

**МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ**
федеральное государственное автономное образовательное учреждение высшего
образования «Балтийский федеральный университет имени Иммануила Канта»
Высшая школа компьютерных наук и прикладной математики

АННОТАЦИИ РАБОЧИХ ПРОГРАММ ДИСЦИПЛИН

Шифр: 10.05.01

**Специальность: «Компьютерная безопасность»
Специализация: «Математические методы защиты информации»**

Квалификация (степень) выпускника: Специалист по защите информации

Калининград
2023

**Аннотации рабочих программ дисциплин по
специальности: «Компьютерная безопасность»
Специализация: «Математические методы защиты информации»
Квалификация (степень) выпускника: Специалист по защите информации**

АННОТАЦИЯ рабочей программы дисциплины «Элективные курсы по физической культуре и спорту» по специальности 10.05.01 «Компьютерная безопасность» специализация «Математические методы защиты информации» квалификация выпускника: специалист по защите информации	
Цель изучения дисциплины	Цель дисциплины: формирование физической культуры личности и способности направленного использования разнообразных средств физической культуры, спорта и для сохранения и укрепления здоровья, психофизической подготовки и самоподготовки к будущей жизни и профессиональной деятельности, систематическое физическое самосовершенствование.
Компетенции, формируемые в результате освоения дисциплины	УК-7 Способен поддерживать должный уровень физической подготовленности для обеспечения полноценной социальной и профессиональной деятельности.
Результаты освоения образовательной программы (ИДК)	УК-7.1. Знает виды физических упражнений; научно-практические основы физической культуры и здорового образа и стиля жизни УК-7.2. Демонстрирует необходимый уровень физических кондиций для самореализации в профессиональной деятельности. УК-7.3. Владеет средствами и методами укрепления индивидуального здоровья, физического самосовершенствования
Знания, умения и навыки, получаемые в процессе изучения дисциплины	Знать: Методы оценки и контроля физического развития, функционального состояния и физической подготовленности. Разнообразие средств и методов физической культуры и спорта, систем физических упражнений. Влияние физической культуры на сохранение и укрепление здоровья, профилактику профессиональных заболеваний и вредных привычек. Уметь: Использовать разнообразные средства и методы физической культуры и спорта для профессионально-личностного развития, физического самосовершенствования и самовоспитания, формирования здорового образа и стиля жизни. Владеть: Методами контроля состояния организма при физических нагрузках, опытом участия в физкультурно-оздоровительной и спортивной деятельности и пропаганды здорового образа жизни.
Краткая характеристика учебной дисциплины	Ознакомление с правилами техники безопасности. Оценка уровня функционального и физического состояния организма. Общезначительная подготовка с основами видов двигательной активности. Средства и методы общезначительной подготовки. Совершенствование двигательных действий, воспитание физических качеств.

	<p>Специальная физическая подготовка в избранном виде двигательной активности. Разучивание и совершенствование упражнений различных видов спорта. Рекомендации по составлению комплексов упражнений по совершенствованию отдельных физических качеств с учетом исходного уровня и (или) имеющихся отклонений в состоянии здоровья.</p> <p>Правила соревнований в избранном виде двигательной активности. Судейская практика. Мастер-классы.</p> <p>Оценка уровня физической подготовленности в избранном виде двигательной активности.</p> <p>Оценка уровня развития физических качеств: выносливость, сила, скоростные способности, координационные способности, гибкость. Индивидуальный уровень физической подготовленности.</p>
Разработчики	<p>К.п.н, доцент Д.И. Воронин, К.п.н, доцент О.Б. Томашевская, старший преподаватель Л.Л. Соболева</p>

АННОТАЦИЯ рабочей программы дисциплины «Введение в специальность» по специальности 10.05.01 «Компьютерная безопасность» специализация «Математические методы защиты информации» квалификация выпускника: специалист по защите информации	
Цель изучения дисциплины	<p>Целями освоения дисциплины «Введение в специальность» являются:</p> <ul style="list-style-type: none"> - обеспечение освоения студентами основ обучения в высшей школе, знакомство с ФГОС и учебными планами по направлению подготовки, учебной образовательной программой, структуры университета, 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	<p>Процесс изучения дисциплины направлен на формирование следующих компетенций:</p> <p>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 (ПК-4)</p>
Результаты освоения образовательной программы (ИДК)	<p>ПК-4.1. Осуществляет подбор, изучение и обобщение научно-технической информации, методических материалов отечественного и зарубежного опыта по проблемам компьютерной безопасности.</p> <p>ПК-4.2. Знает основные руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации.</p> <p>ПК-4.3. Применяет действующую законодательную базу в области обеспечения защиты информации.</p>
Знания, умения и навыки, получаемые в процессе	<p>В результате освоения дисциплины студент должен:</p> <p>Знать:</p> <ul style="list-style-type: none"> - основные закономерности исторического процесса, этапы исторического развития России, место и роль России в истории человечества и в

<p>изучения дисциплины</p>	<p>современном мире, правовые основы обеспечения национальной безопасности Российской Федерации;</p> <ul style="list-style-type: none"> - основные требования и положения «Закона о высшем профессиональном образовании» РФ, ФГОС и учебные планы по направлению подготовки своей специальности; - основные руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации. <p><u>Уметь:</u></p> <ul style="list-style-type: none"> - осуществлять подбор, изучение и обобщение научно-технической информации, методических материалов отечественного и зарубежного опыта по проблемам компьютерной безопасности; - применять действующую законодательную базу в области обеспечения защиты информации <p><u>Владеть:</u></p> <ul style="list-style-type: none"> - 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.
<p>Краткая характеристика учебной дисциплины (основные блоки и темы)</p>	<p style="text-align: center;">Содержание основных разделов (тем) дисциплины:</p> <p><u>1. Организация высшего образования в области информационной безопасности:</u> Правовые аспекты высшего образования: правовое регулирование отношений в сфере образования (Конституция РФ, Закон об образовании Р Ф) , п р а в а и</p> <p><u>2. Введение в информационную безопасность:</u> История развития проблемы защиты информации, понятия национальной информационной защиты, понятия информационной войны. Общее представление о защищаемой информации: понятие об информации как предмете защиты, основные виды информации, свойства информации, основные положения информационного законодательства. н</p> <p><u>3. Человек и информация. Общие понятия о передаче информации на расстоянии:</u> Информация, сообщение, сигнал; канал обработки и передачи информации; виды сигналов и их свойства. Спектры сигналов и их характеристики. Основные каналы утечки информации: актуальность вопроса, основные каналы утечки информации при её обработке в информационно-телекоммуникационных системах, другие виды каналов утечки информации.</p> <p><u>4. Информационные угрозы. Методы и средства защиты информации:</u></p>

	Информационная безопасность, виды информационных угроз, вирусы, методы защиты информации. Организация защиты информации на предприятиях (учреждениях, организациях): содержание концепции и политики информационной безопасности, стратегия защиты организации, организация физической защиты и пропускного режима на предприятии.
Разработчики	Ветров Игорь Анатольевич, к.т.н., доцент

АННОТАЦИЯ рабочей программы дисциплины «Теория чисел» по специальности 10.05.01 «Компьютерная безопасность» специализация «Математические методы защиты информации» квалификация выпускника: специалист по защите информации	
Цель изучения дисциплины	Цель дисциплины: фундаментальная подготовка обучающихся в области теории чисел.
Компетенции, формируемые в результате освоения дисциплины	ПК-5. Способность участвовать в теоретических и экспериментальных научно-исследовательских работах по оценке защищенности информации в компьютерных системах.
Результаты освоения образовательной программы (ИДК)	ПК-5.1. Знает тенденции развития теоретических и экспериментальных исследований в области защиты информации. ПК-5.2. Участвует в теоретических научно-исследовательских работах по оценке защищенности информации в компьютерных системах ПК-5.3. Участвует в экспериментальных научно-исследовательских работах по аудиту безопасности в компьютерных системах.
Знания, умения и навыки, получаемые в процессе изучения дисциплины	- знать основные понятия теории чисел и основные типы задач, возникающие в теории чисел; - уметь использовать полученные теоретические знания для решения конкретных прикладных задач, производить математические расчеты в стандартных постановках, производить содержательный анализ результатов вычислений; - владеть навыками применения понятий и методов дисциплины для решения различных задач, используемых в дальнейшей учебной и профессиональной деятельности.
Краткая характеристика учебной дисциплины	Основные разделы дисциплины. 1. Теория делимости целых чисел. 2. Простые числа. 3. Теория сравнений. 4. Теорема Ферма. 5. Теоретико-числовые функции. 6. Примитивные корни и индексы. 7. Цепные дроби.
Разработчики	Малыгина Екатерина Сергеевна, к.ф.-м.н., доцент

АННОТАЦИЯ рабочей программы дисциплины
--

«ИСТОРИЯ КРИПТОГРАФИИ» по специальности 10.05.01 «Компьютерная безопасность» специализация «Математические методы защиты информации» квалификация выпускника: специалист по защите информации	
Цель изучения дисциплины	Целями освоения дисциплины <i>«История криптографии»</i> являются: <ul style="list-style-type: none"> – 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	ПК-4. Способность осуществлять подбор, изучение и обобщение научно-технической информации, методических материалов отечественного и зарубежного опыта по проблемам компьютерной безопасности, а также нормативных правовых актов сфере профессиональной деятельности
Результаты освоения образовательной программы (ИДК)	ПК-4.1. Осуществляет подбор, изучение и обобщение научно-технической информации, методических материалов отечественного и зарубежного опыта по проблемам компьютерной безопасности ПК-4.2. Знает основные руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации ПК-4.3. Применяет действующую законодательную базу в области обеспечения защиты информации
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) Тема 2. Дешифровка египетских иероглифов. Дешифровка слогового линейного письма Б Тема 3. Криптография в Западной Европе в новое время Тема 4. История шифровального дела в России. Тема 5. История теории чисел. Нерешенные проблемы в теории чисел.
Разработчик и	Болтнев Юрий Федорович, старший преподаватель

АННОТАЦИЯ рабочей программы дисциплины «СИСТЕМЫ КОМПЬЮТЕРНОЙ АЛГЕБРЫ И РЕАЛИЗАЦИЯ КРИПТОГРАФИЧЕСКИХ АЛГОРИТМОВ» по специальности 10.05.01 «Компьютерная безопасность» специализация «Математические методы защиты информации» квалификация выпускника: специалист по защите информации	
Цель изучения дисциплины	<p>Целями освоения дисциплины являются:</p> <ul style="list-style-type: none"> – 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	ПК-5. Способность участвовать в теоретических и экспериментальных научно-исследовательских работах по оценке защищенности информации в компьютерных системах
Результаты освоения образовательной программы (ИДК)	<p>ПК-5.1. Знает тенденции развития теоретических и экспериментальных исследований в области защиты информации.</p> <p>ПК-5.2. Участвует в теоретических научно-исследовательских работах по оценке защищенности информации в компьютерных системах</p> <p>ПК-5.3. Участвует в экспериментальных научно-исследовательских работах по аудиту безопасности в компьютерных системах</p>
Знания, умения и навыки, получаемые в процессе изучения дисциплины	<p>В результате освоения дисциплины студент должен:</p> <p><i>Знать:</i></p> <ul style="list-style-type: none"> – 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. <p><i>Уметь:</i></p> <ul style="list-style-type: none"> – 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;

