балтийский федеральный университет имени Иммануила Канта»
Институт физико-математических наук и информационных технологий

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

«Методы и алгоритмы генерации эллиптических кривых для криптографии»

Шифр: 10.05.01
Специальность: «Компьютерная безопасность»
Специализация: «Математические методы защиты информации»
Квалификация (степень) выпускника: специалист по защите информации

Калининград
2022

Лист согласования

Составитель: Малыгина Екатерина Сергеевна, к.ф.-м.н., доцент

Рабочая программа утверждена на заседании учебно-методического совета института физико-математических наук и информационных технологий

Протокол № 01/22 от «01» февраля 2022 г.

Председатель учебно-методического
совета института физико-
математических наук и информационных
технологий

Первый заместитель директора Шпилевой А. А
ИФМНиИТ, к. ф.-м. н., доцент

Ведущий менеджер Е.П.Ставицкая

Содержание

1.Наименование дисциплины:

«Методы и алгоритмы генерации эллиптических кривых для криптографии».

Цель дисциплины: целью освоения дисциплины «Методы и алгоритмы генерации эллиптических кривых для криптографии» является углубление подготовки студентов в современной арифметической теории эллиптических кривых и алгебраической теории чисел до уровня, необходимого для освоения метода генерации эллиптических кривых для криптографии и оценки его эффективности, а также подготовка к написанию теоретической части выпускной квалификационной работы в области современной криптографии на основе освоения совокупности математических моделей и методов комплексного умножения на эллиптических кривых, умения анализировать стойкость получаемых криптосистем и эффективность применяемых алгоритмов.

2. Перечень планируемых результатов обучения по дисциплине, соотнесенных с планируемыми результатами освоения образовательной программы

Код компетенции	Результаты освоения образовательной программы (ИДК)	Результаты обучения по дисциплине
ПКС-7. Способность проводить анализ и участвовать в разработке математических моделей безопасности компьютерных систем.	ПКС-7.1. Знает математические методы моделирования безопасных компьютерных систем. ПКС-7.2. Осуществляет анализ математических моделей безопасности компьютерных систем. ПКС-7.3. Участвует в разработке математических моделей безопасности компьютерных систем.	- **знать** базовые алгоритмы алгебраической теории чисел и теории эллиптических кривых; - **уметь** разрабатывать и реализовывать алгоритмы редукции бинарных квадратичных форм, вычисления классового числа, вычисления гильбертова классового многочлена, генерации эллиптических кривых, пригодных для криптографических приложений; - **владеть** навыками программной реализации общего алгоритма генерации эллиптических кривых на основе метода комплексного умножения и его модификаций.

3. Место дисциплины в структуре образовательной программы

Дисциплина «Методы и алгоритмы генерации эллиптических кривых для криптографии» представляет собой дисциплину части, формируемой участниками образовательных отношений блока дисциплин подготовки обучающихся.

4. Виды учебной работы по дисциплине.

Виды учебной работы по дисциплине зафиксированы учебным планом основной профессиональной образовательной программы по указанному направлению и профилю, выражаются в академических часах. Часы контактной работы и самостоятельной работы

обчающегося и часы, отводимые на процедуры контроля, могут различаться в учебных планах ОПОП по формам обучения. Объем контактной работы включает часы контактной аудиторной работы (лекции/практические занятия/ лабораторные работы), контактной внеаудиторной работы (контроль самостоятельной работы), часы контактной работы в период аттестации. Контактная работа, в том числе может проводиться посредством электронной информационно-образовательной среды университета с использованием ресурсов сети Интернет и дистанционных технологий

5. Содержание дисциплины, структурированное по темам (разделам)

Исходя из рамок, установленных учебным планом по трудоемкости и видам учебной работы по дисциплине, преподаватель самостоятельно выбирает тематику занятий по формам и количеству часов проведения контактной работы: лекции и иные учебные занятия, предусматривающие преимущественную передачу учебной информации преподавателем и (или) занятия семинарского типа (семинары, практические занятия, практикумы, лабораторные работы, коллоквиумы и иные аналогичные занятия), и (или) групповые консультации, и (или) индивидуальную работу обучающихся с преподавателем, в том числе индивидуальные консультации (по курсовым работам/проектам – при наличии курсовой работы/проекта по данной дисциплине в учебном плане). Рекомендуемая тематика занятий максимально полно реализуется в контактной работе с обучающимися очной формы обучения. В случае реализации образовательной программы в заочной / очно-заочной форме трудоемкость дисциплины сохраняется, однако объем учебного материала в значительной части осваивается обучающимися в форме самостоятельной работы. При этом требования к ожидаемым образовательным результатам обучающихся по данной дисциплине не зависят от формы реализации образовательной программы.

№	Наименование раздела	Содержание раздела
1	Некоторые главы алгебраической теории чисел	Функция Вейерштрасса. j-функции. Квадратичные формы. Гильбертово поле классов.
2	Теория эллиптических кривых	Группа точек эллиптической кривой. Комплексное умножение. Эллиптические кривые над комплексными числами. Эллиптические кривые над конечными полями. Теорема Дойринга о поднятии.
3	Методы генерации эллиптических кривых на базе комплексного умножения	“Наивный” метод. Классический метод комплексного умножения. Численные значения j-функций. Комплексно-аналитический подход. Построение многочлена Гильберта. Метод на основе китайской теоремы об остатках. Некоторые модификации метода комплексного умножения.

