МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

Балтийский федеральный университет им. Иммануила Канта

Институт физико-математических наук и информационных технологий

«Согласовано»
Ведущий менеджер ООП ИФМНиИТ
_____ Е.П.Ставицкая
«22» марта 2021 г.

«Утверждаю»
Директор ИФМНиИТ
_____ А.В.Юров
«___» _____ 2021 г.

АННОТАЦИИ РАБОЧИХ ПРОГРАММ ДИСЦИПЛИН

Специальность
10.05.01 КОМПЬЮТЕРНАЯ БЕЗОПАСНОСТЬ

Специализация
«Математические методы защиты информации»

Квалификация

Специалист по защите информации

Форма обучения

Очная

Год начала подготовки 2021

ДОКУМЕНТ ПОДПИСАН ЭЛЕКТРОННОЙ ПОДПИСЬЮ
Сертификат: 34219E685EE8D891F77F96F99B3B8407
Владелец: Федоров Александр Александрович
Действителен: с 28.12.2022 до 22.03.2024

Калининград 2021

Аннотация учебной дисциплины

Учебная дисциплина **«МАТЕМАТИЧЕСКИЙ АНАЛИЗ»**	
Цель изучения дисциплины	***Цель*** дисциплины «*Математический анализ*» – изложить классические основы математического анализа и методику решения задач в указанной области, подготовить студентов к чтению математической и прикладной научной литературы, где широко применяется язык этой математической дисциплины, выработать у студентов умение использовать методы математического анализа в своей исследовательской деятельности.
Компетенции, формируемые в результате освоения дисциплины	Процесс изучения дисциплины направлен на формирование следующих ***компетенций***: - Способен на основании совокупности математических методов разрабатывать, обосновывать и реализовывать процедуры решения задач профессиональной деятельности; (ОПК-3).
Знания, умения и навыки, получаемые в процессе изучения дисциплины	В результате освоения дисциплины студент должен: ***знать:*** • основные положения теории пределов функций, теории рядов; • основные теоремы дифференциального и интегрального исчисления функций одного и нескольких переменных; • понятие меры, измеримые функции и их свойства; • абстрактный интеграл Лебега и его основные свойства; ***уметь:*** • определять возможности применения методов математического анализа; • решать основные задачи теории пределов функций, дифференцирования, интегрирования и разложения функций в ряды; ***владеть:*** • навыками использования стандартных методов и моделей математического анализа и их применения к решению прикладных задач профессиональной деятельности.
Краткая характеристика учебной дисциплины (основные блоки и темы)	**Содержание основных разделов и тем курса.** **Введение.** **Раздел 1. Основные понятия теории множеств, действительные (вещественные) числа, предел числовой последовательности.** Тема 1. Введение. Задачи и программа дисциплины. Литература. Предмет математического анализа. Краткий исторический очерк. Связь с другими фундаментальными науками. Место и значение курса в процессе формирования мировоззрения. Приложения к специальным задачам. Методика изучения дисциплины. Формы самостоятельной работы слушателей по изучению дисциплины. Тема 2. Элементы теории множеств.

	Операции над множествами. Бинарные отношения. Функциональные отношения, отношения эквивалентности и порядка. Основные классы отображений. Обратные отображения. Тема 3. Действительные (вещественные) числа. Аксиомы действительных чисел и некоторые следствия из них. Верхние и нижние грани числовых множеств. Теорема о существовании верхней (нижней) граней. Важнейшие классы действительных чисел. Принцип Архимеда. Действительная прямая R, расширенная действительная прямая. Основные классы подмножеств действительной прямой. Теорема Коши-Кантора, теорема Бореля-Лебега и теорема Больцано-Вейерштрасса и некоторые следствия из этих теорем. Понятие мощности. Счетные множества и некоторые их свойства. Несчетность множества R. Множества мощности континуум. Тема 4. Предел числовой последовательности. Последовательности. Определение предела последовательности и основные свойства пределов последовательностей. Критерий Коши существования предела числовой последовательности. Теорема Больцано-Вейерштрасса для последовательностей. Частичные пределы, верхний и нижний пределы последовательности и их свойства. **Раздел 2. Предел и непрерывность действительных функций одной действительной переменной.** Тема 5. Предел функции. Предел функции по Коши и по Гейне. Свойства предела функции. Локальные свойства функций, имеющих предел. Критерий Коши существования предела функции. Предел сложной функции. Бесконечно малые и бесконечно большие функции. О-символика, эквивалентные функции. Вычисление пределов функций с помощью О-символики и эквивалентных функций. Тема 6. Непрерывные функции и их свойства. Определение непрерывности функции в точке и на множестве. Локальные свойства функции, непрерывной в точке. Непрерывность сложной функции. Точки разрыва и их классификация, точки разрыва монотонной функции. Свойства функций, непрерывных на отрезке: теорема Больцано-Коши, первая и вторая теоремы Вейерштрасса, равномерная непрерывность и теорема Кантора. Признак непрерывности обратной функции. Основные элементарные функции. Тригонометрические и обратные тригонометрические функции. **Раздел 3. Дифференциальные исчисления функции одной действительной переменной.** Тема 7. Дифференцируемость функций, производная. Определение дифференцируемой функции и производной функции в точке и на множестве. Дифференциал. Таблица производных. Производная суммы, произведения и частного двух функций. Производная сложной и обратной функций. Инвариантность формы первого дифференциала. Производные и дифференциалы высших порядков. Формула Лейбница. Теоремы Ролля, Лагранжа, Коши. Правило Лопиталя. Формула Тейлора. Тема 8. Некоторые приложения дифференциального исчисления.

Признаки монотонности функции. Исследование функции на экстремум. Направление вогнутости, точки перегиба. Асимптоты. Построение графиков с помощью производных.

Раздел 4. Числовые ряды.

Тема 9. Числовые ряды с действительными и комплексными членами, признаки сходимости знакопостоянных рядов.

Комплексные числа. Поле комплексных чисел. Предел последовательности комплексных чисел, связь с пределами последовательностей действительных и мнимых частей. Числовые ряды с действительными и комплексными членами. Их связь. Основные свойства сходящихся числовых рядов. Критерий Коши. Основные признаки сходимости рядов с действительными знакопостоянными членами: признаки сравнения, Даламбера, Коши, Гаусса, интегральный признак сходимости Коши-Маклорена.

Тема 10. Общие числовые ряды.

Абсолютная и условная сходимость рядов. Признаки сходимости Лейбница, Абеля, Дирихле. Перестановка членов абсолютно сходящегося числового ряда, теорема Римана. Произведение рядов по Коши.

Раздел 5. Интегральное исчисление функций одного действительного переменного.

Тема 11. Неопределенный интеграл.

Первообразная и неопределенный интеграл, их основные свойства. Табличные интегралы. Замена переменного и интегрирование по частям. Интегрирование рациональных и некоторых иррациональных и трансцендентных функций.

Тема 12. Интеграл Римана-Стилтьеса.

Суммы Дарбу и их свойства. Интеграл Римана-Стилтьеса относительно неубывающей функции. Критерии интегрируемости. Основные свойства интеграла Римана-Стилтьеса. Классы интегрируемых функций. Интегральные суммы, пределы интегральных сумм и их связь с интегралом Римана-Стилтьеса. Интеграл Римана. Свойства интеграла Римана как функции верхнего предела интегрирования, формула Ньютона-Лейбница. Интегрирование по частям и замена переменной в интеграле Римана. Первая и вторая теоремы о среднем значении. Интегрирование векторнозначных функций. Функции ограниченной вариации. Интеграл Римана-Стилтьеса по функции ограниченной вариации. Несобственные интегралы. Абсолютная сходимость. Признаки сходимости.

Тема 13. Приложения определенного интеграла.

Приложения определенного интеграла к вычислению площадей, объемов и площадей поверхностей вращения. Спрямляемые кривые, длина кривой.

Раздел 6. Функциональные последовательности и ряды.

Тема 14. Функциональные последовательности и ряды.

Равномерная сходимость. Признаки равномерной сходимости. Теоремы о непрерывности предельной функции (суммы ряда) и о почленном дифференцировании и интегрировании функциональной последовательности (ряда).

Тема 15. Степенные ряды и их свойства.

	Определение степенного ряда, теоремы Абеля. Интервал (круг) и радиус сходимости. Ряды Тейлора и Маклорена, свойство единственности. Аналитические функции и их свойства. Показательная функция и тригонометрические функции комплексной переменной. Формула Эйлера. **Раздел 7. Абстрактные пространства и их отображения.** Тема 16. Топологические, метрические и нормированные пространства. Определения топологических, метрических и нормированных пространств и их основные свойства. Фундаментальные последовательности и полные метрические пространства. Связные подмножества. Компактные метрические пространства. Свойства компактов. Компакты в n-мерном евклидовом пространстве. Предел последовательности в n-мерном евклидовом пространстве. Предел и непрерывность векторных функций нескольких переменных. Предел последовательности и его основные свойства. Предел и непрерывность векторных функций нескольких переменных и их связь с пределами и непрерывностью координатных функций. Локальные свойства функции, непрерывной в точке. Свойства функций, непрерывных на компакте. **Раздел 8. Функции нескольких вещественных переменных.** Тема 17. Дифференциальные исчисления функций многих вещественных переменных. Дифференцируемые вектор-функции (отображения) нескольких переменных. Полная производная, дифференциал. Связь с дифференцируемостью координатных функций. Частные производные. Матрица Якоби и якобиан. Производные по направлению. Градиент. Необходимое условие дифференцируемости. Достаточное условие дифференцируемости. Основные свойства дифференцируемых функций. Дифференцируемость сложных функций. Частные производные высших порядков. Теорема Шварца. Дифференциалы высших порядков. Формула и ряд Тейлора для вещественной функции многих переменных. Тема 18. Приложения дифференциального исчисления функции многих переменных. Экстремум функции многих переменных. Необходимое и достаточные условия экстремума. Условные и безусловные экстремумы. Неявные функции и обратные отображения. **Раздел 9. Интегралы, зависящие от параметра.** Тема 19. Собственные интегралы, зависящие от параметра. Непрерывность, интегрирование и дифференцирование собственных интегралов, зависящих от параметра. Тема 20. Несобственные интегралы, зависящие от параметра. Равномерная сходимость, признаки равномерной сходимости. Непрерывность, интегрирование и дифференцирование несобственных интегралов, зависящих от параметра. Вычисление некоторых несобственных интегралов с помощью интегралов, зависящих от параметра. Эйлеровы интегралы. Бета и гамма функции и их свойства. **Раздел 10. Основы теории меры, ряды и интеграл Фурье.** Тема 21. Основные классы множеств.

	Кольца и алгебры множеств. Полукольца. Борелевские алгебры. Борелевские множества. Строение минимального кольца над полукольцом. Тема 22. Основные понятия теории меры. Функции множеств, понятие меры. Свойства меры, заданной на кольце множеств. Счетно-аддитивные меры. Критерий счетной аддитивности меры, заданной на кольце. Меры Стилтьеса на прямой. Производящая функция. Критерий счетной аддитивности меры Стилтьеса. Тема 23. Продолжение меры. Меры Лебега-Стилтьеса на прямой. Продолжение меры с полукольца на минимальное кольцо над ним. Внешняя мера и индуцированная внешняя мера. Измеримые множества. Меры Лебега и Лебега-Стилтьеса на прямой и некоторые их свойства. Тема 24. Измеримые функции и их свойства. Измеримые и борелевские функции, их свойства. Арифметические операции над измеримыми функциями. Теорема об измеримости сложной функции. Сходимость почти всюду и сходимость по мере. Теорема Д.Ф.Егорова. Тема 25. Абстрактный интеграл Лебега и его свойства. Абстрактный интеграл Лебега: определение и основные свойства. Теоремы Б.Леви, Фату, Лебега о предельном переходе под знаком интеграла. Интеграл Лебега и Лебега-Стилтьеса на прямой. Связь интегралов Лебега и Римана. Тема 26. Кратные и повторные интегралы, теорема Фубини. Произведение мер. Меры Лебега и Лебега-Стилтьеса в n-мерном евклидовом пространстве. Теорема Фубини. Теорема о замене переменных в кратном интеграле. Тема 27. Ряды и интеграл Фурье. Ряд Фурье по тригонометрической системе функций. Признаки сходимости рядов Фурье. Неравенство Бесселя и равенство Парсеваля. Теорема Фейера. Преобразование и интеграл Фурье. Заключение. Методологические вопросы математического анализа. Логическая структура и взаимоотношение основных понятий курса математического анализа. Многообразие и общность аналитических методов и их использование в других математических, технических и специальных дисциплинах и в практике. Роль математического анализа в изучении прикладных математических дисциплин. Обзор направлений дальнейшего развития основных понятий математического анализа в теории функций комплексной переменной, функциональном анализе и теории дифференциальных уравнений. Литература для дальнейшего изучения математического анализа и его приложений.
Трудоёмкость (з.е. / часы)	Согласно рабочему учебному плану курс читается в полном объёме в течении 4-х семестров **14 ЗЕТ/504** часов
Форма итогового	1 зачёт 4 **экзамена**

контроля знаний	

Аннотация учебной дисциплины

Учебная дисциплина **«ИНОСТРАННЫЙ ЯЗЫК (НЕМЕЦКИЙ ЯЗЫК)»**	
Цель изучения дисциплины	Данная рабочая программа предусматривает формирование у учащихся общеучебных умений и навыков, универсальных способов деятельности и ключевых компетенций в следующих направлениях: использование учебных умений, связанных со способами организации учебной деятельности, доступных учащимся I, II курсов и способствующих самостоятельному изучению немецкого языка и культуры стран изучаемого языка; а также развитие специальных учебных умений, таких как нахождение ключевых слов при работе с текстом, их семантизация на основе языковой догадки, словообразовательный анализ, выборочное использование перевода; умение пользоваться двуязычными словарями; участвовать в проектной деятельности межпредметного характера.
Компетенции, формируемые в результате освоения дисциплины	Процесс изучения дисциплины направлен на формирование следующих ***компетенций***: - Способен применять современные коммуникативные технологии, в том числе на иностранном(ых) языке(ах), для академического и профессионального взаимодействия (УК-4); - Способен анализировать и учитывать разнообразие культур в процессе межкультурного взаимодействия (УК-5).
Знания, умения и навыки, получаемые в процессе изучения дисциплины	**В результате изучения немецкого языка студент должен** **Знать:** • знаки транскрипции немецкого языка; • основные значения изученных лексических единиц (слов, словосочетаний); основные способы словообразования (аффиксация, словосложение); • особенности структуры простых и сложных предложений изучаемого иностранного языка; интонацию различных коммуникативных типов предложений; • признаки изученных грамматических явлений (видо-временных форм глаголов, модальных глаголов и их эквивалентов, артиклей, существительных, степеней сравнения прилагательных и наречий, местоимений, числительных, предлогов); • основные нормы речевого этикета (реплики-клише, наиболее распространенная оценочная лексика), принятые в стране изучаемого языка; • роль владения иностранными языками в современном мире, особенности образа жизни, быта, культуры стран изучаемого языка (всемирно известные достопримечательности, выдающиеся люди и их вклад в мировую культуру), сходство и различия в традициях своей страны и стран изучаемого языка; **Владеть:** - минимум 4000 лексическими единицами общего и терминологического характера.

	- грамматическими навыками, обеспечивающими коммуникацию общего характера без искажения смысла при письменном и устном общении. - иностранным языком в объеме, необходимом для возможности получения информации из зарубежных источников; - способностью к деловым коммуникациям в профессиональной сфере; **Уметь:** ***(1) говорение*** ▪ начинать, вести/поддерживать и заканчивать беседу в стандартных ситуациях общения, соблюдая нормы речевого этикета, при необходимости переспрашивая, уточняя; ▪ расспрашивать собеседника и отвечать на его вопросы, высказывая свое мнение, просьбу, отвечать на предложение собеседника согласием/отказом, опираясь на изученную тематику и усвоенный лексико-грамматический материал; ▪ рассказывать о себе, своей семье, друзьях, своих интересах и планах на будущее, сообщать сведения о своем городе/селе, о своей стране и стране изучаемого языка; ▪ делать сообщения, описывать события/явления (в рамках пройденных тем), передавать основное содержание, основную мысль прочитанного или услышанного, выражать свое отношение к прочитанному/услышанному, давать характеристику персонажей; ▪ использовать синонимичные средства в процессе устного общения; ***(2) аудирование*** ▪ понимать основное содержание аутентичных прагматических текстов и выделять для себя значимую информацию; ▪ понимать основное содержание аутентичных текстов, относящихся к разным коммуникативным типам речи (сообщение/рассказ), уметь определить тему текста, выделить главные факты в тексте, опуская второстепенные; ▪ использовать переспрос, просьбу повторить; ***(3) чтение*** ▪ ориентироваться в иноязычном тексте: прогнозировать его содержание по заголовку; ▪ читать аутентичные тексты разных жанров преимущественно с пониманием основного содержания (определять тему, выделять основную мысль, выделять главные факты, опуская второстепенные, устанавливать логическую последовательность основных фактов текста); ▪ читать несложные аутентичные тексты разных жанров, в том числе и технической направленности с полным и точным пониманием, используя различные приемы смысловой переработки текста (языковую догадку, анализ, выборочный перевод), оценивать полученную информацию, выражать свое мнение; ▪ читать текст с выборочным пониманием нужной или интересующей информации; ***(4) письменная речь*** ▪ заполнять анкеты и формуляры; ▪ писать поздравления, личные письма с опорой на образец: расспрашивать адресата о его жизни и делах, сообщать то же о себе, выражать благодарность, просьбу, употребляя формулы речевого этикета, принятые в странах изучаемого языка.

	К завершению обучения планируется достижение учащимися общеевропейского уровня подготовки по иностранному языку (немецкому языку)(уровень В-1, В-2).
Краткая характеристика учебной дисциплины (основные блоки и темы)	**1 семестр.** **1. Вводно-фонетический курс.** • Немецкий алфавит • Знаки немецкой транскрипции • Общие сведения о произносительной норме немецкого языка • Общая характеристика немецких гласных звуков • Основные правила ударения в словах • Немецкие согласные • Особенности некоторых согласных звуков • Ударение в глаголах с отделяемыми и неотделяемыми приставками • Ударение в группах слов • Немецкие дифтонги • Аффрикаты • Интонация в немецких предложениях **2. Тексты для чтения.** • Unser Studium • Jugendprobleme • Onkel Franz kommt zu Besuch • Die Brüder Grimm • Familie Schmidt aus Hannover **2 семестр.** **1. Тексты для чтения.** 1. Was trinken die Deutschen gern? 2. Die Mahlzeiten. 3. Urlaub am Bodensee. 4.Kulturleben und Staatsform Österreichs. 5. Allgemeines über die Schweiz. 6. Geographie Deutschlands. Hamburg. 7. Das Elektroauto. 8. Algebra. **3 семестр.** **1. Тексты для чтения.** 1. Bade-und Kurort Sverlogorsk. 2. Erzeugnisse aus Bernstein. 3. Heimkehr nach fünfzig Jahren. 4. Computer. 5. Der Computer, die elektronische Datenverarbeitung. **4 семестр.** **1. Тексты для чтения.** 1. Reisen mit dem Zug. Reisen mit der Bahn. 2. Industrie Deutschlands. 3. Hochschule (Universität). 4. Der berühmte deutsche Philosoph Immanuel Kant. 5. Mikroelektronik. 6. Robotertechnik. 7. Das Internet – grenzlose Freiheit für jede Nachricht. 8. Multimedia – ein modernes Informationssystem.

	9. Leonard Euler.
Трудоёмкость (з.е. / часы)	**10** ЗЕТ / **360** часов.
Форма итогового контроля знаний	1 экзамен, 3 зачета

Аннотация учебной дисциплины

Учебная дисциплина **«ИНОСТРАННЫЙ (АНГЛИЙСКИЙ) ЯЗЫК»**	
Цель изучения дисциплины	Основной **целью курса** является повышение исходного уровня владения иностранным языком, достигнутого на предыдущей ступени образования, и овладение студентами необходимым и достаточным уровнем коммуникативной компетенции для решения социально- коммуникативных задач в различных областях бытовой, культурной, профессиональной и научной деятельности при общении с зарубежными партнерами, а также для дальнейшего самообразования.
Компетенции, формируемые в результате освоения дисциплины	Процесс изучения дисциплины направлен на формирование следующих ***компетенций***: - Способен применять современные коммуникативные технологии, в том числе на иностранном(ых) языке(ах), для академического и профессионального взаимодействия (УК-4); - Способен анализировать и учитывать разнообразие культур в процессе межкультурного взаимодействия (УК-5).
Знания, умения и навыки, получаемые в процессе изучения дисциплины	**Основные требования** студентам после курса изучения дисциплины: **Студенты должны знать** специфику артикуляции звуков, интонации; основные особенности полного стиля произношения, характерные для сферы профессиональной коммуникации; **должны знать** чтение транскрипции. **Студенты должны владеть** минимум 4000 лексическими единицами общего и терминологического характера. **Студенты должны знать** дифференциацию лексики по сферам применения (бытовая, терминологическая, общенаучная, официальная). **Студенты должны знать** свободные и устойчивые словосочетания, фразеологические единицы. **Студенты должны знать** основные способы словообразования. **Студенты должны владеть** грамматическими навыками, обеспечивающими коммуникацию общего характера без искажения смысла при письменном и устном общении. **Студенты должны знать** основные грамматические явления, характерные для профессиональной речи. **Студенты должны знать** культуру и традиции страны изучаемого языка, правила речевого этикета. **Студенты должны уметь** читать и переводить несложные прагматические тексты и тексты по широкому и узкому профилю специальности.

	Студенты должны уметь вести диалогическую и монологическую речь с использованием наиболее употребительных и относительно простых лексико-грамматических средств в основных коммуникативных ситуациях неофициального и официального общения. **Студенты должны иметь** навыки публичной речи: устное сообщение, доклад. **Студенты должны понимать** диалогическую и монологическую речь в сфере бытовой и профессиональной коммуникацию **Студенты должны уметь написать** частное письмо, деловое письмо; **уметь составить** аннотацию к тексту, **уметь написать** реферат, **уметь составить** резюме.
Краткая характеристика учебной дисциплины (основные блоки и темы)	**Содержание дисциплины и виды учебной работы** ***Модуль 1 I Семестр*** *Тема: Коррективный фонетический курс* Специфика артикуляции звуков, интонации, акцентуации и ритма нейтральной речи в изучаемом языке; основные особенности полного стиля произношения, характерные для сферы профессиональной коммуникации; чтение транскрипции. *1. 1. Звуковые явления* - особенности произношения английских звонких и глухих согласных - сочетание двух взрывных согласных - ассимиляция в сочетании альвеолярных согласных - ассимиляция в сочетаниях согласных с сонантом [r] и связующее [r] - ассимиляция в сочетаниях согласных со звуком [w] - сочетание звонких и глухих согласных - сочетание дифтонгов [ou] [au] [u] с нейтральным гласным *1. 2. Интонация* - нисходящий ядерный тон в повествовательных фразах - фразовое ударение; редукция гласных в служебных словах - восходящий тон; употребление восходящего тона в общих вопросах - интонация разделительных вопросов - интонация специальных вопросов - интонация альтернативных вопросов - употребление низкого восходящего тона в незавершенных интонационных группах - интонация разговорных формул. *1.3.Аудиторное чтение.* Чтение. Виды текстов: несложные прагматические тексты и тексты по широкому и узкому профилю специальности *(Unit 1 учебник Дорожкина В.П.)Лексический минимум 200 единиц терминологического характера.* Teaching Material The New Role of University Education The Internet Distance Education My University Studies The Kant Russian State University *2.2. Грамматический материал* Word Structure. Parts of Speech Sentence Structure The Interrogative Sentences: General, Special, Alternative and Disjunctive

	Questions Tense Forms in the Active Voice: Indefinite, Continuous, Perfect Pronouns: Personal, Possessive, Reflective, in Objective Case, Demonstrative Indefinite Pronouns: “Some”, “Any”, “No” and their derivatives. *1.4. Тексты для чтения дома.(Unit 2 Дорожкина В.П.) Лексический минимум 200 единиц терминологического характера.* What is Mathematics? Mathematics – the Language of Science Myths in Mathematics Mathematics and Art *1.5. Говорение.* Понятие дифференциации лексики по сферам применения (бытовая, терминологическая, общенаучная, официальная и другая). Понятие о свободных и устойчивых словосочетаниях, фразеологических единицах. Понятие об основных способах словообразования. Грамматические навыки, обеспечивающие коммуникацию общего характера без искажения смысла при письменном и устном общении; основные грамматические явления, характерные для профессиональной речи. Понятие об обиходно-литературном, официально-деловом, научном стилях, стиле художественной литературы. Основные особенности научного стиля. *Разговорные темы (Unit 1-5- Рыжков В.Д.) Лексический минимум 100 единиц общего характера.* Travelling by Railway Travelling by Plane At the Customs House At the Hotel Sights of London New York City *1.6. Речевой этикет. Формулы речевого общения* Культура и традиции стран изучаемого языка, правила речевого этикета Meeting people/Introducing someone Giving clarification, Correcting yourself. Intentions and predictions about future. *1.7Аудирование.* Аудирование. Понимание диалогической и монологической речи в сфере бытовой и профессиональной коммуникации *Диалоги из Universal English Course. Диалогическая речь в бытовой сфере* Personal Information Travelling by Plane Travelling by Train At a Hotel Asking the Way Describing the Way *1.8.Письмо* Письмо. Виды речевых произведений: аннотация, реферат, тезисы, сообщения, частное письмо, деловое письмо, биография Написать письмо личного характера. ***Модуль 2 II Семестр*** *2.1. Аудиторное чтение. (Unit 3 Дорожкина В.П.) Лексический минимум 100 единиц терминологического характера.* Counting. Natural Numbers. Notations

	Number Systems of Mathematics Mathematical Proofs Basic Geometric Concepts J.E. Freund's System of Natural Number Postulates *2.2.Грамматический материал.* Much, Many, Little, Few, a little, a few Countable, Uncountable Nouns The Modal Verbs: can (could), to be able to, may (might), must, to have to (to have got to), to be to, should, ought to, need Adjectives and Adverbs: Degrees of Comparison To be going + Infinitive Passive Voice: Indefinite, Continuous, and Perfect *2.3. Тексты для чтения дома. (Unit 4 Дорожкина В.П.) Лексический минимум 200 единиц терминологического и общенаучного характера* Unsolved problems of Antiquity: Unsolved Mathematical Problems(extracts From the lecture delivered by D. Hilbert): "Squaring the Circle", "Duplication of the Cube", "Trisecting the Angle". *2.4. Говорение.* Говорение. Диалогическая и монологическая речь с использованием наиболее употребительных и относительно простых лексико-грамматических средств в основных коммуникативных ситуациях неофициального и официального общения. Основы публичной речи (устное сообщение, доклад) *Разговорные темы. (Units 6-11 Рыжков В.Д.) Лексический минимум 100 единиц общего характера.* Shopping in Britain and USA Meals Holiday Making Climate. Weather At the Theatre. Theatres in England Holidays and Festivals in Britain Holidays and Festivals in America Holidays and Festivals in Russia *2.5. Речевой этикет. Формулы речевого общения* Expressing interest/ Expressing indifference Expressing Sympathy. Doubts. Expressing need and use. *2.6. Аудирование. Диалоги из (Universal English Course I) Диалогическая речь в сфере бытовой коммуникации* Shopping At a Restaurant At a Cafe At a Theatre Conversational Formulas *2.7. Письмо.* Составить отчет по форме: Покупки в Лондоне. Сочинение на тему: Мои Каникулы. ***Модуль 3 III Семестр*** *3.1. Аудиторное чтение.(Unit 5 Дорожкина В.П.) Лексический минимум 100 единиц терминологического и общенаучного характера.*

	Greek Schools of Mathematics The History of Geometry Euclid's Elements Non-Euclidean Geometries A Modern View of Geometry Topology *3.2. Грамматический материал.* Substitutes of the Noun Emphatic Constructions Impersonal Sentences Adverbial Clauses of Time and Conditions Complex Object with the Infinitive Complex Subject with the Infinitive *3.3. Тексты для чтения дома. (Unit 6 Дорожкина В.П.) Лексический минимум 200 единиц терминологического и общенаучного характера.* Descartes' and Fermat's Coordinate Geometry Analysis Incarnate – Leonard Euler Analytic Geometry Higher Dimensions Four – Dimensional Geometry *3.4. Говорение. Разговорные темы. (Units 12-16 Рыжков В.Д.) Лексический минимум 200 единиц общего характера.* Education in Britain Education in the USA Sports and Games Health Matters Our Home *3.5. Речевой этикет. Формулы речевого общения.* Expressing Hypothesis and Supposition Logical assumptions and Guesses Deductions about the aim of something. *3.6. Аудирование из (Ideas and Issues) Монологическая речь в бытовой сфере.* Sport. Avoiding sports injuries by avoiding sport Film and TV. The effects of TV on children Family. Arranged marriages Friendship. Roommates at college. *3.7. Письмо.* Заполнение форм и бланков для участия в студенческих программах. Сообщение «Великие математики» ***Модуль 4 IV семестр*** *4.1. Аудиторное чтение. (Units 7, 8, Дорожкина В.П.) Лексический минимум 200 единиц общенаучного и терминологического характера.* The Scientific Method Scientific Laws Mathematics and Modern Civilization The History of Algebra Fields, Rings, Groups Linear Algebra *4.2.Грамматическийматериал.* Participle (I, II)

	Absolute Participle Construction Gerund Sequence of Tenses Direct and Indirect Speech The Subjunctive Mood *4.3. Тексты для чтения дома. (Units 9, 10 Дорожкина В.П.) Лексический минимум 200 единиц общенаучного и терминологического характера.* Cybernetics and Informatics The World Wide Web Web Site Management Strategies The Web Pages. The Internet Programming languages Development of Modern Mathematics Set Theory *4.4.Говорение. Разговорные темы. (Units 17-21 Рыжков В.Д.) Лексический минимум 100 единиц общего характера.* Post Office Telephone Conversation Office Applying for a Job Bank operations English speaking countries *4.5. Аудирование из (Ideas and Issues) Монологическая речь в бытовой сфере.* New Technology. The Computer revolution Language. Global English Poverty. Homeless in the USA Racism, Racial discrimination in Britain *4.6. Письмо.* Написать деловое письмо. Составить резюме и CV Сообщение «Современные технологии» (общая тема)
Трудоёмкость (з.е. / часы)	Согласно рабочему учебному плану курс читается в полном объёме в течение 1-4 семестров **10** ЗЕ / **360**часов.
Форма итогового контроля знаний	1 ***экзамен***, 3 **зачет**а

Аннотация учебной дисциплины

Учебная дисциплина **«БЕЗОПАСНОСТЬ ЖИЗНЕДЕЯТЕЛЬНОСТИ»**	
Цель изучения дисциплины	***Цель дисциплины «Безопасность жизнедеятельности»*** - повысить социально-психологическую и медико-биологическую компетентность студентов, что позволит сформировать навыки безопасного поведения в повседневной жизни.