	<ul style="list-style-type: none"> – ориентироваться в современных и перспективных математических методах защиты информации, оценивать возможность и эффективность их применения в конкретных задачах защиты информации. <p><i>Владеть:</i></p> <ul style="list-style-type: none"> – 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)	<p>Содержание разделов дисциплины</p> <p>Тема 1. Решение задач алгебры и математического анализа. Тема 2. Решение задач прикладной математики средствами математических пакетов Тема 3. Алгоритмы элементарной теории чисел. Тема 4. Вычисления в конечных полях. Тема 5. Криптосистемы с открытым ключом</p>
Разработчики	Болтнев Юрий Федорович, старший преподаватель

<p>АННОТАЦИЯ рабочей программы дисциплины «Основы технической физики» по специальности 10.05.01 «Компьютерная безопасность» специализация «Математические методы защиты информации» квалификация выпускника: специалист по защите информации</p>	
Цель изучения дисциплины	Формирование необходимых знаний для глубокого понимания физических процессов, лежащих в основе образования технических каналов утечки информации, а также для грамотной организации защиты информации при помощи технических средств.
Компетенции, формируемые в результате освоения дисциплины	ПК-3 Способность организовывать и проводить работы по технической защите информации.
Результаты освоения образовательной программы (ИДК)	<p>ПК-3.1. Разрабатывает модели угроз безопасности информации в организации; разрабатывает техническое задание на создание системы защиты информации в организации.</p> <p>ПК-3.2. Организует установку и настройку технических, программных (программно-технических) средств защиты информации, входящих в состав системы защиты информации организации, в соответствии с техническим проектом и инструкциями по эксплуатации.</p> <p>ПК-3.3. Вводит систему защиты информации в эксплуатацию.</p>
Знания, умения и навыки, получаемые в процессе изучения дисциплины	<p>Знать: фундаментальные физические законы и явления, лежащие в основе образования технических каналов утечки информации.</p> <p>Уметь: формировать требования по технической защите информации; применять наиболее эффективные методы и средства технической защиты информации; контролировать эффективность мер защиты информации.</p>

	Владеть: методами технической защиты информации; навыками расчета и инструментального контроля показателей технической защиты информации; методиками проверки защищенности объектов информатизации на соответствие требованиям нормативных документов.
Краткая характеристика учебной дисциплины	<ol style="list-style-type: none"> 1. Введение. 2. Основы теории электрических цепей и сигналов. 3. Гармонические сигналы в линейных электрических цепях. 4. Избирательные свойства электрических цепей. 5. Основы теории линейных четырехполюсников. 6. Аналоговые электрические фильтры. 7. Длинные линии и волноводы. 8. Сигналы и их свойства. 9. Модуляция сигналов.
Разработчики	Горбачев Андрей Александрович, к.т.н, доцент

АННОТАЦИЯ рабочей программы дисциплины «Математические методы диагностики компьютерных систем» по специальности 10.05.01 «Компьютерная безопасность» специализация «Математические методы защиты информации» квалификация выпускника: специалист по защите информации	
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 (ПК-7)
Результаты освоения образовательной программы (ИДК)	ПК-7.1. Знает математические методы моделирования безопасных компьютерных систем ПК-7.2. Осуществляет анализ математических моделей безопасности компьютерных систем ПК-7.3. Участвует в разработке математических моделей безопасности компьютерных систем
Знания, умения и навыки, получаемые в процессе изучения дисциплины	В результате освоения дисциплины студент должен: знать: - математические методы моделирования безопасных компьютерных систем уметь: - разрабатывать математических моделей диагностики компьютерных систем

	<p>владеть: - методами анализа математических моделей безопасности компьютерных систем.</p>
<p>Краткая характеристика учебной дисциплины</p>	<p>Содержание основных разделов (тем) дисциплины:</p> <p>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).</p> <p>2. Математические методы и модели надёжности компьютерных систем. Основные понятия и термины теории надёжности, методы и математические модели расчёта надёжности КС, статистическая оценка показателей надёжности, пути обеспечения надёжности компьютерных систем, резервирование.</p> <p>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.</p>

	4.Заключение. Основные тенденции и направления совершенствования современных способов диагностики компьютерных систем.
Разработчики	Ветров Игорь Анатольевич, к.т.н., доцент

АННОТАЦИЯ рабочей программы дисциплины «Основы криптовалют и блокчейна» по специальности 10.05.01 «Компьютерная безопасность» специализация «Математические методы защиты информации» квалификация выпускника: специалист по защите информации	
Цель изучения дисциплины	Цель дисциплины: целью освоения дисциплины «Основы криптовалют и блокчейна» является изучение студентами технологии блокчейн и основных принципов построения и работы криптовалют Bitcoin, Ethereum, Monero и Zcash, а также овладение навыками написания простейших смарт-контрактов криптовалют Bitcoin и Ethereum, необходимых для построения, защиты и анализа приложений на базе технологии блокчейн.
Компетенции, формируемые в результате освоения дисциплины	ПК-6. - Способность проводить анализ безопасности компьютерных систем на соответствие отечественным и зарубежным стандартам в области компьютерной безопасности.
Результаты освоения образовательной программы (ИДК)	ПК-6.1. Знает отечественные и зарубежные стандарты в области компьютерной безопасности ПК-6.2. Осуществляет анализ безопасности компьютерных систем на соответствие отечественным и зарубежным стандартам в области компьютерной безопасности ПК-6.3. Применяет национальные, межгосударственные и международные стандарты в области защиты информации
Знания, умения и навыки, получаемые в процессе изучения дисциплины	<ul style="list-style-type: none"> ● знать принципы построения и работы основных криптовалют и блокчейн технологий, криптографические инструменты, применяемые в криптовалютах Bitcoin, Ethereum, Monero и Zcash, основные уязвимости смарт-контрактов, механизмы анонимизации и деанонимизации в криптовалютах Bitcoin, Ethereum, Monero и Zcash; ● уметь грамотно писать скрипты криптовалюты Bitcoin, разрабатывать простейшие смарт-контракты на языке Solidity в криптовалюте Ethereum, проверять смарт-контракты на наличие уязвимостей, анализировать уровень анонимности и безопасности в криптовалютах Bitcoin, Ethereum, Monero и Zcash; ● владеть практическими навыками работы с библиотеками языка Python для криптовалюты Bitcoin, навыками программирования на языке Solidity, навыками работы с криптографическими инструментами, используемыми в криптовалютах Bitcoin, Ethereum, Monero и Zcash.
Краткая характеристика учебной дисциплины	Основные разделы дисциплины. <ol style="list-style-type: none"> 1. Введение в криптовалюты 2. Bitcoin. UTXO модель 3. Ethereum. Аккаунтная модель блокчейна. 4. Смарт-контракты. Основы языка Solidity.

	<p>5. Основные уязвимости смарт-контрактов</p> <p>6. Ethereum 2.0</p> <p>7. Monero</p> <p>8. Основы анонимизации и деанонимизации в криптовалютах</p>
Разработчики	Мельничук Евгений Михайлович, ассистент

<p>АННОТАЦИЯ</p> <p>рабочей программы дисциплины</p> <p>«Методы алгебраической теории чисел в криптографии»</p> <p>по специальности 10.05.01 «Компьютерная безопасность»</p> <p>специализация «Математические методы защиты информации»</p> <p>квалификация выпускника: специалист по защите информации</p>	
Цель изучения дисциплины	Цель дисциплины: изложение основы теории алгебраических чисел, в частности, теории разложения идеалов; изучение теории вещественных и мнимых квадратичных полей; описание конструкции криптосистем с открытым ключом в квадратичных полях; применение методов алгебраической теории чисел в криптографических приложениях.
Компетенции, формируемые в результате освоения дисциплины	ПК-7. Способность проводить анализ и участвовать в разработке математических моделей безопасности компьютерных систем.
Результаты освоения образовательной программы (ИДК)	<p>ПК-7.1. Знает математические методы моделирования безопасных компьютерных систем.</p> <p>ПК-7.2. Осуществляет анализ математических моделей безопасности компьютерных систем.</p> <p>ПК-7.3. Участвует в разработке математических моделей безопасности компьютерных систем.</p>
Знания, умения и навыки, получаемые в процессе изучения дисциплины	<p>- знать базовые алгоритмы теории чисел и алгебраической теории чисел; конструкцию криптосистем с открытым ключом в мнимых квадратичных полях;</p> <p>- уметь разрабатывать и реализовывать алгоритмы редукции и умножения идеалов квадратичного поля, вычисления числа классов идеалов числового поля, основные криптографические алгоритмы на базе числовых полей; оценивать эффективность криптосистем в квадратичных полях;</p> <p>- владеть навыками эффективного вычисления в группе классов идеалов квадратичного поля.</p>
Краткая характеристика учебной дисциплины	<p>Основные разделы дисциплины.</p> <ol style="list-style-type: none"> 1. Алгебраические числа. 2. Следы, нормы, дискриминанты. 3. Разложение простых чисел в произведение простых идеалов. 4. Группа единиц числового поля. 5. Число классов числового поля. 6. Редукция и умножение идеалов в квадратичных полях. 7. Криптография в квадратичных полях.
Разработчики	Малыгина Екатерина Сергеевна, к.ф.-м.н., доцент

АННОТАЦИЯ

<p>рабочей программы дисциплины «Квантовая защита и обработка информации» по специальности 10.05.01 «Компьютерная безопасность» специализация «Математические методы защиты информации» квалификация выпускника: специалист по защите информации</p>	
Цель изучения дисциплины	Цель дисциплины: углубление и расширение знаний в области новейших перспективных направлений в информационных технологиях, новых принципов кодирования, обработки, передачи информации и вычислений, основанных на квантовой физике.
Компетенции, формируемые в результате освоения дисциплины	ПК-5 Способность участвовать в теоретических и экспериментальных научно-исследовательских работах по оценке защищенности информации в компьютерных системах
Результаты освоения образовательной программы (ИДК)	ПК-5.1. Знает тенденции развития теоретических и экспериментальных исследований в области защиты информации. ПК-5.2. Участвует в теоретических научно-исследовательских работах по оценке защищенности информации в компьютерных системах. ПК-5.3. Участвует в экспериментальных научно-исследовательских работах по аудиту безопасности в компьютерных системах.
Знания, умения и навыки, получаемые в процессе изучения дисциплины	Знать 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 неклонированности 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 истолковывать действия логических цепей классических и квантовых компьютеров, протоколов квантовой криптографии; составлять схемы логических цепей, осуществляющих квантовый параллелизм; составлять схемы логических цепей, осуществляющих квантовые вычисления, коррекцию ошибок, квантовую телепортацию и генерацию квантового секретного ключа • Владеть обозначениями элементов квантовых логических цепей; схемами управления кубитами; правилами составления квантовых логических цепей и навыками их изображения; приемами составления протоколов, осуществляющих квантовый параллелизм, квантовые вычисления, коррекцию ошибок, квантовую телепортацию; протоколами генерации квантового секретного ключа
Краткая характеристика учебной дисциплины	<ol style="list-style-type: none"> 1. Аксиомы квантовой механики. 2. Квантовая информация. 3. Квантовые коммуникации. 4. Классические и квантовые логические гейты, квантовые цепи. 5. Квантовые алгоритмы. 6. Квантовая коррекция ошибок.
Разработчики	Иванов А.И., д.ф.-м.н., профессор