6. Рекомендуемая тематика учебных занятий в форме контактной работы

Рекомендуемая тематика учебных занятий *лекционного* типа (предусматривающих преимущественную передачу учебной информации преподавателями):

№	Наименование раздела	Темы лекций

1	Некоторые главы алгебраической теории чисел	Лекция 1. Функция Вейерштрасса. j-функции. Лекция 2-3. Квадратичные формы, их взаимосвязь с числовыми полями. Лекция 4. Гильбертово поле классов мнимого квадратичного поля. Лекция 5. Уравнение Карначчи.
2	Теория эллиптических кривых	Лекция 6. Основные понятия теории эллиптических кривых. Инварианты. Классы изоморфизмов. Кольца эндоморфизмов. Лекция 7. Групповой закон на множестве точек эллиптической кривой. Комплексное умножение. Лекция 8-9. Эллиптические кривые над полем комплексных чисел. Решетки. Эллиптические функции. Структура кольца эндоморфизмов. Лекция 10-11. Эллиптические кривые над конечными полями. Отображение Фробениуса. Число рациональных точек. След Фробениуса. Кольцо эндоморфизмов. Лекция 12. Теорема Дойринга о поднятии.
3	Методы генерации эллиптических кривых на базе комплексного умножения	Лекция 13. “Наивный” метод. Лекция 14. Метод комплексного умножения: вычислительные аспекты. Лекция 15. Метод комплексного умножения: Численное значение j-функции. Лекция 16-17. Вычисление многочлена Гильберта: комплексно-аналитический подход. Лекция 18. Модификация метода комплексного умножения на базе китайской теоремы об остатках. Лекция 19-21. Некоторые модификации метода комплексного умножения в зависимости классификации дискриминанта числового поля.

Рекомендуемая тематика *практических* занятий:

1. Вычисление группы классов идеалов и числа классов.
2. Разложение идеалов в числовом поле.
3. Вычисления с квадратичными формами.
4. Решение уравнения Карначчи.
5. Вычисление числа рациональных точек эллиптической кривой над конечным полем.
6. Построение эллиптической кривой по ее инвариантам.
7. Вычисление квадратичного скручивания для заданной эллиптической кривой.
8. Реализация “наивного” метода.
9. Построение гильбертова классового многочлена.
10. Реализация метода комплексного умножения.
11. Реализация метода комплексного умножения на базе китайской теоремы об остатках.
12. Реализация некоторых модификаций метода комплексного умножения.

На практических занятиях решаются задачи по теме занятия.

Требования к самостоятельной работе обучающихся

1. Работа с лекционным материалом, предусматривающая проработку конспекта лекций и учебной литературы, по всем темам из п. 6 настоящей рабочей программы.

2. Выполнение домашнего задания, предусматривающего решение задач, выполнение упражнений, выдаваемых на практических занятиях, по всем темам из п. 6 настоящей рабочей программы.

Руководствуясь положениями статьи 47 и статьи 48 Федерального закона от 29 декабря 2012 г. N 273-ФЗ «Об образовании в Российской Федерации» научно-педагогические работники и иные лица, привлекаемые университетом к реализации данной образовательной программы, пользуются предоставленными академическими правами и свободами в части свободы преподавания, свободы от вмешательства в профессиональную деятельность; свободы выбора и использования педагогически обоснованных форм, средств, методов обучения и воспитания; права на творческую инициативу, разработку и применение авторских программ и методов обучения и воспитания в пределах реализуемой образовательной программы и отдельной дисциплины.

Исходя из рамок, установленных учебным планом по трудоемкости и видам учебной работы по дисциплине, преподаватель самостоятельно выбирает тематику занятий по формам и количеству часов проведения контактной работы: лекции и иные учебные занятия, предусматривающие преимущественную передачу учебной информации преподавателем и (или) занятия семинарского типа (семинары, практические занятия, практикумы, лабораторные работы, коллоквиумы и иные аналогичные занятия), и (или) групповые консультации, и (или) индивидуальную работу обучающихся с преподавателем, в том числе индивидуальные консультации (по курсовым работам/проектам – при наличии курсовой работы/проекта по данной дисциплине в учебном плане).

Рекомендуемая тематика занятий максимально полно реализуется в контактной работе с обучающимися очной формы обучения. В случае реализации образовательной программы в заочной / очно-заочной форме трудоемкость дисциплины сохраняется, однако объем учебного материала в значительной части осваивается обучающимися в форме самостоятельной работы. При этом требования к ожидаемым образовательным результатам обучающихся по данной дисциплине не зависят от формы реализации образовательной программы.

7. Методические рекомендации по видам занятий

Лекционные занятия.

В ходе лекционных занятий обучающимся рекомендуется выполнять следующие действия. Вести конспектирование учебного материала. Обращать внимание на категории, формулировки, раскрывающие содержание тех или иных явлений и процессов, научные выводы и практические рекомендации по их применению. Задавать преподавателю уточняющие вопросы с целью уяснения теоретических положений, разрешения спорных ситуаций.

Желательно оставить в рабочих конспектах поля, на которых во внеаудиторное время можно сделать пометки из рекомендованной литературы, дополняющие материал прослушанной лекции, а также подчеркивающие особую важность тех или иных теоретических положений.

Практические и семинарские занятия.

На практических и семинарских занятиях в зависимости от темы занятия выполняется поиск информации по решению проблем, практические упражнения,

контрольные работы, выработка индивидуальных или групповых решений, итоговое обсуждение с обменом знаниями, участие в круглых столах, разбор конкретных ситуаций, командная работа, представление портфолио и т.п.

Самостоятельная работа.

Самостоятельная работа осуществляется в виде изучения литературы, эмпирических данных по публикациям и конкретных ситуаций из практики, подготовке индивидуальных работ, работа с лекционным материалом, самостоятельное изучение отдельных тем дисциплины; поиск и обзор литературы и электронных источников; чтение и изучение учебника и учебных пособий.

8. Фонд оценочных средств

8.1. Перечень компетенций с указанием этапов их формирования в процессе освоения образовательной программы в рамках учебной дисциплины

Основными этапами формирования указанных компетенций при изучении обучающимися дисциплины являются последовательное изучение содержательно связанных между собой тем учебных занятий. Изучение каждой темы предполагает овладение обучающимися необходимыми компетенциями. Результат аттестации обучающихся на различных этапах формирования компетенций показывает уровень освоения компетенций.