Компетенции, формируемые в результате освоения дисциплины	- Способен создавать и поддерживать в повседневной жизни и в профессиональной деятельности 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);
Знания, умения и навыки, получаемые в процессе изучения дисциплины	В результате изучения курса студенты должны уметь: - создать комфортное состояние среды обитания в зонах трудовой деятельности и отдыха человека; - идентифицировать негативные воздействия среды обитания естественного, техногенного и антропогенного происхождения; - разработать и реализовать меры защиты человека и среды обитания от негативных воздействий; - обеспечить устойчивость функционирования объектов и технических систем в штатных и чрезвычайных ситуациях; - принять решения по защите производственного персонала и населения от возможных последствий аварий, катастроф, стихийных бедствий и применения современных средств поражения, а также принятия мер по ликвидации их последствий; - прогнозировать развитие негативных воздействий и оценки последствий их действия.
Краткая характеристика учебной дисциплины (основные блоки и темы)	Содержание дисциплины *1. Введение. Основные понятия, термины и определения.* Цель и содержание дисциплины, ее основные задачи, место и роль в подготовке специалиста. Основные понятия. Человек и среда обитания. 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. Кривая Фармера. Экономический риск. Потенциальный территориальный риск. Профессиональный риск. Оценка травматизма и профзаболеваний на производстве. Оценка экономических потерь предприятия. Показатель сокращения продолжительности жизни, методика определения. Концепция приемлемого риска и оценка безопасности профессиональной деятельности в РФ. Мотивированный и немотивированный риск. Методы определения риска. Управление риском. Анализ риска. Качественные методы анализа опасностей и риска. Проверочный лист. Предварительный анализ опасностей. Анализ видов и последствий отказов. Анализ опасности и работоспособности. Анализ ошибок персонала. Причинно-следственный анализ. Анализ «дерева отказов» или «дерева причин». Анализ «дерева событий» или «дерева последствий». *2. Безопасность жизнедеятельности и природная среда. Экологические опасности. Классификация. Источники загрязнения среды обитания.* Экологическая безопасность. Критерии оценки качества окружающей среды, экологическое нормирование. Безопасность и экологичность технических систем. 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. Основные загрязнители атмосферного воздуха: классификация с ссылкой на ГОСТ; $ПДК_{сс}$ и $ПДК_{мр}$. Оценка выбросов ЗВ по ЮНЕП. Критерии оценки состояния загрязнения атмосферы. КИЗА. Оценка рассеивающей способности атмосферы. Экологический мониторинг. Цель, ступени и структура. (ЕГСЭМ) РФ. Примеры. Экологическая экспертиза. Законодательная и нормативная база. Принципы экологической экспертизы. Методы экологической экспертизы. Федеральные и региональные уровни. Общественная экологическая экспертиза. Ресурсные критерии оценки состояния поверхностных вод. Экологическое законодательство и нормативные документы в области водопользования, водосбережения и безопастности водных объектов. Нормирование качества воды. Классификация водоемов и ПДК. Методы комплексной оценки загрязненности поверхностных вод. Классы качества вод в зависимости от ИЗВ и индекса сапробности S. Гидрохимический метод комплексной оценки загрязнения вод: K_iH_i, B_i, Z_c.. Теория «биогеохимических провинций». Эндемические заболевания. Примеры. Общие и суммарные показатели качества вод, нормативные требования по качеству. Значение водного фактора в распространении острых кишечных инфекций и инвазий. Болезнь легионеров. Санитарно-микробиологическая оценка качества вод. Методы и объекты индикации, их общая характеристика. Показатели санитарно-микробиологической чистоты вод по СанПиНу 2.1.4.1074-01. Мероприятия, направленные на сохранение гидроресурсов. Замкнутые водооборотные системы. Кратность использования воды в обороте. Аэробная биохимическая очистка-минерализация. Анаэробная биохимическая очистка. Технология и степень эффективности очистки. 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. Коэффициент концентрации химического вещества (K_i). Суммарный показатель загрязнения (Z_c). Оценочная шкала опасности загрязнения почв. Утилизация твердых и жидких бытовых отходов как экологический пример. *3. Основы физиологии труда и комфортные условия жизнедеятельности. Вредные и опасные производственные 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. Категории работ по интенсивности энергозатрат в соответствие с Р 2.2.2006–05. Динамический стереотип как фактор, определяющий функциональные возможности организма. Работоспособность. Определение физической работоспособности при помощи тестаPWC$_{170}$ (Physicalworkingcapacity). Общая физическая работоспособность. Относительная работоспособность. Оценка фактического состояния условий труда и классификация условий труда по степени вредности (Р 2.2.2006–05). Динамические и статические нагрузки. Методика расчета. Физиологические изменения в организме при физической и умственной нагрузке. Производственный травматизм. Причины производственного травматизма. Профессиональные заболевания. Острые и хронические профзаболевания, их характеристика и примеры. Аттестация рабочих мест по условиям труда. Рабочая зона. Рабочее место. Условия труда. Тяжесть труда. Напряжённость труда. Методика расчета. Опасные и вредные факторы производственной среды. АПФД. Общая характеристика и классификация АПФД. Аэрозоли дезинтеграции. Аэрозоли конденсации. Действие пыли на организм человека (классификация). Фиброгенность пыли. Нормирование и оценка степени воздействия АПФД. Классификация условий труда при профессиональном контакте с АПФД в соответствие с Р 2.2.2006-05. Принцип защиты временем при воздействии АПФД. Расчет допустимого стажа работы. Наиболее вредные характеристики пыли. Воздействие пыли на различные органы и ткани человека. Пневмокониозы. Токсико-пылевой бронхит. Бронхиальная астма. Профилактика пылевых заболеваний. Лечебно-профилактические мероприятия. Санитарно-технические мероприятия. СИЗ. УФ-излучение. Характеристика, классификация. Гигиеническое нормирование УФ в соответствие с СН № 4557-88 и МУ № 5046—89.Классификация условий труда по Р 2.2.2006 – 05. Биологическая оценка ультрафиолетового облучения. 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. Расчет теплового облучения работающего. Гигиеническое нормирование ИК в соответствии с СанПиН 2.2.4.548-96. Категории работ (классификация по энергозатратам). Классификация условий труда по Р 2.2.2006 – 05. Определение ТНС-индекса и классы условий труда по этому показателю. Принцип защиты временем и нормирование температуры воздуха на рабочем месте выше или ниже допустимых величин. Нормирование перепадов температур на рабочих местах в зависимости от категорий.СИЗ. Свет. Основные светотехнические характеристики и гигиенические требования по освещенности к рабочему месту. Нормирование освещенности по СНиП 23-05-95 и СанПиН 2.2.1/2.1.1.1278-03. Классификация условий труда по Р 2.2.2006 – 05. Классы условий труда в зависимости от дополнительных параметров световой среды. Разряды зрительных работ. Расчет естественного и искусственного освещения (метод светового потока). 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. Классификация шума по ГОСТ 12.1.029-80 и ГОСТ 12.1.003-83. Основные характеристики звуковых волн. Уровень громкости звука. Гигиеническое нормирование шума по ГОСТ 12.l.003-83 и СН 2.2.4/2.1.8.562-96. Нормирование постоянного и непостоянного шума. Нормирование шума для ориентировочной оценки. Коррекция уровня звукового давления. Доза шума. Оценка источников шума (2 и более) одинаковых и разных по своему уровню. Количественная оценка тяжести и напряженности трудового процесса в зависимости от уровня шума. Классификация условий труда по Р 2.2.2006 – 05. Категории тяжести трудового процесса по СН 2.2.4/2.1.8.562-96.Переход от дБ к разам. Профилактика профзаболеваний. Инфразвук. Гигиеническая классификация и нормирование постоянного и непостоянного инфразвука по СН 2.2.4/2.18.583-96. ПДУ инфразвука. Биологическое действие. Профилактика. Ультразвук. Классификация и гигиеническое нормирование по СанПиН 2.2.4./2.1.8.582—96 и ГОСТ 12.1.001 — 89. 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). Безопасность автоматизированных объектов. Системы автоматического контроля. Психологические факторы при работе с информационными системами. *4. Безопасность в чрезвычайных ситуациях. 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. Безопасность в ЧС. 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. *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, эпицентральная зона (плейстосейстовая область). 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. *6. ЧС техногенного характера. Безопасность и экологичность технических систем. 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. НРБ-99. Категории облучаемых лиц. Нормирование радиационной безопасности в случае радиационной аварии. Пределы доз (ПД). Гигиеническая оценка и классификация условий труда при работе с источниками ионизирующего излучения. Максимальные потенциальные эффективные и эквивалентные дозы, их МПД. Допустимая мощность годовой потенциальной дозы (ДМПД). Классификация условий труда по Р 2.2.2006 – 05. Радиационная защита. РОО и зоны безопасности. Международная шкала тяжести событий на АС. Аварии на РОО. Классификация аварий. Радиационная опасность аварии. Состав выброса и воздействие излучений по стадиям аварии (стадии РА). Состав защитных мероприятий при авариях на РОО. Заблаговременные и оперативные мероприятия РЗ. Зонирование территории

	при авариях на РОО. ЗРА и ЗРК. Типовые режимы радиационной защиты при авариях на АС. Зона радиационного загрязнения на ранней и промежуточной стадиях аварии (ЗРА). Зонирование внутри зоны отселения по степеням фактического загрязнения местности. Зонирование на восстановительной стадии аварии РОО. ЗРА и ЗРК. Зонирование ЗРА. Вмешательство и его принципы. Классификация противорадиационных укрытий. Классификация радиопротекторов. Типовые режимы радиационной защиты при авариях АЭС. Основы электробезопасности. Безопасность систем связи. Эвакуация населения, ее предназначение, порядок проведения мероприятий при эвакуации. *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. *8. Защита населения в 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. *9. Управление безопасностью жизнедеятельности. Нормативно-техническая документация.* Управление безопасностью жизнедеятельности. 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.

	Законодательные акты директивных органов. Подзаконные акты по охране труда. Чрезвычайные ситуации в законах и подзаконных актах. Государственное управление в чрезвычайных ситуациях. *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. Анатомо-физиологические и психологические воздействия на человека опасных и вредных факторов при работе с защищенными автоматизированными системами. Психологическая устойчивость в чрезвычайных ситуациях. Норма 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.
Трудоёмкость (з.е. / часы)	**2 ЗЕТ / 72** часа.
Форма итогового контроля знаний	***зачет.***

Аннотация учебной дисциплины

Учебная дисциплина **«Языки программирования» (2 семестр)**

Цель изучения дисциплины	***Цели*** освоения дисциплины «Языки программирования»: является получение студентами начальной подготовки в области программирования на языке Си
Компетенции, формируемые в результате освоения дисциплины	Процесс изучения дисциплины направлен на формирование следующих ***компетенций***: - 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); - Способен разрабатывать компоненты программных и программно-аппаратных средств защиты информации в компьютерных системах и проводить анализ их безопасности (ОПК-13);
Знания, умения и навыки, получаемые в процессе изучения дисциплины	В результате освоения дисциплины студент должен ***знать***: - различия функционального и структурного программирования ***уметь***: - применять приемы рационального программирования ***владеть***: - навыками работы со стандартными компьютерными программами, используемыми при разработке программного обеспечения
Краткая Характеристика учебной дисциплины (основные блоки и темы)	**Содержание основных разделов (тем) курса** Интегрированная среда разработки QtCreator. Структура рабочего стола среды программирования. Структура проекта в QtCreator. Создание простейшего консольного приложения. Компиляция программы. Запуск программы на выполнение. Работа с ошибками в QtCreator. Стиль программирования. Структура простейшей программы на Си Именование переменных. Определение переменных и инициализация. Область видимости переменных. Типы данных языка Си. Базовые типы char, int, long, float и double. Операции над базовыми типами данных. Различие знаковых и беззнаковых целых чисел. Ввод с клавиатуры и вывод на консоль. Условный оператор if. Старшинство операций. Оператор выбора. Триарный оператор. Назначение операторов цикла. Оператор цикла for. Оператор цикла while. Оператор цикла do while. Оператор досрочного прекращения цикла break. Оператор продолжения цикла continue. Операции сдвига >> и <<. Особенности работы операции сдвига вправо. Побитовые операции. Побитовое умножение &, побитовое сложение |, побитовая инверсия ~. Операция sizeof. Операция явного и неявного преобразования типов. Определение функции. Передача аргументов в функцию. Возврат значения из функции. Возврат функцией более одного значения. Область определения переменных функции. Рекурсивные функции. Массивы. Объявление одномерных массивов. Инициализация одномерных массивов. Машинно-независимое определение размерности одномерного массива. Символьные массивы. Многомерные массивы. Инициализация многомерных массивов. Указатели. Операции над указателями. Адресная арифметика. Эквивалентность указателей и массивов. Сравнение указателей. Константные указатели. Нулевой указатель и указатель void *. Структуры и объединения. Динамическое распределение памяти.

Трудоёмкость (з.е. / часы)	Согласно рабочему учебному плану курс читается в полном объёме в течение 2 семестра **3** ЗЕТ / **108** часов.
Форма итогового контроля знаний	В конце **2**-го семестра предусмотрен ***зачёт***.

Учебная дисциплина **«Языки программирования» (3 семестр)**	
Цель изучения дисциплины	***Цели*** освоения дисциплины «Языки программирования»: является получение студентами начальной подготовки в области программирования на языке С++ -
Компетенции, формируемые в результате освоения дисциплины	Процесс изучения дисциплины направлен на формирование следующих ***компетенций***: - 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); - Способен разрабатывать компоненты программных и программно-аппаратных средств защиты информации в компьютерных системах и проводить анализ их безопасности (ОПК-13);
Знания, умения и навыки, получаемые в процессе изучения дисциплины	В результате освоения дисциплины студент должен ***знать***: - различия функционального и структурного программирования ***уметь***: - применять приемы рационального программирования ***владеть***: - навыками работы со стандартными компьютерными программами, используемыми при разработке программного обеспечения
Краткая Характеристика учебной дисциплины (основные блоки и темы)	**Содержание основных разделов (тем) курса** Определение класса. Использование класса. Определения полей и методов класса. Квалификаторы видимости полей и методов класса - public и private. Статические методы и поля класса. Что такое getter’s и setters. Конструктор по умолчанию и конструкторы преобразований. Вызов конструктора из конструктора. Перегрузка операций. Константы в классе. Поля-массивы в классе. Когда необходимо определять деструкторы в классе. Необходимость в определении конструктора копирования и перегрузке оператора присваивания. Простое открытое наследование. Конструкторы и деструкторы при наследовании. Поля и методы при наследовании. Статические элементы класса при наследовании. Закрытое наследование. Защищенное наследование. Виртуальные функции. Чистые виртуальные функции и абстрактные классы.
Трудоёмкость (з.е. / часы)	Согласно рабочему учебному плану курс читается в полном объёме в течение 3 семестра **5** ЗЕТ / **180** часов.
Форма итогового контроля знаний	В конце **3**-го семестра предусмотрен ***экзамен***.

Аннотация учебной дисциплины

Учебная дисциплина **«ФИЗИЧЕСКАЯ КУЛЬТУРА И СПОРТ»**	
Цель ия дисциплины	**Цель** дисциплины «Физическая культура» состоит в формировании способностью использовать разнообразные формы физической культуры и спорта в повседневной жизни для сохранения и укрепления своего здоровья и здоровья своих близких, семьи и трудового коллектива для качественной жизни и эффективной профессиональной деятельности.
Компетенции, формируемые в результате освоения дисциплины	- Способен поддерживать должный уровень физической подготовленности для обеспечения полноценной социальной и профессиональной деятельности (УК-7).
Знания, умения и навыки, получаемые в процессе изучения дисциплины	По окончании изучения курса студент должен: Знать: – ценности физической культуры и спорта; значение физической культуры в жизнедеятельности человека; культурное, историческое наследие в области физической культуры; – факторы, определяющие здоровье человека, понятие здорового образа жизни и его составляющие; – принципы и закономерности воспитания и совершенствования физических качеств; – способы контроля и оценки физического развития и физической подготовленности; – методические основы физического воспитания, основы самосовершенствования физических качеств и свойств личности; основные требования к уровню его психофизической подготовки к конкретной профессиональной деятельности; влияние условий и характера труда специалиста на выбор содержания производственной физической культуры, направленного на повышение производительности труда. Уметь: – оценить современное состояние физической культуры и спорта в мире; – придерживаться здорового образа жизни; – самостоятельно поддерживать и развивать основные физические качества в процессе занятий физическими упражнениями; осуществлять подбор необходимых прикладных физических упражнений для адаптации организма к различным условиям труда и специфическим воздействиям внешней среды. Владеть: – различными современными понятиями в области физической культуры; – методиками и методами самодиагностики, самооценки, средствами оздоровления для самокоррекции здоровья различными формами двигательной деятельности, удовлетворяющими потребности человека в рациональном использовании свободного времени; – методами самостоятельного выбора вида спорта или системы физических упражнений для укрепления здоровья; здоровьесберегающими технологиями;

	средствами и методами воспитания прикладных физических (выносливость, быстрота, сила, гибкость и ловкость) и психических (смелость, решительность, настойчивость, самообладание, и т.п.) качеств, необходимых для успешного и эффективного выполнения определенных трудовых действий
Краткая характеристика учебной дисциплины (основные блоки и темы)	1. Гимнастика. Основы техники безопасности на занятиях гимнастикой. Основы производственной гимнастики. Составление комплексов упражнений (различные видов и направленности воздействия). 2. Легкая атлетика. Основы техники безопасности на занятиях легкой атлетикой. Ознакомление, обучение и овладение двигательными навыками и техникой видов лёгкой атлетики. Совершенствование знаний, умений, навыков и развитие физических качеств в лёгкой атлетике. 3. Меры безопасности на занятиях лёгкой атлетикой. Техника выполнения легкоатлетических упражнений. Развитие физических качеств и функциональных возможностей организма средствами лёгкой атлетики. Специальная физическая подготовка в различных видах лёгкой атлетики. Способы и методы самоконтроля при занятиях лёгкой атлетикой. Особенности организации и планирования занятий лёгкой атлетикой в связи с выбранной профессией. 4. Спортивные игры. Основы техники безопасности на занятиях спортивными играми. Баскетбол. Волейбол. Футбол. Настольный теннис. Бадминтон. 5. Специализация. Избранный вид спорта. Общая и специальная физическая подготовка в избранном виде спорта. Спортивное совершенствование. Участие в соревнованиях. Помощь в судействе. 6. Закрепление материала. Виды и элементы видов двигательной активности, включенных в практические занятия в семестре обучения. Подготовка к тестированию физической и функциональной подготовленности, сдача контрольных испытаний и зачетных нормативов. 7. Плавание. Основы техники безопасности на занятиях по плаванию. Начальное обучение плаванию. Подвижные игры в воде. Освоение техники способов плавания. Старты и повороты. Правила поведения на воде. Спасение утопающих, первая помощь. Общая и специальная подготовка пловца (общие и специальные упражнения на суше). Аквааэробика. Правила соревнований, основы судейства. 8. Лыжный спорт. Основы техники безопасности на занятиях по лыжному спорту. Освоение техники лыжных ходов. Повороты. Подъемы и спуски с гор. Прохождение дистанции. Правила соревнований, основы судейства.
Трудоёмкость (з.е. / часы)	**2** ЗЕТ / **72** часа
Форма итогового контроля знаний	**Зачет.**

Аннотация учебной дисциплины

Учебная дисциплина **«История (история России, всеобщая история)»**	
Цель изучения дисциплины	**Цель** изучения дисциплины «История (история России, всеобщая история)» является освоение истории России с древнейших времен до наших дней, с учетом изменений территориальных границ страны, состава народонаселения, эволюции

	государственного строя, развития народного хозяйства, общественной мысли и политических движений, культуры. Общая цель преподавания курса – формирование грамотных и творчески мыслящих специалистов. Предметом изучения данной учебной дисциплины является история России от её истоков до сегодняшнего дня, в пределах постоянно менявшихся территориальных рамок страны; народы, в курсе Отечественной истории изучается история российского государства; история общественной мысли и политических движений, история культуры народов населяющих нашу страну.
Компетенции, формируемые в результате освоения дисциплины	Процесс изучения дисциплины направлен на формирование следующих ***компетенций***: - 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);
Знания, умения и навыки, получаемые в процессе изучения дисциплины	**Знать:** - объект, предмет цель и задачи учебной дисциплины; - основные события, даты, явления и процессы Отечественной истории, ее место в контексте мировой истории; - ключевые методологические, исторические и источниковедческие проблемы истории Отечества; - важнейшие понятия, термины и их определения, имена, географические названия и даты, связанные с историей России; **Уметь:** - характеризовать явления и исторические процессы, изучаемые в курсе; - вырабатывать собственную позицию в отношении изучаемых исторических проблем; - выявлять закономерности и основные этапы в развитии событий, устанавливать причинно-следственные связи; - ориентироваться в историческом и этнокультурном пространстве истории Отечества; - иметь навыки сопоставления фактов истории России в контексте других знаний гуманитарного и специально профессионального характера; **Владеть:** - навыками организации самостоятельной работы; - навыками самостоятельного поиска, анализа и отбора необходимой информации, ее структурирования и преобразования.
Краткая характеристика учебной дисциплины (основные блоки и темы)	Тема 1. Проблемы методологии истории Тема 2. Территория и население России с древности до наших дней Тема 3. От Руси к России (VI –XVII вв.) Тема 4. Российская империя (XVIII – начало XX в.) Тема 5. Революция 1917 г. и Гражданская война Тема 6. Советская Россия и СССР в 1920-е-1930-е гг. Тема 7. СССР в годы Великой Отечественной войны и послевоенного развития Тема 8 . СССР в 1950-е – начале 1980-х гг. Тема 9. От СССР к России (1985-1991 гг.). Современная Россия (1991-2010 гг.)
Трудоёмкость	**3** ЗЕТ /108 часов.

(з.е. / часы)	
Форма итогового контроля знаний	зачет

Аннотация учебной дисциплины

Учебная дисциплина **«ОСНОВЫ ПРЕДПРИНИМАТЕЛЬСКОЙ ДЕЯТЕЛЬНОСТИ В ПРОФЕССИОНАЛЬНОЙ СФЕРЕ»**	
Цель изучения дисциплины	Цель: используя современные образовательные технологии познакомить студентов с понятийным аппаратом, лежащим в основе деятельности любого предпринимателя, сформировать систему профессиональных знаний, умений и навыков в вопросах понимания законов и принципов, по которым развивается предпринимательство, существующих в нем проблем.
Компетенции, формируемые в результате освоения дисциплины	- Способен осуществлять критический анализ проблемных ситуаций на основе системного подхода, вырабатывать стратегию действий (УК-1); - Способен управлять проектом на всех этапах его жизненного цикла (УК-2); - Способен организовывать и руководить работой команды, вырабатывая командную стратегию для достижения поставленной цели (УК-3); - Способен определять и реализовывать приоритеты собственной деятельности и способы ее совершенствования на основе самооценки и образования в течение всей жизни (УК-6); - Способен принимать обоснованные экономические решения в различных областях жизнедеятельности (УК-9); - Способен формировать нетерпимое отношение к коррупционному поведению (УК-10);
Знания, умения и навыки, получаемые в процессе изучения дисциплины	Для успешного освоения дисциплины студенты **должны знать**: - теоретические основы предпринимательства; - законодательные и нормативные акты, регламентирующие предпринимательскую деятельность на территории Российской Федерации; **иметь навыки**: - выбора организационно-правовой формы предпринимательской деятельности; - применения различных методов исследования рынка; - сбора и анализа информации о конкурентах, потребителях, поставщиках; - осуществлять планирование производственной деятельности; - разрабатывать бизнес-план;
Краткая характеристика учебной дисциплины (основные блоки и темы)	1. Содержание предпринимательской деятельности. 2. Производительный процесс фирмы. 3. Учреждения предприятия. 4. Организационно-правовые формы предпринимательской деятельности в РФ. 5. Принятие предпринимательского решения. 6. Предпринимательский договор. 7. Основы построения оптимальной структуры предпринимательской деятельности. 8. Формирование цены товара. 9. Разработка предпринимательских схем.

	10. Культура предпринимательства.
Трудоёмкость (з.е. / часы)	3 ЗЕТ / **108** часов.
Форма итогового контроля знаний	Зачет

Аннотация учебной дисциплины

Учебная дисциплина **«ФИЛОСОФИЯ»**	
Цель изучения дисциплины	*Цель изучения дисциплины* - дать целостное представление о философии как самостоятельной области духовной культуры и теоретических исследований.
Компетенции, формируемые в результате освоения дисциплины	Процесс изучения дисциплины направлен на формирование следующих ***компетенций***: - Способен анализировать и учитывать разнообразие культур в процессе межкультурного взаимодействия (УК-5);
Знания, умения и навыки, получаемые в процессе изучения дисциплины	В результате освоения дисциплины обучающийся должен: **Знать**: - основные этапы развития и современное состояние философской мысли; - место философии в системе современного гуманитарного знания; - основные понятия и проблемы философских исследований -основные концепции, родившиеся при решении наиболее значимых философских проблем **Уметь**: - анализировать философские тексты - критически анализировать плоды чужого и собственного философского творчества - сотрудничать с представителями других областей знания в ходе решения исследовательских задач - ставить и решать собственные перспективные исследовательские задачи.
Краткая характеристика учебной дисциплины (основные	**СОДЕРЖАНИЕ ДИСЦИПЛИНЫ** **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 характер философского знания. Сомнение как методологическая предпосылка

блоки и темы)	философского рассуждения. Феномен философской веры, её отличие от веры религиозной. Структура философского знания. **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. **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. **Тема 4. Основные этапы истории 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. **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. **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. **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. **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. **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. **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. **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. **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. **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. **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. **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, эволюционистская, синергетическая. Формационная и цивилизационная концепции общественного развития. **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.
Трудоёмкость (з.е. / часы)	Согласно рабочему учебному плану курс читается в полном объёме в течение 2-го семестра **3** ЗЕТ / **108** часов.
Форма итогового контроля знаний	В конце 2-го семестра предусмотрен ***зачет***.

Аннотация учебной дисциплины

Учебная дисциплина **«ОСНОВЫ ДЕЛОВЫХ КОММУНИКАЦИЙ»**	
Цель изучения дисциплины	Цель программы состоит в обеспечении овладения слушателями знаний и навыков в области деловых и научных коммуникаций, необходимых для успешной профессиональной деятельности.
Компетенции, формируемые в результате освоения дисциплины	- Способен применять современные коммуникативные технологии, в том числе на иностранном(ых) языке(ах), для академического и профессионального взаимодействия (УК-4); - Способен анализировать и учитывать разнообразие культур в процессе межкультурного взаимодействия (УК-5).
Знания, умения и навыки, получаемые в процессе изучения дисциплины	В результате освоения дисциплины обучающиеся должны • знать: - основные теории взаимодействия людей в организации, включая вопросы мотивации, групповой динамики, командообразования, коммуникаций, лидерства и управления конфликтами • уметь:

	- анализировать коммуникационные процессы в организации и разрабатывать предложения по повышению эффективности • владеть: - навыками деловых коммуникаций
Краткая характеристика учебной дисциплины (основные блоки и темы)	1. Введение в предмет. Характеристика курса. 2. Коммуникации: виды и функции. Модели и стили делового общения. 3. Средства делового общения: вербальные и невербальные. Этика делового общения. 4. Речевое воздействие. Слушание в ДК. Барьеры в общении причины их возникновения. 5. Сознательное и бессознательное. Ложь в речевой коммуникации. Манипуляции в общении. 6. Критика и комплименты в деловом общении. 7. Имидж делового человека. Репутация. Корпоративная культура.
Трудоёмкость (з.е. / часы)	**3** ЗЕТ **/ 108** часов.
Форма итогового контроля знаний	Зачет

Аннотация учебной дисциплины

Учебная дисциплина **«АЛГЕБРА»**	
Цель изучения дисциплины	***Главной целью*** преподавания этой дисциплины является обеспечение фундаментальной подготовки будущего специалиста в одной из важнейших областей современной математики, изучение им основ классической и современной алгебры, ознакомление с основными направлениями и методами алгебраических исследований, демонстрация возможностей применения этих методов в различных областях математики и ее приложениях.
Компетенции, формируемые в результате освоения дисциплины	Преподавание дисциплины нацелено на формирование следующих компетенций обучающихся: - Способен на основании совокупности математических методов разрабатывать, обосновывать и реализовывать процедуры решения задач профессиональной деятельности (ОПК-3).
Знания, умения и навыки, получаемые в процессе изучения дисциплины	Студент, изучивший курс алгебры, должен ***иметь представление:*** 1. О роли и значении основных понятий алгебры. 2. О делении алгебры на классические разделы и взаимосвязи между ними. 3. Об областях применения алгебраических методов. Студент должен ***знать:*** 1. Основные свойства важнейших алгебраических структур (группы, кольца, поля, алгебры), взаимосвязь между различными структурами. 2. Основы линейной алгебра над произвольными полями. 3. Кольцо многочленов и его свойства. 4. Векторные пространства над полями и их свойства. 5. Основы теории групп и групп подстановок.

	Студент должен ***уметь:*** 1. Выполнять любые действия с матрицами, вычислять определители произвольных порядков. 2. Выполнять любые действия над комплексными числами в алгебраической и тригонометрической форме. 3. Выполнять различные действия над многочленами, находить корни многочленов, исследовать свойства многочленов. 4. Исследовать на совместность и находить решения систем алгебраических уравнений различных типов над различными полями. 5. Определять алгебраическую структуру различных множеств и исследовать отображения, заданные на них. 6. Определять линейную зависимость векторов. Определять координаты вектора в различных базисах. 7. Выделять различные подпространства и находить их размерность. 8. Приводить квадратичную форму к каноническому и нормальному виду. 9. Задавать операторы матрицами. Находить ядро и образ линейного оператора, его собственные векторы и значения, его инвариантные подпространства. Студент должен ***владеть:*** 1. Навыками использования методов векторной алгебры в смежных дисциплинах и в физике. 2. Методами решения основных алгебраических задач.
Краткая характеристика учебной дисциплины (основные блоки и темы)	**Содержание дисциплины** **Тема 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. **Тема 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. **Тема 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. Каноническое разложение многочлена. 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. **Тема 4. Основные алгебраические структуры**

	Внутренние бинарные и внешние операции на множестве. Понятие алгебраической структуры. Понятия полугруппы и 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. Основные свойства элементов кольца. Примеры. Кольцо матриц. Кольцо классов вычетов. Подкольца. Идеалы. Подполя. **Тема 5. Нормальная форма матрицы над полем** Понятие λ-матрицы. Элементарные преобразования λ-матриц. Канонические λ-матрицы. Приведение λ-матрицы к каноническому виду. Теорема единственности канонической λ-матрицы. Унимодулярные λ-матрицы, их свойства. Элементарные λ-матрицы. Критерий эквивалентности λ-матриц. Нахождение обратной матрицы с помощью элементарных преобразований. Матричные многочлены. Деление λ-матриц. Теорема Безу для матричных многочленов. Подобные матрицы. Критерий подобия матриц. Жорданова клетка. Жорданова матрица. Канонический вид характеристической жордановой матрицы. Критерий подобия жордановых матриц. Жорданова нормальная форма матрицы. Теорема о приводимости матрицы к жордановой нормальной форме в комплексном и вещественном пространстве. Единственность жордановой нормальной формы. Необходимое и достаточное условие диагонализируемости матрицы. (Материал данной темы дается студентам для самостоятельного изучения.) **Тема 6. Векторные пространства и системы линейных уравнений** Понятие векторного пространства. Линейная зависимость векторов. Свойства линейной зависимости. Базис пространства. Координаты вектора. Теоремы о базисах. Размерность 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. **Тема 7. 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. **Тема 8. 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.

Тема 9. 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.

Тема 10. 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.

1.5. Тематика практических занятий

Первый семестр

1. Отображения множеств. Типы отображений. Перестановки. Подстановки.
2. Матрицы и действия над ними.
3. Понятие определителя n-го порядка. Основные свойства определителей.
4. Вычисление определителей. Правило Крамера.
5. Методы вычисления определителей порядка n.
6. Обратная матрица. Матричные уравнения. Матричный метод решения систем линейных уравнений.
7. Метод Гаусса решения систем линейных уравнений.
8. Поле комплексных чисел. Действия над комплексными числами в алгебраической форме.
9. Извлечение корня квадратного из комплексных чисел в алгебраической форме. Решение квадратных уравнений.
10. Тригонометрическая форма комплексного числа.
11. Деление многочленов с остатком. Наибольший общий делитель многочленов.
12. Схема Горнера. Корни многочленов. Кратность корней. Самостоятельная работа.
13. Обобщенная теорема Виета.
14. Разложение многочлена на неприводимые множители над полем действительных и комплексных чисел.
15. Нахождение рациональных корней полинома.
16. Разложение правильной рациональной дроби на простейшие.
17. Группы. Кольца. Поля.
18. .Кольцо классов вычетов.

Второй семестр

1. Векторные пространства. Линейная зависимость векторов.
2. Базиспространства. Разложение вектора по базису.

	3. Формулы преобразования базиса. Формулы преобразования координат. 4. Ранг матрицы. Ранг системы векторов. Линейная оболочка векторов. 5. Исследование системы линейных неоднородных уравнений на совместность. 6. Фундаментальная система решений. 7. Подпространства векторного пространства. 8. Сумма и пересечения подпространств, определение их базисов. 9. Линейные операторы векторных пространств. 10. Матрица линейного оператора. 11. Действия над линейными операторами. 12. Образ и ядро линейного оператора. 13. Характеристические корни и собственные векторы. 14. Инвариантные подпространства линейного оператора. 15. Евклидовы пространства. Процесс ортогонализации векторов. 16. Ортогональное дополнение и ортогональная проекция подпространства.. 17. Симметрические и ортогональные операторы. 18. Приведение квадратичной формы к каноническому виду методом элементарных преобразований. 19. Приведение квадратичной формы к каноническому виду методом Лагранжа. 20. Отношение эквивалентности на множестве. Фактор-множество. 21. Разложение группы по подгруппе. Нормальный делитель. Фактор-группа. 22. Изоморфизм и гомоморфизм групп. 23. Конечные группы. Группа подстановок. 24. Расширения колец и полей. Простое алгебраическое расширение поля.
Трудоёмкость (з.е. / часы)	**9 ЗЕТ/324** часов.
Форма итогового контроля знаний	**Зачет, 2 экзамена**

Аннотация учебной дисциплины

Учебная дисциплина «ГЕОМЕТРИЯ»	
Цель изучения дисциплины	**Цели дисциплины**: - передать студентам определенную систему знаний, умений, навыков, научить использованию математических методов познания реальной действительности, научить самостоятельной работе с учебной литературой. - воспитать устойчивый интерес к изучению математики, развитию математического мышления, формированию культуры, логики. - научить применять знания для решения практических задач аналитической геометрии (и практических задач при изучении других дисциплин).
Компетенции, формируемы	В результате изучения курса «Геометрия» у студентов должны быть сформированы следующие профессиональные **компетенции:**

е в результате освоения дисциплины	- Способен на основании совокупности математических методов разрабатывать, обосновывать и реализовывать процедуры решения задач профессиональной деятельности (ОПК-3).
Знания, умения и навыки, получаемые в процессе изучения дисциплины	В результате изучения дисциплины студенты **должны**: - з**нать** содержание основных разделов геометрии: линейную зависимость векторов, скалярное, векторное и смешанное произведения, уравнения прямой на плоскости и в пространстве, линии и поверхности 2-го порядка, плоские сечения, изометрические, аффинные и проективные преобразования плоскости и пространства, аффинную и проективную классификацию линий и поверхностей.; **-уметь:** - решать задачи по геометрии на плоскости и в пространстве методом прямоугольных координат с использованием векторной алгебры; - приводить общее уравнение линии 2-го порядка к каноническому виду; - исследовать простейшие геометрические объекты по их уравнениям в различных системах координат. - и**меть навыки:** - использования методов аналитической геометрии и векторной алгебры в смежных дисциплинах и физике; - применения преобразований координат; - пользования библиотекой прикладных программ для ЭВМ при решении прикладных задач.
Краткая характеристика учебной дисциплины (основные блоки и темы)	**Содержание разделов дисциплины.** <u>Раздел 1. Элементы векторной алгебры.</u> 1.1 Понятие вектора. Основные операции над векторами Направленные отрезки. Векторы. Координаты вектора. Сложение и вычитание векторов. Умножение вектора на число. Признак коллинеарности векторов. Линейная зависимость векторов и ее свойства. Проекция вектора на ось. Теоремы о проекциях векторов на ось. 1.2 Скалярное, векторное и смешанное произведения векторов. Скалярное произведение векторов и его свойства. Векторное произведение векторов и его свойства. Смешанное произведение векторов и его свойства. Некоторые векторные тождества. Признак компланарности векторов. 1.3 Метод координат на плоскости. Метод координат на плоскости. Вектор-функция одной и двух переменных. <u>Раздел 2. Аффинная и декартовы системы координат на плоскости и в пространстве.</u> 2.1 Деление отрезка в данном отношении. Деление отрезка в данном отношении. Расстояние между двумя точками. Полярные координаты. Переход от полярных координат к декартовым и обратно. Обобщенные полярные координаты. Преобразование аффинной (декартовой) системы координат в аффинную (декартову). 2.2 Алгебраическая линия и ее порядок. Прямая линия на плоскости. Различные способы задания прямой на плоскости. Общее уравнение прямой. Расстояние от точки до прямой. Угол между двумя прямыми. Взаимное расположение двух прямых. Пучок прямых. <u>Раздел 3. Кривые второго порядка на плоскости.</u> 3.1 Общее уравнение окружности.