АННОТАЦИЯ рабочей программы дисциплины «Прикладная алгебра» по специальности 10.05.01 «Компьютерная безопасность» специализация «Математические методы защиты информации» квалификация выпускника: специалист по защите информации	
Цель изучения дисциплины	Цель дисциплины: 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, находящихся непосредственные приложения в задачах защиты информации.
Компетенции, формируемые в результате освоения дисциплины	ПК-4. Способность осуществлять подбор, изучение и обобщение научно-технической информации, методических материалов отечественного и зарубежного опыта по проблемам компьютерной безопасности, а также нормативных правовых актов в сфере профессиональной деятельности.
Результаты освоения образовательной программы (ИДК)	ПК-4.1. Осуществляет подбор, изучение и обобщение научно-технической информации, методических материалов отечественного и зарубежного опыта по проблемам компьютерной безопасности. ПК-4.2. Знает основные руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации. ПК-4.3. Применяет действующую законодательную базу в области обеспечения защиты информации.
Знания, умения и навыки, получаемые в процессе изучения дисциплины	- знать основные понятия и результаты дисциплины (группы, кольца, поля), понимать логические связи между ними; современное программное обеспечение для решения алгебраических задач; алгебраические методы для решения прикладных задач; - уметь производить вычисления в конкретных кольцах и алгебрах, выполнять операции над идеалами в коммутативных кольцах, осуществлять вычисления с перестановками конечного множества; использовать систему компьютерной алгебры для решения задач; - владеть методикой исследования свойств коммутативных колец, методикой исследования свойств групп перестановок конечного множества; навыками решения задач прикладной алгебры, в том числе, применяя системы компьютерной алгебры; способностью и готовностью применять методы прикладной алгебры к решению практических задач.
Краткая характеристика учебной дисциплины	Основные разделы дисциплины. 1. Введение. 2. Теория групп. 3. Теория колец. 4. Теория полей.
Разработчики	Малыгина Екатерина Сергеевна, к.ф.-м.н., доцент.

АННОТАЦИЯ рабочей программы дисциплины «Вычислительная алгебра» по специальности 10.05.01 «Компьютерная безопасность»	
--	--

специализация «Математические методы защиты информации» квалификация выпускника: специалист по защите информации	
Цель изучения дисциплины	Цель дисциплины: целью освоения дисциплины « Вычислительная алгебра » является расширение и углубление фундаментальной алгебраической подготовки студентов, обеспечивающей возможность овладения современными математическими методами, используемыми в криптографии, теории кодирования и общих моделях безопасности компьютерных систем, изучение дополнительных разделов алгебры, находящихся непосредственные приложения в задачах защиты информации.
Компетенции, формируемые в результате освоения дисциплины	ПК-4. Способность осуществлять подбор, изучение и обобщение научно-технической информации, методических материалов отечественного и зарубежного опыта по проблемам компьютерной безопасности, а также нормативных правовых актов в сфере профессиональной деятельности.
Результаты освоения образовательной программы (ИДК)	ПК-4.1. Осуществляет подбор, изучение и обобщение научно-технической информации, методических материалов отечественного и зарубежного опыта по проблемам компьютерной безопасности. ПК-4.2. Знает основные руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации. ПК-4.3. Применяет действующую законодательную базу в области обеспечения защиты информации.
Знания, умения и навыки, получаемые в процессе изучения дисциплины	Знать типовые алгоритмы преобразования информации в компьютерных системах и оценки их эффективности; перспективные методы и алгоритмы преобразования информации в компьютерных системах и методику оценки их эффективности; российские и иностранные стандарты безопасности компьютерных систем. Уметь строить математические модели информационных процессов в компьютерных системах и алгоритмизировать вычислительные процедуры в этих моделях; поводить аналитическую работу по компьютерной безопасности. Владеть навыками построения математических моделей информационных процессов в компьютерных системах и навыками их анализа относительно безопасности.
Краткая характеристика учебной дисциплины	Основные разделы дисциплины. 1. Вычисления в кольцах и алгебрах. 2. Вычисления с многочленами. 3. Решение систем алгебраических уравнений. 4. Вычисления с группами и перестановками. 5. Вычисления в числовых полях и группах Галуа.
Разработчики	Малыгина Екатерина Сергеевна, к.ф.-м.н., доцент.

<p>АННОТАЦИЯ рабочей программы дисциплины «ТЕОРИЯ АВТОМАТОВ» по специальности 10.05.01 «Компьютерная безопасность» специализация «Математические методы защиты информации» квалификация выпускника: специалист по защите информации</p>

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	ПК-7. Способность проводить анализ и участвовать в разработке математических моделей безопасности компьютерных систем.
Результаты освоения образовательной программы (ИДК)	ПК-7.1. Знает математические методы моделирования безопасных компьютерных систем ПК-7.2. Осуществляет анализ математических моделей безопасности компьютерных систем ПК-7.3. Участвует в разработке математических моделей безопасности компьютерных систем
Знания, умения и навыки, получаемые в процессе изучения дисциплины	В результате освоения дисциплины студент должен знать: <ul style="list-style-type: none"> - 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: <ul style="list-style-type: none"> - 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: <ul style="list-style-type: none"> - 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)	<p style="text-align: center;">Содержание основных разделов (тем) курса</p> <ol style="list-style-type: none"> 1. Формальные языки. Контекстно-свободные грамматики. 2. Конечные и магазинные автоматы. 3. Контекстно-зависимые грамматики. Машины Тьюринга

блоки и темы)	
Разработчик и	Болтнев Юрий Федорович, старший преподаватель

АННОТАЦИЯ рабочей программы дисциплины «ФОРМАЛЬНЫЕ ЯЗЫКИ» по специальности 10.05.01 «Компьютерная безопасность» специализация «Математические методы защиты информации» квалификация выпускника: специалист по защите информации	
Цель изучения дисциплины	Цели освоения дисциплины «Формальные языки»: <ul style="list-style-type: none"> - 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	ПК-7. Способность проводить анализ и участвовать в разработке математических моделей безопасности компьютерных систем.
Результаты освоения образовательной программы (ИДК)	ПК-7.1. Знает математические методы моделирования безопасных компьютерных систем ПК-7.2. Осуществляет анализ математических моделей безопасности компьютерных систем ПК-7.3. Участвует в разработке математических моделей безопасности компьютерных систем
Знания, умения и навыки, получаемые в процессе изучения дисциплины	В результате освоения дисциплины студент должен знать: <ul style="list-style-type: none"> - 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: <ul style="list-style-type: none"> - 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. - использовать полученные теоретические знания для решения конкретных прикладных задач, производить математические расчеты в стандартных постановках, производить содержательный анализ результатов вычислений владеть:

	<ul style="list-style-type: none"> - 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 блоки и темы)	<p style="text-align: center;">Содержание основных разделов и тем курса</p> <ol style="list-style-type: none"> 1. Языки и их представление. Грамматики 2. Конечные автоматы и регулярные грамматики. Контекстно-свободные грамматики. 3. Магазинные автоматы. Машины Тьюринга
Разработчик и	Болтнев Юрий Федорович, старший преподаватель

АННОТАЦИЯ рабочей программы дисциплины «Функциональные поля и их приложения» по специальности 10.05.01 «Компьютерная безопасность» специализация «Математические методы защиты информации» квалификация выпускника: специалист по защите информации	
Цель изучения дисциплины	Цель дисциплины: целью освоения дисциплины «Функциональные поля и их приложения» является расширение и углубление фундаментальной подготовки студентов в области алгебры и теории чисел до уровня, необходимого для анализа и формализации задач в области защиты информации и разработки математических моделей защищаемых информационных потоков; овладение основными принципами и результатами теории алгеброгеометрических кодов, вычислительными процедурами кодирования и декодирования и методикой оценки эффективности соответствующих кодов.
Компетенции, формируемые в результате освоения дисциплины	ПК-7. Способность проводить анализ и участвовать в разработке математических моделей безопасности компьютерных систем
Результаты освоения образовательной программы (ИДК)	ПК-7.1. Знает математические методы моделирования безопасных компьютерных систем. ПК-7.2. Осуществляет анализ математических моделей безопасности компьютерных систем ПК-7.3. Участвует в разработке математических моделей безопасности компьютерных систем.
Знания, умения и навыки, получаемые в процессе изучения дисциплины	<ul style="list-style-type: none"> • <i>знать</i> 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

	<ul style="list-style-type: none"> • <i>уметь</i> 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; • <i>владеть</i> 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	<p>Основные разделы дисциплины.</p> <ol style="list-style-type: none"> 1. Функциональные поля. 2. Дифференциалы и теорема Римана – Роха 3. P-адические разложения и вычеты 4. Алгеброгеометрические коды 5. Расширения функциональных полей 6. Примеры расширений 7. Дзета-функция 8. Эллиптические функциональные поля.
Разработчики	Мельничук Евгений Михайлович, ассистент

<p>АННОТАЦИЯ рабочей программы дисциплины «Локальные поля и их приложения» по специальности 10.05.01 «Компьютерная безопасность» специализация «Математические методы защиты информации» квалификация выпускника: специалист по защите информации</p>	
Цель изучения дисциплины	<p>Цель дисциплины: целью освоения дисциплины «Локальные поля и их приложения» расширение и углубление специализированной алгебраической подготовки и подготовки студентов в области теории чисел до уровня, необходимого для анализа и формализации задач в области защиты информации и разработки математических моделей защищаемых информационных потоков; овладение методикой использования групп Брауэра в задачах анализа стойкости и эффективности криптосистем, изучение вычислительных процедур в локальных полях и подготовка к написанию теоретической части выпускной квалификационной работы.</p>
Компетенции, формируемые в результате освоения дисциплины	ПК-7. Способность проводить анализ и участвовать в разработке математических моделей безопасности компьютерных систем
Результаты освоения	ПК-7.1. Знает математические методы моделирования безопасных компьютерных систем.