Контролируемые разделы (темы) дисциплины	Индекс контроли-руемой компетенции (или её части)	Оценочные средства по этапам формирования компетенций
		текущий контроль по дисциплине
1. Некоторые главы алгебраической теории чисел	ПКС-7	Опрос, решение задач.
2. Теория эллиптических кривых		Опрос, решение задач, контрольная работа
3. Методы генерации эллиптических кривых на базе комплексного умножения		Опрос, программная реализация алгоритмов

8.2. Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений и навыков и (или) опыта деятельности процессе текущего контроля

Примеры вопросов для устного опроса:

1. Как определяются группы кручения точек эллиптической кривой?
2. Дать определения изогении и эндоморфизма эллиптической кривой. Сформулировать их основные свойства.
3. Изложить алгоритм Корначчи.
4. Дать определение функции Вейерштрасса. Сформулировать основные свойства функции Вейерштрасса.
5. Дать определение модулярной группы. Привести пример.
6. Каким образом задаются отображения между эллиптическими кривыми над комплексными числами и торами?

7. Дать определение дискриминанта и j-инварианта эллиптической кривой. Сформулировать их основные свойства.
8. Каким образом осуществляется редукция эллиптических кривых?

Типовые контрольные задания:

1. Вычислить непосредственно группу классов идеалов поля $K = \mathbb{Q}(\sqrt{m})$ для заданного m.
2. Написать программу, которая при заданном дискриминанте $D < 0$ вычисляет группу классов идеалов кольца целых мнимого квадратичного числового поля $\mathbb{Q}(\sqrt{D})$.
3. Написать программу сложения точек на эллиптической кривой над Φ_p, $p \neq 2, 3$. Кривая задана уравнением $y^2 = x^3 + ax + b$.
4. Написать программу, которая при задании нечётного простого числа p вычисляет число точек на эллиптической кривой $y^2 = x^3 + x$ над Φ_p.
5. Запрограммировать алгоритм генерации эллиптических кривых на основе комплексного умножения. Входом должен быть дискриминант D_K максимального порядка O_K, $|D_K| < 1000$. Выходом должно быть уравнение эллиптической кривой E над конечным полем Φ_p, где $|E(\Phi_p)| = k \cdot q$, $k \leq 1000$, q – простое число. По шагам:
   - Найти случайным поиском элемент $w \in O_K$, такое, что $w\bar{w} = p$ – простое число и $(1 - w)(1 - \bar{w}) = k \cdot q$ для упомянутых k и q.
   - Подсчитать классовый многочлен $H_{D_K}(X)$ для O_K.
   - Найти корень $j \in \Phi_p$ многочлена $H_{D_K}(X) \pmod p$.
   - Положим

$$E_1 : y^2 = x^3 - kx - k, \qquad E_2 : y^2 = x^3 - kc^2x - kc^3,$$

   где $k = \frac{27j}{j-1728}$ и c – квадратичный невычет по модулю p.

   - Выбрать случайную точку $P \in E_i$ и проверить, выполняется ли равенство $(k \cdot q)P = O$.

8.3. Перечень вопросов и заданий для промежуточной аттестации по дисциплине

Вопросы для промежуточного контроля (зачета)

1. Модулярные формы.
2. j-функции.
3. Метод вычисления $j(\tau)$.
4. Основные определения алгебраической теории чисел: числовое поле; кольцо алгебраических целых; дедекиндовы кольца; поле вычетов; дробные идеалы; группа классов идеалов.
5. Ветвление в числовых полях.
6. Квадратичные поля.
7. Порядки в мнимых квадратичных полях.
8. Квадратичные формы.
9. Вычисление классового числа квадратичных форм с отрицательным дискриминантом.
10. Вычисление редуцированных квадратичных форм с отрицательным дискриминантом.

11. Порядки и квадратичные формы.
12. Гильбертово поле классов.
13. Отображение Артина.
14. Определение эллиптической кривой над полем *k*.
15. Основные инварианты эллиптической кривой над *k*.
16. Изоморфные эллиптические кривые над *k*.
17. Скручивание эллиптических кривых.
18. Закон сложения точек эллиптической кривой над *k*.
19. Приведение эллиптической кривой к форме Вейерштрасса.
20. Кольцо эндоморфизмов эллиптической кривой над *k*.
21. Классификация колец эндоморфизмов.
22. Решётки и базисы.
23. Эллиптические функции и их свойства.
24. Функция Вейерштрасса и ее свойства.
25. Двояко-периодические функции и их свойства.
26. *j*-инвариант решетки.
27. Голоморфные отображения.
28. Эллиптическая кривая, ассоциированная с решеткой.
29. Классификация эллиптических кривых над X.
30. Структура кольца эндоморфизмов.
31. Комплексное умножение.
32. Гомоморфизм Фробениуса и его свойства.
33. Число рациональных точек эллиптической кривой над конечным полем.
34. След эндоморфизма Фробениуса. Основная теорема.
35. Кольцо эндоморфизмов эллиптической кривой над конечным полем.
36. Редукция эллиптической кривой по модулю p.
37. Невырожденная редукция.
38. Теорема Дойринга.
39. Метод комплексного умножения.
40. Вычисление гильбертова классового многочлена.
41. Альтернативный метод комплексного умножения.