	Общее уравнение окружности. Теоремы о задании окружности уравнением второй степени. 3.2 Эллипс, гипербола, парабола и их свойства. Эллипс, гипербола, парабола и их свойства. Задание линии 2-го порядка в полярной системе координат. Классификация линий 2-го порядка. Раздел 4. Прямая и плоскость в пространстве. 4.1 Плоскость в пространстве Формулы преобразования систем координат в пространстве. Различные способы задания плоскости в пространстве. 4.2 Прямая в пространстве Различные способы задания прямой в пространстве. Угол между двумя плоскостями. Угол между двумя прямыми и угол между прямой и плоскостью. Взаимные расположения двух прямых, двух плоскостей, прямой и плоскости в пространстве. Расстояние между скрещивающимися прямыми. Расстояние от точки до плоскости в пространстве. Раздел 5. Поверхности 2-го порядка. 5.1 Поверхности вращения. Сферы. Поверхность вращения. Цилиндрические поверхности. Конические поверхности 2-го порядка. Изучение эллипсоида, гиперболоида по их каноническим уравнениям. 5.2 Прямолинейные образующие поверхностей 2-го порядка. Прямолинейные образующие поверхностей 2-го порядка. Классификация поверхностей 2-го порядка. Раздел 6. Преобразования плоскости и пространства. 6.1 Аффинные преобразования плоскости и пространства. Аффинные преобразования плоскости и пространства. Группы преобразований плоскости и пространства. Элементы проективной геометрии. 6.2 Многомерная евклидова геометрия. Многомерная евклидова геометрия. Дифференциальная геометрия кривых и поверхностей. Элементы топологии и римановой геометрии.
Трудоёмкость (з.е. / часы)	**3** ЗЕТ/ **108** часов.
Форма итогового контроля знаний	***Экзамен***

Аннотация учебной дисциплины

Учебная дисциплина **«ИНФОРМАТИКА»**	
Цель изучения дисциплины	Дисциплина «Информатика» имеет **целью** обучить студентов принципам построения информационных моделей, проведению анализа полученных результатов, применению современных информационных технологий, а также содействовать фундаментализации образования, формированию научного мировоззрения и развитию системного мышления.
Компетенции, формируемые в результате	После изучения курса "Информатика" выпускник должен обладать **следующими профессиональными компетенциями:** - Способен применять программные средства системного и прикладного назначений, в том числе отечественного производства, для решения задач профессиональной деятельности (ОПК-2);

освоения дисциплины	
Знания, умения и навыки, получаемые в процессе изучения дисциплины	Студент в рамках данного учебного курса **должен**: ***иметь представление:*** - об информатике как математической дисциплине, ее связи с прикладными науками; - об информации, методах ее хранения, обработки и передачи; - об информационных системах; - о позиционных системах счисления; - об архитектуре компьютера; - о средствах определения данных (типы данных, переменные), принятых в большинстве языков программирования; - о технологии проектирования сложных модульных программ; - о языках программирования; - о технологии проектирования сложных модульных программ; - о принципах взаимодействия программ, написанных на языках высокого уровня, с файлами данных; - о способах формирования изображений и цветопередачи в информационных системах; - о методах и средствах взаимодействия человека и ЭВМ; - об экономических и правовых аспектах информационных технологий. ***знать***: - основные принципы сбора, передачи и обработки информации; - основные этапы решения задач с помощью ЭВМ; - возможности ЭВМ для решения различных задач; - функции и структуру аппаратного и программного обеспечения ЭВМ; ***уметь***: - формализовать поставленную задачу; - применять полученные знания в различных предметных областях; ***владеть***: - навыками работы с компьютерами, с различными программными средами и оболочками.
Краткая характеристика учебной дисциплины (основные блоки и темы)	**СОДЕРЖАНИЕ ДИСЦИПЛИНЫ** **Введение. Основные понятия информации** Виды информации. Свойства информации. Определение количества информации. Общая характеристика процессов сбора, передачи, обработки и накопления информации. **1. Технические и программные средства реализации информационных процессов. Модели решения функциональных и вычислительных задач** Использование ЭВМ для реализации информационных процессов. Поколения ЭВМ. Классификация ЭВМ. Системы счисления. Элементы алгебры логики. Представление информации в памяти ЭВМ. Содержание методики. Постановка задачи, её анализ и выбор способа решения. Согласование методики с этапами работы на ЭВМ. **2. Алгоритмизация и программирование. Языки программирования высокого уровня** Понятие алгоритма. Свойства алгоритма. Способы записи алгоритмов. Элементарные алгоритмические конструкции. Методы разработки алгоритмов. Способы записи алгоритмов. Принципы структурного

	программирования. Основные алгоритмические структуры и их суперпозиции. Роль и характеристика языков программирования. История развития языков программирования. Основные понятия языков программирования. Алфавит, синтаксис, семантика. Понятие переменной. Классификация языков программирования. Структура программы на языке высокого уровня, преставление текста программы, оформление программы. Реализация операции и операторов языка высокого уровня на языке ассемблера. Перспективы развития языков программирования. **3. Основы и методы защиты информации** Основные понятия. Методы защиты информации. Технические и программные способы защиты информации. «Электронные» ключи. «Электронная подпись». **4. Средства и алгоритмы представления, хранения и обработки текстовой и числовой информации. Программные среды** Простой и бинарный поиск. Сортировки: выбором, обменом, вставкой. Анализ сложности алгоритмов на примере сортировок. Динамически распределяемая память и ее использование при работе со стандартными типами данных. Однонаправленные списки. Двунаправленные списки. Стеки. Очереди. Деки. Двоичные деревья поиска. Понятие системного программного обеспечения: назначение, возможности, структура. Операционные системы для различных ЭВМ: файловая система, система управления работой пользователей, командные языки. Трансляторы. ОС Unix: назначение, структура, понятие процесса, иерархия процессов, организация доступа к объектам. ОС Windows: компоненты, подсистемы, диспетчеры программ, файлов, печати, панель управления. **5. Организация и средства человеко-машинного интерфейса, мультисреды и гиперсреды** Понятие человеко-машинного интерфейса. Основные типы интерфейсов. Элементы создания интерфейса. Многопользовательские системы. Гипертекст. Принципы формирования и функционирования мультисред и гиперсред. **6. Назначение и основы использования систем искусственного интеллекта** Основные понятия систем искусственного интеллекта. Направления разработки искусственного интеллекта: распознавание образов, распознавание речи, системы интеллектуального управления. **7. Понятие об информационных технологиях на сетях. Основы телекоммуникаций и распределенной обработки информации** Назначение и возможностей. Формы использования компьютерных сетей. Организация информационных потоков в сетях. Электронная почта. Электронные конференции и электронные доски объявлений. Информационно-справочные системы. Проблемы и перспективы развития вычислительной техники и программирования. Многомашинные и мультипроцессорные вычислительные системы. **8. Понятие об экономических и правовых аспектах информационных технологий, аксиоматический метод** Правовые аспекты разработки и эксплуатации программных средств. Защита программных продуктов от несанкционированного использования и

	распространения. Преступления в сфере компьютерной информации и ответственность за них. Маркетинг программных продуктов. Стандартизация и сертификация программных продуктов и информационных технологий. **ТЕМЫ ЛАБОРАТОРНЫХ РАБОТ** 1. Разработка линейных алгоритмов. 2. Разработка алгоритмов с ветвлением. 3. Разработка циклических алгоритмов (циклы спред- и постусловием, цикл с параметром). 4. Трассировка алгоритма. 5. Разработка алгоритмов с подпрограммами. 6. Однонаправленные списки. 7. Двунаправленные списки. 8. Стеки. 9. Очереди. 10. Деки. 11. Двоичные деревья поиска. 12. Организация защиты информации в ОС Windows. 13. Принципы разработки программного способа защиты информации. 14. Методы шифрования информации. 15. Правила разработки пользовательского интерфейса. 16. Типы многооконного интерфейса. 17. Разработка многопользовательского программного продукта. 18. Создание гипертекстовой системы.
Трудоёмкость (з.е. / часы)	**7 ЗЕ/252** часов
Форма итогового контроля знаний	***экзамен***

Аннотация учебной дисциплины

Учебная дисциплина **«ДИФФЕРЕНЦИАЛЬНЫЕ УРАВНЕНИЯ»**	
Цель изучения дисциплины	Целью курса является изучение теории дифференциальных уравнений и методики решения задач в указанной области, получение студентами представления о роли и месте теории обыкновенных дифференциальных уравнений в фундаментальных и прикладных науках.
Компетенции, формируемые в результате освоения дисциплины	Процесс изучения дисциплины направлен на формирование следующих ***компетенций***: - Способен на основании совокупности математических методов разрабатывать, обосновывать и реализовывать процедуры решения задач профессиональной деятельности (ОПК-3).
Знания, умения и навыки, получаемые в процессе	В результате изучения дисциплины студенты должны: иметь представление об основных типах задач, возникающих в теории дифференциальных уравнений; знать содержание основных разделов теории дифференциальных уравнений;

изучения дисциплины	уметь использовать аппарат дифференциальных уравнений в процессе проведения самостоятельных исследований; иметь навыки применения стандартных алгоритмов нахождения решений типовых дифференциальных уравнений и исследования решений на устойчивость.
Краткая характеристика учебной дисциплины (основные блоки и темы)	**Содержание основных разделов и тем курса** **Понятие дифференциального уравнения** Геометрическая интерпретация: расширенное фазовое пространство, поле направлений, интегральные кривые, изоклины. Элементарные методы интегрирования дифференциальных уравнений. **Теорема существования и единственности решения задачи Коши для систем и уравнений произвольного порядка.** Теорема о продолжении решений. Непрерывная зависимость решений от начальных значений **Общая теория дифференциальных систем и уравнений.** Определитель Вронского, формула Лиувилля-Остроградского. Метод вариации постоянных. Линейные уравнения и системы с постоянными коэффициентами. Уравнения и системы со специальной правой частью. Экспонента матрицы **Фазовое пространство** Векторное поле, фазовые кривые, фазовый портрет **Нули решений** Теоремы сравнения (Штурма). Краевые задачи, функция Грина **Устойчивость по Ляпунову и асимптотическая устойчивость.** Критерий устойчивости линейной системы с постоянными коэффициентами. Теорема Ляпунова об устойчивости по первому приближению. Функция Ляпунова **Фазовая плоскость.** Классификация линейных особых точек на плоскости: узел, седло, фокус, центр. Предельный цикл. **Дифференцируемость решения по параметру и начальным данным. Уравнения в вариациях** Непрерывная зависимость решений от параметра и начальных условий. Дифференциальная зависимость решения от параметра и начальных условий. Уравнения в вариациях **Первые интегралы автономной системы.** Существование полной системы первых интегралов**0** **Линейные и квазилинейные уравнения с частными производными первого порядка.** Характеристики. Задача Коши. Теорема существования и единственности решения задачи Коши **Тематика практических занятий** 1. Геометрическая интерпретация: расширенное фазовое пространство, поле направлений, интегральные кривые, изоклины. 2. Элементарные методы интегрирования дифференциальных уравнений. 3. Формула Лиувилля-Остроградского. Метод вариации постоянных. 4. Линейные уравнения и системы с постоянными коэффициентами. 5. Уравнения и системы со специальной правой частью.. 6. Нули решений, теоремы сравнения (Штурма). 7. Краевые задачи, функция Грина. 8. Устойчивость по Ляпунову и асимптотическая устойчивость.

	9. Классификация линейных особых точек на плоскости: узел, седло, фокус, центр. 10. Первые интегралы автономной системы. 11. Линейные и квазилинейные уравнения с частными производными первого порядка.
Трудоёмкость (з.е. / часы)	**3** ЗЕТ / **108** часов
Форма итогового контроля знаний	**Зачет.**

Аннотация учебной дисциплины

Учебная дисциплина **«КОМПЛЕКСНЫЙ АНАЛИЗ»**	
Цель изучения дисциплины	Целями освоения дисциплины «Теория функции комплексного переменного»являются: 1) фундаментальная подготовка в области комплексного анализа; 2) освоение методов работы с функциями комплексного переменного и отображениями комплексной плоскости, 3) обучения основам применения теории функций комплексного переменного в естественнонаучных, математических и профессиональных дисциплинах, 4) овладение современным математическим аппаратом для дальнейшего использования в приложениях.
Компетенции, формируемые в результате освоения дисциплины	Процесс изучения дисциплины направлен на формирование следующих компетенций: - Способен на основании совокупности математических методов разрабатывать, обосновывать и реализовывать процедуры решения задач профессиональной деятельности (ОПК-3).
Знания, умения и навыки, получаемые в процессе изучения дисциплины	В результате освоения дисциплины студент должен: ***Знать***: 1. Основные свойства поля комплексных чисел. 2. Основные понятия функций комплексного переменного (производная, дифференцируемость, условия Коши-Римана, голоморфность). 3. Основные определения: интеграла по комплексному переменному, рядов голоморфных функций, рядов Лорана, теории вычетов. ***Уметь***: 1. Находить пределы числовых последовательностей и функций. 2. Находить производные. 3. Восстанавливать голоморфную функцию по ее вещественной или мнимой части. 4. Находить различные интегралы по комплексному переменному. 5. Разлагать функции в степенные ряды и ряды Лорана. 6. Находить вычеты и их использовать в определении интегралов. 7. Строить римановы поверхности для элементарных функций. ***Владеть***: 1. Техникой конформных отображений.

	2. Техникой построения рядов Лорана. 3. Техникой интегрирования по комплексному переменному.
Краткая характеристика учебной дисциплины (основные блоки и темы)	**Раздел 1. Предел. Непрерывность. Дифференциальное исчисление функций комплексного переменного** **1. Комплексные числа.** Определение и действия с комплексными числами. Модуль и аргумент комплексного числа. Простейшие свойства. Расширенная комплексная плоскость. Последовательности и ряды комплексных чисел **Функции комплексного переменного.** Предел и непрерывность. Голоморфные функции. Условия Коши-Римана. Правила дифференцирования. Дифференцирование сложной и обратной функций. Степенные ряды в комплексной области **Однолистные и многозначные функции.** Экспонента и логарифмы в комплексной области. Области однолистности, дифференцируемость. Функция $\mathrm{Ln}z$ и её стандартные ветви. Функция $\ln z$ и её свойства. Многозначная функция z^n **Раздел 2. Интегральное исчисление функций комплексного переменного** **Основные определения и простейшие свойства.** Гладкие пути. Дифференциальные формы. Криволинейные интегралы по гладким и составным путям. Гомотопия. Односвязные и звездные области. Формула Грина. Интеграл типа Коши. **Формула Коши для круга.** Аналитические функции, их бесконечная дифференцируемость. Свойства аналитических функций. Ряды Тейлора. Разложение в ряд Тейлора аналитических функций. Целые функции. Теорема Лиувилля. Основная теорема алгебры. Принцип максимума модуля. Гармонические функции и их связь с аналитическими функциями. **Формула Коши для кольца.** Ряды Лорана. Представление аналитических функций рядами Лорана и единственность таких представлений **2. Особые точки.** Изолированные особые точки и их классификация. Поведение аналитической функции в окрестности изолированной особой точки. Теорема Сохоцкого. Нули и полюсы аналитических функций. Мероморфные функции. Вычеты. Основная теорема о вычетах. Принцип аргумента. Вычисление интегралов с помощью вычетов.
Трудоёмкость (з.е. / часы)	**3 ЗЕТ / 108 часов**
Форма итогового контроля знаний	***зачет***

Аннотация учебной дисциплины

Учебная дисциплина «*Теория вероятностей и математическая статистика*»

Цель изучения дисциплины	***Цели*** 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.
Компетенции, формируемые в результате освоения дисциплины	Процесс изучения дисциплины направлен на формирование следующих ***компетенций***: Способен на основании совокупности математических методов разрабатывать, обосновывать и реализовывать процедуры решения задач профессиональной деятельности (ОПК – 3).
Знания, умения и навыки, получаемые в процессе изучения дисциплины	В результате освоения дисциплины студент должен -*знать* аксиоматику, основные понятия и теоремы теории вероятностей и математической статистики; -*уметь* формулировать задачу, используя логический и вычислительный аппарат теории вероятностей и математической статистики, пользоваться расчетными формулами, таблицами, графиками при решении задач; вычислять выборочные характеристики и находить оценки неизвестных параметров; использовать критерии проверки статистических гипотез. -*владеть практическими навыками* построения и анализа вероятностных и статистических моделей; навыками работы с библиотеками прикладных программ для решения вероятностных и статистических прикладных задач.
Краткая Характеристика учебной дисциплины (основные блоки и темы)	**Содержание основных разделов (тем) курса** 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
Трудоёмкость (з.е. / часы)	Согласно рабочему учебному плану курс читается в полном объёме в течение 5 и 6 семестров **6** ЗЕТ / **216** часов.
Форма итогового	В конце 5-го семестра предусмотрен ***экзамен,*** в конце 6-го семестра предусмотрен **зачет с оценкой**.

контроля знаний	

Аннотация учебной дисциплины

Учебная дисциплина **«ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ»**	
Цель изучения дисциплины	**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. Изучение дисциплины “Основы информационной безопасности” должно развивать творческий подход при решении сложных научно-технических задач, связанных с обеспечением информационной безопасности государства и его информационной инфраструктуры; способствовать развитию профессиональной культуры, формированию научного мировоззрения и развитию системного мышления; прививать стремление к поиску оптимальных, простых и надежных решений; способствовать расширению кругозора.
Компетенции, формируемые в результате освоения дисциплины	Процесс изучения дисциплины направлен на формирование следующих ***компетенций***: - способен оценивать роль информации, информационных технологий и информационной безопасности в современном обществе, их значение для обеспечения объективных потребностей личности, общества и государства; (ОПК-1); - способен применять нормативные правовые акты, нормативные и методические документы, регламентирующие деятельность по защите информации (ОПК-5).
Знания, умения и навыки, получаемые в процессе изучения дисциплины	В результате изучения дисциплины «Основы информационной безопасности» студент должен: **знать**: – сущность и понятие информации, информационной безопасности и характеристику ее составляющих; – место и роль информационной безопасности в системе национальной безопасности Российской Федерации, основы государственной информационной политики, стратегию развития информационного общества в России; – источники и классификацию угроз информационной безопасности; – основные средства и способы обеспечения информационной безопасности, принципы построения систем защиты информации;

	уметь: – классифицировать защищаемую информацию по видам тайны и степеням конфиденциальности; – классифицировать и оценивать угрозы информационной безопасности для объекта информатизации; **владеть**: – профессиональной терминологией в области информационной безопасности; – средствами поиска, обобщения научно-технической информации, нормативных и методических материалов в сфере своей профессиональной деятельности.

Краткая характеристика учебной дисциплины (основные блоки и темы)	**Содержание основных разделов (тем) дисциплины** **1. Информационная безопасность Российской Федерации**. Угрозы информационной безопасности Российской Федерации. Доктрина информационной безопасности. Общие принципы защиты информации. Классификация угроз. **2. Безопасность (защищенность) компьютерных систем**. Обзор средств и методов информационной/компьютерной безопасности. Интегрированная программно-аппаратная защита информации TrustedPlatformModule (TPM). Методы нарушения конфиденциальности, целостности и доступности информации. Модели управления доступом. Контроль прав доступа. 3. **Модели нарушителя и типичные атаки**. Модель действий вероятного нарушителя и модель построения защиты. Классификация основных видов атак. Сетевая разведка. Средства и методы нейтрализации атак. 4. **Вредоносное программное обеспечение**. Классификация вредоносных программ. Признаки присутствия вредоносного ПО. Методы защиты. Методы обнаружения. Способы внедрения. Примеры сетевых атак. Троянские программы, люки, эксплойты. Технологии самозащиты. Место и роль межсетевых экранов в обеспечении безопасности ресурсов АС. Возможности и ограничения антивирусных программ. Специализированные средства и методы выявления вредоносных программ. 5. **Средства защиты и нападения.** Информационная война и информационное оружие. Особенности технических средств информационной войны. Классификация средств защиты и нападения. Классификация электронных устройств перехвата информации, внедряемых в средства вычислительной техники. Средства силового деструктивного воздействия (СДВ). 6. **Уничтожение информации**. Необходимость уничтожения документов. Особенности удаления информации с электронных носителей. Политика уничтожения данных. Уничтожение конфиденциальной информации (плановое и экстренное). Следы в сети. Уникальные идентификаторы интернет-пользователей и электронные "отпечатки". Конфиденциальность в социальных сетях. 7. **Защита информации от утечки по техническим каналам.** Утечки: понятие, виды. Типовые каналы утечки информации. Технические каналы утечки. Средства и методы обнаружения технических каналов утечки информации. Системы защиты конфиденциальных данных от внутренних угроз. Технология цифровых отпечатков. 8. **Компьютерно-техническая экспертиза.** Компьютерно-техническая экспертиза**.** Методы экспертизы. Проведение расследования компьютерных инцидентов. Исследование носителей компьютерной информации. Аппаратно-программные средства расследования компьютерных инцидентов.
Трудоёмкость (з.е. / часы)	**3 ЗЕ / 108** часов
Форма итогового контроля знаний	**Зачет, КР**

Аннотация учебной дисциплины

Учебная дисциплина **«ДИСКРЕТНАЯ МАТЕМАТИКА»**	
Цель изучения дисциплины	***Главной целью*** преподавания этой дисциплины является обеспечение формирования у студентов знаний по дискретной математике, а также навыков и умений в применении знаний в конкретных условиях деятельности, возникающих в ходе решения практических задач из области математики и компьютерной безопасности. Кроме того, целью дисциплины является развитие в процессе обучения системного и логического мышления, необходимого для решения задач дискретной математики с учетом требований системного подхода.
Компетенции, формируемые в результате освоения дисциплины	Изучение дисциплины нацелено на формирование следующих компетенций обучающихся: - Способен на основании совокупности математических методов разрабатывать, обосновывать и реализовывать процедуры решения задач профессиональной деятельности (ОПК-3)
Знания, умения и навыки, получаемые в процессе изучения дисциплины	Студент, изучивший курс, должен ***иметь представление***: 1. О стандартных методах и моделях дискретной математики и их применении к решению прикладных задач. Студент должен ***знать:*** 1. Основные понятия и методы дискретной математики, включая дискретные функции, конечные автоматы, комбинаторный анализ и теорию графов. Студент должен ***уметь:*** 1. Применять аппарат производящих функций и рекуррентных соотношений для решения перечислительных задач. 2. Пользоваться математическим аппаратом дискретной математики.
Краткая характеристика учебной дисциплины (основные блоки и темы)	**Содержание основных разделов (тем) курса** **Введение** Предмет курса. Принципы построения и изучения курса. Краткое содержание. Роль и место курса в формировании специалистов. Рекомендации по изучению курса, самостоятельной работе и литературе. **Тема 1. Основы теории графов** Графы и орграфы. Степени. Теорема Эйлера о сумме степеней. Изоморфизмы. Группа автоморфизмов. Пути. Маршруты. Разложение графа на компоненты связности. **Тема 2. Циклы в графах** Цикломатическое число. Пространство и базис циклов. Соотношение между числами независимых циклов, вершин, ребер и компонент. Разрезы. **Тема 3. Деревья** Теорема о характеризации деревьев. Остовы графа. Наименьший остов. Реберная и вершинная связность. Неравенство Уитни-Харари. **Тема 4. Эйлеровы графы** Необходимые и достаточные условия. Построение эйлеровой цепи. **Тема 5. Планарные графы**

	Теорема о том, что K_5 и $K_{3,3}$ не планарны. Теорема Куратовского (без доказательства). Критерий планарности (без доказательства). **Тема 6. Некоторые применения теории графов** 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. Графы, связанные с группами. **Тема 7. Основные определения теории автоматов** Конечные автоматы. Определение конечного автомата. Частные виды. Примеры. Подавтоматы, гомоморфизмы и конгруэнции. Операции с автоматами. Способы задания автоматов. Автоматные базисы и проблема полноты. **Тема 8. Эквивалентность в автоматах** Эквивалентность состояний автоматов. Эквивалентность автоматов. Некоторые обобщения понятия эквивалентности и гомоморфизма. **Тема 9. Функционирование автоматов** Обратимость автоматов и автоматы БПИ. Автоматы с конечной памятью. Цепочки и языки. Автоматные языки. Понятие формальной грамматики. Примеры грамматик. Бесконтекстные грамматики. Применение грамматик для построения языков высокого уровня, в частности для языков программирования. **Тема 10. Эксперименты с автоматами** Основные понятия теории экспериментов с автоматами. Диагностические эксперименты. Установочные эксперименты. Эксперименты по распознаванию автоматов. Тестирование автоматов. Тестирование комбинационных схем. Методы построения тестов. Вероятностное тестирование. Оценки вероятности обнаружения неисправности. Псевдослучайное тестирование. **Тема 11. Вероятностные автоматы** Определение и частные виды. Декомпозиция. Эквивалентность состояний. Применения. **Тема 12. Основные комбинаторные методы** Принцип сложения и умножения. Подмножества. Примеры использования принципа сложения и умножения. Принцип включения и исключения. Выборки. Размещениями с повторениями. Размещения без повторений. Сочетания без повторений. Бином Ньютона и полиномиальная формула (комбинаторный смысл). Сочетания с повторениями. Перестановки без повторений. Свойства перестановок. Перестановки без повторений. Таблица инверсий. Задача о разупорядочении. Субфакториалы. Перестановки с повторениями. Задача о размещениях. **Тема 13. Рекуррентные соотношения** Простые примеры рекуррентных последовательностей. Числа Фибоначчи. Свойства чисел Фибоначчи. Нерекуррентная формула для чисел Фибоначчи. Вывод нерекуррентной формулы для чисел Фибоначчи с помощью производящей функции. Фибоначчиева система счисления. Числа Каталана. Нелинейная рекуррентная формула. Нерекуррентная формула. Задача о триангуляции многоугольника. Пути Дика. **Тема 14. Числа Стирлинга и их свойства** Разбиения. Числа Стирлинга второго рода. Числа Белла. Разбиения на циклы. Числа Стирлинга первого рода. Разбиение числа на слагаемые.

	Тема 15. Производящие функции Рекуррентные соотношения и производящие функции. Производящие функции. Задача о расстановке чёрных и белых шаров. Операции над рядами. Производящие функции. Примеры. **Тема 16. Ладейные полиномы** Ладейные полиномы. Связь ладейных полиномов с перестановками. Примеры. **Тема 17. Комбинаторные методы в решении экстремальных задач** Латинские прямоугольники и квадраты. Ортогональные латинские квадраты. Матрицы Адамара. Перечисление графов отображений. Экстремальные задачи и перебор. Оптимизационные задачи. Универсальные задачи. Метод ветвей и границ. Комбинаторные конфигурации, блок-схемы. Трансверсали. Конечные проективные плоскости. Перечисление графов и отображений. **3.2. Тематика практических занятий** **Тема 1.** Основы теории графов. **Тема 2.** Циклы в графах. **Тема 3.** Деревья. **Тема 4.** Эйлеровы графы. **Тема 5.** Планарные графы. **Тема 6.** Некоторые применения теории графов. **Тема 7.** Основные определения теории автоматов. **Тема 8.** Эквивалентность в автоматах. **Тема 9.** Функционирование автоматов. **Тема 10.** Эксперименты с автоматами. **Тема 11.** Вероятностные автоматы. **Тема 12.** Основные комбинаторные методы. **Тема 13.** Рекуррентные соотношения. **Тема 14.** Числа Стирлинга и их свойства. **Тема 15.** Производящие функции. **Тема 16.** Ладейные полиномы. **Тема 17.** Комбинаторные методы в решении экстремальных задач.
Трудоёмкость (з.е. / часы)	**6** ЗЕ /**216** часа.
Форма итогового контроля знаний	***Экзамен***.

Аннотация учебной дисциплины

Учебная дисциплина **"МАТЕМАТИЧЕСКАЯ ЛОГИКА И ТЕОРИЯ АЛГОРИТМОВ"**	
Цель изучения дисциплины	***Целью*** освоения дисциплины ***"Математическая логика и теория алгоритмов***" является изучение студентами основных разделов математической логики и теории алгоритмов, ознакомление с формализацией математического языка, с формальным аксиоматическим

	методом построения математических теорий, обучение методам логического вывода, ознакомление с методами оценки сложности алгоритмов и построения эффективных алгоритмов, формирование системного мышления.
Компетенции, формируемые в результате освоения дисциплины	Изучение дисциплины нацелено на формирование следующих ***компетенций*** обучающихся: - Способен на основании совокупности математических методов разрабатывать, обосновывать и реализовывать процедуры решения задач профессиональной деятельности (ОПК-3).
Знания, умения и навыки, получаемые в процессе изучения дисциплины	Студент, изучивший курс, должен ***знать:*** • основные понятия математической логики и теории алгоритмов; • язык и средства современной математической логики; • представления булевых функций и способы минимизации формул; • типовые свойства и способы задания функций многозначной логики; • различные подходы к определению алгоритма и доказательства алгоритмической неразрешимости отдельных массовых задач; • подходы к оценкам сложности алгоритмов; • методы построения эффективных алгоритмов; • возможности применения общих логических принципов в математике и профессиональной деятельности. Студент должен ***уметь:*** • находить и исследовать свойства представлений булевых и многозначных функций формулами в различных базисах; • оценивать сложность алгоритмов и вычислений; • классифицировать алгоритмы по классам сложности; • применять методы математической логики и теории алгоритмов к решению задач математической кибернетики; Студент должен ***владеть:*** • навыками использования языка современной символической логики; • навыками применения методов и фактов теории алгоритмов, относящимися к решению переборных задач; • навыками упрощения формул алгебры высказываний и алгебры предикатов; • навыками составления программ на машинах Тьюринга.
Краткая характеристика учебной дисциплины (основные блоки и темы)	**Содержание основных разделов (тем) курса** **Введение** История развития математической логики и теории алгоритмов. Математическая логика и основания математики. Теория алгоритмов и принципиальные возможности вычислительных машин. Сложность алгоритмов и ее значение для практики **Тема 1. Алгебра высказываний и алгебра предикатов** Основные логические операции и их свойства. Понятие булевой алгебры. Алгебра высказываний и алгебра подмножеств, множества как примеры булевых алгебр. Предикаты на множестве и их связь с отношениями. Логические операции над предикатами. Определение формулы алгебры предикатов. Выполнимые, тождественно истинные и тождественно ложные формулы. Равносильность формул, основные

	соотношения равносильности и их использование для упрощения формул. Существование для каждой формулы алгебры высказываний приведенной формы, дизъюнктивной и конъюнктивной нормальных форм. **Тема 2. Булевы функции и их обобщение** Понятие булевой функции и функции многозначной логики. Их представление формулами над заданной системой функций. Представление булевых функций формулами алгебры высказываний и многочленами Жегалкина. Замкнутые классы функций. Критерии полноты для булевых функций и функций многозначной логики. Представление функций многозначной логики рядами Фурье. Методы вычисления коэффициентов Фурье. Псевдобулевы функции и их задание. Минимизация булевых функций. **Тема 3. Исчисление высказываний** Общее понятие о логическом исчислении. Язык, аксиомы и правила вывода исчисления высказываний. Выводимость и доказуемость формул в исчислении высказываний. Теорема дедукции. Непротиворечивость и полнота исчисления высказываний. **Тема 4. Исчисление предикатов** Язык, аксиомы и правила вывода исчисления предикатов. Выводимость и доказуемость формул в исчислении предикатов. Вспомогательные правила вывода: правило силлогизма, правила умножения и разделения формул, правила умножения и разделения посылок, правило умножения заключений, правило перестановки посылок, правило контрапозиции, правила де Моргана, правила противоречия, закон исключенного третьего. Теорема дедукции для замкнутой формулы. Эквивалентность формул. Приведение формул к нормальным формам. Понятие об интерпретации исчисления предикатов. Непротиворечивость исчисления предикатов. Непротиворечивые, полные и выполнимые системы формул. Теорема Геделя о полноте исчисления предикатов. Элементы теории моделей. Теорема Мальцева о компактности и ее приложения. Применение исчисления предикатов для записи математических утверждений и для автоматического доказательства теорем. **Тема 5. Метод резолюции** Применение исчисления предикатов для доказательства теорем. Секвенциальный и натуральный вывод в исчислении предикатов. Эрбановские интерпретации. Теорема Эрбрана. Сколемовская стандартная форма. Семантические деревья. Метод резолюции для логики предикатов. Унификация. Теорема о наиболее общем унификаторе. Теорема о полноте метода резолюции для логики предикатов. Применение логики предикатов в дедуктивных базах данных и экспертных системах. Основные понятия логического программирования: хорновские дизъюниты, SLD - резолюция. Методика составления и реализация логических программ. **Тема 6. Элементы теории алгоритмов** Интуитивное понятие алгоритма и его характерные черты. Необходимость уточнения понятия алгоритма. Определение нормального алгоритма. Примеры. Принцип Маркова. Композиция нормальных алгоритмов. Определение машины Тьюринга-Поста. Принцип Тьюринга-Поста. **Тема 7. Алгоритмическая разрешимость и неразрешимость**

	Нумерация слов в счетном алфавите и арифметизация алгоритмов. Определение рекурсивных и частично рекурсивных функций. Примеры. Соотношения между классами примитивно рекурсивных, общерекурсивных и частично рекурсивных функций. Примеры алгоритмически неразрешимых массовых задач. Примеры алгоритмически разрешимых и неразрешимых задач из алгебры и теории автоматов (без доказательства). Теорема Черча о неразрешимости исчислений предикатов (без доказательства). **Тема 8. Сложность алгоритмов и вычислений** Подходы к оценкам сложности алгоритмов и вычислений. Модели вычислений. Сложность вычисления на машине Тьюринга. Меры сложности. Свойства функций сложности. Нижние оценки. Сложности вычисления. Метод следов. Сложность распознавания симметрии слов. Сложность распознавания функциональной полноты системы булевых функций. Существование сколь угодно сложно вычислимых функций. **Тема 9. Методы построения эффективных алгоритмов** Метод разбиения и рекурсии. Сложность рекурсивных алгоритмов. Умножение чисел и матриц. Быстрое преобразование Фурье. **Тема 10. Сложностная классификация переборных задач** Класс задач, детерминировано решаемых с полиномиальной сложностью. Класс задач, решаемых с полиномиальной сложностью на недетерминированной машине Тьюринга. Полиномиальная сводимость. NP-полные и NP-трудные задачи. **Тема 11. Теория алгоритмов и задачи использования ЭВМ** Вычислительные возможности современных ЭВМ. Модель ЭВМ - машина произвольного доступа (МПД).МПД - вычислимые функции и их связь с частично рекурсивными функциями. **Тематика практических занятий** **Тема 1.** Алгебра высказываний и алгебра предикатов. **Тема 2.** Булевы функции и их обобщение. **Тема 3.** Исчисление высказываний. **Тема 4.** Исчисление предикатов. **Тема 5.** Метод резолюции. **Тема 6.** Элементы теории алгоритмов. **Тема 7.** Алгоритмическая разрешимость и неразрешимость. **Тема 8.** Сложность алгоритмов и вычислений. **Тема 9.** Методы построения эффективных алгоритмов. **Тема 10.** Сложностная классификация переборных задач. **Тема 11.** Теория алгоритмов и задачи использования ЭВМ.
Трудоёмкость (з.е. / часы)	Курс ***“Математической логики и теории алгоритмов”*** изучается в 4 семестре **6 ЗЕТ / 216** часов.
Форма итогового контроля знаний	***зачёт***

Аннотация учебной дисциплины

Учебная дисциплина **«МЕТОДЫ ПРОГРАММИРОВАНИЯ»**	
Цель изучения дисциплины	**Цель** освоения дисциплины «Методы программирования»: научить студентов решать прикладные задачи численными методами с использованием компьютера.
Компетенции, формируемые в результате освоения дисциплины	**Компетенции**, формируемые у студентов в результате освоении дисциплины «Методы программирования»: - 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); - Способен разрабатывать компоненты программных и программно-аппаратных средств защиты информации в компьютерных системах и проводить анализ их безопасности (ОПК-13);
Знания, умения и навыки, получаемые в процессе изучения дисциплины	Знать: - основные характеристики численного метода: погрешность, сходимость, невязка, устойчивость численного решения; - основные численные методы решения задач теории функций и их характеристики; - основные численные методы решения задач алгебры и их характеристики; - основные численные методы решения задач математической физикии их характеристики; Уметь: - выбрать подходящий численный метод решения типовых математических задач; - применять на практике численные методы решения основных задач анализа, алгебры, математической физики. Владеть: - методологией и навыками решения научных и практических задач.
Краткая характеристика учебной дисциплины (основные блоки и темы)	Тема 1. Особенности математических вычислений, реализуемых на ЭВМ. Представление чисел в форме с фиксированной и плавающей запятой, диапазон и погрешности представления. Операции над числами, свойства арифметических операций. Тема 2. Теоретические основы численных методов. Погрешности вычислений. Устойчивость и сложность алгоритма по памяти, по времени. Тема 3. Численные методы линейной алгебры. Основные задачи линейной алгебры, метод Гаусса. Метод простой итерации, теорема о достаточном условии сходимости, необходимое и достаточное условие сходимости. Метод Зейделя. Проблема собственных значений. Тема 4. Решение нелинейных уравнений и систем.