образовательной программы (ИДК)	ПК-7.2. Осуществляет анализ математических моделей безопасности компьютерных систем ПК-7.3. Участвует в разработке математических моделей безопасности компьютерных систем.
Знания, умения и навыки, получаемые в процессе изучения дисциплины	<ul style="list-style-type: none"> ● знать: номенклатуру и основные характеристики сертифицированных программно-аппаратных средств защиты информации, выпускаемых российской промышленностью; математические методы и алгоритмы, применяемые в программно-аппаратных средствах защиты информации; перспективные математические методы защиты информации; ● уметь: осуществлять самостоятельную проектно-аналитическую работу; проводить сравнительный анализ эффективности математических методов и алгоритмов; ● владеть: навыками сравнительного анализа эффективности различных моделей, методов, алгоритмов, реализованных в средствах защиты информации, анализа их технических характеристик.
Краткая характеристика учебной дисциплины	<ol style="list-style-type: none"> 1. Локальные поля. 2. Группы Брауэра. 3. Группы Брауэра локального и глобального поля, применение в криптографии. 4. Локальные вычисления инвариантов. 5. Локально-глобальные методы.
Разработчики	Мельничук Евгений Михайлович, ассистент

АННОТАЦИЯ рабочей программы дисциплины «Криптографические протоколы для защиты банковской информации» по специальности 10.05.01 «Компьютерная безопасность» специализация «Математические методы защиты информации» квалификация выпускника: специалист по защите информации	
Цель изучения дисциплины	Целью изучения дисциплины « <i>Криптографические протоколы для защиты банковской информации</i> » является формирование знаний об основополагающих принципах защиты информации с помощью криптографических методов и примеров реализации этих методов на практике.
Компетенции, формируемые в результате освоения дисциплины	ПК-2. Способен разрабатывать требования по защите, формировать политики безопасности компьютерных систем и сетей.
Результаты освоения образовательной программы (ИДК)	ПК-2.1. Выполняет анализ безопасности компьютерных систем и разрабатывает рекомендации по эксплуатации системы защиты информации. ПК-2.2. Разработка модели угроз безопасности информации. ПК-2.3. Формирует политики безопасности компьютерных систем и сетей
Знания, умения и навыки,	● знать основы построения системы защиты компьютерных систем, базовые криптографические протоколы, применяемые в

получаемые в процессе изучения дисциплины	электронной коммерции и в электронном документообороте; виды атак на протоколы; <ul style="list-style-type: none"> • уметь: проводить аналитическую работу в области информационной безопасности компьютерных систем, проводить сравнительный анализ криптографических протоколов, решающих сходные задачи; • владеть: навыками работы с ПК, криптографической терминологией; навыками построения моделей криптографических протоколов, которые используются на практике
Краткая характеристика учебной дисциплины	Основные разделы дисциплины. 9. Основные виды криптографических протоколов. Роль криптографических протоколов в системах защиты информации. 10. Протокол электронной подписи. 11. Криптографические протоколы в электронной коммерции и в электронном документообороте.
Разработчики	Белова Ольга Олеговна, к.ф.-м.н., доцент

АННОТАЦИЯ рабочей программы дисциплины «Анализ стойкости финансовых протоколов» по специальности 10.05.01 «Компьютерная безопасность» специализация «Математические методы защиты информации» квалификация выпускника: специалист по защите информации	
Цель изучения дисциплины	Целью изучения дисциплины <i>«Анализ стойкости финансовых протоколов»</i> формирование знаний об основополагающих принципах защиты информации с помощью криптографических методов и примеров реализации этих методов на практике.
Компетенции, формируемые в результате освоения дисциплины	ПК-2. Способен разрабатывать требования по защите, формировать политики безопасности компьютерных систем и сетей.
Результаты освоения образовательной программы (ИДК)	ПК-2.1. Выполняет анализ безопасности компьютерных систем и разрабатывает рекомендации по эксплуатации системы защиты информации ПК-2.2. Разработка модели угроз безопасности информации. ПК-2.3. Формирует политики безопасности компьютерных систем и сетей
Знания, умения и навыки, получаемые в процессе изучения дисциплины	<ul style="list-style-type: none"> • знать базовые криптографические протоколы, применяемые в электронной коммерции и в электронном документообороте; виды атак на протоколы; • уметь: проводить сравнительный анализ криптографических протоколов, решающих сходные задачи; • владеть: криптографической терминологией; навыками построения моделей криптографических протоколов, которые используются на практике
Краткая характеристика	Основные разделы дисциплины.

учебной дисциплины	12. Основные виды криптографических протоколов. Роль криптографических протоколов в системах защиты информации. 13. Протокол электронной подписи. 14. Криптографические протоколы в электронной коммерции и в электронном документообороте.
Разработчики	Белова Ольга Олеговна, к.ф.-м.н., доцент

АННОТАЦИЯ рабочей программы дисциплины «Программирование микроконтроллеров» по специальности 10.05.01 «Компьютерная безопасность» специализация «Математические методы защиты информации» квалификация выпускника: специалист по защите информации	
Цель изучения дисциплины	Цель дисциплины: формирование у обучающихся понимания основных принципов проектирования современных цифровых электрических схем общего назначения, а также развитие навыков интеграции в такие схемы микроконтроллерной и микропроцессорной техники, написания для них программ на языках программирования высокого и низкого уровня.
Компетенции, формируемые в результате освоения дисциплины	ПК-1. Способен разрабатывать программно-аппаратные средства защиты информации компьютерных систем и сетей
Результаты освоения образовательной программы (ИДК)	ПК-1.1. Проводит анализ существующих методов и средств, применяемых для контроля и защиты информации. ПК-1.2. Разрабатывает проекты программных и аппаратных средств защиты информации в соответствии с техническим заданием. ПК-1.3. Проводит аттестацию программ и алгоритмов на предмет соответствия требованиям защиты информации.
Знания, умения и навыки, получаемые в процессе изучения дисциплины	- знать структуру и принцип работы 8-битных микроконтроллеров (архитектура, технология производства, электрические характеристики, порядок выполнения машинного кода, назначение периферийных устройств), инструкции ассемблера, интерфейсы (I2C, SPI), задачи интеграции микроконтроллеров в различных системах защиты информации; - уметь разрабатывать электрические схемы электронно-вычислительных устройств общего назначения, основанные на микроконтроллерах, выполнять программирование и отладку программ на микроконтроллерах; - владеть методами разработки эффективного программного кода с помощью использования регистров памяти специального назначения и машинных команд (команд ассемблера); методами оптимизации программ для микроконтроллеров.
Краткая характеристика учебной дисциплины	Основные разделы дисциплины. 1 Схемотехника цифровых устройств. 2 Устройство и функциональные возможности 8-битных микроконтроллеров. 2.1 Архитектура микроконтроллеров PIC16. Порты ввода-вывода

	<p>2.2 Прерывания и таймеры.</p> <p>2.3 ШИМ управление.</p> <p>2.4 Шина I2C, внутренняя и внешняя память EEPROM.</p> <p>3 Реализация протоколов обмена данными. Протокол 1-Wire.</p> <p>4 Реализация криптографических алгоритмов на микроконтроллерах.</p>
Разработчики	Колесников Никита Сергеевич, мл. науч. сотрудник лаборатории «Математические методы защиты и обработки информации»

АННОТАЦИЯ рабочей программы дисциплины «Технология инфраструктуры открытых ключей» по специальности 10.05.01 «Компьютерная безопасность» специализация «Математические методы защиты информации» квалификация выпускника: специалист по защите информации	
Цель изучения дисциплины	Цель дисциплины: освоение студентами основ теоретических знаний о технологии РКІ, необходимые будущим специалистам в области информационной безопасности; сформировать представление о современных подходах к развертыванию инфраструктур открытых ключей.
Компетенции, формируемые в результате освоения дисциплины	ПК-1. Способен разрабатывать программно-аппаратные средства защиты информации компьютерных систем и сетей
Результаты освоения образовательной программы (ИДК)	<p>ПК-1.1. Проводит анализ существующих методов и средств, применяемых для контроля и защиты информации.</p> <p>ПК-1.2. Разрабатывает проекты программных и аппаратных средств защиты информации в соответствии с техническим заданием.</p> <p>ПК-1.3. Проводит аттестацию программ и алгоритмов на предмет соответствия требованиям защиты информации.</p>
Знания, умения и навыки, получаемые в процессе изучения дисциплины	<ul style="list-style-type: none"> • знать: номенклатуру и основные характеристики сертифицированных программно-аппаратных средств защиты информации, выпускаемых российской промышленностью; математические методы и алгоритмы, применяемые в программно-аппаратных средствах защиты информации; перспективные методы обработки информации в компьютерных системах; методы алгебры, теории чисел, алгебраической геометрии и дискретной математики и их применение в моделях информационных процессов; • уметь: строить математические модели информационных процессов, возникающих при работе программно-аппаратных средств; проводить анализ адекватности существующих математических моделей на основе сравнения их показателей эффективности с перспективными моделями; проводить анализ адекватности существующих математических моделей на основе компьютерного моделирования и получения статистических оценок эффективности; • владеть: методикой разработки математических моделей информационных процессов в компьютерных системах, используя методы алгебры, теории чисел, алгебраической геометрии и дискретной математики; навыками оценки адекватности моделей информационных процессов в программно-аппаратных средствах.

Краткая характеристика учебной дисциплины	Тема 1. Введение Тема 2. Основные компоненты и сервисы PKI. Тема 3. Модели удостоверяющих центров. Тема 4. Сертификаты открытых ключей. Тема 5. Типы архитектуры PKI. Тема 6. Описание политики PKI. Тема 7. Проблемы реализации PKI.
Разработчики	Колесников Никита Сергеевич, мл. науч. сотрудник лаборатории «Математические методы защиты и обработки информации»

АННОТАЦИЯ рабочей программы дисциплины «Внешний аудит безопасности корпоративных сетей» по специальности 10.05.01 «Компьютерная безопасность» специализация «Математические методы защиты информации» квалификация выпускника: специалист по защите информации	
Цель изучения дисциплины	Целью освоения дисциплины « Внешний аудит безопасности корпоративных сетей » является расширение и углубление фундаментальной и практической подготовки студентов, обеспечивающей возможность овладения современными методами выявления уязвимостей компьютерных сетей, овладение практическими навыками проведения тестовых вторжений для практической оценки безопасности корпоративных сетей; изучение методологии тестового вторжения и составления отчетности о выявленных уязвимостях.
Компетенции, формируемые в результате освоения дисциплины	ПК-2 Способен разрабатывать требования по защите, формировать политики безопасности компьютерных систем и сетей
Результаты освоения образовательной программы (ИДК)	ПК-2.1. Выполняет анализ безопасности компьютерных систем и разрабатывает рекомендации по эксплуатации системы защиты информации. ПК-2.2. Разработка модели угроз безопасности информации. ПК-2.3. Формирует политики безопасности компьютерных систем и сетей.
Знания, умения и навыки, получаемые в процессе изучения дисциплины	Знать: <ul style="list-style-type: none"> • 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: <ul style="list-style-type: none"> • проводить аудит безопасности сети и анализ найденных уязвимостей;

	<ul style="list-style-type: none"> • пользоваться системами анализа сетевого трафика, сканерами безопасности и сетевыми сканерами; • составлять рекомендации по устранению уязвимостей, настройке средств защиты и улучшению политики безопасности <p>Владеть:</p> <ul style="list-style-type: none"> • практическими навыками проведения аудита безопасности сетей, инструментами систем тестового вторжения Metasploit и Kali Linux, сканерами безопасности <p>навыками аудита исходного кода для нахождения уязвимостей</p>
Краткая характеристика учебной дисциплины	<p>Тема 1. Введение.</p> <p>Тема 2. Основные виды уязвимостей программ и веб-приложений</p> <p>Тема 3. Сетевой сканер nmap.</p> <p>Тема 4. Скриптовый движок Nmap</p> <p>Тема 5. Анализ сетевого трафика с целью выявления атак.</p> <p>Тема 6. Сканеры безопасности.</p> <p>Тема 7. Система тестового вторжения METASPLOIT.</p> <p>Тема 8. Система тестового вторжения Kali Linux.</p>
Разработчики	Новоселов Семен Александрович, старший преподаватель

<p>АННОТАЦИЯ рабочей программы дисциплины «Системы тестового вторжения» по специальности 10.05.01 «Компьютерная безопасность» специализация «Математические методы защиты информации» квалификация выпускника: специалист по защите информации</p>	
Цель изучения дисциплины	<p>Целью освоения дисциплины «Системы тестового вторжения» является расширение и углубление фундаментальной и практической подготовки студентов, обеспечивающей возможность овладения современными методами выявления уязвимостей компьютерных сетей, а также овладение практическими навыками проведения тестовых вторжений для последующей ликвидации выявленных уязвимостей; изучение методологии тестового вторжения и составления отчетности о выявленных уязвимостях.</p>
Компетенции, формируемые в результате освоения дисциплины	ПК-2 Способен разрабатывать требования по защите, формировать политики безопасности компьютерных систем и сетей
Результаты освоения образовательной программы (ИДК)	<p>ПК-2.1. Выполняет анализ безопасности компьютерных систем и разрабатывает рекомендации по эксплуатации системы защиты информации.</p> <p>ПК-2.2. Разработка модели угроз безопасности информации.</p> <p>ПК-2.3. Формирует политики безопасности компьютерных систем и сетей.</p>
Знания, умения и навыки, получаемые в процессе изучения дисциплины	<ul style="list-style-type: none"> • знать: основные современные отечественные и зарубежные стандарты в области компьютерной безопасности и проведения аудита безопасности. • уметь: грамотно проводить анализ безопасности систем на соответствие стандартам, уметь выявлять уязвимости компьютерных систем и проводить их классификацию.