8.4. Планируемые уровни сформированности компетенций обучающихся и критерии оценивания

Уровни	Содержательное описание уровня	Основные признаки выделения уровня (этапы формирования компетенции, критерии оценки сформированности)	Пятибалльная шкала (академическая) оценка	Двухбалльная шакала, зачет	БРС, % освоения (рейтинговая оценка)
Повышенный	Творческая деятельность	*Включает нижестоящий уровень.* Умение самостоятельно принимать решение, решать проблему/задачу теоретического и прикладного характера на основе изученных методов, приемов, технологий	отлично	зачтено	86-100

Базовый	Применение знаний и умений в более широких контекстах учебной и профессиональной деятельности, нежели по образцу с большей степени самостоятельности и инициативы	*Включает нижестоящий уровень.* Способность собирать, систематизировать, анализировать и грамотно использовать информацию из самостоятельно найденных теоретических источников и иллюстрировать ими теоретические положения или обосновывать практику применения	хорошо		71-85
Удовлетворительный (достаточный)	Репродуктивная деятельность	Изложение в пределах задач курса теоретически и практически контролируемого материала	удовлетворительно		55-70
Недостаточный	Отсутствие признаков удовлетворительного уровня		неудовлетворительно	не зачтено	Менее 55

9. Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины.

Основная литература

1. Математические методы защиты информации: практ. пособие/ *С. И. Алешников, Ю. Ф. Болтнев*; Балт. федер. ун-т им. И. Канта. - Калининград: БФУ им. И. Канта Ч. 4: Вычислительный практикум по эллиптическим кривым и криптографии на эллиптических кривых. - Калининград: БФУ им. И. Канта, 2015 **on-line**, 60 с. ЭБС Кантиана

Дополнительная литература

1. Математические методы защиты информации: практ. пособие/ *С. И. Алешников, Е. С. Алексеенко*; Балт. федер. ун-т им. И. Канта Ч. 5: Методы алгебраических кривых. - Калининград: БФУ им. И. Канта, 2015 **on-line**,156 с. ЭБС Кантиана

10. Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины (модуля).

- НЭБ Национальная электронная библиотека, диссертации и прочие издания
- eLIBRARY.RU Научная электронная библиотека, книги, статьи, тезисы докладов конференций

- Гребенников Электронная библиотека ИД журналы
- ЭБС Лань книги, журналы
- ЭБС Консультант студента
- ПРОСПЕКТ ЭБС
- ЭБС ZNANIUM.COM
- РГБ Информационное обслуживание по МБА
- БЕН РАН
- Электронно-библиотечная система (ЭБС) Кантитана (https://elib.kantiana.ru/)

11. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине.

Программное обеспечение обучения включает в себя:

- система электронного образовательного контента БФУ им. И. Канта – www.lms-3.kantiana.ru, обеспечивающую разработку и комплексное использование электронных образовательных ресурсов;
- серверное программное обеспечение, необходимое для функционирования сервера и связи с системой электронного обучения через Интернет;
- корпоративная платформа Microsoft Teams;
- установленное на рабочих местах обучающихся ПО: Microsoft Windows 7, Microsoft Office Standart 2010, антивирусное программное обеспечение Kaspersky Endpoint Security.
- специализированное ПО не требуется.

12. Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине.

Для проведения занятий лекционного типа, практических и семинарских занятий используются специальные помещения (учебные аудитории), оборудованные техническими средствами обучения – мультимедийной проекционной техникой. Для проведения занятий лекционного типа используются наборы демонстрационного оборудования.

Для проведения лабораторных работ, (практических занятий – при необходимости) используются специальные помещения (учебные аудитории), оснащенные специализированным лабораторным оборудованием: персональными компьютерами с возможностью выхода в интернет и с установленным программным обеспечением, заявленным в п.11.

Для проведения групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации используются специальные помещения (учебные аудитории), оборудованные специализированной мебелью (для обучающихся), меловой / маркерной доской.

Для организации самостоятельной работы обучающимся предоставляются помещения, оснащенные компьютерной техникой с возможностью подключения к сети «Интернет» и обеспечением доступа в электронную информационно-образовательную среду университета.

Для обучения инвалидов и лиц с ограниченными возможностями здоровья университетом могут быть представлены специализированные средства обучения, в том числе технические средства коллективного и индивидуального пользования.

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
федеральное государственное автономное образовательное учреждение высшего образования
«Балтийский федеральный университет имени Иммануила Канта»
Институт физико-математических наук и информационных технологий

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

«Спаривание на эллиптических кривых»

Шифр: 10.05.01
Специальность: «Компьютерная безопасность»
Специализация: «Математические методы защиты информации»
Квалификация (степень) выпускника: специалист по защите информации

Калининград
2022

Лист согласования

Составитель: Малыгина Екатерина Сергеевна, к.ф.-м.н., доцент

Рабочая программа утверждена на заседании учебно-методического совета института физико-математических наук и информационных технологий
Протокол № 01/22 от «01» февраля 2022 г.
Председатель учебно-методического
совета института физико-
математических наук и информационных
технологий
Первый заместитель директора Шпилевой А. А
ИФМНиИТ, к. ф.-м. н., доцент

Ведущий менеджер Е.П.Ставицкая

Содержание

1.Наименование дисциплины:
«Спаривание на эллиптических кривых».

Цель дисциплины: целью освоения дисциплины «Спаривание на эллиптических кривых» является изучение специфических свойств эллиптических кривых, лежащих в основе спариваний и овладение процедурами вычисления спариваний; овладение методикой расчёта и изучение оценок стойкости криптосистем, основанных на спариваниях.

2. Перечень планируемых результатов обучения по дисциплине, соотнесенных с планируемыми результатами освоения образовательной программы

Код компетенции	Результаты освоения образовательной программы (ИДК)	Результаты обучения по дисциплине
ПКС-7. Способность проводить анализ и участвовать в разработке математических моделей безопасности компьютерных систем.	ПКС-7.1. Знает математические методы моделирования безопасных компьютерных систем. ПКС-7.2. Осуществляет анализ математических моделей безопасности компьютерных систем. ПКС-7.3. Участвует в разработке математических моделей безопасности компьютерных систем.	• ***знать*:** перспективные методы криптографической защиты информации и помехоустойчивого кодирования; принципы функционирования и возможности перспективных инструментальных средств и компьютерных технологий для реализации вычислительных алгоритмов; структуры данных и методы построения вычислительных алгоритмов в алгебраических структурах, специфичных для перспективных систем защиты информации; • ***уметь*:** анализировать корректность и быстродействие вычислительных алгоритмов, специфичных для перспективных систем защиты информации; • ***владеть*:** практическими навыками построения вычислительных алгоритмов в алгебраических структурах, используемых в системах криптографической защиты и помехоустойчивого кодирования.