	Методы решения нелинейных уравнений: метод бисекций, метод простой итерации и метод Ньютона. Тема 5. Интерполяция функций. Постановка задачи интерполяции. Интерполяционный многочлен Лагранжа. Его существование и единственность. Оценка погрешности интерполяционной формулы Лагранжа. Понятие о количестве арифметических операций, как об одном из критериев оценки качества алгоритма. Тема 6. Методы приближения функций. Наилучшее приближение в нормированном пространстве. Существование элемента наилучшего приближения. Чебышевский альтернанс, единственность многочлена наилучшего приближения. Тема 7. Равномерное приближение функций. Ортогональные многочлены. Процесс ортогонализации Шмидта. Запись многочлена в виде разложения по ортогональным многочленам. Тема 8. Решение обыкновенных дифференциальных уравнений. Метод разложения в ряд Тейлора решения задачи Коши для ОДУ. Метод Эйлера и его модификации, методы Рунге-Кутта. Тема 9. Численное интегрирование и дифференцирование. Интегрирование сильно осциллирующих функций. Вычисление интегралов в нерегулярных случаях. Численное дифференцирование, вычислительная погрешность формул численного дифференцирования. Правило Рунге оценки погрешности. Тема 10. Преобразование Фурье, Уолша, быстрое преобразование Фурье. Преобразование Фурье, Уолша, быстрое преобразование Фурье. Тема 11. Обзор и анализ численных методов, применяемых в пакетах программ линейной алгебры. Метод простой итерации, необходимое и достаточное условие сходимости. Процесс ускорения сходимости итераций. Метод наискорейшего градиентного спуска.
Трудоёмкость (з.е. / часы)	Согласно рабочему учебному плану курс читается в полном объёме в течение **4** семестра **8** ЗЕ / **288** часов.
Форма итогового контроля знаний	В конце **4**-го семестра предусмотрен **зачет**.

Аннотация учебной дисциплины

Учебная дисциплина **«ТЕОРИЯ ПСЕВДОСЛУЧАЙНЫХ ГЕНЕРАТОРОВ»**

Цель изучения дисциплины	***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
Компетенции, формируемые в результате освоения дисциплины	Процесс изучения дисциплины направлен на формирование следующих ***компетенций***: − Способен разрабатывать и анализировать математические модели механизмов защиты информации (ОПК-2.2)
Знания, умения и навыки, получаемые в процессе изучения дисциплины	В результате освоения дисциплины обучающийся должен ***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.

Краткая характеристика учебной дисциплины (основные блоки и темы)	Содержание основных разделов (тем) курса **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.
Трудоёмкость (з.е. / часы)	Согласно рабочему учебному плану курс читается в полном объёме в течение **5** семестра **6** ЗЕ / **216** часов.

Форма итогового контроля знаний	В конце семестра предусмотрен **экзамен**.

Учебная дисциплина **«КОМПЬЮТЕРНЫЕ СЕТИ»**	
Цель изучения дисциплины	**Цель дисциплины** - обеспечить знание теоретических и практических основ в организации и функционировании компьютерных сетей, умение применять в профессиональной деятельности распределенные данные, программы и ресурсы сетей.
Компетенции, формируемые в результате освоения дисциплины	**В результате изучения дисциплины у студентов должны быть сформированы следующие компетенции:** - Способен администрировать компьютерные сети и контролировать корректность их функционирования (ОПК-15);
Знания, умения и навыки, получаемые в процессе изучения дисциплины	**В результате изучения дисциплины студенты должны:** **I. ЗНАТЬ:** • технологии и принципы построения компьютерных сетей; • принципы функционирования и взаимодействия аппаратных и программных средств компьютерной техники; • способы настройки ОС Microsoft Windows для работы в сетях; • сетевые прикладные программы; • прикладные программы для создания Web-сайтов и Web-страниц; • Российские и международные поисковые средства в Internet; • основные возможности электронного бизнеса и коммерции. **II. УМЕТЬ:** • использовать вычислительные системы и сети передачи данных в профессиональной деятельности; • подключать ПК к сетям, и работать в сетях; • работать с сетевыми прикладными программами; • создавать и оформлять Web-страницы и Web-сайты. **III. ВЛАДЕТЬ ПРАКТИЧЕСКИМИ НАВЫКАМИ:** • работы с механизмами передачи данных по каналам связи; • работы с возможными ресурсами локальных сетей • работы с сервисом сети Internet.
Краткая характеристика учебной дисциплины (основные	**Содержание тем дисциплины** ***Тема 1. Введение. Основы организации и функционирования вычислительных сетей*** 1.1. Проблемы распределенной обработки данных. Задачи и проблемы распределенной обработки данных. 1.2. Классификация сетей по способам распределения данных, сравнительная характеристика различных типов сетей. 1.3 Основы организации и функционирования сетей. 1.4. Сетевые стандарты верхних уровней OSI-модели.

блоки и темы)	1.5. Сетевые операционные системы. Обзор сетевых средств на примере операционной системы (ОС) UNIX. ***Тема 2. Уровни сессий и представлений*** 2.1. Основные сетевые стандарты. 2.2 Средства взаимодействия процессов в сетях. 2.3 Распределенная обработка информации в системах клиент-сервер. 2.4 Взаимодействие клиент-сервер и удаленный вызов процедур. 2.2. Особенности протокола TCP/IP 2.3. Интерфейс TLI 2.4. Интерфейс Berkley Sockets **Тема 3. Прикладной уровень вычислительных сетей** 3.1. Архитектура клиент-сервер 3.2 Одноранговые сети. 3.3 Средства идентификации и аутентификации. 3.4. Сетевые графические пользовательские интерфейсы 3.5. Файловая система NFS и информационная служба NIS 3.6. Серверы баз данных, серверы приложений и почтовые серверы 3.7. Протокол SMTP 3.8. Стандарты удаленных терминалов **Тема 4. Сетевые операционные системы Novell NetWare и Windows NT** 4.1. Архитектура сетевой ОС NetWare и Windows NT. Средства повышения надежности функционирования сетей. 4.2. Средства разработки сетевых приложений для среды NetWare и Windows NT. 4.3. Интеграция NetWare и Windows NT с другими сетями. 4.4 Интеграция локальных сетей в региональные и глобальные сети, неоднородные вычислительные сети. **Тема 5. Сети IBM SNA, DECNet и AppleTalk** 5.1. Архитектура сети SNA: организация и функционирование сетей SNA. 5.2. Архитектура сети DECNet 5.3. Архитектура сети AppleTalk **Тема 6. Средства и методы организации вычислительных сетей** 6.1. Маршрутизаторы, мосты, узлы коммутации пакетов. Серверы удаленного доступа. Основные принципы управления ими 6.2. Некоторые принципы проектирования топологии локальных и глобальных сетей. 6.3. Тенденции и перспективы развития сетевых технологий 6.4 Организация сетей на базе операционной системы UNIX: основные протоколы, службы, функционирование, сопровождение и разработка приложений, особенности реализации на различных платформах. 6.5 Организация сетей на базе операционной системы NetWare: основные протоколы, службы, функционирование, генерация, сопровождение и разработка приложений. 6.6 Организация сетей на базе операционной системы Windows NT: основные протоколы, службы, функционирование, генерация, сопровождение и разработка приложений. 6.7 Глобальные сети: Internet, основные службы и предоставляемые услуги, стандарты,перспективы развития. 6.8 Организация корпоративных сетей интернет. **Тема 7. Прикладные сетевые сервисы**

	7.1 DomainNameSystem (DNS). Структура доменных имен. Авторизованные серверы и делегирование ответственности. Понятия сервера и ресолвера DNS, зоны, записи ресурса. Алгоритм разрешения имен. Прямое и обратное разрешение имен. Формат записи ресурса. Типы записей SOA, NS, A, CNAME, PTR, MX, SRV. Реализации сервера DNS для UNIX и Windows. 7.2 Dynamic Host Configuration Protocol (DHCP). Понятия область, исключаемый диапазон, пул адресов, аренда, резервирование. Параметры, настраиваемые на DHCP-сервере. Получение и продление лицензии DHCP-клиентом. 7.3 Доставка почты. Компоненты доставки почты. Конфигурация sendmail. Типовые случаи настройки почтового сервера. **Тема 8. Сетевая безопасность.** 8.1Проблема сетевой безопасности и терминология. Механизмы безопасности. 8.2Сервисы безопасности: неотрекаемость, целостность, конфиденциальность, аутентификация, защита от повторений, контроль доступа. IPSec. VPN. 8.3 Фильтрация пакетов на примере iptables. Правила, цепочки правил, таблицы. Условия отбора пакетов, действия над пакетами. Трансляция сетевых адресов.
Трудоёмкость (з.е. / часы)	**3** ЗЕ/**108** часов
Форма итогового контроля знаний	***зачёт***

Аннотация учебной дисциплины

Учебная дисциплина **«СИСТЕМЫ УПРАВЛЕНИЯ БАЗАМИ ДАННЫХ»**	
Цель изучения дисциплины	**Цель курса** – 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.
Компетенции, формируемые в результате освоения дисциплины	После изучения курса "Системы управления базами данных" выпускник должен обладать **следующей профессиональной компетенцией:** - Способен проектировать базы данных, администрировать системы управления базами данных в соответствии с требованиями по защите информации.
Знания, умения и навыки,	После изучения курса " Системы управления базами данных " студент **должен:**

получаемые в процессе изучения дисциплины	**знать**: - области построения и работы с базами данных. Инфологическое моделирование. Языковые средства современных СУБД. Даталогическое моделирование. Проектирование на физическом уровне. Средства и методы проектирования БД. Реляционные СУБД. СУБД на инвертированных файлах. Гипертекстовые и мультимедийные БД. XML-серверы. Объектно-ориентированные БД. Распределенные БД. Коммерческие БД. **уметь** - формулировать и представлять конкретные задачи на программирование, связанные с базами данных. **владеть** - навыками практической работы в одной из современных баз данных.
Краткая характеристика учебной дисциплины (основные блоки и темы)	**Содержание разделов дисциплины** **1. Базы данных и системы управления базой данных. Выбор системы управления базами данных. Жизненный цикл базы данных.** Информационные процессы. Информация. Представление информации. Автоматизированные информационные системы (АИС). Структура и классификация информационных систем. Система представления и обработки данных фактографических АИС. **2. Уровни моделей и этапы проектирования БД.** Иерархическая, сетевая и реляционная модели организации данных. Концептуальное и схемно-структурное проектирование. **3. Инфологическое моделирование** Основные понятия и этапы инфологического моделирования. **4. Языковые средства современных СУБД** Функции, классификация и структура СУБД. Языки программирования. Язык структурированных запросов SQL. **5. Даталогическое моделирование** Основные понятия и этапы даталогического моделирования. **6. Проектирование на физическом уровне** Проектирование схемы базы данных. Проектирование и создание таблиц. **7. Средства и методы проектирования БД** Проектирование с условием нормализации. Семантическое моделирование данных, ER-диаграммы. **8. Реляционные СУБД** Внутренняя схема базы данных. Физическая структура данных. Индексирование данных. Сильные и слабые стороны данных СУБД. **9. СУБД на инвертированных файлах** Внутренняя схема базы данных. Физическая структура данных. Индексирование данных. Сильные и слабые стороны данных СУБД. **10. Гипертекстовые и мультимедийные БД** Внутренняя схема базы данных. Физическая структура данных. Индексирование данных. Сильные и слабые стороны данных СУБД. **11. XML-серверы** Внутренняя схема базы данных. Физическая структура данных. Индексирование данных. Сильные и слабые стороны данных СУБД. **12. Объектно-ориентированные БД** Внутренняя схема базы данных. Физическая структура данных. Индексирование данных. Сильные и слабые стороны данных СУБД.

	13. Распределенные БД. Коммерческие БД Понятие распределенных информационных систем, принципы их создания и функционирования. Представления. Технологии и модели «Клиент-сервер». Модели файлового сервера, удаленного доступа к данным, сервера базы данных, сервера приложений. Мониторы транзакций. Технологии объектного связывания данных. Технологии реплицирования данных. Типы коммерческих БД. **14. Организация процессов обработки данных в БД. Ограничения целостности** Поиск, фильтрация и сортировка данных. Запросы. Процедуры, правила (триггеры) и события в базах данных. Особенности обработки данных в СУБД с сетевой моделью организации данных. Вывод данных. **15. Технология оперативной обработки транзакций (OLTP – технология). Информационные хранилища. OLAP – технология.** Управление транзакциями. Методы сериализация транзакций. Метод временных меток. **16. Проблема создания и сжатия больших информационных массивов, информационных хранилищ и складов данных. Управление складами данных.** Организация резервного копирования. Различные алгоритмы сжатия информации в базах данных. Архивирование информации в базах данных. Журнализация изменений БД. **17. Основные математические методы, применяемые при сжатии информации. Фрактальные методы в архивации.** Анализ основных математических методов сжатия информации: их сильные и слабые стороны. Понятие фракталов. Их применение для сжатия информации. **18. 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.
Трудоёмкость (з.е. / часы)	Согласно рабочему учебному плану курс читается в полном объёме в течение 5 и 6 семестра **7** ЗЕ / **252** часа.
Форма итогового контроля знаний	В конце **5**-го семестра предусмотрен **зачёт**, в конце **6**-го - ***экзамен***.

Аннотация учебной дисциплины

Учебная дисциплина **«ОПЕРАЦИОННЫЕ СИСТЕМЫ»**

Цель изучения дисциплины	***Целями*** освоения дисциплины «***Операционные системы***» являются: - изучение основных архитектурных особенностей операционных систем; - изучение ключевых понятий, присущих операционным системам; - изучение абстракций, предоставляемых операционными системами; - изучение основных принципов работы операционных систем.
Компетенции, формируемые в результате освоения дисциплины	- Способен администрировать операционные системы и выполнять работы по восстановлению работоспособности прикладного и системного программного обеспечения (ОПК-12);
Знания, умения и навыки, получаемые в процессе изучения дисциплины	Для успешного освоения дисциплины студенты должны знать: ***знать***: - основные понятия в области операционных систем; - архитектурные особенности операционных систем; - абстракции, предоставляемые операционными системами; - как осуществляется управление ресурсами в операционных системах. ***уметь***: - инсталлировать операционные системы; - диагностировать и исправлять неполадки в операционных системах; - управлять ресурсами в операционных системах; - управлять безопасностью в операционных системах. ***владеть***: - навыками установки операционных систем; - базовыми навыками назначения локальных политик безопасности; - навыками управления ресурсов операционной системы; - навыками резервирования и хранения данных.
Краткая характеристика учебной дисциплины (основные блоки и темы)	**Содержание основных разделов (тем) курса** **Тема 1.** Введение в операционные системы (ОС). Задачи и программа курса. Место курса «***Операционные системы***» в ряду других математических дисциплин. Формы самостоятельной работы студентов по изучению курса. Литература к курсу. Понятие ОС. Понятие программы. Отличия ОС от обычных программ. Назначение и функции ОС. Назначение и возможности систем клона UNIX, систем группы Windows. Обзор ОС. Клоны Unix и системы Windows. Понятия ОС. Прерывания. Обработка прерываний, стратегии и дисциплины диспетчеризации. Обработка исключений. Системные вызовы. Интерфейс ОС с пользователями. Классификация интерфейсов. Диалоговые и пакетные интерфейсы. Структура ОС. Виртуальные машины. Виртуальные программы. Сопровождение ОС. Задачи и принципы сопровождения системного программного обеспечения, генерация, настройка, измерение и модификация систем. **Тема 2.** Процессы и задачи. Планирование процессов. Понятие процессов. Виртуальные процессоры у процессов. Модель процесса. Создание процесса. Завершение процесса. Иерархия процессов. Наследование ресурсов. Зомби-процессы. Состояния процессов. Реализация процессов. Потоки. Применение потоков. Классическая модель потоков. Реализация потоков в пользовательском пространстве. Реализация потоков в

	ядре. Гибридная реализация. Активация планировщика. Синхронизация процессов. Обмен сообщениями. Состязательная ситуация. Критические области. Взаимное исключение с активным ожиданием. Приостановка и активизация. Планирование. Стратегии и дисциплины планирования. Планирование в пакетных системах. Планирование в интерактивных системах. Планирование в системах реального времени. **Тема 3.**Управление памятью. Понятие памяти. Типы реальной памяти и их основные характеристики. Иерархическая организация памяти. Кэш-память. Память без использования абстракций. Абстракции памяти. Свопинг. Виртуальная память. Представление виртуальной внешней памяти. Алгоритмы замещения страниц. Вопросы разработки систем страничной организации памяти. Вопросы реализации. Сегментация. **Тема 4.** Файловые системы. Назначение файловых систем. Понятие файла. Имена файлов. Типы файлов. Режимы использования. Доступ к файлам. Атрибуты файлов. Операции с файлами. Состав файловых систем. Каталоги. Системы с одноуровневыми каталогами. Иерархические системы каталогов. Операции с каталогами. Уровни и иерархия функций файловой системы. Реализация файловых систем. Структура файловой системы и ее элементы. Реализация файлов. Непрерывное размещение. Размещение с использованием связанного списка. Размещение с помощью связанного списка, использующего таблицу в памяти. i-узлы. Реализация каталогов. **Тема 5.** Ввод-вывод информации. Назначение и функции системы управления устройствами. Основы аппаратного обеспечения ввода-вывода. Устройства ввода-вывода. Контроллеры устройств. Ввод-вывод, отображаемый на пространство памяти. Управление операциями обмена: режимы управления вводом-выводом. Принципы создания программного обеспечения ввода-вывода. Задачи, стоящие перед программным обеспечением ввода-вывода. Программный ввод-вывод. Блокирование устройств. Активное ожидание. Ввод-вывод, управляемый прерываниями. Уровни программного обеспечения ввода-вывода. Обработчики прерываний. Драйверы внешних устройств. Программное обеспечение ввода-вывода, не зависящее от внешних устройств. Предоставление унифицированного интерфейса для драйверов устройств. Буферизация. Сообщения об ошибках. Распределение и высвобождение выделенных устройств. Предоставление размера блока, не зависящего от конкретных устройств. Программное обеспечение ввода-вывода, работающее в пространстве пользователя. Спулинг. **Тема 6.** Проблема тупиков и методы борьбы с ними. Ресурсы. Взаимоблокировки. Тупиковые ситуации. Исключения. Примеры тупиковых ситуаций. Виртуальные ресурсы. Виды и иерархия ресурсов. Запрос ресурса. Понятия стратегии и дисциплины управления ресурсами. Условия возникновения ресурсных взаимоблокировок. Моделирование взаимоблокировок. Обнаружение взаимоблокировок. Страусиный алгоритм. Обнаружение взаимоблокировок. Сохранение и восстановление процессов. Восстановление за счет приоритетного овладения ресурсом. Восстановление путем отката. Восстановление путем уничтожения процессов. Уклонение от взаимоблокировок. Траектории ресурса. Безопасное и

	небезопасное состояние. Алгоритм банкира. Предотвращение взаимоблокировок. Атаки условий возникновения взаимоблокировок. **Тема 7.**Безопасность. Использование криптографии в операционных системах. Механизмы защиты. Аутентификация. Инсайдерские атаки. Использование дефектов программного кода. Вредоносные программы. Средства защиты.
Трудоёмкость (з.е. / часы)	**8** ЗЕТ / **288** часов.
Форма итогового контроля знаний	**зачет, экзамен**

Аннотация учебной дисциплины

Учебная дисциплина **«СЕТИ И СИСТЕМЫ ПЕРЕДАЧИ ИНФОРМАЦИИ»**	
Цель изучения дисциплины	**Цель курса** - ввести студентов в круг понятий и задач, связанных с использованием информационных систем, с тем, чтобы студенты могли самостоятельно анализировать и решать теоретические и практические задачи, связанные с этой областью знаний.
Компетенции, формируемые в результате освоения дисциплины	**Изучение дисциплины направлено на формирование следующих компетенций студентов:** - 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);
Знания, умения и навыки, получаемые в процессе изучения дисциплины	***В результате освоения дисциплины студенты должны:*** **знать:** 1) основные понятия построения систем и сетей электросвязи и особенности их эксплуатации; 2) тактико-технические характеристики основных телекоммуникационных систем, сигналов и протоколов, применяемых для передачи различных видов сообщений; **3)** перспективы развития систем и сетей связи; **уметь:** 1) творчески применять знания о системах электрической связи для решения задач по созданию защищенных телекоммуникационных систем; 2) отслеживать тенденции развития систем и сетей электросвязи, внедрения новых служб и услуг связи; 3) разрабатывать структурные схемы систем связи с заданными характеристиками; **4)** читать структурные и функциональные схемы систем и сетей связи; **владеть:**

	1) навыками анализа основных электрических характеристик и возможностей телекоммуникационных систем по передаче оперативных и специальных сообщений; анализа сетевых протоколов; 2) навыками работы с научно-технической литературой по изучению перспективных систем и сетей связи с целью повышения эффективности использования защищенных телекоммуникационных систем.
Краткая характеристика учебной дисциплины (основные блоки и темы)	**Содержание разделов (тем) дисциплин** **1. Состояние и пути развития телекоммуникационных систем и сетей** 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. Основные понятия и определения. Информация, сообщение, сигнал, канал связи. Архитектура связи: телекоммуникации, инфокоммуникационная система, система электросвязи, телекоммуникационная сеть, служба связи. Классификация систем связи. 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. **2. Способы представления и преобразования сообщений и сигналов в системах и сетях связи** 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. Схемная реализация. Классификация помехоустойчивых кодов. Обнаружение и исправление ошибок. Простейшие помехоустойчивые коды. Циклические коды. Кодеры и декодеры циклических кодов. Алгоритмы декодирования. 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 многоканальных передач 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. Основные типы модемов, уплотнение информации в системах связи. Цифровая обработка аналоговых сигналов. Дискретные вокодеры **3. Типовые системы передачи информации и виды информационного обслуживания** Особенности цифровых систем многоканальных передач сообщений.Способы объединения цифровых потоков. Особенности передачи дискретных сообщений по цифровым каналам Системы телефонной связи. Особенности систем передачи речи. 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. Цифровая телефонияСистемы телеграфной связи. 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. Структура телеграфной сети России. Направления развития телеграфной связи.Сети подвижной сотовой связи. Принцип повторного использования частот. Эволюция стандартов СПСС. 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. Радиорелейные системы связи. Принцип радиорелейной связи. Структура радиорелейной станции. Цифровые радиорелейные станции. Системы тропосферной и спутниковой связи. Принцип тропосферной связи. Сущность тропосферной связи. Принцип разнесенного приема. Спутниковые системы связи. Принцип спутниковой связи. Радиолиния спутниковой связи. Особенности спутниковой связи. Телевизионные системы. Волоконно-оптические системы связи. Краткий исторический обзор использования оптического диапазона. Обобщенные структурные схемы ООЛС 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. Современные виды информационного обслуживания. Традиционные службы. Телематические службы. Факсимильная передача информации; электронная почта; телеконференция; видеотекст; телетекст. **4. Общая характеристика организации сетей электросвязи**

	Сети связи; структура сетей связи. Архитектура сети связи. Обобщенная структура сети связи. Сеть доступа. Магистральная сеть. Методы коммутации информации в сетях связи. Особенности сетей с коммутацией каналов сообщений и пакетов. Коммутация каналов. Коммутация пакетов. Общие сведения о протоколах эталонной семиуровневой модели. 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. Классификация сетей: локальные, городские, региональные и глобальные сети. Технологии локальных сетей. Технология Ethernet. Дальнейшее развитие технологии Ethernet. Локальные сети на основе разделяемой среды. Коммутируемые локальные сети. Интеллектуальные функции коммутаторов. Технологии сетей TCP- IP. Адресация в сетях TCP-IP. Протокол межсетевого взаимодействия. Базовые протоколы TCP-IP. Дополнительные функции маршрутизаторов IP-сетей. Сети с интегрированным обслуживанием на основе технологии ATM. Основные принципы технологии ATM. Стек протоколов ATM: уровень адаптации ATM, протокол ATM. Категории услуг протокола ATM. Особенности передачи речи по IP-сетям. Построение VoIP на базе семейства протоколов H.323. Построение VoIP на базе протокола SIP. Построение VoIP на базе протокола MGCP. Факторы, влияющие на качество речи, передаваемой по сетям передачи данных с пакетной коммутацией. Особенности современных сетевых архитектур. Архитектурные особенности современных локальных сетей. Протоколы физического и канального уровней. Технические характеристики и принципы функционирования современных модемов. Маршрутизация и управление потоками в сетях связи. Сети интегрального обслуживания.
Трудоёмкость (з.е. / часы)	**3** ЗЕТ / **108** часов.
Форма итогового контроля знаний	**зачёт**

Аннотация учебной дисциплины

Учебная дисциплина **«ФИЗИКА»**	
Цель изучения дисциплины	**Целями** освоения дисциплины ***«Физика»*** являются: • формирование представлений, понятий, знаний о фундаментальных зако классической физики; • формирование у студентов общего физического мировоззрения и разви физического мышления • формирование навыков применения в профессиональной деятельно универсальных методов, законов и моделей современной физики.
Компетенции, формируемые в результате	Процесс изучения дисциплины направлен на формирование следующих **компетенций**: - Способен анализировать физическую сущность явлений и процессов, лежащих в основе функционирования микроэлектронной техники, применять

освоения дисциплины	основные физические законы и модели для решения задач профессиональной деятельности (ОПК-4);
Знания, умения и навыки, получаемые в процессе изучения дисциплины	В результате освоения дисциплины студент должен ***знать***: • Основные законы механики. • Основные законы термодинамики и молекулярной физики. • Основные законы электричества и магнетизма. • Основы теории колебаний и волн, оптики. • Основы квантовой физики и физики твердого тела. • Физически явления и эффекты, используемые при обработке, хранении, передаче, уничтожении и защите информации. ***уметь***: • На основе законов механики описывать основные виды движения тел. • Строить математические модели физических явлений и процессов. • Решать типовые прикладные физические задачи. • Применять основные законы общей физики при решении практических задач. ***владеть***: • Методами теоретического исследования физических явлений и процессов. • Навыками проведения физического эксперимента и обработки его результатов.
Краткая характеристика учебной дисциплины (основные блоки и темы)	Тема 1. Введение Предмет физики. Направления развития современной физики **I. Механика.** Тема 2. Кинематика материальной точки. Описание движения материальной точки. Системы отсчета. Кинематические уравнения. Прямолинейное движение. Криволинейное движение. Ускорение при криволинейном движении. Движение по окружности, центростремительное ускорение. Тема 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. Тема 4. Законы сохранения в механике. Импульс тела. Закон сохранения импульса в механике. Энергия и работа. Закон сохранения механической энергии. Тема 5. Вращательное движение. Угол поворота, угловая скорость, угловое ускорение. Момент импульса тела и системы тел. Моменты сил. Закон сохранения момента импульса. Тема 6. Статика Виды равновесия тел. Момент силы. Условия равновесия тел. Центр масс тела. Тема 7. Кинематика движения твёрдого тела. Кинематические уравнения, описывающие движение твердых тел. Поступательное, вращательное и сложное движение твердого тела. Тема 8. Динамика твёрдого тела. Основные законы динамики поступательного и вращательного движение твердого тела. Тема 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.

	Тема 10. Относительность в классической механике. Принцип относительности в классической механике. Преобразования Галилея. Эквивалентность инерциальных систем отсчета. Тема 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. **II. Молекулярная физика и термодинамика** Тема 12. Молекулярно-кинетическая теория. Основы МКТ. Экспериментальное подтверждение основных положений МКТ. Броуновское движение, диффузия, несжимаемость жидкости, теплота парообразования. Тема 13. 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. Тема 14. Состояние термодинамической системы. Виды термодинамических систем. Внутренняя энергия термодинамической системы. Работа, совершаемая при изменении состояния системы. Тема 15. Первое начало термодинамики. Теплота, теплопередача. Первое начало термодинамики как закон сохранения энергии. Внутренняя энергия и теплоёмкость идеального газа. Классическая теория теплоёмкости идеального газа. Тема 16. Работа, совершаемая идеальным газом. Работа, совершаемая идеальным газом в разных процессах. Работа в изобарном процессе. Работа в изохорном процессе. Работа в изотермическом процессе. Тема 17. Циклы в термодинамике. Циклы в термодинамике. Работа, совершаемая рабочим телом в цикле. Работа на диаграмме. КПД циклов. Цикл Карно. **III. Электричество и магнетизм.** Тема 18. Взаимодействие зарядов. Взаимодействие точечных зарядов. Закон Кулона. Взаимодействие системы точечных зарядов. Тема 19. Электростатическое поле. Напряженность электрического поля. Силовые линии электростатического поля. Принцип суперпозиции полей. Однородное электростатическое поле. Тема 20. 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. Тема 21. Теорема Остроградского-Гаусса для электростатического поля. Поток вектора напряженности электрического поля через площадку. Теорема Остроградского-Гаусса для электростатического поля. Тема 22. Проводники в электрическом поле. Электроёмкость. Проводники в электрическом поле. Поверхностная плотность зарядов. Электроёмкость. Емкость уединенного проводника, емкость шара. Конденсатор. Типы конденсаторов. Соединение конденсаторов. Тема 23.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.

	Тема 24. Магнитное поле. Вектор индукции магнитного поля. Силовые линии магнитного поля. Действие магнитного поля на движущийся заряд. Сила Лоренца. Тема 25. Закон Ампера. Взаимодействие проводников с током. Действие магнитного поля на проводник с током. Закон Ампера. Тема 26. Закон Био-Савара-Лапласа. Магнитное поле, создаваемое проводником с током. Закон Био-Савара-Лапласа. Тема 27. Теорема о циркуляции и теорема Остроградского-Гаусса для магнитного поля Понятие циркуляции 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. Тема 28. Магнитное поле в веществе. Магнитные моменты атомов. Магнитное поле в веществе. Напряженность магнитного поля. Диамагнетики, парамагнетики и ферромагнетики. Петля гистерезиса. Тема 29. Электромагнитная индукция. Явление электромагнитной индукции. Правило Ленца. Явление самоиндукции. Индуктивность. Явление взаимной индукции. Тема 30. Уравнения Максвелла. Первое уравнение Максвелла. Токи смещения. Второе уравнение Максвелла. Третье и четвертое уравнения Максвелла. Тема 31. Электромагнитные колебания и волны. Колебательный контур. Свободные незатухающие колебания. Затухающие и вынужденные колебания. Основные свойства электромагнитных волн. Шкала электромагнитных волн. **IV. Оптика. Квантовая физика.** Тема 32. Оптика. Основы геометрической оптики. Волновые свойства света. Спектроскоп, критерий Релея. Рентгеноструктурный анализ. Взаимодействия света с веществом(дисперсия, поглощение и рассеяние света).Поляризация света. Тема 33. Тепловое излучение Закон Кирхгофа. Правило Прево. Излучение абсолютно черного тела. Формула Релея-Джинса. Ультрафиолетовая катастрофа. Формула Планка. Законы Стефана-Больцмана и Вина. Тема 34. Волновые и корпускулярные свойства частиц. Гипотеза де Бройля. Корпускулярно-волновой дуализм. Опыт Дэвиссона-Джермера. Тема 35. Строение атома. Модели строения по Томпсону, Резерфорду. Постулаты Бора. Квантование энергии и момента импульса. Радиусы разрешенных орбит. Тема 36. Основные понятия квантовой механики атомов и молекул Волновая функция и ее интерпретация. Уравнение Шредингера. Соотношение неопределенностей Гейзенберга. Квантовые числа. Принцип Паули. Тема 37. Основные понятия ядерной физики. Строение ядра. Нуклоны. Изотопы. Радионуклиды. Сильное взаимодействие. Закон радиоактивного распада. Метод радиоактивного датирования. Тема 38. Основы физики элементарных частиц. Типы взаимодействий. Классификация элементарных частиц Кварки.
Трудоёмкость (з.е. / часы)	Согласно рабочему учебному плану курс читается в полном объёме в течение **5 и 6** семестров **8 ЗЕТ / 288** часа.
Форма итогового	В конце **5**-го и **6**-го семестров предусмотрен ***зачет с оценкой***.