	<ul style="list-style-type: none"> • владеть: практическими навыками проведения аудита безопасности сетей и составления отчета; навыками аудита исходного кода для нахождения уязвимостей
Краткая характеристика учебной дисциплины	<p>Тема 1. Введение</p> <p>Тема 2. Сетевой сканер nmap</p> <p>Тема 3. Анализ сетевого трафика с целью выявления атак</p> <p>Тема 4. Сканеры безопасности XSpider, Nessus, OpenVAS</p> <p>Тема 5. Система тестового вторжения METASPLOIT</p> <p>Тема 6. Разработка модулей к Metasploit</p> <p>Тема 7. Система тестового вторжения Kali Linux</p>
Разработчики	Новоселов Семен Александрович, старший преподаватель.

<p>АННОТАЦИЯ</p> <p>рабочей программы дисциплины</p> <p>«Методы и алгоритмы генерации эллиптических кривых для криптографии»</p> <p>по специальности 10.05.01 «Компьютерная безопасность»</p> <p>специализация «Математические методы защиты информации»</p> <p>квалификация выпускника: специалист по защите информации</p>	
Цель изучения дисциплины	Цель дисциплины: углубление подготовки студентов в современной арифметической теории эллиптических кривых и алгебраической теории чисел до уровня, необходимого для освоения метода генерации эллиптических кривых для криптографии и оценки его эффективности, а также подготовка к написанию теоретической части выпускной квалификационной работы в области современной криптографии на основе освоения совокупности математических моделей и методов комплексного умножения на эллиптических кривых, умения анализировать стойкость получаемых криптосистем и эффективность применяемых алгоритмов.
Компетенции, формируемые в результате освоения дисциплины	ПК-7. Способность проводить анализ и участвовать в разработке математических моделей безопасности компьютерных систем.
Результаты освоения образовательной программы (ИДК)	<p>ПК-7.1. Знает математические методы моделирования безопасных компьютерных систем.</p> <p>ПК-7.2. Осуществляет анализ математических моделей безопасности компьютерных систем.</p> <p>ПК-7.3. Участвует в разработке математических моделей безопасности компьютерных систем.</p>
Знания, умения и навыки, получаемые в процессе изучения дисциплины	<ul style="list-style-type: none"> - знать базовые алгоритмы алгебраической теории чисел и теории эллиптических кривых; - уметь разрабатывать и реализовывать алгоритмы редукции бинарных квадратичных форм, вычисления классового числа, вычисления гильбертова классового многочлена, генерации эллиптических кривых, пригодных для криптографических приложений; - владеть навыками программной реализации общего алгоритма генерации эллиптических кривых на основе метода комплексного умножения и его модификаций.

Краткая характеристика учебной дисциплины	Основные разделы дисциплины. 1. Некоторые главы алгебраической теории чисел. 2. Теория эллиптических кривых. 3. Методы генерации эллиптических кривых на базе комплексного умножения.
Разработчики	Малыгина Екатерина Сергеевна, к.ф.-м.н., доцент

АННОТАЦИЯ рабочей программы дисциплины «Спаривание на эллиптических кривых» по специальности 10.05.01 «Компьютерная безопасность» специализация «Математические методы защиты информации» квалификация выпускника: специалист по защите информации	
Цель изучения дисциплины	Цель дисциплины: целью освоения дисциплины «Спаривание на эллиптических кривых» является изучение специфических свойств эллиптических кривых, лежащих в основе спариваний и овладение процедурами вычисления спариваний; овладение методикой расчёта и изучение оценок стойкости криптосистем, основанных на спариваниях.
Компетенции, формируемые в результате освоения дисциплины	ПК-7. Способность проводить анализ и участвовать в разработке математических моделей безопасности компьютерных систем.
Результаты освоения образовательной программы (ИДК)	ПК-7.1. Знает математические методы моделирования безопасных компьютерных систем. ПК-7.2. Осуществляет анализ математических моделей безопасности компьютерных систем. ПК-7.3. Участвует в разработке математических моделей безопасности компьютерных систем.
Знания, умения и навыки, получаемые в процессе изучения дисциплины	<ul style="list-style-type: none"> • знать: перспективные методы криптографической защиты информации и помехоустойчивого кодирования; принципы функционирования и возможности перспективных инструментальных средств и компьютерных технологий для реализации вычислительных алгоритмов; структуры данных и методы построения вычислительных алгоритмов в алгебраических структурах, специфичных для перспективных систем защиты информации; • уметь: анализировать корректность и быстродействие вычислительных алгоритмов, специфичных для перспективных систем защиты информации; • владеть: практическими навыками построения вычислительных алгоритмов в алгебраических структурах, используемых в системах криптографической защиты и помехоустойчивого кодирования.
Краткая характеристика учебной дисциплины	1. Предварительные сведения. 2. Спаривание Вейля 3. Спаривание Тэйта. 4. Степень вложения. 5. Отображение деформации. 6. Криптография на эллиптических кривых.

	7. Криптография на основе идентификационных данных 8. Приложения спариваний.
Разработчики	Малыгина Екатерина Сергеевна, к.ф.-м.н., доцент

АННОТАЦИЯ рабочей программы дисциплины «Иностранный язык (английский)» по специальности 10.05.01 «Компьютерная безопасность» специализация «Математические методы защиты информации» квалификация выпускника: специалист по защите информации	
Цель изучения дисциплины	Целью освоения дисциплины «Иностранный язык» является владение иностранным языком как средством, обеспечивающим потребности социально-культурной деятельности, что предполагает, прежде всего, умение самостоятельно, «через всю жизнь», работать над изучением языка, поддерживать и пополнять свои знания и умения, развивать свою коммуникативную и информационную культуру.
Компетенции, формируемые в результате освоения дисциплины	УК-4. Способен применять современные коммуникативные технологии, в том числе на иностранном(ых) языке(ах), для академического и профессионального взаимодействия УК-5. Способен анализировать и учитывать разнообразие культур в процессе межкультурного взаимодействия
Результаты освоения образовательной программы (ИДК)	УК.4.1. Грамотно и ясно строит диалогическую речь в рамках межличностного и межкультурного общения на русском и иностранном языках. УК.4.2. Демонстрирует умение осуществлять деловую переписку на русском и иностранном языках с учетом социокультурных особенностей. УК.4.3. Осуществляет выбор коммуникативных стратегий и тактик при ведении деловых переговоров. УК.5.1. Имеет представление о межкультурном разнообразии общества в социально-историческом аспекте. УК.5.2. Демонстрирует знания межкультурного разнообразия общества в этическом контексте. УК.5.3. Умеет выстраивать взаимодействие с учетом национальных и социокультурных особенностей.
Знания, умения и навыки, получаемые в процессе изучения дисциплины	Знать: - иностранный язык, на уровень, предусмотренный рамками высшего образования; - знать способы поиска новой и нужной языковой информации. Уметь: - особенности социальной организации общества, специфику менталитета и мировоззрения культур России, Запада и Востока; - особенности представлений культур друг о друге с учетом наличия общего ценностного контекста, этностерео и гетеростереотипов, формируемых информационной средой; - основы теории коммуникации, проблемы культурной идентичности и межкультурных контактов.

-пользоваться наиболее употребительными и относительно простыми языковыми средствами во всех видах речевой деятельности: устной речи, аудировании, чтении и письме;

-планировать работу;

-ставить перед собой цели и задачи предстоящей деятельности;

-уметь целесообразно распределять нагрузку.

- достигать эффективности коммуникации;

- преодолевать культурный барьер, воспринимая межкультурные различия избегать предубеждений и настраиваться на совместные действия с представителями других культур;

- сохраняя национальную идентичность, избегать этноцентризма;

- соблюдать нормы этикета, моральные и культурные нормы.

Владеть:

компьютерной грамотностью (навыки работы в компьютерных программах “Word”, “Power Point”, навыки работы с принтером, сканером, навыки работы с электронной почтой и в сети Интернет, в том числе дистанционными платформами обучения, навыки общения онлайн).

- способностью преодолевать стереотипы; - творческим отношением к процессу коммуникации;

- способностью использовать набор коммуникативных средств и делать их правильный выбор в зависимости от ситуации общения (тон, стиль, стратегии, речевые жанры, тематика и т. д.).

Краткая характеристика учебной дисциплины	№	Наименование раздела	Содержание раздела
	1.	Модуль 1: IDENTITY	<p><i>Грамматический материал</i></p> <p>“to be”, to have в Present Simple, повелительное наклонение; личные местоимения; указательные местоимения; множественное число существительных.</p> <p>Present Simple, Present Continuous, Past Simple, Past Continuous.</p> <p>Виды вопросительных предложений.</p> <p><i>1.1 Устные разговорные темы</i></p> <p>Personality types. About Myself. Men and women. Family and friends. Talking about yourself. Interview advice.</p> <p><i>1.2 Аудирование</i></p> <p>Personality types. Child of our time.</p> <p><i>1.3 Письмо</i></p> <p>Email of Introduction</p> <p><i>1.4 Чтение</i></p> <p>Carl Jung, who do you think you are?</p> <p><i>1.5 DVD</i></p> <p>BBC film Second life</p> <p><i>1.6 Лексико-грамматический тест</i></p> <p><i>Lookback</i></p> <p><i>1.7 Самостоятельная работа студентов</i></p> <p>Изучение грамматического материала. Грамматика (My grammar lab) : модуль1,2 5,6. Презентации студентов по темам, связанным со специальностью.</p>
	2.	Модуль 2: TALES	<p><i>Грамматический материал</i></p> <p>Present Perfect, Past Simple, Past Perfect</p> <p><i>2.1 Устные разговорные темы</i></p> <p>Your life experience, Important news/ event, Tell a true story or lie</p> <p><i>2.2 Аудирование</i></p> <p>Radio program about important roles in films, News report, People talking anecdotes.</p> <p><i>2.3 Письмо</i></p>