3. Место дисциплины в структуре образовательной программы

Дисциплина «Спаривание на эллиптических кривых» представляет собой дисциплину части, формируемой участниками образовательных отношений блока дисциплин подготовки обучающихся.

4. Виды учебной работы по дисциплине.

Виды учебной работы по дисциплине зафиксированы учебным планом основной профессиональной образовательной программы по указанному направлению и профилю, выражаются в академических часах. Часы контактной работы и самостоятельной работы обучающегося и часы, отводимые на процедуры контроля, могут различаться в учебных планах ОПОП по формам обучения. Объем контактной работы включает часы контактной аудиторной работы (лекции/практические занятия/ лабораторные работы), контактной внеаудиторной работы (контроль самостоятельной работы), часы контактной работы в период аттестации. Контактная работа, в том числе может проводиться посредством электронной информационно-образовательной среды университета с использованием ресурсов сети Интернет и дистанционных технологий

5. Содержание дисциплины, структурированное по темам (разделам)

Исходя из рамок, установленных учебным планом по трудоемкости и видам учебной работы по дисциплине, преподаватель самостоятельно выбирает тематику занятий по формам и количеству часов проведения контактной работы: лекции и иные учебные занятия, предусматривающие преимущественную передачу учебной информации преподавателем и (или) занятия семинарского типа (семинары, практические занятия, практикумы, лабораторные работы, коллоквиумы и иные аналогичные занятия), и (или) групповые консультации, и (или) индивидуальную работу обучающихся с преподавателем, в том числе индивидуальные консультации (по курсовым работам/проектам – при наличии курсовой работы/проекта по данной дисциплине в учебном плане). Рекомендуемая тематика занятий максимально полно реализуется в контактной работе с обучающимися очной формы обучения. В случае реализации образовательной программы в заочной / очно-заочной форме трудоемкость дисциплины сохраняется, однако объем учебного материала в значительной части осваивается обучающимися в форме самостоятельной работы. При этом требования к ожидаемым образовательным результатам обучающихся по данной дисциплине не зависят от формы реализации образовательной программы.

№ п/п	Наименование темы	Содержание темы
1	Предварительные сведения.	Задачи и программа курса. Место теории спариваний в современной криптографии. Формы самостоятельной работы студентов по изучению курса. Основная литература к курсу. Эллиптические кривые. Функции на эллиптических кривых. Кратности нулей и полюсов. Теория дивизоров. Вычисление функции главного дивизора.
2	Спаривание Вейля	Основные определения. Основные свойства. Альтернативное определение. Алгоритм Миллера для спаривания Вейля.
3	Спаривание Тэйта.	Основные определения. Основные свойства. Алгоритм Миллера для спаривания Тэйта. Сравнительный анализ спаривания Тэйта со спариванием Вейля: алгебраическое

		отношение; эффективность спариваний. Эффективная реализация спаривания Тэйта: адаптация алгоритма, выбор параметров.
4	Степень вложения.	Нижняя граница. Дополнительные условия. Кривые с малой степенью вложения: суперсингулярные кривые, MNT-кривые.
5	Отображение деформации.	Основные определения. Модифицированные спаривания. Криптографическое использование: ассиметричные и симметричные спаривания.
6	Криптография на эллиптических кривых.	Введение в проблему дискретного логарифма (ПДЛ). Дискретный логарифм и относительные проблемы. Атаки на ПДЛ. Некоторые стандартные протоколы. Дискретный логарифм на эллиптических кривых. Редукция. Безопасность.
7	Криптография на основе идентификационных данных	Основные определения. Криптография с открытым ключом. Безопасность криптосистем на основе идентификационных данных. Сравнение с инфраструктурой открытых ключей. Реализация спариваний: схемы шифрования Боне и Франклина, схема цифровой подписи на основе идентификационных данных. Приложения.
8	Приложения спариваний.	Трёхсторонний алгоритм Жу обмена ключами по Дифии-Хеллману. Короткие подписи.

6. Рекомендуемая тематика учебных занятий в форме контактной работы

Рекомендуемая тематика учебных занятий *лекционного* типа (предусматривающих преимущественную передачу учебной информации преподавателями):

№	Наименование раздела	Тема лекции
1	Тема 1. Предварительные сведения.	Лекция 1. Эллиптические кривые. Функции на эллиптических кривых
2	Тема 2. Спаривание Вейля.	Лекция 2. Спаривание Вейля.
3	Тема 3. Спаривание Тэйта.	Лекция 3. Спаривание Тэйта.
4	Тема 4. Степень вложения.	Лекция 4. Степень вложения.
5	Тема 5. Отображение деформации.	Лекция 5. Отображение деформации.
6	Тема 6. Криптография на эллиптических кривых.	Лекция 6. Криптография на эллиптических кривых.
7	Тема 7. Криптография на основе идентификационных данных.	Лекция 7. Криптография на основе идентификационных данных. Лекция 8. Реализация спариваний: схемы шифрования Боне и Франклина, схема цифровой подписи на основе идентификационных данных.
8	Тема 8. Приложения спариваний.	Тема 9. Трёхсторонний алгоритм Жу обмена ключами по Дифии-Хеллману.