контроля знаний	

Аннотация учебной дисциплины

Учебная дисциплина **«ТЕОРИЯ КОДИРОВАНИЯ, СЖАТИЯ И ВОССТАНОВЛЕНИЯ ИНФОРМАЦИИ»**	
Цель изучения дисциплины	**Цель курса** – овладение основными понятиями и методами теории кодирования информации и сжатия данных.
Компетенции, формируемые в результате освоения дисциплины	В результате освоения дисциплины у обучающегося формируются следующие **компетенции:** - 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); - 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); - Способен разрабатывать алгоритмы, реализующие современные математические методы защиты информации (ОПК-2.1);
Знания, умения и навыки, получаемые в процессе изучения дисциплины	После окончания курса студент ***должен знать:*** ▪ основные алгоритмы кодирования информации; ▪ основные алгоритмы сжатия различных типов данных; ***должен уметь:*** ▪ оценивать качество сжатия информации различными алгоритмами; ▪ строить алгоритмы сжатия для данных с различными видами избыточности; ▪ восстанавливать информацию при известном алгоритме кодирования; ▪ осуществлять выбор схемы кодирования информации, адекватной заданным угрозам безопасности компьютерных систем. ***должен владеть:*** ▪ навыками разработки, реализации и практического применения алгоритмов кодирования информации; ▪ навыками разработки, реализации и практического применения алгоритмов сжатия данных.
Краткая характеристика учебной дисциплины (основные блоки и темы)	**Содержание основных разделов и тем курса** **Раздел 1.Основы теории кодирования информации**. **Линейные коды** Понятие линейный код и его основные параметры. Проверочная и порождающая матрицы линейного кода. Примеры линейных кодов. Основные свойства линейных кодов. Расстояние и вес Хэмминга. Минимальное расстояние линейного кода. Понятие дуальный код и его основные параметры. Количество ошибок, исправляемых кодом. Декодирование линейных кодов. Граничные соотношения между параметрами помехоустойчивых кодов: граница Хэмминга. **Раздел 2. Циклические коды**

	Понятие циклический код. Конструкция циклического кода. Порождающий и проверочный многочлены циклического кода. Максимальный циклический код. Неприводимый циклический код. Конструкция БЧХ-кодов. Основные свойства БЧХ-кодов. Примеры построения БЧХ-кодов. Конструкция кодов Рида-Соломона. Основные свойства кодов Рида-Соломона. Примеры построения кодов Рида-Соломона. **Раздел 3. Коды Юстесена** Конструкция кодов Юстесена. Основные свойства кодов Юстесена. Примеры построения кодов Юстесена. **Раздел 4.Другие основные методы кодирования и декодирования** Конструкции кодов. Основные свойства кодов. Примеры построения кодов. **Раздел 5.Основы теории сжатия информации** Определение энтропии и количества информации. Виды избыточности, способы устранения. Типы моделей. Словарные модели. Статистические модели. Алгоритмы на основе преобразований. Префиксные коды. Классический алгоритм Хаффмана. Адаптивное сжатие. Алгоритм динамического кодирования Хаффмана (FGK). Проблемы адаптивного кодирования Хаффмана. Эффективная реализация адаптивного метода Хаффмана. Алгоритм быстрого перестроения дерева. Кодирование длинных последовательностей. Вычисление кода по дереву. Декодирование кода по дереву. Семейство алгоритмов арифметического кодирования. Простое кодирование и детали реализации метода. Потеря значащих цифр. Адаптивное арифметическое кодирование. Эффективная реализация арифметического кодирования - модель с настраиваемым источником: инициализация, кодирование, декодирование. **Раздел 6. Сжатие текстовых данных** Алгоритмы сжатия текстовой информации первого поколения. Словарные методы. Алгоритмы LZ77, LZSS, LZ78, LZW. Алгоритмы сжатия текстовой информации второго поколения. Алгоритмы PPM. Оценки вероятности ухода в PPM: априорные и адаптивные методы. Преобразование BWT. Алгоритм декодирования BWT. Сжатие с использованием BWT. Методы, используемые совместно с BWT. Способы сжатия преобразованных BWT данных. Формат Deflate. Общее описание. Алгоритм декодирования. Кодирование длин и смещений. Кодирование блоков фиксированными и динамическими кодами Хаффмана. Основные моменты реализации компрессора PPM на примере контекстной модели первого порядка без исключения символов и статистическим кодированием на основе арифметического кодера. **Раздел 7. Сжатие графических данных** Типы изображений. Подходы к сжатию изображений. Интуитивные подходы. Преобразование изображений: ортогональные преобразования, матричные преобразования, дискретное косинус-преобразование. Прогрессирующее сжатие изображений. Метод сжатия изображений с использованием вейвлетных преобразований. Преобразование Хаара. Поддиапазонные преобразования. Банк фильтров. Вейвлеты Добеши. Преобразование DWT. Алгоритм SPHIT: описание метода, основные шаги кодера, алгоритм кодирования. Сжатие JPEG. Практическое DCT в JPEG. Квантование в JPEG. Кодирование в JPEG. Сжатый файл JPEG. Сжатие JPEG2000. Структурная

	схема сжатия в JPEG2000. Основные шаги алгоритма сжатия JPEG2000. Сжатие JPEG без потерь. Коды Голомба. Основы метода JPEG-LS. Алгоритм работы кодера. **Раздел 8. Сжатие видео и звуковых данных** Основные принципы сжатия видео. Интуитивные методы. Компенсация движения. Методы подоптимального поиска: сигнатурные методы, поиск с разбавленным расстоянием, локализованный поиск, монотонный поиск по квадрантам, методы иерархического поиска. Особенности стандарта MPEG-4. Представление натурального видео. Основы сжатия звуковой информации. Основные понятия: импульсная кодовая модуляция, сжатие звука с потерями. Общепризнанные методы. Стандарт MPEG-1. Сжатие звука в стандарте MPEG-1: кодирование частотной области, формат сжатых данных. Сжатие звука MPEG-1 слой III. Основные шаги сжатия звука MPEG-1 слой III: MDCT, удаление пре-эха, удаление паразитного сигнала, кодирование. Алгоритм назначения битов слоем III. **Тематика практических работ** **Практическая работа №1** Исследование структуры и свойств линейного кода. **Практическая работа №2** Исследование структуры и свойств циклического кода. **Практическая работа №3** Исследование структуры и свойств кода Рида-Соломона. **Практическая работа №4** Исследование структуры и свойств каскадного кода. **Практическая работа №5** Модифицирование кодов и их анализ. **Практическая работа №6** Метод Хаффмана сжатия информации. **Практическая работа №7** Арифметическое кодирование. **Практическая работа №8** Словарные методы компрессии.
Трудоёмкость (з.е. / часы)	**5** ЗЕТ / **180** часов
Форма итогового контроля знаний	**экзамен**

Аннотация учебной дисциплины

Учебная дисциплина **«Теория информации»**	
Цель изучения дисциплины	***Цели*** освоения дисциплины «Теория информации»: - формирование у обучающихся чёткого понимания предмета теории информации и её основных концепций;

	- развитие навыков применения методов теории информации для решения проблем, связанных с хранением, обработкой и передачей информации.
Компетенции, формируемые в результате освоения дисциплины	Процесс изучения дисциплины направлен на формирование следующих ***компетенций***: - Способен на основании совокупности математических методов разрабатывать, обосновывать и реализовывать процедуры решения задач профессиональной деятельности (ОПК-3); - Способен разрабатывать алгоритмы, реализующие современные математические методы защиты информации (ОПК-2.1).
Знания, умения и навыки, получаемые в процессе изучения дисциплины	В результате освоения дисциплины студент должен ***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; - методы формального представления информации; основные процедуры машинной обработки информации; основные поисковые системы, их функции, возможности и способы работы с ними; основные источники информации по дисциплинам. ***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; - работать с научно-технической литературой по тематике дисциплины; запускать и использовать поисковые системы; анализировать и систематизировать большие массивы информации; составлять аналитические обзоры литературы по информационной безопасности. ***владеть***: - основами построения математических моделей текстовой информации и моделей систем передачи информации; навыками применения математического аппарата для решения прикладных теоретико-информационных задач; - навыками использования поисковых систем в сети Интернет; навыками составления библиографических описаний.
Краткая Характеристика учебной дисциплины (основные блоки и темы)	**Содержание основных разделов (тем) курса** **Тема 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. **Тема 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. **Тема 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. **Тема 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.

	Тема 5. Теоремы кодирования для дискретных каналов 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.
Трудоёмкость (з.е. / часы)	Согласно рабочему учебному плану курс читается в полном объёме в течение 7 семестра **5** ЗЕТ / **180** часов.
Форма итогового контроля знаний	В конце **7**-го семестра предусмотрен ***зачёт***.

Аннотация учебной дисциплины

Учебная дисциплина **«МОДЕЛИ БЕЗОПАСНОСТИ КОМПЬЮТЕРНЫХ СИСТЕМ»**	
Цель изучения дисциплины	**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.
Компетенции, формируемые в результате освоения дисциплины	Процесс изучения дисциплины направлен на формирование следующих ***компетенций***: - способность применять методы научных исследований при проведении разработок в области обеспечения безопасности компьютерных систем и сетей (ОПК-8); - способность разрабатывать политики безопасности, политики управления доступом и информационными потоками в компьютерных системах с учетом угроз безопасности информации и требований по защите информации (ОПК-11);
Знания, умения и навыки, получаемые в процессе	В результате освоения дисциплины студент должен ***знать***: - основные формальные модели безопасности компьютерных систем; угрозы безопасности информации; основные виды политик управления доступом;

изучения дисциплины	- основные формальные модели дискреционного, мандатного, ролевого управления доступом, модели изолированной программной среды и безопасности информационных потоков; ***уметь***: - анализировать угрозы безопасности КС; разрабатывать формальные модели политик безопасности, политик управления доступом и информационными потоками; - формализовывать задачи по безопасности КС; разрабатывать модели нарушителя безопасности КС; разрабатывать политики безопасности КС; ***владеть***: - навыками построения моделей защищаемых систем и систем обеспечения безопасности КС; - навыками разработки и анализа моделей безопасности КС;
Краткая Характеристика учебной дисциплины (основные блоки и темы)	**Содержание основных разделов (тем) курса** **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.
Трудоёмкость (з.е. / часы)	Согласно рабочему учебному плану курс читается в полном объёме в течение 8 семестра **5** ЗЕТ / **180** часов.
Форма итогового контроля знаний	В конце **8**-го семестра предусмотрен ***зачёт***.

Аннотация учебной дисциплины

Учебная дисциплина **«АППАРАТНЫЕ СРЕДСТВА ВЫЧИСЛИТЕЛЬНОЙ ТЕХНИКИ»**

Цель изучения дисциплины	Целью курса " Аппаратные средства вычислительной техники" является дать необходимые знания будущему специалисту, которое он будет использовать в своей деятельности, связанной с эксплуатацией и обслуживанием аппаратуры и оборудования, содержащего современные средства вычислительной техники, в подразделениях ФСБ России, ФАПСИ при Президенте РФ, СВР РФ и МО РФ и других организациях и предприятиях. А также сформировать у студентов системный подход к изучению и проектированию сложных систем.
Компетенции, формируемые в результате освоения дисциплины	Изучение дисциплины нацелено на формирование следующих компетенций обучающихся: ОПК-4: - Способен анализировать тенденции развития методов и средств криптографической защиты информации, использовать средства криптографической защиты информации при решении задач профессиональной деятельности;
Знания, умения и навыки, получаемые в процессе изучения дисциплины	В результате освоения дисциплины студент должен: ***Знать***: - архитектуру основных типов современных компьютерных систем; - структуру и принципы работы современных и перспективных микропроцессоров; - 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 ПЭВМ и периферийного оборудования; - навыками формирования структуры СВТ и выбора режимов их функционирования.
Краткая характеристика учебной дисциплины (основные блоки и темы)	**Содержание основных разделов и тем курса** 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. Арифметические и логические основы цифровых машин. Физическое представление данных в компьютерах. Основные логические элементы, их физические основы работы. Таблицы истинности.

	Синтез логических элементов. Системы счисления. Представления в двоичной, восьмеричной, шестнадцатиричной системах. Переводы из одной системы в другую. Двоично-десятичный код. Выполнение арифметических операций. Цифровая математика. Представление чисел с фиксированной и плавающей точкой. Стандарт IEE 754. Форматы представления данных и кодирование информации. 3. Функциональные элементы и узлы ЭВМ. Элементы и узлы ЭВМ. Функциональные узлы комбинационного типа: сумматоры, шифраторы, дешифраторы, мультиплексоры, демультиплексоры, компараторы, преобразователи кодов. Функциональные узлы последовательностного типа: триггеры, регистры, счетчики, защелки. Их назначение, условные обозначения, логические схемы, таблицы истинности, состояния неустойчивости. 4. 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. 5. 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. 6. 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. 7. 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. 8. 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. 9. 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. 10. 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. Тематика лабораторных работ Для практического закрепления материала предусматривается выполнение лабораторных работ трех видов: 1. Моделирующие лабораторные работы. Они выполняются в системе моделирования "MULTISIM 12" и дают наглядное представление о физических особенностях и принципах работы узлов аппаратных средств, таких как ; - логические элементы, счетчики, регистры, мультиплексоры, дешифраторы и др. Моделирующие лабораторные работы. Темы: - Источник питания для MCU. Линейный стабилизатор напряжения 7805. - Индикация шины данных с помощью LED. - Счетчик событий и таймер. - Символьный 7-сегментный дисплей 2x16 управляемый контроллером. - Последовательная передача данных. RS-232. USB. - Создание генератора импульсов сложной формы. - Цифро-аналоговое преобразование. - Анализ сигнала с помощью БПФ (разложение в ряд Фурье). 2. Стендовые лабораторные работы. Стендовые лабораторные работы проводятся на базе комплектов **EasyPIC5** , **EasyAVR** – отладочных плат с обширным набором периферии для разработки и отладки приложений на основе микроконтроллеров семейства PICmicro от Microchip. Стендовые лабораторные работы. Темы: - Изучение источника питания отладочной платы. - Изучение принципа работы встроенного USB 2.0 программатора. - Работа генератора микроконтроллера. - Аппаратный внутрисхемный отладчик. - Назначение LED индикаторов отладочной платы. - Управление контроллером с помощью кнопочных переключателей. Символьный ЖК-дисплей (опционально добавлен в комплект). - Графический монохромный дисплей и сенсорная панель управления. - USB соединение двух устройств. - Цифровой термометр DS1820. - Аналого-цифровое преобразование переменного тока. 3. Макетные лабораторные работы. Эти работы выполняются на действующих макетах средств вычислительной техники и периферийного оборудования. Макетные лабораторные работы. Темы: - Структурная организация ЭВМ.

	- Организация и структура памяти. - ПЭВМ. - Рабочие станции и серверы. - Периферийные устройства.
Трудоёмкость (з.е. / часы)	**4 ЗЕ/ 144** часов.
Форма итогового контроля знаний	**экзамен.**

Аннотация учебной дисциплины

Учебная дисциплина **«ТЕХНИЧЕСКАЯ ЗАЩИТА ИНФОРМАЦИИ»**	
Цель изучения дисциплины	**Целью** курса "Техническая защита информации" является дать необходимые знания будущему специалисту об угрозах утечки информации по техническим каналам, а также о методах и технических средствах ее защиты. Полученные знания будущий специалист сможет использовать в своей деятельности, связанной с эксплуатацией и обслуживанием аппаратуры и оборудования, содержащего современные средства вычислительной техники, в подразделениях ФСБ России, ФАПСИ при Президенте РФ, СВР РФ и МО РФ и других организациях и предприятиях. А также сформировать у студентов системный подход к изучению и проектированию защиты сложных информационных систем.
Компетенции, формируемые в результате освоения дисциплины	Изучение дисциплины нацелено на формирование следующих компетенций обучающихся: 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); - Способен разрабатывать компоненты программных и программно-аппаратных средств защиты информации в компьютерных системах и проводить анализ их безопасности (ОПК-13);
Знания, умения и навыки, получаемые в процессе изучения дисциплины	В результате освоения дисциплины студент должен: ***Знать***: - основные угрозы безопасности информации и модели нарушителя в компьютерных системах; - возможности различных видов технической разведки; - виды технических средств, используемых при защите объектов информатизации. ***Уметь***: - пользоваться нормативными документами по технической защите информации; - применять наиболее эффективные методы и средства технической защиты информации; - контролировать эффективность мер защиты информации.

	Владеть: - навыками выявления угроз информационной безопасности с помощью технических средств; - методами технической защиты информации; - навыками организации защиты информации от утечки по техническим каналам.
Краткая характеристика учебной дисциплины (основные блоки и темы)	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. 2.1 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. 2.2 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. 2.3 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. 2.4 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. 2.5 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. 3.1 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. 3.2 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. 3.3 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. 4.1 Средства технической разведки. Визуально-оптические приборы. Фотоаппараты. 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. 4.2 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. 4.3 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.

	5.1 Государственная система защиты 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. 5.2 Контроль эффективности технической защиты информации. Виды контроля эффективности технической защиты информации. Виды зон безопасности. Методы технического контроля. Особенности инструментального контроля эффективности технической защиты информации. 6.1 Моделирование технической защиты информации. Основные положения методологии технической защиты информации. Принципы моделирования объектов защиты. Моделирование угроз безопасности информации. Методические рекомендации по выбору рациональных вариантов защиты. Пути оптимизации мер инженерно-технической защиты информации. 6.2 Принципы оценки эффективности технической защиты информации. Методы расчета и инструментального контроля показателей защиты информации. Возможности оценки видовых признаков объектов наблюдения. Подходы к определению безопасности речевой информации в помещении. Принципы оценки размеров зон I и II. Оценка дальности перехвата сигналов.
Трудоёмкость (з.е. / часы)	**5** ЗЕТ / **180** часа
Форма итогового контроля знаний	**экзамен**.

Аннотация учебной дисциплины

Учебная дисциплина **«Теоретико-числовые методы в криптографии»**	
Цель изучения дисциплины	***Целью*** освоения дисциплины «*Теоретико-числовые методы в криптографии*» являются: - 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 информационной безопасности.

Компетенции, формируемые в результате освоения дисциплины	Процесс изучения дисциплины направлен на формирование следующих ***компетенций***: - способен применять методы научных исследований при проведении разработок в области обеспечения безопасности компьютерных систем и сетей (ОПК-8); - способен анализировать тенденции развития методов и средств криптографической защиты информации, использовать средства криптографической защиты информации при решении задач профессиональной деятельности (ОПК-10).
Знания, умения и навыки, получаемые в процессе изучения дисциплины	В результате освоения дисциплины студент должен ***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; основные задачи и вопросы, лежащие в основе защиты и обработки информации; теоретические основы естественно-научных дисциплин, общие принципы экспериментального и теоретического исследования теоретико-числовых алгоритмов. ***уметь***: применять типовые теоретико-числовые алгоритмы к решению практических задач; проводить оценку сложности алгоритмов; разрабатывать эффективные алгоритмы и программы; работать с литературой, в том числе зарубежной, касающейся основных методов передачи и защиты информации; производить содержательный анализ результатов вычислений. ***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; информацией о современных теоретико-числовых методах в криптографии; практическими навыками применения современного математического инструментария для решения прикладных задач, владеть навыками исследования примененных алгоритмов.
Краткая Характеристи каучебной дисциплины (основные блоки и темы)	**Содержание основных разделов (тем) курса** Тема 1. Сложность арифметических операций. Тема 2. Быстрые вычисления. Тема 3. Алгоритмы проверки чисел на простоту. Тема 4. Алгоритмы построения больших простых чисел. Тема 5. Алгоритмы факторизации чисел. Тема 6. Анализ криптосистемы RSA. Тема 7. Основные методы дискретного логарифмирования.
Трудоёмкость (з.е. / часы)	Согласно рабочему учебному плану курс читается в полном объёме в течение **5** и **6** семестров **3** ЗЕТ / **108** часов и **3** ЗЕТ / **108** часов.
Форма итогового контроля знаний	В конце **5**-го семестра предусмотрен ***зачёт***, в конце **6**-го семестра – ***курсовая работа*** и ***экзамен***.

Учебная дисциплина **«Теория конечных полей и их приложения»**	
Цель изучения дисциплины	***Целью*** освоения дисциплины «*Теория конечных полей и их приложения*» является фундаментальная подготовка студентов в области конечных полей, овладение быстрыми вычислениями в конечных полях, ознакомление с

	приложениями теории конечных полей в современной теории кодирования и криптографии.
Компетенции, формируемые в результате освоения дисциплины	Процесс изучения дисциплины направлен на формирование следующих ***компетенций***: - способен разрабатывать и анализировать математические модели механизмов защиты информации (ОПК-2.2)
Знания, умения и навыки, получаемые в процессе изучения дисциплины	В результате освоения дисциплины студент должен ***знать***: основные понятия, свойства и связанные с ними алгоритмы вычислений в конечных полях, а также основные приложения, возникающие в теории кодирования и криптографии; алгебраические методы для решения прикладных задач; оценки сложности основных вычислений в конечных полях; общие принципы экспериментального и теоретического исследования быстрых вычислений в конечных. ***уметь***: реализовывать быстрые вычисления в конечных полях; грамотно применять изученные математические методы, современные пакеты компьютерной алгебры для реализации алгоритмов в конечных полях; проводить анализ и формализацию задач, возникающих при реализации алгоритмов быстрых вычислений в конечных полях. ***владеть***: методикой исследования свойств конечных полей применительно к криптографии, процедурой построения конечных расширений, вычисления различных базисов конечного поля; навыками решения задач теории конечных полей, в том числе, применяя системы компьютерной алгебры; способностью и готовностью применять быстрые вычисления в конечных полях к решению практических задач.
Краткая Характеристи каучебной дисциплины (основные блоки и темы)	**Содержание основных разделов (тем) курса** Тема 1. Введение в теорию конечных полей. Тема 2. Неприводимые многочлены. Тема 3. Примитивные многочлены. Тема 4. Базисы. Тема 5. Основные вычислительные алгоритмы. Тема 6. Приложения конечных полей в криптографии и теории кодирования.
Трудоёмкость (з.е. / часы)	Согласно рабочему учебному плану курс читается в полном объёме в течение **6** семестра **3** ЗЕТ / **108** часов.
Форма итогового контроля знаний	В конце **6**-го семестра предусмотрен ***зачёт***.

Аннотация учебной дисциплины

Учебная дисциплина **«Методы и средства криптографической защиты информации»**	
Цель изучения дисциплины	***Цель курса*** – сформировать представление о современных методах и средствах криптографической защиты информации, используемых, в частности, для решения проблем компьютерной безопасности. Предметом курса является изложение основ криптографии и примеров реализации криптографических методов на практике
Компетенции, формируемые в результате	Изучение дисциплины нацелено на формирование следующих компетенций обучающихся:

освоения дисциплины	- Способен анализировать тенденции развития методов и средств криптографической защиты информации, использовать средства криптографической защиты информации при решении задач профессиональной деятельности (ОПК-10);
Знания, умения и навыки, получаемые в процессе изучения дисциплины	В результате изучения курса **студент должен знать**: • задачи информационной безопасности, решаемые криптографическими методами; • основные криптографические примитивы и их использование в решении основных задач защиты информации; • принципы построения и основные виды симметричных и асимметричных криптографических алгоритмов; • математические модели шифров; • требования к шифрам и основные характеристики шифров; • криптографические стандарты; • частотные характеристики открытых текстов и их применение к анализу простейших симметричных криптосистем. В результате изучения дисциплины студенты должны**уметь:** • применять полученные знания к исследованию простых шифров; • пользоваться научно-технической литературой в области криптографии; • корректно применять симметричные и асимметричные криптографические алгоритмы для решения задач защиты информации. В результате изучения дисциплины студенты должны **иметь представление:** • о роли математики, ее месте в криптографии; • о методах решения задач криптоанализа. В результате изучения дисциплины студенты должны **иметь навыки:** • применения отечественной терминологии в области криптографии для выражения количественных и качественных требований по защите информации; • использования математического аппарата в проведении исследований. В результате изучения дисциплины студенты должны **владеть**: • криптографической терминологией; • навыками использования типовых криптографических алгоритмов; • навыками математического моделирования в криптографии.
Краткая характеристика учебной дисциплины (основные блоки и темы)	**Содержание дисциплины** **Раздел 1. Введение в криптографию.** 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. 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.*

	Раздел 2. Основные классы шифров и их свойства. 4. Поточные шифры замены. *Шифры простой замены и их анализ. Многоалфавитные шифры замены.* *Шифры гаммирования. Использование неравновероятной гаммы. Повторное использование гаммы.* *Криптоанализ шифра Вижинера.* 5. Шифры перестановки. *Разновидности шифров перестановки. Элементы криптоанализа шифров перестановки.* 6. Блочные шифры. *Блочные шифры простой замены Плейфера и Хилла.* *Архитектура современных блочных шифров: сеть Фейстеля. Режимы использования блочных шифров.* *Российский блочный шифр ГОСТ 28147-89.* *Криптоалгоритмы: RIJNDAEL и IDEA.* *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.* **Раздел 3. Надежность шифров.** 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.* 10. Помехоустойчивость шифров. *Шифры, не размножающие искажений типа замена знаков. Шифры не распространяющие искажений типа вставка-пропуск знаков.* **Раздел 4. Методы синтеза и анализа симметричных криптосистем.** 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.* 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. **Раздел 5. Криптографические хеш-функции.** 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.* 15. Целостность данных и аутентификация источника данных. *Конструкции схем аутентификации на основе хеш-функций. Коды аутентичности сообщений: HMAC, UMAC.* *СистемыCBC-MAC, EMAC, XOR-MAC, PCS-MAC.* **Раздел 6. Методы синтеза криптографических алгоритмов с открытым ключом.** 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.*
Трудоёмкость (з.е. / часы)	**10** ЗЕТ / **360 часов**.
Форма итогового контроля знаний	**зачет, экзамен**

Аннотация учебной дисциплины

Учебная дисциплина **«КРИПТОГРАФИЧЕСКИЕ ПРОТОКОЛЫ»**	
Цель изучения дисциплины	***Цель курса*** – ознакомление студентов с существующими подходами к анализу и синтезу криптографических протоколов, с государственными и международными стандартами в этой области. Дисциплина обеспечивает приобретение знаний и умений в области использования криптографических протоколов для защиты информации, способствует освоению принципов корректного применения современных защищенных информационных технологий.
Компетенции, формируемые в результате освоения дисциплины	**Компетенции, формируемые у обучающегося в результате освоения дисциплины** - Способен анализировать тенденции развития методов и средств криптографической защиты информации, использовать средства криптографической защиты информации при решении задач профессиональной деятельности (ОПК-10);

Знания, умения и навыки, получаемые в процессе изучения дисциплины	В результате изучения дисциплины студент должен **знать:** • алгоритмы генерации и проверки электронной цифровой подписи в государственных стандартах США и России; • принципы построения криптографических хеш-функций; • особенности использования паролей и систем открытого шифрования для идентификации; • протоколы идентификации, основанные на доказательстве с нулевым разглашением; • протокол Диффи-Хэллмана открытого распределения ключей и его модификации. В результате изучения дисциплины студент должен **уметь**: • использовать симметричные и асимметричные шифрсистемы для построения криптографических протоколов; • анализировать свойства криптографических протоколов; • проводить сравнительный анализ криптографических протоколов, решающих сходные задачи. В результате изучения дисциплины студент должен **владеть**: • навыками сведения задачи оценивания уровня стойкости криптографических протоколов к известным математическим проблемам; • навыками построения моделей криптографических протоколов, которые используются на практике.
Краткая характеристика учебной дисциплины (основные блоки и темы)	**Введение.** 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. **Тема 2. Криптографические хеш-функции и коды аутентификации** Требования к криптографическим хеш-функциям. Бесключевые хеш-функции. Основные свойства. Принципы построения и выбора параметров хеш-функций. Хеш-функции на основе схем блочного шифрования. Алгоритмы MD4 и MD5. Стандарты криптографических хеш-функций США и России. Хеш-функции на основе дискретного логарифмирования. Хеш-функции, определяемые ключом. Коды аутентификации, определения и свойства. Вероятности навязывания и понятие оптимального кода аутентификации. Понятие ортогонального массива. Свойства. Связь оптимальных кодов аутентификации с ортогональными массивами. **Тема3. Схемы цифровых подписей** Определение схемы цифровой подписи. Примеры. Схема Фиата – Шамира. Схема Эль-Гамаля и ее анализ. Семейство схем типа Эль-Гамаля. Стандарты США и России электронной цифровой подписи. Одноразовые подписи. Понятие инфраструктуры открытых ключей. Рекомендации X-509. Схема цифровой подписи вслепую. Схема конфиденциальной цифровой подписи. **Тема 4. Протоколы идентификации**

	Протоколы идентификации на основе паролей. Протоколы идентификации типа «запрос-ответ». Понятие протоколов интерактивного доказательства и доказательства знания. Протоколы с нулевым разглашением. Протоколы идентификации, использующие технику доказательства знания. Протоколы Фиата-Шамира и Шнорра. Связь между протоколами электронной цифровой подписи и идентификации. Протоколы с самосертифицируемыми ключами. **Тема 5. Протоколы распределения ключей** Протоколы генерации и передачи ключей. Примеры протоколов передачи ключей на основе симметричного и открытого шифрования. Двух и трех сторонние протоколы. Функции доверенной третьей стороны и выполняемые ею роли. Протоколы открытого распределения ключей. Протокол Диффи-Хэллмана и его модификации. Понятие аутентифицированного протокола распределения ключей. Примеры. Схемы предварительного распределения ключей. Схемы Блома и на основе пересечений множеств. Групповые протоколы. Протоколы разделения секрета и распределения ключей для телеконференции. **Тема 6. Прикладные протоколы.** Протоколы битовых обязательств и их свойства. Протокол подписания контракта и сертифицированной электронной почты. Протоколы электронного голосования.
Трудоёмкость (з.е. / часы)	Согласно рабочему учебному плану курс читается в полном объёме в течение **9**семестра **6** ЗЕ/**216** часа.
Форма итогового контроля знаний	***Зачёт***.

Аннотация учебной дисциплины

Учебная дисциплина **«ОСНОВЫ ПОСТРОЕНИЯ ЗАЩИЩЕННЫХ КОМПЬЮТЕРНЫХ СЕТЕЙ»**	
Цель изучения дисциплины	**Целью курса** 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.
Компетенции, формируемые в результате освоения дисциплины	Процесс изучения дисциплины направлен на формирование следующих ***компетенций***: - 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); - Способен проводить мониторинг работоспособности и анализ эффективности средств защиты информации в компьютерных системах и сетях (ОПК-16);

Знания, умения и навыки, получаемые в процессе изучения дисциплины	**В результате освоения дисциплины студенты должны:** **знать:** 1) средства и методы хранения и передачи аутентификационной информации; 2) механизмы реализации атак в сетях TCP/IP; 3) основные протоколы идентификации и аутентификации абонентов сети; 4) защитные механизмы и средства обеспечения сетевой безопасности; 5) средства и методы предотвращения и обнаружения вторжений; **уметь:** 1) формулировать и настраивать политику безопасности основных операционных систем, а также локальных компьютерных сетей, построенных на их основе; 2) применять защищенные протоколы, межсетевые экраны и средства обнаружения вторжений для защиты информации в сетях; 3) осуществлять меры противодействия нарушениям сетевой безопасности с использованием различных программных и аппаратных средств защиты; **владеть:** 1) навыками настройки межсетевых экранов; 2) методиками анализа сетевого трафика; 3) методиками анализа результатов работы средств обнаружения вторжений;
Краткая характеристика учебной дисциплины (основные блоки и темы)	**Содержание разделов (тем) дисциплин** **Раздел 1. Типовые угрозы сетевой безопасности** Тема №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. Тема №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. Тема №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. Целочисленное переполнение при аутентификации в OpenSSH (CVE-2002-0639). Уязвимость в веб сервере Apache при обработке частичных запросов (CVE-2002-0392). Изменение конфигурации и состояния хостов. Недостатки протоколов семейства TCP/IP с точки зрения обеспечения безопасности информации. Технические меры защиты от сетевых атак. Тема №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. **Раздел 2. Криптографические методы защиты информации в компьютерных сетях** Тема № 5. 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. Тема № 6. 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. **Раздел 3. Программно-аппаратные средства обеспечения безопасности в компьютерных сетях** Тема № 7. 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. Системы проверки целостности TripWire и LinuxsXid. Электронная цифровая подпись. Удостоверяющие центры. Тема №8. 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. Тема № 9. 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.
Трудоёмкость (з.е. / часы)	Согласно рабочему учебному плану курс читается в полном объёме в течение **7** семестра **3** ЗЕТ / **108** часа.

Форма итогового контроля знаний	В конце **7**-го семестра предусмотрен **зачёт**.