		<p>News report.</p> <p>2.4 <i>Чтение</i> Hollywood versus history, The world's best-known conspiracy theories.</p> <p>2.5 <i>DVD</i> Hustle</p> <p>2.6 <i>Лексико-грамматический тест на закрепление материала</i> Lookback</p> <p>2.7 <i>Самостоятельная работа студентов</i> Внеаудиторное чтение - 5 тыс. знаков (по специальности). Изучение грамматического материала. Грамматика (My grammar lab): модуль 7. Презентация: «Моя жизнь в кино». Презентации по темам, связанным со специальностью.</p>
3.	Модуль 3: CONTACT	<p><i>Грамматический материал</i> The future (plans): the present continuous, going to, will, might The future (predictions): will, might, may, could, going to, likely</p> <p>3.1 <i>Устные разговорные темы</i> Talk about how things will change in the future, Talk about communication preferences.</p> <p>3.2 <i>Аудирование</i> Listen to predictions about future communications, listen to telephone conversations involving misunderstanding.</p> <p>3.3 <i>Письмо</i> Writing a memo.</p> <p>3.4 <i>Чтение</i> Life on planet teen</p> <p>3.5 <i>DVD</i> The Virtual Revolution</p> <p>3.6 <i>Лексико-грамматический тест на закрепление материала</i> Lookback</p> <p>3.7 <i>Самостоятельная работа студентов</i> Внеаудиторное чтение - 5 тыс. знаков (по специальности). Изучение грамматического материала. Грамматика (My grammar lab): модуль 8. Презентация «Виртуальная революция». Презентации по темам, связанным со специальностью.</p>
4.	Модуль 4: PROJECT	<p>Проектная групповая деятельность студентов по представленным ниже темам: Living in a digital age? What is a computer? Types. What is inside a PC system? Зачет. Структура зачета: 1. Монологическое высказывание по одной из предложенных тем: Personality types. My personality; My Family and friends; Men and women; Conspiracy theories; Teenage communication. 2. Лексико-грамматический тест (ЛИМС).</p>
5.	Модуль 5: JOBS	<p><i>Грамматический материал</i> Modal verbs, used to</p> <p>5.1 <i>Устные разговорные темы</i> The qualities needed for different jobs, Homeworking, talking about past habits, creating business plan, Describing a day in your life</p>

		<p>5.2 <i>Аудирование</i> Dream Jobs gone wrong, Jobs</p> <p>5.3 <i>Письмо</i> Covering letter Write about daily routines</p> <p>5.4 <i>Чтение</i> Have you got what it takes? Childhood dreams. Homeworking.</p> <p>5.5 <i>DVD</i> Gavin and Stacey</p> <p>5.6 <i>Лексико-грамматический тест на закрепление материала</i> Lookback</p> <p>5.7 <i>Самостоятельная работа студентов</i> Внеаудиторное чтение - 5 тыс. знаков (по специальности). Изучение грамматического материала. Грамматика (My grammar lab): модуль 9. Составление резюме и сопроводительного письма. Презентации по темам, связанным со специальностью.</p>
6.	Модуль 6: SOLUTIONS	<p><i>Грамматический материал</i> Comparatives/ Superlatives</p> <p>6.1 <i>Устные разговорные темы</i> Different forms of transport and their uses, Describing a new machine.</p> <p>6.2 <i>Аудирование</i> Conversation about technical problems, People answering difficult questions</p> <p>6.3 <i>Письмо</i> An advantage/ disadvantage essay Advertisement Write about daily routines</p> <p>6.4 <i>Чтение</i> 20th Century, The advantages and disadvantages of modern technology</p> <p>6.5 <i>DVD</i> Top Gear</p> <p>6.6 <i>Лексико-грамматический тест на закрепление материала</i> Lookback</p> <p>6.7 <i>Самостоятельная работа студентов</i> Внеаудиторное чтение - 5 тыс. знаков (по специальности). Изучение грамматического материала. Грамматика (My grammar lab): модуль 4. Презентации по темам, связанным со специальностью.</p>
7.	Модуль 7: EMOTION	<p><i>Грамматический материал</i> Zero and first conditionals, Second Conditional -Ing/ Ed adjectives</p> <p>7.1 <i>Устные разговорные темы</i> Talk about your emotions, discuss what you would do in different situations, Talk about memorable moments</p> <p>7.2 <i>Аудирование</i> Radio show about therapies, Conversation where people hear news</p> <p>7.3 <i>Письмо</i> A letter of advice A website entry</p> <p>7.4 <i>Чтение</i> The six basic emotions, The people watchers</p> <p>7.5 <i>DVD</i> My worst week.</p>

		<p>7.6 <i>Лексико-грамматический тест на закрепление материала</i> Lookback.</p> <p>7.7 <i>Самостоятельная работа студентов</i> Внеаудиторное чтение - 5 тыс. знаков (по специальности).</p> <p>Изучение грамматического материала. Грамматика (My grammar lab) : модуль 4,10. Презентации по темам, связанным со специальностью.</p>
8.	Модуль 8: PROJECT	<p>Проектная групповая деятельность студентов по представленным ниже темам: The eyes of your computer? How screen displays work? Printer</p> <p>Зачет. Структура зачета: 1. Монологическое высказывание по одной из предложенных тем: Jobs. My dream Job Working from home Machines. Transport Six basic emotions How to cope with stress</p> <p>2. Лексико-грамматический тест (БРС).</p>
9.	Модуль 9: SUCCESS	<p><i>Грамматический материал</i> Present Perfect/ Present Perfect Continuous Modal Verbs</p> <p>7.8 <i>Устные разговорные темы</i> Talk about success, talk about your abilities, describe an achievement</p> <p>7.9 <i>Аудирование</i> Radio program about success</p> <p>7.10 <i>Письмо</i> Summary An internet post</p> <p>7.11 <i>Чтение</i> What is the secret of success? The human camera</p> <p>7.12 <i>DVD</i> Water ski challenge</p> <p>7.13 <i>Лексико-грамматический тест на закрепление материала</i> Lookback</p> <p>7.14 <i>Самостоятельная работа студентов</i> Внеаудиторное чтение - 5 тыс. знаков (по специальности).</p> <p>Изучение грамматического материала. Грамматика (My grammar lab) : модуль 10. Презентации по темам, связанным со специальностью.</p>
10.	Модуль 10: COMMUNITIES	<p>Аудиторная работа – 12 часов, самостоятельная работа – 12 часов.</p> <p>8.1 <i>Грамматический материал</i> Articles and Quantifiers Relative clauses</p> <p>8.2 <i>Устные разговорные темы</i> Describe your neighbourhood, compare real-world and online activities, Discuss social situations</p> <p>8.3 <i>Аудирование</i> Listen to descriptions of online communities, listen to people describing guest /host experience</p> <p>8.4 <i>Письмо</i> Website review An advertisement</p> <p>8.5 <i>Чтение</i> How well do you know your neighbours? How to be the world's best guest</p>

		<p>8.6 DVD Tribe</p> <p>8.7 Лексико-грамматический тест на закрепление материала Lookback</p> <p>8.8 Самостоятельная работа студентов Внеаудиторное чтение - 5 тыс. знаков (по специальности). Изучение грамматического материала. Грамматика (My grammar lab): модуль 1,2. Презентация «Успешный человек». Презентации по темам, связанным со специальностью.</p>
11.	Модуль 11: HISTORY	<p>Грамматический материал Third Conditional Passive voice</p> <p>9.1 Устные разговорные темы Talk about important events in history, talk about your own history, Describe a role model</p> <p>9.2 Аудирование Listen to descriptions of past decades, listen to people doing a quiz in history</p> <p>9.3 Письмо Short essay A wiki entry</p> <p>9.4 Чтение Leaps Time travel</p> <p>9.5 DVD Michelangelo</p> <p>9.6 Лексико-грамматический тест на закрепление материала Lookback</p> <p>9.7 Самостоятельная работа студентов Внеаудиторное чтение - 5 тыс. знаков (по специальности). Изучение грамматического материала. Грамматика (My grammar lab): модуль 10,16. Презентация «Величайший шаг человечества». Презентации по темам, связанным со специальностью.</p>
12.	Модуль 12: PROJECT	<p>Проектная групповая работа студентов по предложенным темам: Computers for the disabled Magnetic storage Optical discs and drivers Flash memory Spreadsheets and databases ЗАЧЕТ : лексико-грамматический тест (БРС)</p>
13.	Модуль 13: WORLD	<p>Грамматический материал Reported speech</p> <p>11.1 Устные разговорные темы Eco-living, ask for/give travel advice, Talk about special place</p> <p>11.2 Аудирование Description of the world's best cities People giving advice/warning</p> <p>11.3 Письмо A restaurant review An email campaigning for action</p> <p>11.4 Чтение Ethical man World food Ten things not to do in an airport</p> <p>11.5 DVD</p>

			<p>The great melt</p> <p>11.6 Лексико-грамматический тест на закрепление материала</p> <p>Lookback</p> <p>11.7 Самостоятельная работа студентов</p> <p>Внеаудиторное чтение - 5 тыс. знаков (по специальности).</p> <p>Изучение грамматического материала. Грамматика (My grammar lab): модуль 13.</p> <p>Презентация «Защита окружающей среды».</p> <p>Презентации по темам, связанным со специальностью.</p>
	14.	Модуль 14: PROJECT	<p>Проектная групповая работа студентов по предложенным темам:</p> <p>The Web. Cybersecurity.</p> <p>Internet Security.</p> <p>Graphics and design.</p>
	15.	Модуль 15: ПОДГОТОВКА К ЭЗАМЕНУ	<p>Самостоятельная работа студентов+ грамматика</p> <p>Внеаудиторное чтение - 5 тыс. знаков (по специальности).</p> <p>Изучение грамматического материала. Грамматика (My grammar lab): модуль 3,11,14,15,17,18,19,20</p> <p>Экзамен. Структура экзамена:</p> <ol style="list-style-type: none"> 1. Лексико-грамматический тест (проводиться до экзамена) 2. Перевод текста и краткое его изложение (проводиться до экзамена) <p>Беседа по теме (в день экзамена).</p>
Разработчики	Игнатович Юлия Олеговна, старший преподаватель Ресурсного центра иностранных языков		

<p>АННОТАЦИЯ</p> <p>рабочей программы дисциплины «Иностранный язык (немецкий)» по специальности 10.05.01 «Компьютерная безопасность» специализация «Математические методы защиты информации» квалификация выпускника: специалист по защите информации</p>	
Цель изучения дисциплины	Целью дисциплины является использование немецкого языка как средства общения для решения задач межличностного и профессионального взаимодействия с представителями других культур.
Компетенции, формируемые в результате освоения дисциплины	<p>УК-4. Способен применять современные коммуникативные технологии, в том числе на иностранном(ых) языке(ах), для академического и профессионального взаимодействия</p> <p>УК-5. Способен анализировать и учитывать разнообразие культур в процессе межкультурного взаимодействия</p>
Результаты освоения образовательной программы (ИДК)	<p>УК.4.1. Грамотно и ясно строит диалогическую речь в рамках межличностного и межкультурного общения на русском и иностранном языках.</p> <p>УК.4.2. Демонстрирует умение осуществлять деловую переписку на русском и иностранном языках с учетом социокультурных особенностей.</p> <p>УК.4.3. Осуществляет выбор коммуникативных стратегий и тактик при ведении деловых переговоров.</p> <p>УК.5.1. Имеет представление о межкультурном разнообразии общества в социально-историческом аспекте.</p>