Рекомендуемая тематика *практических* занятий:

№	Наименование	Содержание темы

п/п	Темы	
1	Предварительные сведения.	Вычисление локальных параметров точек эллиптической кривой. Определение нулей и полюсов рациональной функции на эллиптической кривой. Вычисление кратностей нулей и полюсов. Отыскание функции по заданному главному дивизору.
2	Спаривание Вейля	Вычисление спаривания Вейля с помощью алгоритма Миллера.
3	Спаривание Тэйта.	Вычисление спаривания Тэйта с помощью алгоритма Миллера.
4	Степень вложения.	По данной теме практических занятий не предусмотрено.
5	Отображение деформации.	Вычисление модифицированных спариваний для различных отображений деформации.
6	Криптография на эллиптических кривых.	Маркировка единичных сообщений точками эллиптической кривой. Шифрование на кривой.
7	Криптография на основе идентификационных данных	Шифрование данных по протоколу Боне – Франклина. Реализация цифровой подписи.
8	Приложения спариваний.	По данной теме практических занятий не предусмотрено.

Требования к самостоятельной работе обучающихся

1. Работа с лекционным материалом, предусматривающая проработку конспекта лекций и учебной литературы, по всем темам из п. 6 настоящей рабочей программы.
2. Выполнение домашнего задания, предусматривающего решение задач, выполнение упражнений, выдаваемых на практических занятиях, по всем темам из п. 6 настоящей рабочей программы.

Руководствуясь положениями статьи 47 и статьи 48 Федерального закона от 29 декабря 2012 г. N 273-ФЗ «Об образовании в Российской Федерации» научно-педагогические работники и иные лица, привлекаемые университетом к реализации данной образовательной программы, пользуются предоставленными академическими правами и свободами в части свободы преподавания, свободы от вмешательства в профессиональную деятельность; свободы выбора и использования педагогически обоснованных форм, средств, методов обучения и воспитания; права на творческую инициативу, разработку и применение авторских программ и методов обучения и воспитания в пределах реализуемой образовательной программы и отдельной дисциплины.

Исходя из рамок, установленных учебным планом по трудоемкости и видам учебной работы по дисциплине, преподаватель самостоятельно выбирает тематику занятий по формам и количеству часов проведения контактной работы: лекции и иные учебные занятия, предусматривающие преимущественную передачу учебной информации преподавателем и (или) занятия семинарского типа (семинары, практические занятия, практикумы, лабораторные работы, коллоквиумы и иные аналогичные занятия), и (или) групповые консультации, и (или) индивидуальную работу обучающихся с преподавателем, в том числе индивидуальные консультации (по курсовым

работам/проектам – при наличии курсовой работы/проекта по данной дисциплине в учебном плане).

Рекомендуемая тематика занятий максимально полно реализуется в контактной работе с обучающимися очной формы обучения. В случае реализации образовательной программы в заочной / очно-заочной форме трудоемкость дисциплины сохраняется, однако объем учебного материала в значительной части осваивается обучающимися в форме самостоятельной работы. При этом требования к ожидаемым образовательным результатам обучающихся по данной дисциплине не зависят от формы реализации образовательной программы.

7. Методические рекомендации по видам занятий

Лекционные занятия.

В ходе лекционных занятий обучающимся рекомендуется выполнять следующие действия. Вести конспектирование учебного материала. Обращать внимание на категории, формулировки, раскрывающие содержание тех или иных явлений и процессов, научные выводы и практические рекомендации по их применению. Задавать преподавателю уточняющие вопросы с целью уяснения теоретических положений, разрешения спорных ситуаций.

Желательно оставить в рабочих конспектах поля, на которых во внеаудиторное время можно сделать пометки из рекомендованной литературы, дополняющие материал прослушанной лекции, а также подчеркивающие особую важность тех или иных теоретических положений.

Практические и семинарские занятия.

На практических и семинарских занятиях в зависимости от темы занятия выполняется поиск информации по решению проблем, практические упражнения, контрольные работы, выработка индивидуальных или групповых решений, итоговое обсуждение с обменом знаниями, участие в круглых столах, разбор конкретных ситуаций, командная работа, представление портфолио и т.п.

Самостоятельная работа.

Самостоятельная работа осуществляется в виде изучения литературы, эмпирических данных по публикациям и конкретных ситуаций из практики, подготовке индивидуальных работ, работа с лекционным материалом, самостоятельное изучение отдельных тем дисциплины; поиск и обзор литературы и электронных источников; чтение и изучение учебника и учебных пособий.

8. Фонд оценочных средств

8.1. Перечень компетенций с указанием этапов их формирования в процессе освоения образовательной программы в рамках учебной дисциплины

Основными этапами формирования указанных компетенций при изучении обучающимися дисциплины являются последовательное изучение содержательно связанных между собой тем учебных занятий. Изучение каждой темы предполагает овладение обучающимися необходимыми компетенциями. Результат аттестации обучающихся на различных этапах формирования компетенций показывает уровень освоения компетенций.

Контролируемые разделы (темы) дисциплины	Индекс контроли-	Оценочные средства по этапам формирования компетенций

	руемой компетенции (или её части)	текущий контроль по дисциплине
Тема 1. Предварительные сведения.	ПКС-7	Устный опрос, решение задач
Тема 2. Спаривание Вейля.		Устный опрос, решение задач
Тема 3. Спаривание Тэйта.		Устный опрос, решение задач, письменный опрос
Тема 4. Степень вложения.		Устный опрос
Тема 5. Отображение деформации.		Устный опрос, решение задач
Тема 6. Криптография на эллиптических кривых.		Устный опрос, решение задач
Тема 7. Криптография на основе идентификационных данных.		Устный опрос, решение задач, письменный опрос

8.2. Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений и навыков и (или) опыта деятельности процессе текущего контроля

Примеры вопросов для устного опроса:

Тема 1. Предварительные сведения

1. Дать определение абстрактной эллиптической кривой.
2. Как записываются изоморфизмы эллиптических кривых в форме Вейерштрасса в зависимости от характеристики основного поля?
3. Записать формулы сложения точек эллиптической кривой в зависимости от характеристики основного поля.
4. Какова структура группы точек кручения эллиптической кривой над конечным полем?
5. Какова каноническая форма рациональной функции на эллиптической кривой?
6. выписать локальные параметры точек эллиптической кривой.
7. Как вычисляется порядок рациональной функции в точке?
8. В чём состоит закон взаимности Вейля?