Аннотация учебной дисциплины

Учебная дисциплина **«ЗАЩИТА В ОПЕРАЦИОННЫХ СИСТЕМАХ»**	
Цель изучения 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.
Компетенции, формируемые в результате освоения дисциплины	Процесс изучения дисциплины направлен на формирование следующих ***компетенций***: - Способен разрабатывать политики безопасности, политики управления доступом и информационными потоками в компьютерных системах с учетом угроз безопасности информации и требований по защите информации (ОПК-11); - Способен разрабатывать компоненты программных и программно-аппаратных средств защиты информации в компьютерных системах и проводить анализ их безопасности (ОПК-13);
Знания, умения и навыки, получаемые в процессе изучения дисциплины	В результате освоения дисциплины студент должен ***знать:*** – защитные механизмы и средства обеспечения безопасности операционных систем; – средства и методы хранения и передачи аутентификационной информации; – требования к подсистеме аудита и политике аудита. ***уметь:*** – формулировать и настраивать политику безопасности основных операционных систем, а также локальных вычислительных сетей, построенных на их основе. ***владеть:*** – навыками работы с различными ОС и их администрирования; – навыками разработки программных модулей, реализующих задачи, связанные с обеспечением безопасности операционных систем распространенных семейств.
Краткая характеристика учебной дисциплины (основные блоки и темы)	Содержание основных разделов (тем) курса **Раздел 1. ВВЕДЕНИЕ. ОСНОВНЫЕ ПОНЯТИЯ И ОПРЕДЕЛЕНИЯ** **Тема 1. Введение** Цели и задачи курса. Место дисциплины в учебном процессе. Методические рекомендации по изучению курса. Обзор литературы. **Тема 2. Понятие защищенной операционной системы** Угрозы безопасности операционной системы, классификация угроз, наиболее распространенные угрозы. Понятие защищенной операционной

	системы. Подходы к организации защиты. Этапы построения защиты. Административные меры защиты. **Раздел 2. ОСНОВНЫЕ ФУНКЦИИ ПОДСИСТЕМЫ ЗАЩИТЫ ОПЕРАЦИОННОЙ СИСТЕМЫ** **Тема 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. Расширения дискреционной системы управления доступом: автоматическое наследование атрибутов защиты объектов, ограниченные маркеры доступа, мандатный контроль целостности, контроль учетных записей, элементы изолированной программной среды. **Тема № 4. Идентификация, аутентификация и авторизация** Понятия идентификации, аутентификации и авторизации пользователей. Средства и методы хранения эталонных копий аутентификационной информации. Протоколы передачи аутентификационной информации по каналам вычислительной сети. Криптографическое обеспечение аутентификации пользователей. Аутентификация на основе паролей. 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 ключа. Проблемы генерации, рассылки и смены ключей. Биометрическая аутентификация: общая схема, преимущества, проблемы. Достоинства и недостатки различных схем биометрической аутентификации. **Тема № 5. Аудит** Необходимость аудита в защищенной системе. Требования к подсистеме аудита. Реализация аудита в UNIX и Windows. **Раздел 3. ИНТЕГРАЦИЯ ЗАЩИЩЕННЫХ ОПЕРАЦИОННЫХ СИСТЕМ В ЗАЩИЩЕННУЮ СЕТЬ** **Тема № 6. Домены Windows**

	Преимущества доменной архитектуры локальной сети. Понятие домена, контроллер домена. Сквозная аутентификация, возникающие проблемы и способы их решения. Порядок наделения пользователей домена полномочиями на отдельных компьютерах. Централизованное управление политикой безопасности в домене. «Лесная» доменная архитектура Windows 2000/2003, ее преимущества по сравнению с «плоской» доменной архитектурой Windows NT. Идентификация компьютеров в сети. Двусторонние транзитивные отношения доверия. Средства и методы синхронизации баз данных контроллеров разных доменов одного леса. Аутентификация по Kerberos. Групповая политика. Делегирование полномочий. Тематика лабораторных работ **Раздел «Основные функции подсистемы защиты ОС».** 1. Управление доступом в UNIX. 2. Управление доступом в Windows – базовые средства. 3. Управление доступом в Windows – средства реализации принципа минимизации полномочий. 4. Управление доступом в Windows – элементы изолированной программной среды. 5. Управление доступом в Windows – средства контроля целостности. 6. Аутентификация в UNIX. 7. Аутентификация в Windows. 8. Аудит в UNIX. 9. Аудит в Windows. **Раздел «Интеграция защищенных операционных систем в защищенную сеть».** 1. Развертывание леса доменов Windows. 2. Управление доменами Windows. 3. Групповая политика в доменах Windows. 4. Централизованное планирование политики безопасности в лесу доменов Windows.
Трудоёмкость (з.е. / часы)	**3** ЗЕ/**108** часов.
Форма итогового контроля знаний	Зачёт.

Аннотация учебной дисциплины

Учебная дисциплина **«ЗАЩИТА ПРОГРАММ И ДАННЫХ»**	
Цель изучения дисциплины	**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.
Компетенции, формируемые в результате освоения дисциплины	Процесс изучения дисциплины направлен на формирование следующих ***компетенций***: - Способен разрабатывать компоненты программных и программно-аппаратных средств защиты информации в компьютерных системах и проводить анализ их безопасности (ОПК-13);
Знания, умения и навыки, получаемые в процессе изучения дисциплины	В результате освоения дисциплины студент должен ***знать***: - 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; ***уметь***: - строить теоретические модели политик безопасности, политик управления доступом и информационными потоками в компьютерных системах с учётом различных факторов; ***владеть***: - навыками по реализации формальных моделей безопасности на практике.
Краткая Характеристика учебной дисциплины (основные блоки и темы)	**Содержание основных разделов (тем) курса** **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. **2. Защита программ от анализа.** Защита от дизассемблирования. Защита от отладки. Методы встраивания защиты в программное обеспечение. **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. **4. Внедрение программных закладок.** 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.** 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.** 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.
Трудоёмкость (з.е. / часы)	Согласно рабочему учебному плану курс читается в полном объёме в течение 8 семестра **3** ЗЕТ / **108** часов.
Форма итогового контроля знаний	В конце **8**-го семестра предусмотрен ***зачёт***.

Аннотация учебной дисциплины

Учебная дисциплина **«ОСНОВЫ ПОСТРОЕНИЯ ЗАЩИЩЕННЫХ БАЗ ДАННЫХ»**	
Цель изучения дисциплины	Дисциплина **«*Основы построения защищенных баз данных*»** имеет **целью** обучить студентов принципам обеспечения безопасности информации в автоматизированных системах, основу которых составляют базы данных, дать навыки работы со встроенными в СУБД средствами защиты, а также показать возможные пути построения собственных механизмов защиты информации в АИС с СУБД.
Компетенции, формируемые в результате освоения дисциплины	Процесс изучения дисциплины направлен на формирование следующих ***компетенций***: - Способен проектировать базы данных, администрировать системы управления базами данных в соответствии с требованиями по защите информации (ОПК-14); -Способен разрабатывать и анализировать математические модели механизмов защиты информации (ОПК-2.2)

Знания, умения и навыки, получаемые в процессе изучения дисциплины	В результате изучения дисциплины «Основы построения защищенных систем управления базами данных» студент должен: **знать**: • основные угрозы безопасности информации и модели нарушителя в КС; • основные виды политик управления доступом и информационными потоками в КС; • характеристики и типы систем баз данных; • физическую организацию баз данных и принципы (основы) их защиты; • средства и методы хранения и передачи аутентификационной информации; • требования к подсистеме аудита и политике аудита; **уметь**: • формализовать поставленную задачу; • разрабатывать модели угроз и модели нарушителя безопасности КС; • разрабатывать частные политики безопасности КС, в том числе, политики управления доступом и информационными потоками; • организовывать удаленный доступ к базам данных; • пользоваться средствами защиты, предоставляемыми СУБД; **владеть**: • методами и средствами выявления угроз безопасности КС; • методами моделирования безопасности КС, в том числе, моделирования управления доступом и информационными потоками в КС; • навыками анализа программных реализаций.
Краткая характеристика учебной дисциплины (основные блоки и темы)	Содержание основных разделов (тем) курса ***Тема 1. Постановка задачи обеспечения информационной безопасности баз данных.*** Этапы научного формирования проблемы обеспечения информационной безопасности баз данных. Критерии качества баз данных. Сущность понятия безопасности баз данных. Основные подходы к методам построения защищенных информационных систем. Архитектура систем управления базами данных. Структура свойства информационной безопасности баз данных ***Тема 2. Угрозы информационной безопасности баз данных*** Источники угроз информации баз данных. Классификация угроз информационной безопасности баз данных. Угрозы, специфичные для систем управления базами данных. Объекты и субъекты моделей информационной безопасности баз данных на примере СУБД Oracle. ***Тема 3. Политика безопасности баз данных*** Сущность политики безопасности. Цель формализации политики безопасности. Принципы построения защищенных систем баз данных. Стратегия применения средств обеспечения информационной безопасности. ***Тема 4. Атаки, специфичные для баз данных*** Подбор и манипуляция с паролями как метод реализации несанкционированных прав. Нецелевое расходование вычислительных ресурсов сервера. Использование триггеров для выполнения незапланированных функций. Использование SQL-инъекции для нештатного использования процедур и функций. ***Тема 5. Анализ методов аутентификации участников взаимодействия в процессе обработки баз данных.*** Аутентификация, основанная на знании и защита от компрометации паролей. Аутентификация, основанная на наличии, и защита от компрометации.

	Аутентификация, основанная на биометрических характеристиках. Аутентификация пользователей в Oracle. Внешняя аутентификация пользователей Oracle. Аутентификация на основе инфраструктуры сертификатов. ***Тема 6. Методы дискреционного разграничения доступа*** Реализация модели дискреционного управления доступом в Oracle. Базовое понятие системы разграничения доступа — привилегии. Предоставление системных привилегий. Предоставление привилегий доступа к объекту. Отмена привилегий. ***Тема 7. Роли и разграничение доступа на основе ролей.*** Базовая ролевая модель разграничения доступа. Расширенные ролевые модели. Управление привилегиями с помощью ролей в СУБД Oracle. Управление допустимостью использования ролей. Технология обеспечения конфиденциальности системы распределенных баз данных на основе ролевой модели доступа. ***Тема 8. Реализация мандатной модели доступа в СУБД Oracle*** Реализация мандатной модели доступа в СУБД Oracle ***Тема 9. Шифрование элементов баз данных*** Шифрование данных с неявным заданием ключа. Шифрование данных с явным заданием ключа. ***Тема 10. Статическая и динамическая проверка ограничений целостности*** Статическая и динамическая проверка ограничений целостности. ***Тема 11. Обеспечение согласованности данных в многопользовательском режиме обработки.*** Понятие транзакции. Параллельная обработка данных и уровни изоляции. Типы блокировок. ***Тема 12. Анализ включающей инфраструктуры.*** Архитектура сервера с позиций администратора безопасности. Управление прослушивающим процессом. Управление доступностью табличных областей. Тема 13. Аудит систем баз данных. Причины проведения аудита. Общая характеристика средств аудита СУБД. Аудит системных событий в Oracle. Аудит событий, связанных с доступом к объекту. Обработка данных аудита. Прекращение регистрации событий. Возможности избирательного аудита в Oracle. ***Тема 13. Аудит систем баз данных.*** Причины проведения аудита. Общая характеристика средств аудита СУБД. Аудит системных событий в Oracle. Обработка данных аудита. Прекращение регистрации событий. Возможности избирательного аудита в Oracle. Тематика лабораторных работ • Анализ методов аутентификации участников взаимодействия в процессе обработки баз данных • Методы дискреционного разграничения доступа • Роли и разграничение доступа на основе ролей • Шифрование элементов баз данных. • Реализация мандатной модели доступа в СУБД Oracle • Статическая и динамическая проверка ограничений целостности • Обеспечение согласованности данных в многопользовательском режиме обработки • Анализ включающей инфраструктуры • Аудит систем баз данных

Трудоёмкость (з.е. / часы)	**3** ЗЕТ / **108** часа.
Форма итогового контроля знаний	**зачет**

Аннотация учебной дисциплины

Учебная дисциплина **«Защита данных в государственных информационных системах»**	
Цель изучения дисциплины	Дисциплина **«*Защита данных в государственных информационных системах*»** имеет ц**елью** 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.
Компетенции, формируемые в результате освоения дисциплины	Процесс изучения дисциплины направлен на формирование следующих ***компетенций***: - Способность оценивать роль информации, информационных технологий и информационной безопасности в современном обществе, их значение для обеспечения объективных потребностей личности, общества и государства (ОПК-1); - Способность применять нормативные правовые акты, нормативные и методические документы, регламентирующие деятельность по защите информации; (ОПК-5); - 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); - Способность проводить сравнительный анализ и осуществлять обоснованный выбор программных и программно-аппаратных средств защиты информации с учетом реализованных в них математических методов (ОПК-2.3)
Знания, умения и навыки, получаемые в процессе изучения дисциплины	В результате изучения дисциплины «***Защита данных в государственных информационных системах***» студент должен: **знать**: место и роль информационной безопасности в системе национальной безопасности Российской Федерации, основы государственной информационной политики, стратегию развития информационного общества в России**;** законодательство Российской Федерации, государственные стандарты и нормативные документы по защите информации, основные общеметодологические принципы теории информационной безопасности применительно к защите государственных информационных систем; 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; классификацию средств защиты информации, условия сертификации средств защиты информации, требования по выбору средств защиты информации в соответствии с установленным классом государственной информационной системы. **Уметь**: классифицировать защищаемую информацию по видам тайны и степеням конфиденциальности**;** систематизировать информацию, формулировать требования к защищаемым системам на основе требований нормативных и правовых документов; 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; 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**: профессиональной терминологией в области информационной безопасности; средствами поиска, методами обобщения нормативных и методических материалов в сфере своей профессиональной деятельности; средствами поиска, обобщения научно-технической информации, нормативных и методических материалов, опыта в сфере своей профессиональной деятельности, разработки инструкций администраторам и пользователям государственных информационных систем; практическими умениями разработки и ведения технической документации информационных систем, настройки средств защиты информации применительно в установленному классу системы.
Краткая характеристика учебной дисциплины (основные блоки и темы)	**Содержание основных разделов (тем) курса** **Тема 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. **Тема 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. **Тема 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. **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. 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. ***Тема 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.
Трудоёмкость (з.е. / часы)	**3** ЗЕТ / **108** часа.
Форма итогового контроля знаний	**зачет**

Аннотация учебной дисциплины

Учебная дисциплина **«МЕТОДЫ АЛГЕБРАИЧЕСКОЙ ГЕОМЕТРИИ В КРИПТОГРАФИИ»**	
Цель изучения дисциплины	***Целью*** освоения дисциплины **«*Методы алгебраической геометрии в криптографии*»** является: - 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.
Компетенции, формируемые в результате освоения дисциплины	Процесс изучения дисциплины направлен на формирование следующих ***компетенций***: - Способен разрабатывать и анализировать математические модели механизмов защиты информации (ОПК-2.2);
Знания, умения и навыки, получаемые в процессе изучения дисциплины	В результате освоения дисциплины студент должен ***знать***: • определения и свойства аффинных, проективных и абстрактных алгебраических многообразий и их отображений; • начальные понятия теории схем; • методы подсчёта числа точек алгебраических многообразий, определённых над конечным полем. ***уметь***: • строить проективное замыкание аффинного многообразия; • вычислять размерность и находить особые точки многообразий; • строить дзета-функцию многообразия над конечным полем; • Описывать процедуру редукции алгебраических кривых на языке схем; • логически правильно мыслить, обобщать, анализировать, критически осмысливать информацию, систематизировать, прогнозировать, ставить исследовательские задачи и выбирать пути их решения на основе принципов научного познания; ***владеть***: • методикой перехода из категории многообразий и их морфизмов в категорию полей алгебраических функций и их гомоморфизмов и обратно; • общей процедурой редукции алгебраических кривых на языке схем; • методикой применения алгебраической геометрии в задачах оценки стойкости криптосистем и эффективности геометрических кодов; • английским языком на уровне, достаточном для деловой коммуникации, чтения и перевода текстов по применению алгебраической геометрии в задачах защиты информации.
Краткая характеристика учебной дисциплины (основные блоки и темы)	Содержание основных разделов (тем) курса **Тема 1. Предварительные сведения из алгебры** Задачи и программа курса. Место алгебраической геометрии в ряду других математических и прикладных дисциплин. Источники её развития и области приложения. Роль алгебраической геометрии в криптографии и теории кодирования. Формы самостоятельной работы студентов по изучению курса. Основная литература к курсу. Примеры колец и идеалов. Факторизация по идеалу. Модули над кольцом. Алгебры. Тензорные произведения. Расширение кольца скаляров модуля и алгебры. Простые и максимальные идеалы. Локализация. Нётеровы кольца. Целая зависимость. Основные теоремы коммутативной алгебры.

	Тема 2. Аффинные и проективные многообразия Аффинное пространство. Аффинные алгебраические множества. Топология Зариского. Идеал аффинного алгебраического множества, его свойства. Примеры идеалов. Теорема Гильберта о нулях. Аффинные многообразия. Разложение на неприводимые компоненты. Координатное кольцо. Теорема Гильберта о нулях для координатного кольца. Проективная прямая. Проективное пространство. Однородные координаты. Проективное подпространство. Однородные многочлены и идеалы. Проективные алгебраические множества. Топология Зарисского. Идеал проективного алгебраического множества. Проективные многообразия. Аффинный конус проективного множества. Проективная теорема Гильберта о нулях. Гомогенизация и дегомогенизация. Проективное замыкание. **Тема 3. Предмногообразия** Регулярные функции. Морфизмы квазиаффинных алгебраических множеств. Абстрактное аффинное многообразие. Определение предмногообразия. Свойства топологии предмногообразия. Поле рациональных функций. Локальное кольцо в точке. **Тема 4. Морфизмы и рациональные отображения** Морфизмы предмногообразий. Морфизмы проективных многообразий. Рациональные отображения. Произведение аффинных многообразий. Произведение предмногообразий. Абстрактные многообразия. Произведение проективных многообразий. **Тема 5. Локальная теория алгебраических многообразий** Понятие размерности предмногообразия. Размерность Крулля коммутативного кольца. Размерность и степень трансцендентности поля функций. Понятие коразмерности подмногообразия. Связь размерности, коразмерности и высоты идеала. Системы параметров. Касательное пространство к предмногообразию в точке. **Тема 6. Алгебраическая геометрия над незамкнутым полем** Элементы бесконечной теории Галуа. Рациональные точки аффинного пространства над незамкнутым полем, их характеризации. Рациональные точки аффинных алгебраических множеств над незамкнутым полем, их характеризации. Идеал алгебраического множества над незамкнутым полем. Теорема Гильберта о нулях над незамкнутым полем. Координатное кольцо алгебраического множества над незамкнутым полем. Рациональные точки проективного пространства над незамкнутым полем, их характеризации. Рациональные точки проективных алгебраических множеств над незамкнутым полем, их характеризации. Проективная теорема Гильберта о нулях над незамкнутым полем. Регулярные функции над незамкнутым полем. Морфизмы квазипроективных алгебраических множеств, определённые над незамкнутым полем. Рациональные функции над незамкнутым полем. Рациональные отображения над незамкнутым полем. Произведение аффинных и проективных многообразий над незамкнутым полем. **3.2. Тематика практических занятий** **Тема 1.** Решение элементарных задач по коммутативной алгебре. **Тема 2.** Исследование свойств конкретных аффинных алгебраических множеств. Исследование свойств конкретных проективных алгебраических множеств.

	Тема 3. Исследование свойств конкретных морфизмов аффинных алгебраических множеств. **Тема 4.** Исследование свойств конкретных морфизмов проективных алгебраических множеств. Исследование свойств полей рациональных функций, локальных колец и рациональных отображений конкретных квазипроективных многообразий. **Тема 5.** Вычисление размерности конкретных многообразий и коразмерности конкретных подмногообразий. Отыскание минимальной системы параметров, определяющих подмногообразие. **Тема 6.** Исследование свойств конкретных многообразий, их морфизмов и рациональных отображений, определённых над незамкнутым полем.
Трудоёмкость (з.е. / часы)	**3** ЗЕ / **108** часов.
Форма итогового контроля знаний	***Экзамен***

Аннотация учебной дисциплины

Учебная дисциплина **«ОРГАНИЗАЦИОННОЕ И ПРАВОВОЕ ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ»**	
Цель изучения дисциплины	***Целью** освоения дисциплины «**Организационное и правовое обеспечение информационной безопасности**» является:* 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
Компетенции, формируемые в результате освоения дисциплины	Процесс изучения дисциплины «Организационно-правовое обеспечение информационной безопасности» направлен на формирование следующих ***компетенций***: - способен применять нормативные правовые акты, нормативные и методические документы, регламентирующие деятельность по защите информации (ОПК-5); - способен 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).
Знания, умения и навыки, получаемые в процессе изучения дисциплины	В результате изучения дисциплины студент должен: **знать**: - организацию работы и нормативные правовые акты и стандарты по лицензированию деятельности в области обеспечения защиты государственной тайны, технической защиты конфиденциальной информации, по аттестации объектов информатизации и сертификации средств защиты информации;

	- основы организационного и правового обеспечения информационной безопасности, основные нормативные правовые акты в области обеспечения информационной безопасности и нормативные методические документы ФСБ России и ФСТЭК России в области защиты информации; **уметь**: - применять нормативные правовые акты и нормативные методические документы в области обеспечения информационной безопасности; - применять действующую законодательную базу в области обеспечения компьютерной безопасности; - пользоваться нормативными документами по противодействию технической разведке; - применять отечественные и зарубежные стандарты в области компьютерной безопасности для проектирования, разработки и оценивания защищенности компьютерной системы; - разрабатывать проекты нормативных и организационно-распорядительных документов, регламентирующих работу по защите информации; **владеть**: - навыками работы с нормативными правовыми актами.
Краткая характеристика учебной дисциплины (основные блоки и темы)	**Содержание основных разделов (тем) дисциплины:** 1. **Правовое обеспечение информационной безопасности**. Информационные отношения как объект правового регулирования. Законодательство Российской Федерации в области информационной безопасности. Правовой режим защиты государственной тайны. Правовые режимы защиты информации конфиденциального характера. Государственное регулирование деятельности в области защиты информации. Международные и отечественные стандарты в области информационной безопасности. Нормативные методические документы ФСБ России и ФСТЭК России. Правовая охрана результатов интеллектуальной деятельности. Преступления в сфере компьютерной информации. Основы расследования преступлений в сфере компьютерной информации. Иные преступления в информационной сфере. **2. Организационное обеспечение информационной безопасности**. Понятие организационной защиты информации. Понятие «режим защиты информации». Политика информационной безопасности. Подразделения, обеспечивающие ИБ предприятия. Методы обеспечения физической безопасности. Технологические меры поддержания безопасности. Организация режима секретности. Режим секретности как основной порядок деятельности в сфере защиты государственной тайны. Виды представления информации. Пути прохождения информации. Порядок допуска к государственной тайне. Защита компьютерной информации. Основные каналы утечки информации при обработке на компьютерах.
Трудоёмкость (з.е. / часы)	**3 ЗЕ / 108** часов
Форма итогового контроля знаний	**Зачет**.

Аннотация учебной дисциплины

Учебная дисциплина **«КОМПЬЮТЕРНЫЙ ПРАКТИКУМ ПО КРИПТОГРАФИИ НА ЭЛЛИПТИЧЕСКИХ КРИВЫХ»**	
Цель изучения дисциплины	Целями освоения дисциплины **«Компьютерный практикум по криптографии на эллиптических кривых»** являются: – 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.
Компетенции, формируемые в результате освоения дисциплины	Процесс изучения дисциплины направлен на формирование следующих ***компетенций***: - Способен разрабатывать алгоритмы, реализующие современные математические методы защиты информации (ОПК-2.1);
Знания, умения и навыки, получаемые в процессе изучения дисциплины	В результате освоения дисциплины студент должен: **Знать:** – уравнение и основные свойства эллиптических кривых над полем рациональных, действительных и комплексных чисел; – 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; – методы разложения больших чисел на простые множители и тесты на простоту, использующие эллиптические кривые; – конструкцию криптосистем с открытым ключом на эллиптических кривых **Уметь:** – подсчитывать число рациональных точек эллиптической кривой над конечным полем; – определять структуру группы рациональных точек эллиптической кривой над конечным полем; – формировать класс эллиптических кривых над конечным полем, «подходящих» для создания криптосистемы; – оценивать эффективность криптосистем на эллиптических кривых. – производить маркировку и демаркировку единичных сообщений; – производить зашифрование и расшифрование единичных сообщений;

	– моделировать алгоритмы в системах компьютерной алгебры, оценивать их работоспособность и эффективность; – ориентироваться в современных и перспективных математических методах защиты информации, оценивать возможность и эффективность их применения в конкретных задачах защиты информации **Владеть:** – навыками эффективных вычислений в группе точек эллиптической кривой; – методами расчета параметров криптосистем на эллиптических кривых, обеспечивающих их надежность и эффективность. – современными методами и средствами исследования для обеспечения информационной безопасности компьютерных систем.
Краткая характеристика учебной дисциплины (основные блоки и темы)	**Содержание основных разделов и тем курса** Эллиптические кривые над **R**. Уравнение эллиптической кривой. Сложение точек эллиптической кривой над **R**. Эллиптические кривые над **Q**. Точки конечного порядка. Подгруппа кручения. Теорема Лутц-Нагеля. Теорема Мазура. Эллиптические кривые над произвольным полем Основные определения. Дискриминант и j-инвариант. Изоморфизм кривых. Сложение точек. Случай характеристики $\neq 2, 3$ Эллиптические кривые над конечными полями Квадратичный характер и подсчёт числа точек. Дзета-функция эллиптической кривой над конечным полем. Теорема Хассе. Теорема Вейля. L-многочлен. Суперсингулярные эллиптические кривые. 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.
Трудоёмкость (з.е. / часы)	**6** ЗЕТ/**216** часа.
Форма итогового контроля знаний	**Экзамен, курсовая работа**

Аннотация учебной дисциплины

Учебная дисциплина **«Криптография на решётках»**	
Цель изучения дисциплины	***Цели*** освоения дисциплины «Криптография на решетках»: - изучение новых парадигм конструкций пост-квантовых асимметрических механизмов (цифровой подписи, шифрования, обмена ключами);

	- теоретические и практические навыки криптоанализа, в основе которого используются евклидовы решетки.
Компетенции, формируемые в результате освоения дисциплины	Процесс изучения дисциплины направлен на формирование следующих ***компетенций***: - подготовка к процедуре защиты выпускной квалификационной работы (ОПК-8); - способен анализировать тенденции развития методов и средств криптографической защиты информации, использовать средства криптографической защиты информации при решении задач профессиональной деятельности (ОПК-10); - способен разрабатывать алгоритмы, реализующие современные математические методы защиты информации (ОПК-2.1).
Знания, умения и навыки, получаемые в процессе изучения дисциплины	В результате освоения дисциплины студент должен ***знать***: - основные понятия и результаты 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). ***уметь***: - находить редуцированный базис и применять его к криптоаналитическим задачам; - находить короткий вектор решетки, используя готовые библиотеки; - строить схему цифровой подписи на решетке и оценивать её криптографическую стойкость; - строить схему шифрования на решетке и оценивать её криптографическую стойкость; ***владеть***: - методами криптоанализа, основанного на алгоритмах редукции базиса решетки; - навыками программирования задач, связанных с решетками, в системах python, sage; - методами эффективной реализации криптографических алгоритмов (подписи, шифрования) на решетках.
Краткая Характеристика учебной дисциплины (основные блоки и темы)	**Содержание основных разделов (тем) курса** Тема № 1. Основные определения: евклидова решетка, определитель, минимумы. Тема № 2. Теорема Минковского, конструкция А. Тема № 3. LLL алгоритм. Тема № 4. Алгоритм перечисления для SVP. BKZ алгоритм. Тема № 5. Алгоритмы просеивания. Тема № 6. Задачи CVP и SVP. Тема № 7. Задачи BDD, approxSVP, uSVP. Их эквивалентность. Тема № 8. Дуальные решетки и преобразование Фурье. Гауссово распределение на решётке. Тема № 9. Задача SIS, её сложность и алгоритм цифровой подписи на решетках.

	Тема № 10. Задача LWE, её сложность и алгоритм шифрования. Тема № 11. Идеальные решётки.
Трудоёмкость (з.е. / часы)	Согласно рабочему учебному плану курс читается в полном объёме в течение 10 семестра **6** ЗЕТ / **216** часов.
Форма итогового контроля знаний	В конце **10**-го семестра предусмотрен ***экзамен***.

Аннотация учебной дисциплины

Учебная дисциплина **«ЭЛЕКТРОНИКА И СХЕМОТЕХНИКА»**	
Цель изучения дисциплины	**Целью** курса "Электроника и схемотехника" является дать необходимые знания будущему специалисту в области основ построения радиоэлектронной аппаратуры, используемой в построении информационных систем. Полученные знания будущий специалист сможет использовать в своей деятельности, связанной с эксплуатацией и обслуживанием аппаратуры и оборудования, содержащего современные средства вычислительной техники, в подразделениях ФСБ России, ФАПСИ при Президенте РФ, СВР РФ и МО РФ и других организациях и предприятиях. А также сформировать у студентов системный подход к изучению и проектированию сложных электронных систем.
Компетенции, формируемые в результате освоения дисциплины	Изучение дисциплины нацелено на формирование следующих компетенций обучающихся: - Способен 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).
Знания, умения и навыки, получаемые в процессе изучения дисциплины	В результате освоения дисциплины студент должен: ***Знать***: - 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 ЭВМ 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.
Краткая характеристика учебной дисциплины (основные блоки и темы)	1. Основы теории электрических цепей и сигналов. Основные понятия теории электрических цепей. Ток и напряжение, как основные величины, определяющие состояние электрической цепи и как сигналы, переносящие информацию. Основные положения теории электрических цепей. Идеальные элементы цепей. Уравнения пассивных элементов цепей. Источники тока и напряжения. Зависимые источники. Электрические и эквивалентные схемы электрических цепей. Классификация электрических цепей. Топологические понятия: узел, контур и граф цепи. Уравнения соединений. 2. Электрические цепи при гармоническом воздействии. Гармоническое колебание. Комплексная амплитуда гармонического сигнала. Комплексная форма уравнений элементов. Комплексные сопротивления и проводимости. Частотные свойства реактивных элементов цепей. Комплексная форма уравнений соединений. Метод комплексных амплитуд. Векторные диаграммы токов и напряжений. Анализ цепей в частотной области. Мощность переменного тока. Активная и реактивная мощности. 3. Сложные электрические цепи. Особенности анализа сложных электрических цепей. Методы контурных токов и узловых напряжений. Учет зависимых источников в цепях с активными элементами. Теоремы электрических цепей. Теоремы об эквивалентных источниках напряжения и тока. 4. Четырехполюсники, фильтры и длинные линии. Четырехполюсники, их уравнения и параметры. Коэффициенты передачи по напряжению и току, входные и выходные сопротивления четырехполюсника. Амплитудно-частотные и фазо-частотные характеристики. Фильтры: классификация, основные параметры, применение. Колебательные контуры и их частотные характеристики. Цепи с распределенными параметрами. Телеграфные уравнения. Бегущие волны в длинной линии. Коэффициент отражения. Стоячие и смешанные волны. КСВ и КБВ. 5. Сигналы и их спектры. Периодический сигнал и ряд Фурье. Комплексная форма ряда Фурье. Амплитудный и фазовый спектры сигнала. Отрицательные частоты. Физический и двусторонний спектры. Интеграл Фурье и спектр непериодического сигнала. Теоремы о спектрах. Радиотехнические сигналы и их спектры. Модулированные сигналы и их применение. Амплитудная, фазовая и частотная модуляции. Спектры модулированных сигналов. Элементы статистической радиотехники. Воздействие сигналов на линейные электрические цепи. Спектральный метод. Операторный метод анализа динамики цепей, основанный на преобразовании Лапласа. Основные теоремы операторного метода. 6. Полупроводниковые приборы. Полупроводники. Электронно-дырочный переход. Диоды. Виды полупроводниковых диодов, особенности работы и параметры. Биполярные и полевые транзисторы: принципы работы и разновидности. Параметры полупроводниковых приборов. Вольтамперные характеристики транзисторов и их эквивалентные схемы. 7. Электронные усилители.

	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. Интегральные схемы. Элементы интегральных схем. Дифференциальный усилитель. Операционные усилители. Характеристики и параметры операционных усилителей. Аналоговые перемножители сигналов. 8. Нелинейное и параметрическое преобразование сигналов. Воздействие на нелинейный элемент большого по уровню сигнала. Нелинейное усиление и умножение частоты. Воздействие на нелинейный и параметрический элемент двух сигналов. Перемножение сигналов, преобразование частоты, модуляция и демодуляция. Генераторы колебаний. Мультивибраторы. 9. Импульсные и цифровые устройства. Общая характеристика и принципы построения импульсных устройств. Импульсные сигналы и их основные параметры. Диодные и транзисторные ключи. Логические элементы цифровых устройств, их параметры и схемы (ТТЛ, КМОП, ЭСЛ и др.). Комбинационные схемы. Дешифраторы, шифраторы, мультиплексоры. Триггеры RS, T, D, JK. Применение триггеров. Счетчики, регистры, мультивибраторы, компараторы и другие элементы импульсных и цифровых устройств. 10. Цифровая обработка сигналов. Аналоговые, дискретные и цифровые сигналы. Дискретизация и квантование. Погрешность дискретизации. Аналого-цифровые и цифро-аналоговые преобразователи. Дискретное преобразование Фурье. Быстрые преобразования. Цифровые фильтры. Частотные характеристики цифровых фильтров. Перспективы развития радиоэлектроники. **Тематика лабораторных работ** Для практического закрепления материала предусматривается выполнение моделирующих лабораторных работ. Они выполняются в системе моделирования "ElectronicsWorkbench" и дают наглядное представление о физических условиях и принципах работы реальных технических средств. Раздел 1. Основы теории электрических цепей и сигналов. Тема: Исследование элементов электрических цепей. Тема: Преобразования двухполюсников. Раздел 2. Электрические цепи при гармоническом воздействии. Тема: Амплитудно-фазовые соотношения в простых цепях Раздел 3. Сложные электрические цепи. Тема: Исследование разветвленной электрической цепи постоянного тока с линейными элементами. Раздел 4. Четырехполюсники, фильтры и длинные линии. Тема: Исследование электрических фильтров. Раздел 5. Сигналы и их спектры. Тема: Исследование спектров амплитудно-модулированных и частотно-модулированных сигналов. Раздел 6.Полупроводниковые приборы. Тема: Исследование диодов и стабилитронов. Тема: Исследование биполярного транзистора. Тема: Исследование полевого транзистора. Раздел 7.Электронные усилители. Тема: Исследование простейших транзисторных усилителей переменного напряжения.

	Тема: Исследование операционных усилителей. Раздел 8. Нелинейное и параметрическое преобразование сигналов. Тема: Исследование автогенератора. Тема: Исследование активных фильтров на основе операционного усилителя. Раздел 9. Импульсные и цифровые устройства. Тема: Исследование и синтез логических элементов и устройств на их основе. Тема: Исследование и синтез устройств комбинационного типа. Тема: Исследование и синтез устройств последовательностного типа. Раздел 10.Цифровая обработка сигналов. Тема: Исследование цифровых фильтров. Тема: Исследование аналого-цифрового и цифро-аналогового преобразователей.
Трудоёмкость (з.е. / часы)	Курс изучается студентами в 8 семестре **6** ЗЕТ / **216** часов.
Форма итогового контроля знаний	В конце семестра в качестве итогового контроля предусмотрен **экзамен**.