	<p>УК.5.2. Демонстрирует знания межкультурного разнообразия общества в этическом контексте.</p> <p>УК.5.3. Умеет выстраивать взаимодействие с учетом национальных и социокультурных особенностей.</p>													
<p>Знания, умения и навыки, получаемые в процессе изучения дисциплины</p>	<p>Знать:</p> <ul style="list-style-type: none"> - иностранный язык на уровне предусмотренном рамками высшего образования, -знать способы поиска новой и нужной языковой информации, <p>Уметь:</p> <ul style="list-style-type: none"> -пользоваться наиболее употребительными и относительно простыми языковыми средствами во всех видах речевой деятельности: устной речи, аудировании, чтении и письме, -планировать работу, -ставить перед собой цели и задачи предстоящей деятельности, -уметь целесообразно распределять нагрузку. <p>Владеть:</p> <p>компьютерной грамотностью (навыки работы в компьютерных программах “Word”, “Power Point”, навыки работы с принтером, сканером, навыки работы с электронной почтой и в сети Интернет).</p>													
<p>Краткая характеристика учебной дисциплины</p>	<table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th data-bbox="528 846 871 913" style="text-align: center;">Название темы</th> <th data-bbox="871 846 1501 913" style="text-align: center;">Содержание темы</th> </tr> </thead> <tbody> <tr> <td data-bbox="528 913 871 1189">Wohnräume. Wohnträume</td> <td data-bbox="871 913 1501 1189">беседа о видах жилых помещений; сообщение о своем любимом месте в доме/квартире; описание интерьера; порядок слов в простом и вопросительном предложениях; спряжение сильных и слабых глаголов; особенности употребление предлогов in, an, auf, neben, zwischen, vor, hinter, über, unter</td> </tr> <tr> <td data-bbox="528 1189 871 1429">Ausbildung und Praktikum</td> <td data-bbox="871 1189 1501 1429">информирование о видах образовательных учреждений; беседа о возможностях прохождения практики в ходе обучения; сообщение о дуальной системе образования в Германии; описание учебы в университете; модальные глаголы wollen, mögen, müssen; предлоги для указания времени seit, vor, für</td> </tr> <tr> <td data-bbox="528 1429 871 1738">Tagesordnung und Freizeitgestaltung</td> <td data-bbox="871 1429 1501 1738">беседа о плюсах и минусах распорядка дня; сообщение о своем обычном дне; сообщение о любимом виде досуга; беседа об увлечениях; описание возможностей для проведения свободного времени в родном городе; предлоги указания времени um, an, in; глаголы с отделяемыми приставками; модальные глаголы sollen, dürfen</td> </tr> <tr> <td data-bbox="528 1738 871 1944">Essgewohnheiten. Gesundes Leben</td> <td data-bbox="871 1738 1501 1944">беседа о здоровом образе жизни; сообщение о собственных привычках в еде; рекомендации для здорового питания; конструкция du solltest/ Sie sollten для выражения совета, рекомендации; союзы denn/ weil</td> </tr> <tr> <td data-bbox="528 1944 871 2078">Konsum und Geldverhalten</td> <td data-bbox="871 1944 1501 2078">беседа об отношении к деньгам; сообщение о собственных расходах; информирование о потреблении в современном обществе и роли рекламы; вопросительные слова Wofür/ Für wen?;</td> </tr> </tbody> </table>		Название темы	Содержание темы	Wohnräume. Wohnträume	беседа о видах жилых помещений; сообщение о своем любимом месте в доме/квартире; описание интерьера; порядок слов в простом и вопросительном предложениях; спряжение сильных и слабых глаголов; особенности употребление предлогов in, an, auf, neben, zwischen, vor, hinter, über, unter	Ausbildung und Praktikum	информирование о видах образовательных учреждений; беседа о возможностях прохождения практики в ходе обучения; сообщение о дуальной системе образования в Германии; описание учебы в университете; модальные глаголы wollen, mögen, müssen; предлоги для указания времени seit, vor, für	Tagesordnung und Freizeitgestaltung	беседа о плюсах и минусах распорядка дня; сообщение о своем обычном дне; сообщение о любимом виде досуга; беседа об увлечениях; описание возможностей для проведения свободного времени в родном городе; предлоги указания времени um, an, in; глаголы с отделяемыми приставками; модальные глаголы sollen, dürfen	Essgewohnheiten. Gesundes Leben	беседа о здоровом образе жизни; сообщение о собственных привычках в еде; рекомендации для здорового питания; конструкция du solltest/ Sie sollten для выражения совета, рекомендации; союзы denn/ weil	Konsum und Geldverhalten	беседа об отношении к деньгам; сообщение о собственных расходах; информирование о потреблении в современном обществе и роли рекламы; вопросительные слова Wofür/ Für wen?;
Название темы	Содержание темы													
Wohnräume. Wohnträume	беседа о видах жилых помещений; сообщение о своем любимом месте в доме/квартире; описание интерьера; порядок слов в простом и вопросительном предложениях; спряжение сильных и слабых глаголов; особенности употребление предлогов in, an, auf, neben, zwischen, vor, hinter, über, unter													
Ausbildung und Praktikum	информирование о видах образовательных учреждений; беседа о возможностях прохождения практики в ходе обучения; сообщение о дуальной системе образования в Германии; описание учебы в университете; модальные глаголы wollen, mögen, müssen; предлоги для указания времени seit, vor, für													
Tagesordnung und Freizeitgestaltung	беседа о плюсах и минусах распорядка дня; сообщение о своем обычном дне; сообщение о любимом виде досуга; беседа об увлечениях; описание возможностей для проведения свободного времени в родном городе; предлоги указания времени um, an, in; глаголы с отделяемыми приставками; модальные глаголы sollen, dürfen													
Essgewohnheiten. Gesundes Leben	беседа о здоровом образе жизни; сообщение о собственных привычках в еде; рекомендации для здорового питания; конструкция du solltest/ Sie sollten для выражения совета, рекомендации; союзы denn/ weil													
Konsum und Geldverhalten	беседа об отношении к деньгам; сообщение о собственных расходах; информирование о потреблении в современном обществе и роли рекламы; вопросительные слова Wofür/ Für wen?;													

		косвенный вопрос; придаточные предложения с союзом dass
	Urlaubsland Deutschland	беседа о приоритетных направлениях для отдыха; информирование о возможностях для отдыха в Германии; сообщение о своих планах на каникулы; предлоги mit, nach, aus, zu, von, bei, seit, außer, entgegen, gegenüber; Perfekt
	Umweltprobleme: Wie kann jeder zum Umweltschutz beitragen?	информирование о проблемах окружающей среды; беседа о мерах по защите окружающей среды; сообщение о возможностях личного вклада в защиту окружающей среды; придаточное предложение условия
	Filmkunst: Warum sehen Jugendliche Daily-Soaps?	беседа о видах кино; информирование о значимых кинофестивалях; сообщение о собственных предпочтениях; рассуждение об интернете как универсальном СМИ; предлоги um, gegen, durch, ohne, für; Präteritum
	Junge Leute von heute	информирование об отношении молодежи к традиционным ценностям; сообщение о собственных жизненных ориентирах; описание роли семьи; конструкции ich bin der Meinung; meiner Ansicht nach; ich stimme (nicht) zu; инфинитивные обороты um ... zu/statt...zu/ ohne ... zu; придаточное предложение цели
	Fachstudium	информирование о возможностях профессионального обучения в университете; сообщение о направлении обучения в институте; описание учебного дня; определительные придаточные предложения
	Deutsch im Beruf	информирование о возможностях обучения за границей; беседа об образе специалиста, его профессиональных задачах; описание собственных представлений о будущей профессиональной деятельности; причастия в качестве определений
	Die Welt der Technik	беседа о роли научно-технического прогресса в современном обществе; информирование об этапах развития науки и техники; сообщение о современных технологиях в промышленности; описание возможностей применения информационных технологий в разных сферах жизни; страдательный залог
	Ostpreußen: wichtige Abschnitte der Geschichte	беседа об истории региона; информирование об основных этапах в истории Восточной Пруссии; сообщение об интересных исторических местах родного города; придаточные предложения времени с союзами als/wenn/nachdem

	Albertina: erste Universität in Ostpreußen	информирование о становлении Альбертины – первого университета в Восточной Пруссии; сообщение об образовательных учреждениях Кенигсберга; описание деятельности одного из представителей точных наук Альбертины; придаточные предложения времени с союзами während/bevor/bis
	Zur Entwicklung der Zahlen	информирование о концептуальных представлениях о появлении чисел; сообщение о видах чисел и основных вычислительных операциях; глаголы, требующие предложного дополнения
	Digitale Massenmedien	информирование о видах сми; сообщение о цифровых носителях информации; описание возможностей применения цифровых технологий в сми; прилагательные и наречия с предложными дополнениями
	Weiterbildung	информирование о возможностях пост-дипломного образования в России и за рубежом; сообщение о роли постоянного самообразования и повышения квалификации; сослагательное наклонение для описания потенциальной возможности
Разработчики	старший преподаватель Ресурсного центра (кафедры) иностранных языков, Попова М.Г.	

АННОТАЦИЯ рабочей программы дисциплины «Безопасность жизнедеятельности» по специальности 10.05.01 «Компьютерная безопасность» специализация «Математические методы защиты информации» квалификация выпускника: специалист по защите информации	
Цель изучения дисциплины	Формирование представления о неразрывном единстве эффективной профессиональной деятельности с требованиями к безопасности и защищенности человека, формирование навыков безопасного поведения в повседневной жизни и в экстремальных условиях.
Компетенции, формируемые в результате освоения дисциплины	УК-8. 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
Результаты освоения образовательной программы (ИДК)	УК.8.1. Оценивает факторы риска, умеет обеспечивать личную безопасность и безопасность окружающих в повседневной жизни и в профессиональной деятельности. УК.8.2. Оценивает степень потенциальной опасности чрезвычайных ситуаций и военных конфликтов. УК.8.3. Знает и может применять методы защиты в чрезвычайных ситуациях и в условиях военных конфликтов, формирует культуру безопасного и ответственного поведения
Знания, умения и навыки,	Знать:

<p>получаемые в процессе изучения дисциплины</p>	<ul style="list-style-type: none"> • поражающие факторы стихийных бедствий, крупных производственных аварий и катастроф с выходом в атмосферу радиоактивных веществ (РВ) и аварийно-химически опасных веществ (АХОВ), современных средств поражения; • анатомо-физиологические последствия воздействия на человека травмирующих, вредных и опасных производственных факторов; • правовые, нормативно-технические и организационные основы «Безопасности жизнедеятельности»; <p>Уметь:</p> <ul style="list-style-type: none"> • проводить контроль параметров и уровня негативных воздействий на их соответствие нормативным требованиям; • эффективно применять средства защиты от негативных воздействий; • планировать мероприятия по защите производственного персонала и населения в чрезвычайных ситуациях и при необходимости принимать участие в проведении спасательных и других неотложных работ при ликвидации последствий чрезвычайных ситуаций. <p>Владеть:</p> <ul style="list-style-type: none"> • методами защиты в условиях чрезвычайных ситуаций; • методами прогнозирования чрезвычайных ситуаций и предотвращения их негативных последствий; <p>методами повышения стрессоустойчивости. Способами управления эмоциями в экстремальных ситуациях.</p>
<p>Краткая характеристика учебной дисциплины</p>	<p>Основные разделы дисциплины</p> <p>Основные понятия, термины и определения.</p> <p>2 Безопасность жизнедеятельности и природная среда. Экологические опасности. Классификация. Источники загрязнения среды обитания.</p> <p>Физиология и безопасность труда, обеспечение комфортных условий жизнедеятельности. Вредные и опасные произв. Факторы.</p> <p>4. Принципы возникновения и классификация ЧС. Оценка, прогноз и мониторинг ЧС в РФ и за рубежом.</p> <p>5. ЧС природного и биолого-социального характера. Стихийные бедствия, виды, характеристика, основные повреждающие факторы. Действие человека при данных ЧС.</p> <p>6. ЧС техногенного характера. Аварии, взрывы, пожары, и др. Основные повреждающие факторы. Действие человека при данных ЧС.</p> <p>7. ЧС военного времени. Оружие массового поражения. Современная классификация. Действие населения при применении ОМП.</p> <p>8. Защита населения в чрезвычайных ситуациях. Единая государственная система предупреждения и ликвидации чрезвычайных ситуациях (РСЧС). Структура. Задачи. ГО РФ и различных государств. МЧС РФ. Эвакуация. Особенности, задачи.</p> <p>9. Терроризм как реальная угроза безопасности в современном обществе.</p> <p>10. Медико-биологические и психологические основы безопасности жизнедеятельности.</p>
<p>Разработчики</p>	<p>Судоплатов Константин Анатольевич, старший преподаватель</p>