Тема 2. Спаривание Вейля

1. Как вычисляется функция для заданного главного дивизора?
2. Дать определение спаривания Вейля.
3. В чём стостоит корректность определения спаривания Вейля?
4. В чём состоит свойство невырожденности спаривания?
5. Каково альтернативное определение спаривания Вейля.
6. Каковы основные шаги базового алгоритма Миллера для вычисления спаривания Вейля?

Тема 3. Спаривание Тэйта

1. Дать определение спаривания Тэйта.
2. В чём стостоит корректность определения спаривания Тэйта?
3. Перечислить свойства спаривания Тэйта?
4. В чём состоит отличие спаривания Тэйта от спаривания Вейля?
5. Каковы основные шаги базового алгоритма Миллера для вычисления спаривания Тэйта?

6. В чём состоит модификация алгоритма Миллера для спаривания Тэйта?

Тема 4. Степень вложения

1. Каковы свойства кривых, подходящих для криптографии?
2. Сформулировать теорему Баласубраманьяна для нижней границы кривой.
3. Сформулировать теорему Коблица.
4. Дать определение суперсингулярной эллиптической кривой.
5. Дать определение MNT-кривой.
6. Описать основные шаги MOV-атаки.
7. Описать основные шаги FR-редукции.

Тема 5. Отображение деформации

1. Каково назначение отображения деформации?
2. В чём особенность отображения деформации для несуперсингулярных эллиптических кривых?
3. В чём особенность отображения деформации для суперсингулярных эллиптических кривых?
4. В чём сущность модификации спаривания Вейля при помощи отображения деформации?
5. В чём сущность модификации спаривания Тэйта при помощи отображения деформации?

Тема 6. Криптография на эллиптических кривых

1. Каковы основные шаги алгоритма маркировки единичных сообщений точками эллиптической кривой?
2. Кратко описать аналог системы Диффи – Хеллмана обмена ключами на эллиптической кривой.
3. Дать определение пробельных групп Диффи – Хеллмана.
4. Кратко описать аналог протокола Мэсси - Омуры на эллиптической кривой.
5. Каковы основные шаги алгоритма редукции аномальных кривых?

Тема 6. Криптография на основе идентификационных данных

1. В чём сущность идентификационных данных?
2. Каковы основные блоки упрощённого протокола Боне – Франклина?
3. В чём отличие полного протокола Боне – Франклина от упрощённого?
4. Чем обеспечивается безопасность систем на основе идентификационных данных?
5. Сравнить безопасность протокола Боне – Франклина с безопасностью других криптосистем с открытым ключом.
6. Каковы основные шаги цифровой подписи на основе идентификационных данных?

Тема 7. Приложения спариваний

1. Каковы основные шаги алгоритма Жу трёхстороннего обмена ключами?
2. Как формируются короткие цифровые подписи на основе идентификационных данных?
3. Какова безопасность коротких цифровых подписей?
4. Каковы эллиптические кривые, подходящие для криптографии на спариваниях?

Письменные опросы:

Тема 3. Спаривание Тэйта

Задана эллиптическая кривая $E / \square_5$ с уравнением $y^2 = x^3 + x$.

1. Найти все $\mathbb{F}_5$-рациональные точки этой кривой. Указать среди них обыкновенные и специальные. Найти локальные параметры кривой в этих точках.
2. Для заданной полиномиальной функции $G(x, y) = x^3 + y^3$ найти представление вида $G(x, y) = a(x) - b(x)y$, вычислить норму $N(G)$, степень $\deg G$ и дивизор $\operatorname{div} G$.
3. Вычислить спаривание Вейля $e_w(P, Q)$ для точек $P = (2, 0)$, $Q = (3, 0)$ из $E(\mathbb{F}_5)$.
4. Вычислить спаривание Тэйта $e_t(P, Q)$ для точек $P = (0, 0)$, $Q = (2, 0)$ из $E(\mathbb{F}_5)$.

Тема 7. Криптография на основе идентификационных данных

1. Сущность MOV-атаки на проблему дискретного логарифма на эллиптической кривой.
2. Сущность редукции Фрея – Рюка.
3. Схема упрощённого протокола Бонне – Франклина.
4. Схема полного протокола Бонне – Франклина.
5. Схема базового потокола Гентри – Сильверберг.
6. Спаривание Лихтенбаума, его основные свойства.
7. Бессертификатные схемы на основе идентификационных данных.

8.3. Перечень вопросов и заданий для промежуточной аттестации по дисциплине

Вопросы для промежуточного контроля (зачета)

1. Эллиптические кривые. Уравнение Вейерштрасса. Изоморфные эллиптические кривые. Законы сложения точек на эллиптических кривых. Группа точек кручения эллиптической кривой. Эндоморфизм Фробениуса.
2. Каноническая форма функций. Рациональные функции на эллиптических кривых. Нули и полюсы. Пример.
3. Униформизующий параметр. Порядок функции в точке. Кратность нулей и полюсов. Пример.
4. Дивизоры кривой, их носители и степени. Дивизор функции. Главный дивизор. Эквивалентность дивизоров. Группа Пикара. Нормирования функций. Закон взаимности Вейля.
5. Вычисление функции главного дивизора. Пример.
6. Индекс ветвления. Гомоморфизм групп дивизоров. Спаривание Вейля, корректность его определения.
7. Свойства спаривания Вейля.
8. Альтернативное определение спаривания Вейля, его корректность.
9. Свойства альтернативного спаривания Вейля.
10. Алгоритм Миллера для спаривания Вейля.
11. Спаривание Тэйта, его независимость от выбора функции и дивизора.
12. Свойства спаривания Тэйта.
13. Алгоритм Миллера для спаривания Тэйта.
14. Алгебраическое сравнение спариваний Вейля и Тэйта. Эфективность спариваний.
15. Улучшенный алгоритм Миллера для спаривания Тэйта. Выбор параметров.
16. Нижняя граница кривой и ее свойства.
17. Дополнительные условия для нижней границы. Теорема Баласубраманьяна и Коблица. Пример.
18. Суперсингулярные кривые, их свойства. Примеры.
19. MNT-кривые, их свойства. Примеры.
20. Отображение деформации. Случай несуперсингулярных кривых. Случай суперсингулярных кривых.
21. Модификация спариваний Вейля и Тэйта. Ассиметричные и симметричные спаривания.