Аннотация учебной дисциплины

Учебная дисциплина **«ВВЕДЕНИЕ В СПЕЦИАЛЬНОСТЬ»**	
Цель изучения дисциплины	***Целями*** освоения дисциплины **«*Введение в специальность*»** являются: - обеспечение освоения студентами основ обучения в высшей школе, знакомство с ФГОС и учебными планами по направлению подготовки, учебной образовательной программой, структуры университета, института ФМНиИТ, истории развития Института, а также базовых понятий – специальность, бакалавриат, магистратура, аспирантура, лекции, практические занятия, лабораторные работы; - первичных знаний 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
Компетенции, формируемые в результате освоения дисциплины	Процесс изучения дисциплины направлен на формирование следующих ***компетенций***: - 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)
Знания, умения и навыки, получаемые в процессе	В результате освоения дисциплины студент должен: **Знать**: - основные закономерности исторического процесса, этапы исторического развития России, место и роль России в истории человечества и в

изучения дисциплины	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; - понятия информации, информационной безопасности, место и роль информационной безопасности в системе национальной безопасности Российской Федерации, основы государственной информационной политики. **Уметь**: - анализировать общие исторические процессы и отдельные факты, выявлять существенные черты исторических процессов, явлений и событий в интересах национальной безопасности Российской Федерации; - классифицировать защищаемую информацию по видам тайн и степеням конфиденциальности, классифицировать и оценивать угрозы информационной безопасности для объекта информатизации. **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.
Краткая характеристика учебной дисциплины (основные блоки и темы)	**Содержание основных разделов (тем) дисциплины:** **1. Организация высшего образования в области информационной безопасности:** Правовые аспекты высшего образования: правовое регулирование отношений в сфере образования (Конституция РФ, Закон об образовании РФ), п **2. Организация учебного процесса в университете:** Университет, структура, основные направления подготовки; Институт физико-математических наук и информационных технологий, руководство, а т р у к **3. Введение в информационную безопасность:** История развития проблемы защиты информации, понятия национальной информационной защиты, понятия информационной войны. **4. Общее представление о защищаемой информации:** Понятие об информации как предмете защиты, основные виды информационного законодательства. **5. Человек и информация. Общие понятия о передаче информации на расстояние:**

	Информация, сообщение, сигнал; канал обработки и передачи информации; виды сигналов и их свойства. **6. Информационные угрозы. Методы и средства защиты информации:** Информационная безопасность, виды информационных угроз, вирусы, методы защиты информации. **7. Основные каналы утечки информации:** Актуальность вопроса, основные каналы утечки информации при её обработке в информационно-телекоммуникационных системах, другие виды каналов утечки информации. **8. Организация защиты информации на предприятиях (учреждениях, организациях):** С о
Трудоёмкость (з.е. / часы)	**6** ЗЕТ / **216** часов.
Форма итогового контроля знаний	***Зачёт с оценкой***.

Аннотация учебной дисциплины

Учебная дисциплина «**ИСТОРИЯ КРИПТОГРАФИИ**»	
Цель изучения дисциплины	***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
Компетенции, формируемые в результате освоения дисциплины	Процесс изучения дисциплины направлен на формирование следующих ***компетенций***: 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)
Знания, умения и навыки, получаемые в процессе изучения дисциплины	**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.
Краткая характеристика учебной дисциплины (основные блоки и темы)	**Содержание разделов дисциплины** **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. 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**

Трудоёмкость (з.е. / часы)	Согласно рабочему учебному плану курс читается в полном объёме в течение **4** семестра **3 ЗЕ / 108 часов.**
Форма итогового контроля знаний	В конце 4 -го семестра предусмотрен ***зачет***.

Аннотация учебной дисциплины

Учебная дисциплина **«Теория чисел»**	
Цель изучения дисциплины	***Целью*** освоения дисциплины «*Теория чисел*» является развитие и углубление курса для приложений теории чисел к информатике, в частности, к проблемам защиты информации, а также показать связь абстрактных теоретико-числовых конструкций с приложениями в криптографии и теории кодирования.
Компетенции, формируемые в результате освоения дисциплины	Процесс изучения дисциплины направлен на формирование следующих ***компетенций***: - способность проводить анализ и участвовать в разработке математических моделей безопасности компьютерных систем (ПКС-5)
Знания, умения и навыки, получаемые в процессе изучения дисциплины	В результате освоения дисциплины студент должен ***знать***: основополагающие факты теории чисел, лежащие в основе построения многих математических объектов (основная теорема арифметики, бесконечность множества простых чисел и др.); сущность основных понятий и результатов, изучаемых в дисциплине; свойства простых и составных чисел, методы решения сравнений, использование теоретико-числовых функций и теории индексов при решении прикладных задач. ***уметь***: использовать полученные теоретические знания для решения конкретных прикладных задач, производить математические расчеты в стандартных постановках, производить содержательный анализ результатов вычислений; устанавливать разрешимость и находить решения алгебраических сравнений и систем сравнений, показательных сравнений; находить системы первообразных корней; проводить вычисления с основными теоретико-числовыми функциями. ***владеть***: навыками построения теоретико-числовых моделей и умениями произвести соответствующие числовые расчеты; навыками применения понятий и методов дисциплины для решения различных задач, используемых в дальнейшей учебной и профессиональной деятельности.
Краткая Характеристи каучебной дисциплины (основные блоки и темы)	**Содержание основных разделов (тем) курса** Тема 1. Теория делимости целых чисел. Тема 2. Простые числа. Тема 3. Теория сравнений. Тема 4. Теорема Ферма. Тема 5. Теоретико-числовые функции. Тема 6. Примитивные корни и индексы. Тема 7. Цепные дроби.

Трудоёмкость (з.е. / часы)	Согласно рабочему учебному плану курс читается в полном объёме в течение **3** семестра **3** ЗЕТ / **108** часов.
Форма итогового контроля знаний	В конце **3**-го семестра предусмотрен ***зачёт***.

Аннотация учебной дисциплины

Учебная дисциплина **«СИСТЕМЫ КОМПЬЮТЕРНОЙ АЛГЕБРЫ И РЕАЛИЗАЦИЯ КРИПТОГРАФИЧЕСКИХ АЛГОРИТМОВ»**	
Цель изучения дисциплины	***Целями*** освоения дисциплины 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.
Компетенции, формируемые в результате освоения дисциплины	**Компетенции, формируемые у обучающегося в результате освоении дисциплины.** Способность участвовать в теоретических и экспериментальных научно-исследовательских работах по оценке защищенности информации в компьютерных системах (ПКС-5)
Знания, умения и навыки, получаемые в процессе изучения дисциплины	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 возможность и эффективность их применения в конкретных 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.
Краткая характеристика учебной дисциплины (основные блоки и темы)	*Содержание разделов дисциплины* **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. 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
Трудоёмкость (з.е. / часы)	Согласно рабочему учебному плану курс читается в полном объёме в течение 6 семестра **4** ЗЕ / **144** часа.
Форма итогового контроля знаний	В конце **6**-го семестра предусмотрен **зачет**.

Аннотация учебной дисциплины

Учебная дисциплина **«ОСНОВЫ ТЕХНИЧЕСКОЙ ФИЗИКИ»**	
Цель изучения дисциплины	**Целью** курса является изложение той части физических знаний, которые необходимы студентам для успешного усвоения последующих специальных курсов по защите информации и обеспечения возможности творческого решения конкретных задач в своей дальнейшей профессиональной деятельности. Прежде всего это дисциплины "Электроника и схемотехника" и "Техническая защита информации". В основе всех технических каналов утечки информации лежат те или иные физические эффекты. Работа технических средств негласного съема информации и технических средств защиты информации от утечки по техническим каналам основана также на физических явлениях и эффектах, происходящих как в окружающем пространстве, так и в полупроводниковых элементах, на базе которых реализованы технические средства. В отличие от курса общей физики, который преподается студентам вне зависимости от их дальнейшей профессиональной направленности, данный курс предполагает более глубокое изложение отдельных глав или разделов физики с акцентом на техническую реализацию тех или иных физических явлений и эффектов. Предлагаемый курс окажется также может оказаться полезным и специалистам, уже работающим в сфере обеспечения защиты информации от

	ее утечки по техническим каналам в государственных и коммерческих структурах.
Компетенции, формируемые в результате освоения дисциплины	Процесс изучения дисциплины направлен на формирование ***компетенции***: - Способен организовывать и проводить работы по технической защите информации (ПКС-3).
Знания, умения и навыки, получаемые в процессе изучения дисциплины	В результате изучения дисциплины студент должен: ***Знать***: - Физические основы технических каналов утечки информации; - Принципы технической реализации различных физических эффектов; - Физико-технические возможности различных видов технической разведки; - Физико-технические основы, на которых базируются современные средства технической защиты информации. ***Уметь***: - Правильно оценить реальность угрозы утечки информации по тем или иным техническим каналам; - Применять наиболее эффективные методы и средства технической защиты информации; - Оценивать эффективность мер предполагаемой технической защиты информации. ***Владеть***: - Навыками выявления физических эффектов и явлений, способствующих образованию технических каналов утечки информации; - Методами оценки угроз утечки информации по техническим каналам.
Краткая характеристика учебной дисциплины (основные блоки и темы)	**Содержание основных разделов (тем) курса** 1. Введение 1.1 Современные проблемы технической защиты информации. 1.2 Технические каналы утечки информации. 2. Колебательные и волновые процессы. 2.1 Собственные колебания. 2.2 Вынужденные колебания. 2.3 Параметрические колебания. 2.4 Колебания в распределенных системах. 2.5 Волновые уравнения. 3. Физические основы акустики 3.1 Упругие волны. 3.2 Отражение и преломление упругих волн на границе двух сред. 3.3 Энергия упругих волн. 3.4 Поглощение упругих волн. 4. Электромагнитные колебания и волны 4.1 Колебания в электрических линиях передачи. 4.2 Волновое уравнение для электромагнитных волн.

	4.3 Отражение и преломление электромагнитных волн на границе двух сред. 4.4 Энергия электромагнитных волн. 4.5 Излучение диполя. 4.6 Излучение радиоволн антеннами. 5. Оптика 5.1 Электромагнитная природа света. 5.2 Геометрическая оптика. 5.3 Основы фотометрии. 5.4 Интерференция света. 5.5 Дифракция света. 5.6 Поляризация света. 5.7 Взаимодействие света с веществом. 6 Оптические линии связи 6.1 Основные положения. 6.2 Оптическое временное мультиплексирование. 6.3 Оптическое частотное мультиплексирование. 6.4 Основы электродинамики оптических линий связи. 6.5 Типы оптических волокон. 6.6 Геометрические параметры оптических волокон. 6.7 Соединение оптических волокон. 7. Физические основы полупроводниковых приборов 7.1 Строение атома. 7.2 Строение твердых тел. Зонная теория твердых тел. 7.3 Зонная диаграмма собственных полупроводников. 7.4 Зависимость проводимости собственных полупроводников от температуры. 7.5 Примесные полупроводники. Зонные диаграммы донорного и акцепторного полупроводника. 7.7 Зависимость проводимости примесных полупроводников от температуры. 7.8 *P-n*-переход и его свойства. Вольтамперная характеристика *p-n*-перехода, ее зависимость от температуры. 8. Физические основы лазеров 8.1 Принципы действия газовых, твердотельных и полупроводниковых лазеров. 8.2 CO_2-лазер, схема энергетических уровней. Условия и режимы генерации. Способы накачки. 8.3 Nd-YAG-лазер, схема энергетических уровней. Условия и режимы генерации. Способы накачки. 8.4 Полупроводниковые лазеры, их особенности. Принципы создания инверсной населенности. Конструкция простейшего инжекционного лазера. 8.5 Голография. 9. Заключение
Трудоёмкость	**4**ЗЕТ/ **144** часов.

(з.е. / часы)	
Форма итогового контроля знаний	***экзамен***

Учебная дисциплина **«МАТЕМАТИЧЕСКИЕ МЕТОДЫ ДИАГНОСТИКИ КОМПЬЮТЕРНЫХ СИСТЕМ»**	
Цель изучения дисциплины	***Целями*** освоения 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
Компетенции, формируемые в результате освоения дисциплины	Процесс изучения дисциплины направлен на формирование следующих ***компетенций***: - способность проводить анализ и участвовать в разработке математических моделей безопасности компьютерных систем (ПКС-7)
Знания, умения и навыки, получаемые в процессе изучения дисциплины	В результате освоения дисциплины студент должен: **иметь:** - представление об общем содержании математических моделей, используемых в теории диагностики; о роли и свойствах показателей эффективности и качества компьютерных систем; об автоматизированных системах технического диагностирования. **знать:** - основные определения и понятия качества компьютерных систем, свойства показателей надёжности, закономерности и физические процессы возникновения отказов; математические модели диагностики, способы анализа и расчёта показателей диагностики; - методы анализа и оценки компьютерных систем как объектов эксплуатации в составе средств защиты информации, методы оценки их технического состояния, методы локализации мест отказов и неисправностей, основные методы прогнозирования технического состояния КС, принципы построения систем технического диагностирования средств защиты. **уметь:** - выбирать модели и показатели диагностики конкретного типа КС в составе средств защиты информации, производить анализ их эффективности, расчёт и оптимизацию; - формировать технические требования по обеспечению заданной надёжности КС, выбирать наиболее оптимальные технические решения и средства;

	- осуществлять испытания на надёжность КС, обрабатывать их результаты и делать конкретные практические выводы; - анализировать причины возникновения отказов, способы и средства их устранения и предупреждения последствий отказов; - определять вид технического состояния компьютерных систем; - рассчитывать показатели диагностирования, выбирать параметры для оценки работоспособности состояния КС, строить оптимальные алгоритмы поиска мест отказов; - производить оценку функционирования состояния объектов КС в составе средств защиты информации; - определять оптимальные стратегии и режимы эксплуатации этапов жизни компьютерных систем защиты информации. **<u>владеть</u>:** - методами управления техническим состоянием компьютерных систем на основе обработки информации, получаемой с помощью диагностических информационных средств защиты информации.
Краткая характеристика учебной дисциплины (основные блоки и темы)	**Содержание основных разделов (тем) дисциплины:** **1. Введение.** Предмет, содержание и задачи дисциплины. Место и роль дисциплины в подготовке специалистов по защите информации. Связь с другими дисциплинами учебного плана. Основные понятия и термины теории диагностики компьютерных систем (КС). **2. Математические методы и модели надёжности компьютерных систем**. Основные понятия и термины теории надёжности, методы и математические модели расчёта надежности КС, статистическая оценка показателей надёжности, пути обеспечения надёжности судового компьютерных систем, резервирование. **3. Основы диагностики компьютерных систем.** Основные понятия и термины диагностики: объект диагностирования, дефект, неисправность, проверка, глубина поиска и кратность неисправности, тест, система и алгоритм технического диагностирования. Математические методы и модели диагностирования компьютерных систем непрерывного типа: понятие математической модели объекта диагностирования, таблица функций неисправностей, логическая модель объекта диагностирования КС, построение таблицы функций неисправностей (ТФН) по заданной логической модели, кратность диагностирования, методика построения ТФН по заданной логической модели. Алгоритмы технического диагностирования КС: построение тестов диагностирования: проверяющий тест, тест поиска неисправностей, минимальный проверяющий тест (МПТ) и минимальный тест поиска неисправностей (МТПН); 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. Инженерная методика поиска неисправностей КС: 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. Средства контроля и технической диагностики компьютерных систем: общая характеристика средств контроля. Встроенные системы контроля. Диагностические стенды. Автоматизированные диагностические стенды. Применение микропроцессоров и микро-ЭВМ для технического диагностирования объектов компьютерных систем. 4.**Заключение**. Основные тенденции и направления совершенствования современных способов диагностики компьютерных систем.
Трудоёмкость (з.е. / часы)	**5** ЗЕТ / **180**часов.
Форма итогового контроля знаний	***Зачёт с оценкой*, КР**

Учебная дисциплина **«КВАНТОВАЯ ЗАЩИТА И ОБРАБОТКА ИНФОРМАЦИИ»**	
Цель изучения дисциплины	***Целями*** освоения дисциплины **«*Квантовая защита и обработка информации*»** являются: - углубление и расширение знаний в области новейших перспективных направлений в информационных технологиях, новых принципов кодирования, обработки, передачи информации и вычислений, основанных на квантовой физике.
Компетенции, формируемые в результате освоения дисциплины	Процесс изучения дисциплины направлен на формирование следующих ***компетенций***: - Способность участвовать в теоретических и экспериментальных научно-исследовательских работах по оценке защищенности информации в компьютерных системах (ПКС-5)
Знания, умения и навыки, получаемые в процессе изучения дисциплины	В результате освоения дисциплины студент должен: •***Знать:*** -новостную информацию о развитии теоретических и экспериментальных исследований в области квантовой информации и квантовых вычислений; место теории квантовых вычислений в ряду экспериментальных и дедуктивных наук; масштабы ресурсов квантовой информации и квантовых вычислений; возможности телепортации; основные понятия квантовой физики, квантовой информации и квантовых вычислений; способы отображения в абстрактном пространстве чистых, смешанных и перепутанных состояний; особенности квантовых единиц информации; свойства кубита, как единицы квантовой информации, соответствие между логическими цепями классических и квантовых компьютеров; принципы действия классических и квантовых

	компьютеров; основные элементы 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 классических алгоритмов. •***Уметь:*** Оценивать самостоятельно и в общении с коллегами достоверность новостной информации о достижениях в области построения квантовых компьютеров и квантовых вычислений; правильно истолковывать терминологию и понятия теории квантовых вычислений; оценивать значимость новых результатов и реалистичность прогнозов в области квантовых вычислений; описывать состояния кубита с помощью дираковского формализма и в матричной форме, отображать состояния кубита на сфере Блоха, использовать волновую функцию в разных представлениях. 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:*** Текущими сведениями о достижениях в области квантовой информации и квантовых вычислений, навыками их критического анализа; навыками научной аргументации собственных прогнозов и предпочтений о путях развития квантовой информации и квантовых вычислений; навыками изучения библиографии, навыками ориентации в профессиональных источниках информации; основополагающими принципами и понятиями теории квантовой информации и квантовых вычислений; навыками описания состояний кубита; формализмом Дирака описания квантовых состояний; методом отображения кубита на сфере Блоха . 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
Краткая характеристика учебной дисциплины (основные блоки и темы)	**Содержание основных разделов (тем) дисциплины:** 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.** Криптографическией 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.
Трудоёмкость (з.е. / часы)	**3** ЗЕТ / **108** часов.
Форма итогового контроля знаний	***Зачёт***

Учебная дисциплина **«Основы криптовалют и блокчейн»**	
Цель изучения дисциплины	***Цели*** освоения дисциплины «**Основы криптовалют и блокчейн**»: - изучение технологии блокчейн; - изучение принципов построения криптовалют Bitcoin, Ethereum, Monero и Zcash; - овладение навыками написания простейших смарт-контрактов криптовалют Bitcoin и Ethereum; - овладение навыками анализа уровня анонимизации предоставляемого различными криптовалютами, а также отдельными механизмами, использующимися для повышения уровня анонимности;
Компетенции, формируемые в результате	Процесс изучения дисциплины направлен на формирование следующих ***компетенций***:

освоения дисциплины	- способность проводить анализ безопасности компьютерных систем на соответствие отечественным и зарубежным стандартам в области компьютерной безопасности (ПКС-6)
Знания, умения и навыки, получаемые в процессе изучения дисциплины	В результате освоения дисциплины студент должен ***знать***: - принципы построения и работы криптовалют и блокчейн технологий; - криптографические инструменты, применяемые в криптовалютах Bitcoin, Ethereum, Monero и Zcash; - механизмы анонимизации и деанонимизации в криптовалютах Bitcoin, Ethereum, Monero и Zcash; ***уметь***: - работать со скриптами криптовалюты Bitcoin; - разрабатывать простейшие смарт-контракты на языке Solidity в криптовалюте Ethereum; - анализировать уровень анонимности и безопасности в криптовалютах Bitcoin, Ethereum, Monero и Zcash; ***владеть***: - навыками работы с библиотеками языка Python для криптовалюты Bitcoin; - навыками программирования на языке Solidity; - навыками работы с криптографическими инструментами, использующимися в криптовалютах Bitcoin, Ethereum, Monero и Zcash.
Краткая Характеристика учебной дисциплины (основные блоки и темы)	**Содержание основных разделов (тем) курса** - Bitcoin: UTXO-модель, алгоритм Proof-of-Work, подпись ECDSA, язык Script. Проблема масштабируемости сети Bitcoin и методы её решения. Технологии Segregated Witness, Lightning Network и Taproot. - Ethereum. Account-based модель. Proof-of-Stake. Смарт-контракты. язык Solidity - Zcash. Доказательство с нулевым разглашением. Технология Zk-Snark - Monero. Круговые подписи. - Механизмы анонимизации и деанонимизации в криптовалютах Bitcoin и Ethereum, кластеризация адресов, механизмы микширования и анализ их уровня анонимности. Coinjoin транзакции
Трудоёмкость (з.е. / часы)	Согласно рабочему учебному плану курс читается в полном объёме в течение 7 семестра **5** ЗЕТ / **180** часов.
Форма итогового контроля знаний	В конце **7**-го семестра предусмотрен ***зачёт***.

Аннотация учебной дисциплины

Учебная дисциплина **«Методы алгебраической теории чисел в криптографии»**	
Цель изучения дисциплины	***Целью*** освоения дисциплины «*Методы алгебраической теории чисел в криптографии*» является изложение основ теории алгебраических чисел, в частности, теории разложения идеалов; изучение теории вещественных и мнимых квадратичных полей; описание некоторых алгоритмов в квадратичных полях с использованием их в криптографических приложениях.

Компетенции, формируемые в результате освоения дисциплины	Процесс изучения дисциплины направлен на формирование следующих ***компетенций***: - способность проводить анализ и участвовать в разработке математических моделей безопасности компьютерных систем (ПКС-7)
Знания, умения и навыки, получаемые в процессе изучения дисциплины	В результате освоения дисциплины студент должен ***знать***: современные методы и перспективы методов алгебраической теории чисел для криптографии в целом; базовые алгоритмы алгебраической теории чисел; методы и алгоритмы эффективных вычислений в квадратичных полях, применяемых в криптографических исследованиях. ***уметь***: использовать изученные методы и алгоритмы для решения криптографических задач; разрабатывать и реализовывать алгоритмы редукции и умножения идеалов квадратичного поля, вычисления числа классов идеалов числового поля, основные криптографические алгоритмы на базе числовых полей; корректно применять вычислительные методы в числовых полях к конкретным задачам, разрабатывать вычислительные алгоритмы для криптографических приложений. ***владеть***: практическими навыками применения пакетов компьютерной алгебры решения прикладных задач; навыками исследования алгоритмов алгебраической теории чисел; навыками эффективного вычисления в группе классов идеалов квадратичного поля.
Краткая Характеристи каучебной дисциплины (основные блоки и темы)	**Содержание основных разделов (тем) курса** Тема 1. Алгебраические числовые поля: Расширения полей; Алгебраические числа и числовые поля; Вложения; Примитивные элементы; Нормы и следы. Тема 2. Алгебраические целые числа: Основные определения и свойства; Кольца целых и целые базисы; Дискриминант; Алгоритм вычисления кольца алгебраических целых числового поля. Тема 3. Факторизация и идеалы: Единицы, неприводимые и простые элементы; Арифметика с идеалами; Дробные идеалы и единственность разложения; Простые идеалы; Группа классов идеалов. Тема 4. Криптографические приложения.
Трудоёмкость (з.е. / часы)	Согласно рабочему учебному плану курс читается в полном объёме в течение **9** семестра **3** ЗЕТ / **108** часов.
Форма итогового контроля знаний	В конце **9**-го семестра предусмотрен ***зачёт***.

Учебная дисциплина **«Элективные курсы по физической культуре и спорту»**	
Цель изучения лины	Цель дисциплины «Прикладная физическая культура» состоит в формировании способностью использовать разнообразные формы физической культуры и спорта в повседневной жизни для сохранения и укрепления своего здоровья и здоровья своих близких, семьи и трудового коллектива для качественной жизни и эффективной профессиональной деятельности.
Компетенции, формируемые в результате	УК-7 Способен поддерживать должный уровень физической подготовленности для обеспечения полноценной социальной и профессиональной деятельности

освоения дисциплины	
Знания, умения и навыки, получаемые в процессе изучения дисциплины	По окончании изучения курса студент должен: Знать: – ценности физической культуры и спорта; значение физической культуры в жизнедеятельности человека; культурное, историческое наследие в области физической культуры; – факторы, определяющие здоровье человека, понятие здорового образа жизни и его составляющие; – принципы и закономерности воспитания и совершенствования физических качеств; – способы контроля и оценки физического развития и физической подготовленности; – методические основы физического воспитания, основы самосовершенствования физических качеств и свойств личности; основные требования к уровню его психофизической подготовки к конкретной профессиональной деятельности; влияние условий и характера труда специалиста на выбор содержания производственной физической культуры, направленного на повышение производительности труда. Уметь: – оценить современное состояние физической культуры и спорта в мире; – придерживаться здорового образа жизни; – самостоятельно поддерживать и развивать основные физические качества в процессе занятий физическими упражнениями; осуществлять подбор необходимых прикладных физических упражнений для адаптации организма к различным условиям труда и специфическим воздействиям внешней среды. Владеть: – различными современными понятиями в области физической культуры; – методиками и методами самодиагностики, самооценки, средствами оздоровления для самокоррекции здоровья различными формами двигательной деятельности, удовлетворяющими потребности человека в рациональном использовании свободного времени; – методами самостоятельного выбора вида спорта или системы физических упражнений для укрепления здоровья; здоровьесберегающими технологиями; средствами и методами воспитания прикладных физических (выносливость, быстрота, сила, гибкость и ловкость) и психических (смелость, решительность, настойчивость, самообладание, и т.п.) качеств, необходимых для успешного и эффективного выполнения определенных трудовых действий
Краткая характеристика учебной дисциплины (основные блоки и темы)	1. Гимнастика. Основы техники безопасности на занятиях гимнастикой. Основы производственной гимнастики. Составление комплексов упражнений (различные видов и направленности воздействия). 2. Легкая атлетика. Основы техники безопасности на занятиях легкой атлетикой. Ознакомление, обучение и овладение двигательными навыками и техникой видов лёгкой атлетики. Совершенствование

	знаний, умений, навыков и развитие физических качеств в лёгкой атлетике. 3. Меры безопасности на занятиях лёгкой атлетикой. Техника выполнения легкоатлетических упражнений. Развитие физических качеств и функциональных возможностей организма средствами лёгкой атлетики. Специальная физическая подготовка в различных видах лёгкой атлетики. Способы и методы самоконтроля при занятиях лёгкой атлетикой. Особенности организации и планирования занятий лёгкой атлетикой в связи с выбранной профессией. 4. Спортивные игры. Основы техники безопасности на занятиях спортивными играми. Баскетбол. Волейбол. Футбол. Настольный теннис. Бадминтон. 5. Специализация. Избранный вид спорта. Общая и специальная физическая подготовка в избранном виде спорта. Спортивное совершенствование. Участие в соревнованиях. Помощь в судействе. 6. Закрепление материала. Виды и элементы видов двигательной активности, включенных в практические занятия в семестре обучения. Подготовка к тестированию физической и функциональной подготовленности, сдача контрольных испытаний и зачетных нормативов. 7. Плавание. Основы техники безопасности на занятиях по плаванию. Начальное обучение плаванию. Подвижные игры в воде. Освоение техники способов плавания. Старты и повороты. Правила поведения на воде. Спасение утопающих, первая помощь. Общая и специальная подготовка пловца (общие и специальные упражнения на суше). Аквааэробика. Правила соревнований, основы судейства. 8. Лыжный спорт. Основы техники безопасности на занятиях по лыжному спорту. Освоение техники лыжных ходов. Повороты. Подъемы и спуски с гор. Прохождение дистанции. Правила соревнований, основы судейства.
Трудоёмкость (з.е. / часы)	- ЗЕТ/328 часов
Форма итогового контроля знаний	Зачет

Аннотация учебной дисциплины

Учебная дисциплина **«Прикладная алгебра»**	
Цель изучения 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.
Компетенции, формируемые в	Процесс изучения дисциплины направлен на формирование следующих ***компетенций***:

результате освоения дисциплины	- 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)
Знания, умения и навыки, получаемые в процессе изучения дисциплины	В результате освоения дисциплины студент должен ***знать***: основные понятия и результаты дисциплины (группы, кольца, поля, приложения к теории кодирования и теории Галуа), понимать логические связи между ними; современное программное обеспечение для решения алгебраических задач; алгебраические методы для решения прикладных задач; типовые алгоритмы преобразования информации в компьютерных системах и оценки их эффективности; ***уметь***: производить вычисления в конкретных кольцах и алгебрах, выполнять операции над идеалами в коммутативных кольцах, осуществлять вычисления с перестановками конечного множества, вычислять группу Галуа полиномиального уравнения; использовать системы компьютерной алгебры для решения задач. ***владеть***: методикой исследования свойств групп и коммутативных колец; навыками решения задач прикладной алгебры, в том числе, применяя системы компьютерной алгебры; способностью и готовностью применять методы прикладной алгебры к решению практических задач.
Краткая Характеристика учебной дисциплины (основные блоки и темы)	**Содержание основных разделов (тем) курса** Тема 1. Теория групп: Конечные группы; Циклические группы; Группы перестановок; Изоморфизм групп; Классы вычетов и теорема Лагранжа; Внешнее прямое произведение групп; Нормальные подгруппы и факторгруппы; Гомоморфизмы групп; Фундаментальная теорема конечных абелевых групп. Тема 2. Теория колец: Кольца целостности; Идеалы и факторкольца; Гомоморфизмы колец; Полиномиальные кольца; Факторизация многочленов. Тема 3. Теория полей: Векторные пространства; Расширения полей; Алгебраические расширения; Конечные поля. Тема 4. Дополнительно: Приложения в теории кодирования; Введение в теорию Галуа; Круговые расширения.
Трудоёмкость (з.е. / часы)	Согласно рабочему учебному плану курс читается в полном объёме в течение **3** и **4** семестров **2** ЗЕТ / **72** часа и **4** ЗЕТ / **144** часа.
Форма итогового контроля знаний	В конце **4**-го семестра предусмотрена ***курсовая работа*** и ***зачёт с оценкой***.

Аннотация учебной дисциплины

Учебная дисциплина **«ВЫЧИСЛИТЕЛЬНАЯ АЛГЕБРА»**	
Цель изучения дисциплины	***Целями*** освоения дисциплины **«*Вычислительная алгебра*»** являются: - расширение и углубление фундаментальной алгебраической и алгоритмической подготовки студентов, обеспечивающей возможность овладения современными математическими методами, используемыми в криптографии, теории кодирования и общих моделях безопасности компьютерных систем;

	- изучение дополнительных разделов алгебры и алгоритмов алгебраических вычислений, находящих непосредственные приложения в задачах защиты информации.
Компетенции, формируемые в результате освоения дисциплины	Процесс изучения дисциплины направлен на формирование следующих ***компетенций***: - 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)
Знания, умения и навыки, получаемые в процессе изучения дисциплины	В результате освоения дисциплины обучающийся должен ***знать***: • определения и свойства алгебраических структур, используемых непосредственно в приложениях. • принципы построения алгоритмов вычислений в алгебраических структурах; ***уметь***: • производить вычисления в конкретных кольцах и алгебрах. • выполнять операции над идеалами в коммутативных кольцах. • находить базис Грёбнера полиномиального кольца. • осуществлять вычисления с перестановками конечного множества. • вычислять группу Галуа полиномиального уравнения; ***владеть***: • владеть алгоритмами вычислений в коммутативных кольцах. • алгоритмом Бухбергера. • алгоритмами вычислений в группах перестановок конечного множества и алгоритмами генерирования групп перестановок. • алгоритмами вычисления групп Галуа полиномиальных уравнений.
Краткая характеристика учебной дисциплины (основные блоки и темы)	Содержание основных разделов (тем) курса **Тема 1. Введение** Задачи и программа курса. Место курса «***Вычислительная алгебра***» в ряду других математических дисциплин. Формы самостоятельной работы студентов по изучению курса. Литература к курсу. 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. Проблема упрощения системы уравнений. Задача разрешимости полиномиального уравнения в радикалах. **Тема 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.

	Тема 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. Улучшенный алгоритм Бухбергера. **Тема 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. **Тема 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. **Тема 6. Вычисления в числовых полях** 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. **Тема 7. Вычисления групп Галуа** 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. Тематика практических занятий **Тема 1.** По данной теме практических занятий не предусмотрено. **Тема 2.** Отыскание подколец, подполей и гомоморфизмов. Отыскание идеалов факторкольца кольца многочленов от одной и многих переменных и операции над ними. Вычисления с идеалами полиномиальных колец. **Тема 3.** Построение примеров нётеровых колец. Алгоритмические вычисления с многочленами. Редукция и проверка свойств базисов Грёбнера полиномиальных идеалов. Отыскание базисов Грёбнера полиномиальных идеалов. **Тема 4.** Отыскание идеалов аффинных алгебраических множеств. Построение примеров соответствия между алгебраическими множествами и идеалами. Решение систем полиномиальных уравнений с помощью базисов Грёбнера. **Тема 5.** Сопряженность элементов в группах. Сопряженность перестановок. Построение примеров факторгрупп матричных групп. Вычисления в циклических группах. Построение примеров разрешимых групп. Разложение конечной абелевой группы в прямую сумму циклических групп. Алгоритмические вычисления в матричных группах. Вычисления в группах перестановок. Примитивные, импримитивные группы подстановок. Алгоритмическое генерирование перестановок. **Тема 6.** Вычисления в алгебраических числовых полях. Исследование полей разложений многочленов. **Тема 7.** Исследование разрешимости конкретных уравнений в радикалах. Алгоритмическое вычисление групп Галуа многочленов.
Трудоёмкость (з.е. / часы)	Согласно рабочему учебному плану курс читается в полном объёме в течение **3** и **4** семестров **2** ЗЕТ / **72** часа и **4** ЗЕТ / **144** часа.
Форма итогового контроля знаний	В конце **4**-го семестра предусмотрена ***курсовая работа*** и ***зачёт с оценкой***.

Аннотация учебной дисциплины

Учебная дисциплина “ТЕОРИЯ АВТОМАТОВ”

Цель изучения дисциплины	Целью освоения дисциплины «Теория автоматов» является: овладение основами теории формальных языков, грамматик и автоматов, что заложит фундамент понимания принципов построения современных информационных систем.
Компетенции, формируемые в результате освоения дисциплины	Процесс изучения дисциплины направлен на формирование следующих ***компетенций***: способность проводить анализ и участвовать в разработке математических моделей безопасности компьютерных систем (ПКС-7)
Знания, умения и навыки, получаемые в процессе изучения дисциплины	В результате освоения дисциплины студент должен ***знать***: - основы теории формальных языков, грамматик и автоматов; - принципы построения конечных, магазинных автоматов и машин Тьюринга; - основы теории алгоритмов и рекурсивных функций; - 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 ван Вайнгаардена, порождающую указанный контекстно-зависимый язык; - строить машину Тьюринга, принимающую указанный перечислимый язык или вычисляющую заданную функцию. - распознавать, является ли сформулированная проблема алгоритмически разрешимой. ***владеть***: - навыками моделирования перечисленных грамматик и автоматов на компьютере. - навыками применения понятий и методов дисциплины для решения различных задач, используемых в дальнейшей учебной и профессиональной деятельности
Краткая характеристика учебной дисциплины (основные	**Содержание основных разделов (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.