22. Задача дискретного логарифмирования в группе точек эллиптической кривой.
23. Атаки на ПДЛ.
24. MOV- , FR- редукции и редукция аномальных кривых. Вопросы безопасности.
25. Пробельные группы Диффи-Хеллмана.
26. Криптография на основе идентификационных данных.
27. Безопасность криптосистем на основе идентификационных данных.
28. Сравнение криптосистем на основе идентификационных данных с криптосистемами с открытым ключом.
29. Основная схема Боне-Франклина.
30. Полная схема Боне-Франклина.
31. Схема цифровой подписи на основе идентификационных данных.
32. Криптографические приложения на основе идентификационных данных.
33. Трёхсторонний алгоритм Жу обмена ключами по Диффи-Хеллману.
34. Короткие цифровые подписи.
35. Подходящие кривые для спариваний.
36. Криптография на основе спариваний.

8.4. Планируемые уровни сформированности компетенций обучающихся и критерии оценивания

Уровни	Содержательное описание уровня	Основные признаки выделения уровня (этапы формирования компетенции, критерии оценки сформированности)	Пятибалльная шкала (академическая) оценка	Двухбалльная шакала, зачет	БРС, % освоения (рейтинговая оценка)
Повышенный	Творческая деятельность	*Включает нижестоящий уровень.* Умение самостоятельно принимать решение, решать проблему/задачу теоретического и прикладного характера на основе изученных методов, приемов, технологий	отлично	зачтено	86-100
Базовый	Применение знаний и умений в более широких контекстах учебной и профессиональной деятельности, нежели по образцу с большей степени самостоятель	*Включает нижестоящий уровень.* Способность собирать, систематизировать, анализировать и грамотно использовать информацию из самостоятельно найденных теоретических источников и иллюстрировать ими теоретические положения или обосновывать практику	хорошо		71-85

	ности и инициативы	применения			
Удовлетворительный (достаточный)	Репродуктивная деятельность	Изложение в пределах задач курса теоретически и практически контролируемого материала	удовлетворительно		55-70
Недостаточный	Отсутствие признаков удовлетворительного уровня		неудовлетворительно	не зачтено	Менее 55

9. Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины.

Основная литература

1. Математические методы защиты информации: практ. пособие/ *С. И. Алешников, Ю. Ф. Болтнев*; Балт. федер. ун-т им. И. Канта. - Калининград: БФУ им. И. Канта Ч. 4: Вычислительный практикум по эллиптическим кривым и криптографии на эллиптических кривых. - Калининград: БФУ им. И. Канта, 2015 **on-line**, 60 с. ЭБС Кантиана

Дополнительная литература

1. Математические методы защиты информации: практ. пособие/ *С. И. Алешников, Е. С. Алексеенко*; Балт. федер. ун-т им. И. Канта Ч. 5: Методы алгебраических кривых. - Калининград: БФУ им. И. Канта, 2015 **on-line**,156 с. ЭБС Кантиана

10. Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины (модуля).

- НЭБ Национальная электронная библиотека, диссертации и прочие издания
- eLIBRARY.RU Научная электронная библиотека, книги, статьи, тезисы докладов конференций
- Гребенников Электронная библиотека ИД журналы
- ЭБС Лань книги, журналы
- ЭБС Консультант студента
- ПРОСПЕКТ ЭБС
- ЭБС ZNANIUM.COM
- РГБ Информационное обслуживание по МБА
- БЕН РАН
- Электронно-библиотечная система (ЭБС) Кантитана (https://elib.kantiana.ru/)

11. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине.

Программное обеспечение обучения включает в себя:

- система электронного образовательного контента БФУ им. И. Канта – www.lms-3.kantiana.ru, обеспечивающую разработку и комплексное использование электронных образовательных ресурсов;
- серверное программное обеспечение, необходимое для функционирования сервера и связи с системой электронного обучения через Интернет;
- корпоративная платформа Microsoft Teams;
- установленное на рабочих местах обучающихся ПО: Microsoft Windows 7, Microsoft Office Standart 2010, антивирусное программное обеспечение Kaspersky Endpoint Security.
- специализированное ПО не требуется.

12. Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине.

Для проведения занятий лекционного типа, практических и семинарских занятий используются специальные помещения (учебные аудитории), оборудованные техническими средствами обучения – мультимедийной проекционной техникой. Для проведения занятий лекционного типа используются наборы демонстрационного оборудования.

Для проведения лабораторных работ, (практических занятий – при необходимости) используются специальные помещения (учебные аудитории), оснащенные специализированным лабораторным оборудованием: персональными компьютерами с возможностью выхода в интернет и с установленным программным обеспечением, заявленным в п.11.

Для проведения групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации используются специальные помещения (учебные аудитории), оборудованные специализированной мебелью (для обучающихся), меловой / маркерной доской.

Для организации самостоятельной работы обучающимся предоставляются помещения, оснащенные компьютерной техникой с возможностью подключения к сети «Интернет» и обеспечением доступа в электронную информационно-образовательную среду университета.

Для обучения инвалидов и лиц с ограниченными возможностями здоровья университетом могут быть представлены специализированные средства обучения, в том числе технические средства коллективного и индивидуального пользования.