блоки и темы)	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. Грамматики ван Вайнгаардена. 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. 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. Конечные автоматы Мили и Мура 6. Магазинные автоматы. 7. Контекстно-зависимые грамматики. 8. Машины Тьюринга 9. Построение машин Тьюринга для принятия перечислимого языка и для вычисления функции 10. Недетерминированные машины Тьюринга
Трудоёмкость (з.е. / часы)	Согласно рабочему учебному плану курс читается в полном объёме в течение 6 семестра **3** ЗЕ / **108** часов.
Форма итогового контроля знаний	В конце **6**-го семестра предусмотрен **зачет.**

Аннотация учебной дисциплины

Учебная дисциплина **«ФОРМАЛЬНЫЕ ЯЗЫКИ»**	
Цель изучения дисциплины	***Цели*** освоения дисциплины «Формальные языки» : - овладение основами теории формальных языков, грамматик и автоматов, что заложит фундамент понимания принципов построения современных информационных систем; - изучение методологии научных исследований в профессиональной деятельности в области математических методов защиты информации.
Компетенции, формируемые в результате освоения дисциплины	Процесс изучения дисциплины направлен на формирование следующих ***компетенций***: - способность проводить анализ и участвовать в разработке математических моделей безопасности компьютерных систем (ПКС-7)

Знания, умения и навыки, получаемые в процессе изучения дисциплины	В результате освоения дисциплины студент должен ***знать***: - основы теории формальных языков, грамматик и автоматов; - принципы построения конечных, магазинных автоматов и машин Тьюринга; - основы теории алгоритмов и рекурсивных функций; - основные алгоритмически неразрешимые проблемы информатики; - основы теории сложности алгоритмов. ***уметь***: - строить контекстно-свободную грамматику, порождающую указанный язык; - строить конечный автомат, принимающий регулярный язык и детерминизировать его; - строить магазинный автомат, принимающий указанный контекстно-свободный язык; - строить грамматику ван Вайнгаардена, порождающую указанный контекстно-зависимый язык; - строить машину Тьюринга, принимающую указанный перечислимый язык или вычисляющую заданную функцию. - распознавать, является ли сформулированная проблема алгоритмически разрешимой. ***владеть***: - навыками моделирования перечисленных грамматик и автоматов на компьютере.
Краткая характеристика учебной дисциплины (основные блоки и темы)	**Содержание основных разделов (тем) курса** Тема 1. ЯЗЫКИ И ИХ ПРЕДСТАВЛЕНИЕ Алфавиты и языки. Представление языков Тема 2. ГРАММАТИКИ Мотивировка. Формальное определение грамматики. Типы грамматик. Пустое предложение. Рекурсивность контекстно-зависимых грамматик. Деревья вывода в контекстно-свободных грамматиках Тема 3. КОНЕЧНЫЕ АВТОМАТЫ И РЕГУЛЯРНЫЕ 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 Тема 4. КОНТЕКСТНО-СВОБОДНЫЕ ГРАММАТИКИ 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. Тема 5. МАГАЗИННЫЕ АВТОМАТЫ Неформальное описание. Формальное описание. Недетерминированные магазинные автоматы и контекстно-свободные языки. Тема 6. МАШИНЫ ТЬЮРИНГА Неформальное описание. 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 .
Трудоёмкость	Согласно рабочему учебному плану курс читается в полном объёме в течение 6 семестра **3** ЗЕ / **108** часов.

(з.е. / часы)	
Форма итогового контроля знаний	В конце **6**-го семестра предусмотрен **зачет.**

Аннотация учебной дисциплины

Учебная дисциплина **«КРИПТОГРАФИЧЕСКИЕ ПРОТОКОЛЫ ДЛЯ ЗАЩИТЫ БАНКОВСКОЙ ИНФОРМАЦИИ»**	
Цель изучения дисциплины	Целью преподавания данной дисциплины является ознакомление слушателей с основными проблемами защиты банковской информации, анализ криптографических протоколов, применяемых в финансовой и коммерческой деятельности. Дисциплина обеспечивает приобретение знаний и умений в области использования криптографических протоколов для защиты информации в банковском деле. ***Основной целью*** дисциплины является изложение основополагающих принципов защиты информации с помощью криптографических методов и примеров реализации этих методов на практике.
Компетенции, формируемые в результате освоения дисциплины	Процесс изучения дисциплины направлен на формирование следующих ***компетенций***: - Способен разрабатывать требования по защите, формировать политики безопасности компьютерных систем и сетей (ПКС-2);
Знания, умения и навыки, получаемые в процессе изучения дисциплины	В результате изучения дисциплины студент должен: Знать: •базовые криптографические протоколы; •криптографические стандарты; •классификацию и структуру систем электронных платежей; •криптографические протоколы, применяемые в электронной коммерции и в электронном документообороте; •виды атак на протоколы. Уметь: •использовать основные математические методы, применяемые в криптографии; •анализировать свойства криптографических протоколов; •проводить сравнительный анализ криптографических протоколов, решающих сходные задачи; •применять криптографические алгоритмы. Владеть: •криптографической терминологией; •навыками построения моделей криптографических протоколов, которые используются на практике; •навыками математического моделирования в криптографии.
Краткая характеристика	**Содержание основных разделов (тем) курса** **Тема 1. Основные виды криптографических протоколов. Роль криптографических протоколов в системах защиты информации.**

учебной дисциплины (основные блоки и темы)	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. **Тема 2. Протокол электронной подписи.** Схема Эль-Гамаля. Схема RSA. Хэш-функции. Криптостойкость и особенности. **Тема 3. 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. Обзор государственных стандартов и стандартов организаций в области криптографических протоколов. Итоги изучения дисциплины. **3.2. 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.
Трудоёмкость (з.е. / часы)	Согласно рабочему учебному плану курс читается в 10 семестре **3** ЗЕТ / **108** часов.
Форма итогового контроля знаний	В конце семестра предусмотрен ***зачет***.

Аннотация учебной дисциплины

Учебная дисциплина **«АНАЛИЗ СТОЙКОСТИ ФИНАНСОВЫХ ПРОТОКОЛОВ»**	
Цель изучения дисциплины	Целью преподавания данной дисциплины является ознакомление слушателей с основными проблемами защиты банковской информации, анализ стойкости криптографических протоколов, применяемых в финансовой и коммерческой деятельности. Дисциплина обеспечивает приобретение знаний и умений в области использования криптографических протоколов для защиты информации в банковском деле. ***Основной целью*** дисциплины является изложение основополагающих принципов защиты информации с помощью

	криптографических методов и примеров реализации этих методов на практике и анализа их стойкости.
Компетенции, формируемые в результате освоения дисциплины	Процесс изучения дисциплины направлен на формирование следующих компетенций: - Способен разрабатывать требования по защите, формировать политики безопасности компьютерных систем и сетей (ПКС-2);
Знания, умения и навыки, получаемые в процессе изучения дисциплины	В результате изучения дисциплины студент должен: Знать: • базовые криптографические протоколы; • криптографические протоколы, применяемые в электронной коммерции и в электронном документообороте; • виды атак на протоколы. Уметь: • использовать основные математические методы, применяемые в криптографии; • анализировать свойства криптографических протоколов; • анализировать стойкость финансовых протоколов; • проводить сравнительный анализ криптографических протоколов, решающих сходные задачи. Владеть: • криптографической терминологией; • навыками построения моделей криптографических протоколов, которые используются на практике; • навыками математического моделирования в криптографии.
Краткая характеристика учебной дисциплины (основные блоки и темы)	**Содержание основных разделов (тем) курса** **Тема 1. 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. **Тема 2.Модели атак и угроз.** Атаки на криптосистемы с секретным ключом. Типы угроз. Классификация типов атак на схемы электронной подписи. **Тема 3. Криптографические протоколы в электронной коммерции и в электронном документообороте. Их стойкость.** Протоколы аутентификации. Протоколы с центром доверия. Методы анализа стойкости схем аутентификации. Протоколы электронной подписи. Банковские криптографические протоколы. Безопасность электронных платежных систем Итоги изучения дисциплины. **Тематика практических работ** 1. Криптографические протоколы. Их стойкость. 2. Модели атак. 3. Стойкость криптографических протоколов, используемых в финансовой деятельности.

Трудоёмкость (з.е. / часы)	**3** ЗЕ/108 часов.
Форма итогового контроля знаний	***Зачет в 10 семестре***.

Аннотация учебной дисциплины

Учебная дисциплина **«Функциональные поля и их приложения»**	
Цель изучения дисциплины	***Цели*** освоения дисциплины «**Функциональные поля и их приложения** : - 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 алгебро-геометрических кодов, вычислительными процедурами кодирования и декодирования и методикой оценки эффективности соответствующих кодов;
Компетенции, формируемые в результате освоения дисциплины	Процесс изучения дисциплины направлен на формирование следующих ***компетенций***: - способность проводить анализ и участвовать в разработке математических моделей безопасности компьютерных систем (ПКС-7);
Знания, умения и навыки, получаемые в процессе изучения дисциплины	В результате освоения дисциплины студент должен ***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.
Краткая Характеристика учебной дисциплины (основные блоки и темы)	**Содержание основных разделов (тем) курса** - Функциональные поля. - Дифференциалы и теорема Римана-Роха - Р-адические разложения и вычеты - Алгебро-геометрические коды - Расширения функциональных полей - Примеры расширений функциональных полей - Дзета-функция - Эллиптические функциональные поля
Трудоёмкость (з.е. / часы)	Согласно рабочему учебному плану курс читается в полном объёме в течение 9 семестра **3** ЗЕТ / **108** часов.
Форма итогового контроля знаний	В конце **9**-го семестра предусмотрен ***зачёт***.

Аннотация учебной дисциплины

Учебная дисциплина **«ЛОКАЛЬНЫЕ ПОЛЯ И ИХ ПРИЛОЖЕНИЯ»**	
Цель изучения дисциплины	***Целями*** освоения дисциплины **«*Локальные поля и их приложения*»** являются: - 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.
Компетенции, формируемые в результате освоения дисциплины	Процесс изучения дисциплины направлен на формирование следующих ***компетенций***: способность проводить анализ и участвовать в разработке математических моделей безопасности компьютерных систем (ПКС-7);
Знания, умения и навыки, получаемые в процессе изучения дисциплины	В результате освоения дисциплины студент должен ***знать***: • конструкцию и свойства тензорного произведения модулей и алгебр; • структуру и топологическую характеризацию проконечных групп; • определение и свойства когомологий Галуа, в частности когомологий проконечных групп;

	• структуру и свойства локальных полей, в частности, неразветвлённых и слаборазветвлённых расширений; • структуру, свойства и когомологическое описание групп Брауэра, в частности групп Брауэра локальных полей; • определение и свойства отображения инвариантов; ***уметь***: • представлять элементы группы Брауэра локального поля 2-коциклами; • представлять элементы группы Брауэра смежными классами относительно нормы циклического расширения Галуа; • записывать соотношения для вычисления отображений инвариантов в неразветвлённых и слаборазветвлённых расширениях локальных полей, являющихся важнейшей компонентой системы дискретного логарифмирования в группах Брауэра; • переформулировать проблему дискретного логарифма в конечном поле как проблему дискретного логарифма в группе Брауэра в расширении Галуа локального поля, в том числе и по источникам на иностранных языках; ***владеть***: • методикой явного вычисления отображений инвариантов; • методикой формализации и компьютерного моделирования процедур вычисления отображений инвариантов; • владеть методикой решения проблемы дискретного логарифма с помощью групп Брауэра и методикой оценки эффективности данной процедуры.
Краткая характеристика учебной дисциплины (основные блоки и темы)	Содержание основных разделов (тем) курса **Тема 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. 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. **Тема 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. **Тема 3. Группы Брауэра** Центрально-простые алгебры над полем. Теорема Веддербёрна. Теорема Сколема – Нётер. Отношение подобия. Группы Брауэра. Отображение ограничения. Поле расщепления алгебры. Относительная группа Брауэра. Примеры. Скрещенное произведение. Связь группы Брауэра с когомологиями Галуа. Случай циклического расширения Галуа. Связь относительной группы Брауэра с отображением нормы. **Тема 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. **Тема 5. Локальное вычисление 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. **Тема 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.
Трудоёмкость (з.е. / часы)	Согласно рабочему учебному плану курс читается в полном объёме в течение 9 семестра **3** ЗЕТ / **108** часов.
Форма итогового контроля знаний	В конце **9**-го семестра предусмотрен ***зачёт***.

Аннотация учебной дисциплины

«Программирование микроконтроллеров»	
Цель изучения дисциплины	***Целями*** освоения дисциплины «***Программирование микроконтроллеров***» являются: - освоение базовых знаний по вопросам использования и строения микроконтроллерных систем, а также обучение студента базовым понятиям, терминологии и принципами строения микроконтроллерных систем и построение микроконтроллерных устройств различных модификаций. Практическим навыкам работы с микроконтроллерными системами, необходимых для практической работы по специальности и при изучения других дисциплин в сфере информатики тем или иным образом связанных с программным обеспечением учитывая

	особенности строения и функционирования микроконтроллерных систем.
Компетенции, формируемые в результате освоения дисциплины	Процесс изучения дисциплины направлен на формирование следующих ***компетенций***: - Способен разрабатывать программно-аппаратные средства защиты информации компьютерных систем и сетей (ПКС-1);
Знания, умения и навыки, получаемые в процессе изучения дисциплины	В результате освоения дисциплины обучающийся должен • **знать**: основные архитектуры современных микроконтроллеров; • **уметь** выбрать микроконтроллер и написать управляющую программу; разрабатывать структурные и функциональные схемы работы контроллера; • **владеть практическими навыками** разработки управляющих приложений микроконтроллеров;
Краткая характеристика учебной дисциплины (основные блоки и темы)	**Содержание основных разделов (тем) курса** Тема 1. Архитектура микроконтроллеров. Средства разработки Классификация микроконтроллеров и области их применения. Память, виды памяти. Синхронизация Тактовый генератор. Система прерываний. Таймеры- счетчика. Режимы микропроцессоров. Форматы и способы адресации. Подсистема ввода вывода. Тема 2. AVR и STM микроконтролеры. Обмен данными в микроконтроллерных системах. Архитектура контроллера AVR. Состав переферийных устройств микроконтроллера. Особенности ARM процессоров. Контроллер STM на базе ядра Cortex-M3. Конвеер микропроцессоров ARM. Цифровые входы-выходы. Организация обмена данными через параллельную шину. Соединение с внешними устройствами через последовательный интерфейс USART. Последовательная шина I2C. Расширение портов ввода\ввывода. Теория кодирования Тема 3. Работа с внешними датчиками. Цифровые датчики. Принцип работы, внутренняя организация, схемы подключения и программные драйверы. Аналоговые датчики. Выбор аналогового порта. Использование таймера, компаратора, источника тактирования. Управление режимом таймера Тема 4. Основы программирования микроконтроллеров Простейшие программы. Управление светодиодами. Управление внешними датчиками, обмен данными. ЖК экраны, вывод информации на ЖК. Управление памятью. Управление аналоговыми и цифровыми выходами.
Трудоёмкость (з.е. / часы)	**3** ЗЕТ / **108** часов
Форма итогового контроля знаний	***Зачёт***

Аннотация учебной дисциплины

Учебная дисциплина: «ТЕХНОЛОГИЯ ИНФРАСТРУКТУРЫ ОТКРЫТЫХ КЛЮЧЕЙ»	
Цель изучения дисциплины	***Целями*** освоения дисциплины «***Технология инфраструктуры открытых ключей»*** являются: - заложить основы теоретических знаний о технологии PKI, необходимые будущим специалистам в области информационной безопасности; - дать представление о современных подходах к развертыванию инфраструктур открытых ключей.
Компетенции, формируемые в результате освоения дисциплины	Процесс изучения дисциплины направлен на формирование следующих ***компетенций***: - Способен разрабатывать программно-аппаратные средства защиты информации компьютерных систем и сетей (ПКС-1);
Знания, умения и навыки, получаемые в процессе изучения дисциплины	В результате освоения дисциплины обучающийся должен ***знать***: схему построения и проверки электронно-цифровой подписи; • принципы построения PRI; • классификацию сертификатов открытых ключей и методы управления ими; • принципы действия, технологию использования и методику применения программного обеспечения в технологии PKI, на примере «КриптоПРО» или «КриптоАРМ»; • российское законодательство в области создания и использования электронно-цифровой подписи; ***уметь***: • оценивать риски, связанные с применением электронной – цифровой подписи и предлагать варианты их снижения; • обоснованно выбирать варианты использования специализированного программного обеспечения «КриптоПРО», «КриптоАРМ» в инфраструктуру предприятия (организации); ***владеть***: • навыками организации PKI; • навыками разработки проектов отдельных нормативных документов, положений и инструкций в сфере функционирования PKI; • методикой использования специализированного программного обеспечения «КриптоПРО» или «КриптоАРМ».
Краткая характеристика учебной дисциплины (основные блоки и темы)	Содержание основных разделов (тем) курса **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. **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. **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. **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. **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. **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. **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. Тематика практических занятий **Тема 1.** Электронно-цифровая подпись в системах защищенного электронного документооборота. **Тема 2.** Исследование отечественных стандартов хэш-функции (ГОСТ Р 34.11-94) и электронной цифровой подписи (ЭЦП ГОСТ Р 34.10-2001). **Тема 3.** Развертывание инфраструктуры открытых ключей с использованием средств Microsoft Windows. **Тема 4.** Развертывание инфраструктуры открытых ключей с использованием специального программного средства криптографической защиты КриптоПРО. **Тема 5.** Разработка политики PKI. **Тема 6.** Организационно-правовые вопросы функционирования УЦ. **Тема 7.** Практических занятий не предусмотрено.
Трудоёмкость	**3** ЗЕТ / **108** часов

(з.е. / часы)	
Форма итогового контроля знаний	***Зачёт***

Аннотация учебной дисциплины

Учебная дисциплина **«ВНЕШНИЙ АУДИТ БЕЗОПАСНОСТИ КОРПОРАТИВНЫХ СЕТЕЙ»**	
Цель изучения дисциплины	***Цели*** освоения дисциплины «Внешний аудит безопасности корпоративных сетей»: - овладение 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.
Компетенции, формируемые в результате освоения дисциплины	Процесс изучения дисциплины направлен на формирование следующих ***компетенций***: - способен разрабатывать требования по защите, формировать политики безопасности компьютерных систем и сетей (ПКС-2).
Знания, умения и навыки, получаемые в процессе изучения дисциплины	В результате освоения дисциплины студент должен ***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
Краткая Характеристика учебной дисциплины	**Содержание основных разделов (тем) курса** **1. Введение**

(основные блоки и темы)	Задачи и программа курса. 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. **2. Основные виды уязвимостей программ и веб-приложений** Базовые сетевые протоколы и их безопасность: TCP/IP, HTTP(S). Механизмы реализации атак на разных уровнях модели OSI. Удалённое выполнение кода. Уязвимость Shellshock. SQL-инъекции (SQLi). Межсайтовый скриптинг (XSS). Уязвимости памяти: утечки, переполнения буфера. Уязвимость Heartbleed. Эксплойт EternalBlue и шифровальщик WannaCry. **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, 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. **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 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.
Трудоёмкость (з.е. / часы)	Согласно рабочему учебному плану курс читается в полном объёме в течение 10 семестра 3 ЗЕТ / 108 часов.
Форма итогового контроля знаний	В конце **10**-го семестра предусмотрен ***зачёт***.

Учебная дисциплина **«СИСТЕМЫ ТЕСТОВОГО ВТОРЖЕНИЯ»**	
Цель изучения дисциплины	***Цели*** освоения дисциплины «Системы тестового вторжения»: - овладение современными методами выявления уязвимостей компьютерных сетей; - овладение практическими навыками проведения тестовых вторжений для нахождения и исправления уязвимостей в компьютерных сетях - изучение методологии тестового вторжения и составления отчетности о выявленных уязвимостях; - овладение навыками разработки программных средств безопасности.
Компетенции, формируемые в результате освоения дисциплины	Процесс изучения дисциплины направлен на формирование следующих ***компетенций***: - способен разрабатывать требования по защите, формировать политики безопасности компьютерных систем и сетей (ПКС-2).
Знания, умения и навыки, получаемые в процессе изучения дисциплины	В результате освоения дисциплины студент должен ***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 и методы построения защищенных 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 - дорабатывать старые и разрабатывать новые инструменты тестового вторжения под задачу ***владеть***: - практическими навыками проведения аудита безопасности сетей,

	- инструментами систем тестового вторжения Metasploit и Kali Linux, сканерами безопасности - навыками аудита исходного кода для нахождения уязвимостей - навыками разработки средств безопасности
Краткая Характеристика учебной дисциплины (основные блоки и темы)	**Содержание основных разделов (тем) курса** **1. Введение** Задачи и программа курса. 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. **2. Основные виды уязвимостей программ и веб-приложений** Базовые сетевые протоколы и их безопасность: TCP/IP, HTTP(S). Механизмы реализации атак на разных уровнях модели OSI. Удалённое выполнение кода. Уязвимость Shellshock. SQL-инъекции (SQLi). Межсайтовый скриптинг (XSS). Уязвимости памяти: утечки, переполнения буфера. Уязвимость Heartbleed. Эксплойт EternalBlue и шифровальщик WannaCry. **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, 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. **4. 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. **5. 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. **6. 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 атакуемым хостом. **7. Разработка модулей для Metasploit** Разработка скриптов на языке Ruby. Виды модулей Metasploit. Имеющиеся миксины и плагины. Возможности библиотеки Rex. Сбор информации: разработка сканера. Поиск уязвимостей: разработка фаззера. Разработка эксплойтов. **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 maltego. 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.
Трудоёмкость (з.е. / часы)	Согласно рабочему учебному плану курс читается в полном объёме в течение 10 семестра 3 ЗЕТ / 108 часов.
Форма итогового контроля знаний	В конце **10**-го семестра предусмотрен ***зачёт***.

Аннотация учебной дисциплины

Учебная дисциплина **«Методы и алгоритмы генерации эллиптических кривых для криптографии»**	
Цель изучения 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 методов генерации эллиптических кривых для криптографии и оценки их 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.
Компетенции, формируемые в результате освоения дисциплины	Процесс изучения дисциплины направлен на формирование следующих ***компетенций***: - способность проводить анализ и участвовать в разработке математических моделей безопасности компьютерных систем (ПКС-7)
Знания, умения и навыки, получаемые в процессе изучения дисциплины	В результате освоения дисциплины студент должен ***знать***: современные методы и перспективы методов построения эллиптических кривых для криптографии в целом; принципы построения криптографических алгоритмов и их взаимосвязь с эллиптическими кривыми; быстрые алгебраические и теоретико-числовые алгоритмы; структуру и свойства порядков квадратичных полей, структуру и общие свойства эллиптических кривых, современные методы исследования их характеристик, существенных для обеспечения стойкости криптосистем; методы теоретического и экспериментального исследования с использованием эллиптических кривых; общие принципы экспериментального и

	теоретического исследования задачи построения подходящей эллиптической кривой для криптографических приложений; оценки сложности алгоритмов. ***уметь***: использовать изученные методы и алгоритмы для решения криптографических задач; формулировать задачу по оцениванию безопасности криптографического алгоритма применительно к конкретным условиям; применять математические методы исследования криптографических алгоритмов; вычислять число точек эллиптической кривой над конечным полем, вычислять *j*-инвариант эллиптической кривой и записывать классовый многочлен по найденному *j*-инварианту, редуцировать этот многочлен и находить из него *j*-инвариант редуцированной по простому модулю, записывать уравнение эллиптической кривой над простым полем по заданному *j*-инварианту; грамотно применять изученные математические методы, современные пакеты компьютерной алгебры для обработки, детального анализа и систематизации криптографической информации; разрабатывать и реализовывать алгоритмы редукции бинарных квадратичных форм, вычисления классового числа, вычисления гильбертова классового многочлена, генерации эллиптических кривых, пригодных для криптографических приложений; проводить анализ и формализацию задач, возникающих при реализации алгоритма генерации эллиптических кривых. ***владеть***: практическими навыками применения пакетов компьютерной алгебры для решения криптографических задач, владеть навыками исследования алгоритмов, связанных с эллиптическими кривыми; простейшими подходами к анализу безопасности криптографических протоколов, навыками эффективного вычисления в конечных полях и в группе точек эллиптической кривой; методом исследования свойств порядков квадратичных полей с помощью бинарных квадратичных форм, общим алгоритмом генерации эллиптических кривых на основе метода комплексного умножения; практическими навыками применения современных компьютерных технологий, построением математических моделей информационных потоков, возникающих при построении криптографической инфраструктуры на основе эллиптических кривых и оценивать возможность и эффективность их применения в общем алгоритме генерации кривой; общим алгоритмом генерации эллиптических кривых на основе метода комплексного умножения; методикой оценки эффективности алгоритма генерации в целом и отдельных его компонент.
Краткая Характеристи каучебной дисциплины (основные блоки и темы)	**Содержание основных разделов (тем) курса** Тема 1. «Наивный» метод. Тема 2. Модулярный j-инвариант: P-функция Вейерштрасса; j-функция; Квадратичные формы; Гильбертово поле классов мнимого квадратичного поля. Тема 3. Эллиптические кривые: Основные определения и групповой закон; Комплексное умножение; Кривые над полем комплексных чисел; Кривые над конечными полями. Тема 4. Построение классового многочлена (многочлена Гильберта). Тема 5. Классический метод комплексного умножения. Тема 6. Оптимизация метода комплексного умножения с использованием китайской теоремы об остатках. Тема 7. Оптимизация метода комплексного умножения с использованием многочленов Вебера. Тема 8. Некоторые другие оптимизации метода комплексного умножения.
Трудоёмкость (з.е. / часы)	Согласно рабочему учебному плану курс читается в полном объёме в течение **10** семестра **3** ЗЕТ / **108** часов.

Форма итогового контроля знаний	В конце **10**-го семестра предусмотрен ***зачёт***.

Аннотация учебной дисциплины

Учебная дисциплина **«СПАРИВАНИЯ НА ЭЛЛИПТИЧЕСКИХ КРИВЫХ»**	
Цель изучения дисциплины	***Целями*** освоения дисциплины **«*Спаривания на эллиптических кривых*»** являются: - изучение специфических свойств эллиптических кривых, лежащих в основе определений спариваний Вейля и Тэйта; - овладение процедурами вычисления спариваний;
Компетенции, формируемые в результате освоения дисциплины	Процесс изучения дисциплины направлен на формирование следующих ***компетенций***: - способность проводить анализ и участвовать в разработке математических моделей безопасности компьютерных систем (ПКС-7)
Знания, умения и навыки, получаемые в процессе изучения дисциплины	В результате освоения дисциплины студент должен ***знать***: • свойства эллиптических кривых, лежащих в основе определения спариваний; • теорию дивизоров на эллиптических кривых; • основные свойства спариваний Вейля и Тэйта; ***уметь***: • находить число точек эллиптических кривых над конечными полями; • проводить вычисления с дивизорами на эллиптических кривых; • вычислять результаты спариваний Вейля и Тэйта; • строить схемы протоколов обмена данными, цифровой подписи и распределения ключей в криптосистемах на основе спариваний; ***владеть***: • алгоритмом Миллера вычисления спариваний; • методикой подбора эллиптических кривых, подходящих для спариваний.
Краткая характеристика учебной дисциплины (основные блоки и темы)	Содержание основных разделов (тем) курса **Тема 1. Эллиптические кривые** Задачи и программа курса. Место теории спариваний на эллиптических кривых и криптографии, основанной на спариваниях, в ряду других математических дисциплин. Источники её развития и области приложения. Формы самостоятельной работы студентов по изучению курса. Основная литература к курсу. Уравнение Вейерштрасса эллиптической кривой. Морфизмы и изоморфизмы эллиптических кривых. Дискриминант и *j*-инвариант, их основные свойства. Сложение точек эллиптической кривой. Группа точек эллиптической кривой. Изогении и гомоморфизмы эллиптических кривых. Эллиптические кривые над конечными полями. Эндоморфизм Фробениуса. Число точек эллиптической кривой над конечным полем. Теорема Хассе.

	Тема 2. Точки кручения эллиптической кривой Точки кручения эллиптической кривой. Структура подгруппы точек n-кручения. След эндоморфизма Фробениуса. Обыкновенные и суперсингулярные кривые. Многочлены деления, их свойства. Структура группы точек эллиптической кривой. **Тема 3. Теория дивизоров на эллиптических кривых** Определение дивизоров. Степень дивизора. Носитель дивизора. Сложение дивизоров. Полиномиальные функции на кривой. Норма полиномиальной функции, свойств нормы. Рациональные функции на кривой. Нули и полюсы рациональной функции. Униформизующий параметр кривой в точке. Порядок функции в точке. Вычисление порядка. Дивизоры функций на кривой. Степень дивизора функции. Линейная эквивалентность дивизоров. Якобиан. Изоморфизм якобиана и группы точек эллиптической кривой. **Тема 4. Спаривания Вейля и Тэйта на эллиптических кривых** Общее определение спаривания Вейля, его простейшие свойства. Понятие спаривания Тэйта-Лихтенбаума, его простейшие свойства. Структура криптосистем, основанных на спаривании. Шифрующая и дешифрующая функции. Атаки на криптосистемы, основанные на спариваниях. Обоснование стойкости. Явное определение спаривания Вейля. Явное определение спаривания Тэйта-Лихтенбаума. Вывод свойств. **Тема 5. Процедуры вычисления спариваний** Дивизоры линейных функций. Формула Миллера. Алгоритм Миллера. Аддитивные цепочки. Вычисление функции главного дивизора. Рекуррентные формулы для функции главного дивизора. Ускоренный алгоритм Миллера. **Тема 6. Дополнительные свойства спариваний** Эквивалентность различных определений спаривания Вейля. Эквивалентность различных определений спаривания Тэйта-Лихтенбаума. Невырожденность спаривания Тэйта-Лихтенбаума.Применение спариваний для дискретного логарифмирования. Степень вложения. **Тема 7. Кривые и поля, подходящие для спариваний** Общие требования к кривым, подходящим для спариваний. MNT-кривые. Удобные для спаривания суперсингулярные кривые. Искажающий гомоморфизм. Модифицированное спаривание Вейля. Примеры искажающих отображений.Удобные для спаривания кривые с множителем безопасности $k\leq$ 2.Удобные для спаривания поля. Преимущества полей характеристики три. Вычисления в смешанных координатах. Устранение делений. Бинарный алгоритм Миллера. Тернарный алгоритм Миллера. Заключительное экспоненцирование. Устранение делений в случае использования MNT-кривых. **Тема 8. Протоколы на основе спариваний** Криптосистемы на основе идентификационных данных (ID-системы). Система Бонне-Франклина. Схемы цифровой подписи. Протоколы распределения ключей. Протоколы «Электронные деньги» на основе спариваний. Вручения. Снятие со счёта. Выплата одной монеты. Выплата всего кошелька. Выплата n монет. Депонирование по счёту. Определение двойной выплаты.
Трудоёмкость (з.е. / часы)	Согласно рабочему учебному плану курс читается в полном объёме в течение **10** семестра **3** ЗЕТ / **108** часов.
Форма итогового	В конце **10**-го семестра предусмотрен ***зачёт***.

контроля знаний	

Учебная дисциплина **«Основы машинного обучения»**	
Цель изучения дисциплины	***Цели*** освоения дисциплины «Методы машинного обучения»: - формирование знаний и умений по машинному обучению для построения формальных математических моделей и интерпретации результатов моделирования
Компетенции, формируемые в результате освоения дисциплины	Процесс изучения дисциплины направлен на формирование следующих ***компетенций***: - Способен осуществлять критический анализ проблемных ситуаций на основе системного подхода, вырабатывать стратегию действий (УК-1); - 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)
Знания, умения и навыки, получаемые в процессе изучения дисциплины	В результате освоения дисциплины студент должен **Знать** основные принципы, методы и задачи машинного обучение; логические модели машинного обучение; метрические модели машинного обучение; вероятностные модели машинного обучения. **Уметь** применять методы машинного обучения при решении реальных практических задач **Владеть практическими навыками** разработки инструментальных средств анализа данных на языке Python.
Краткая Характеристика учебной дисциплины (основные блоки и темы)	**Содержание основных разделов (тем) курса** Тема 1. Введение в машинное обучение Тема 2. Задача классификации. Наивный байесовский классификатор. Классификация по К ближайшим соседям. Тема 3. Деревья решений. Общий алгоритм построения дерева решений. Правила остановки разбиения дерева. Тема 4. Анализ многомерных данных. Метод главных компонент как декомпозиция матрицы данных. Тема 5. Регрессия. Многомерная регрессия. Кластеризация. Кластеризация как классификация без учителя. Тема 6. Искусственные нейронные сети.
Трудоёмкость (з.е. / часы)	Согласно рабочему учебному плану курс читается в полном объёме в течение 8 семестра **2** ЗЕТ / **72** часа.
Форма итогового контроля знаний	***зачет***

Учебная дисциплина «**Управление командой**»

Цель изучения дисциплины	формирование у студентов системы 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.
Компетенции, формируемые в результате освоения дисциплины	- Способен осуществлять критический анализ проблемных ситуаций на основе системного подхода, вырабатывать стратегию действий (УК-1); - Способен организовывать и руководить работой команды, вырабатывая командную стратегию для достижения поставленной цели (УК-3); - 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)
Знания, умения и навыки, получаемые в процессе изучения дисциплины	В результате изучения дисциплины магистрант должен: **Знать**: современные теории, концепции, методы и инструменты управления командами; стратегии и методы управления конфликтами; типы, стратегию и тактику переговоров; методики формирования команд и определения ее эффективности. **Уметь**: применять различные методики к управлению командами; определять стратегию и методы ведения переговоров и разрешения конфликтов в команде; использовать основные методики для формирования устойчивой команды для работы в банковской сфере. **Владеть практическими** навыками: управления командами; навыками управления и разрешения конфликтов; формирования эффективной команды для банковской сферы;
Краткая характеристика учебной дисциплины (основные блоки и темы)	Тема 1. Управление человеческими ресурсами проекта. Команда проекта. Тема 2. Социально-психологическая структура команды. Формирование эффективных команд Тема 3. Конфликт. Управление конфликтом. Переговоры. Эффективное ведение переговоров. Тема 4. Проблемы управления командой проекта.
Трудоёмкость (з.е. / часы)	2/72
Форма итогового контроля знаний	Зачет