АННОТАЦИЯ
 рабочей программы дисциплины
 «Основы информационной безопасности»
 по специальности 10.05.01 «Компьютерная безопасность»
 специализация «Математические методы защиты информации»
 квалификация выпускника: специалист по защите информации

<p>Цель изучения дисциплины</p>	<p>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.</p> <p>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.</p>
<p>Компетенции, формируемые в результате освоения дисциплины</p>	<p>Процесс изучения дисциплины направлен на формирование следующих компетенций:</p> <ul style="list-style-type: none"> - 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).
<p>Результаты освоения образовательной программы (ИДК)</p>	<p>ОПК.1.1. Демонстрирует знания понятия информации, информационной безопасности, место и роль информационной безопасности в системе национальной безопасности Российской Федерации, основы государственной информационной политики.</p> <p>ОПК.1.2. Демонстрирует знание основных средств и способов обеспечения информационной безопасности, принципов построения систем защиты информации.</p> <p>ОПК.1.3. Классифицирует защищаемую информацию по видам тайны и степеням конфиденциальности; классифицирует и оценивает угрозы информационной безопасности для объекта информатизации.</p> <p>ОПК-5.1. Демонстрирует знание нормативных правовых актов, нормативных и методических документов, регламентирующих деятельность по защите информации в организации; классифицирует и оценивает угрозы информационной безопасности для объекта информатизации.</p>

	<p>ОПК-5.2. Формулирует основные требования по защите конфиденциальной информации, персональных данных и охране результатов интеллектуальной деятельности в организации</p> <p>ОПК-5.3. Анализирует и разрабатывает проекты локальных правовых актов, инструкций, регламентов и организационно-распорядительных документов, регламентирующих работу по обеспечению информационной безопасности в организации</p>
<p>Знания, умения и навыки, получаемые в процессе изучения дисциплины</p>	<p>В результате изучения дисциплины «Основы информационной безопасности» студент должен:</p> <p><u>знать</u>:</p> <ul style="list-style-type: none"> – 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; <p><u>уметь</u>:</p> <ul style="list-style-type: none"> – классифицировать защищаемую информацию по видам тайны и степеням конфиденциальности; – классифицировать и оценивать угрозы информационной безопасности для объекта информатизации; <p><u>владеть</u>:</p> <ul style="list-style-type: none"> – профессиональной терминологией в области информационной безопасности; – средствами поиска, обобщения научно-технической информации, нормативных и методических материалов в сфере своей профессиональной деятельности.

<p>Краткая характеристика учебной дисциплины</p>	<p>Содержание основных разделов (тем) дисциплины</p> <ol style="list-style-type: none"> 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.
<p>Разработчик</p>	<p>Ветров Игорь Анатольевич, к.т.н., доцент</p>

<p>АННОТАЦИЯ</p> <p>рабочей программы дисциплины «Физическая культура и спорт» по специальности 10.05.01 «Компьютерная безопасность» специализация «Математические методы защиты информации» квалификация выпускника: специалист по защите информации</p>	
<p>Цель изучения дисциплины</p>	<p>Цель дисциплины: формирование физической культуры личности и способности направленного использования средств физической культуры и спорта для сохранения и укрепления</p>

	здоровья, повышения уровня работоспособности и физической подготовленности к будущей жизни и профессиональной деятельности.
Компетенции, формируемые в результате освоения дисциплины	УК-7 Способен поддерживать должный уровень физической подготовленности для обеспечения полноценной социальной и профессиональной деятельности.
Результаты освоения образовательной программы (ИДК) УК-7.3.	УК-7.1. Знает виды физических упражнений; научно-практические основы физической культуры и здорового образа и стиля жизни. УК-7.2. Демонстрирует необходимый уровень физических кондиций для самореализации в профессиональной деятельности. УК-7.3. Владеет средствами и методами укрепления индивидуального здоровья, физического самосовершенствования.
Знания, умения и навыки, получаемые в процессе изучения дисциплины	Знать: Роль физической культуры и спорта в развитии личности, подготовке к профессиональной деятельности, влияние физической культуры на укрепления здоровья. Основные средства и методы физического воспитания. Методы оценки и контроля физического развития и физической подготовленности. Уметь: Использовать средства и методы физической культуры для профессионально-личностного развития, физического самосовершенствования и самовоспитания, формирования здорового образа и стиля жизни; Выполнять комплексы упражнений оздоровительной, адаптивной (лечебной) физической культуры и профессионально прикладной направленности. Владеть: Опытном самостоятельно применять средства и методы физического воспитания, методами контроля состояния организма при нагрузках. Опытном ведения здорового образа жизни, участия в физкультурно-оздоровительной и спортивной деятельности.
Краткая характеристика учебной дисциплины	Физическая культура и спорт в общекультурной и профессиональной подготовке студентов.
	Универсиады. История комплексов ГТО и БГТО. Новый Всероссийский физкультурно-спортивный комплекс.
	Социально-биологические основы физической культуры.
	Основы здорового образа жизни студента.
	Лечебная физическая культура и спорт как средство профилактики и реабилитации при различных заболеваниях.
	Психофизиологические основы учебного труда и интеллектуальной деятельности. Средства физической культуры в регулировании работоспособности.
	Физическая подготовка в системе физического воспитания.
	Спорт. Классификация видов спорта. Особенности занятий индивидуальным видом спорта или системой физических упражнений.
	Современные оздоровительные системы физических упражнений.
	Методические основы самостоятельных занятий физическими упражнениями.

	Профессионально-прикладная физическая подготовка студентов. Физическая культура и спорт в профессиональной деятельности специалиста.
	Основы судейства соревнований базовых видов спорта.
Разработчики	К.п.н, доцент Д.И. Воронин, К.п.н, доцент О.Б. Томашевская, старший преподаватель Л.Л. Соболева

АННОТАЦИЯ рабочей программы дисциплины «История России» по специальности 10.05.01 «Компьютерная безопасность» специализация «Математические методы защиты информации» квалификация выпускника: специалист по защите информации	
Цель изучения дисциплины	формирование систематизированных знаний об основных закономерностях и особенностях всемирно-исторического процесса, целостной картины отечественной и мировой истории, учитывающей взаимосвязь всех ее этапов, их значимость для понимания современного места и роли России в мире.
Компетенции, формируемые в результате освоения дисциплины	ОПК-17 - способность 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.
Результаты освоения образовательной программы (ИДК)	ОПК-17.1. Знает базовые принципы исторической науки; видеть причинно-следственные связи; основные этапы и закономерности исторического развития России; понимать историческое своеобразие нашей страны. ОПК-17.2. Оценивает место и роль страны в современном мире, грамотно проводить исторические параллели. ОПК-17.3. Применяет метод анализа исторических закономерностей.
Знания, умения и навыки, получаемые в процессе изучения дисциплины	Знать: - важнейшие понятия и термины, основные события, явления и процессы отечественной и мировой истории; -ключевые методологические, исторические и источниковедческие проблемы отечественной истории; - признаки и характеристики, изучаемых в курсе политических, социальных, культурных процессов и явлений, связанных с отечественной и мировой историей; Уметь: - уметь ориентироваться в историческом и этнокультурном пространстве мировой истории; - использовать полученные знания для формирования собственной гражданской позиции и толерантно воспринимать социальные, этнические, конфессиональные и культурные различия; Владеть: - навыками ведения научной полемики; - методами критического анализа исторической информации;
Краткая характеристика	Основные разделы дисциплины. 1. История как наука.

учебной дисциплины	2. История России в период древности и Средневековья. 3. Отечественная история в период Нового и Новейшего времени.
Разработчики	Жданович Людмила Николаевна, к.и.н., доцент

АННОТАЦИЯ рабочей программы дисциплины «Основы предпринимательской деятельности» по специальности 10.05.01 «Компьютерная безопасность» специализация «Математические методы защиты информации» квалификация выпускника: специалист по защите информации	
Цель изучения дисциплины	Формирование у обучающихся компетенций для организации и реализации предпринимательской деятельности в областях и сферах актуальных в рамках направления профессиональной подготовки
Компетенции, формируемые в результате освоения дисциплины	УК-1. Способен осуществлять критический анализ проблемных ситуаций на основе системного подхода, вырабатывать стратегию действий УК-2. Способен управлять проектом на всех этапах его жизненного цикла УК-3. Способен организовывать и руководить работой команды, вырабатывая командную стратегию для достижения поставленной цели УК-6. Способен определять и реализовывать приоритеты собственной деятельности и способы ее совершенствования на основе самооценки и образования в течение всей жизни УК-9 - Способен принимать обоснованные экономические решения в различных областях жизнедеятельности УК-10 - Способен формировать нетерпимое отношение к коррупционному поведению
Результаты освоения образовательной программы (ИДК)	УК.1.1. Выбирает источники информации и осуществляет поиск информации для решения поставленных задач. УК.1.2. Демонстрирует умение рассматривать различные точки зрения и выявлять степень доказательности на поставленную задачу. УК.1.3. Определяет рациональные идеи для решения поставленных задач. УК.2.1. Демонстрирует знание правовых норм достижения поставленной цели деятельности. УК.2.2. Формулирует в рамках поставленной цели совокупность задач, обеспечивающих ее достижение. УК.2.3. Использует оптимальные способы для решения определенного круга задач, учитывая действующие правовые нормы и имеющиеся условия, ресурсы и ограничения. У К У К У К

	<p>УК.6.1. Определяет свои личные ресурсы, возможности и ограничения для достижения поставленной цели.</p> <p>УК.6.2. Создает и достраивает индивидуальную траекторию саморазвития при получении основного и дополнительного образования.</p> <p>УК.6.3. Владеет умением рационального распределения временных и информационных ресурсов.</p> <p>УК-9.1. Самостоятельно анализирует основные тенденции развития экономики применительно к профессиональной деятельности.</p> <p>УК-9.2. Ориентируется в ходе развития экономических процессов, представляет закономерность их происхождения и логику их развития.</p> <p>УК-10.1. Понимает сущность феномена коррупции</p> <p>УК-10.2. Оценивает негативные последствия коррупционного поведения.</p>
<p>Знания, умения и навыки, получаемые в процессе изучения дисциплины</p>	<p>Студент, изучивший данный курс, должен:</p> <p>Знать:</p> <ul style="list-style-type: none"> - критерии постановки задач в соответствии с целью; - основные правила и приемы работы в команде; - знать основы методов формирования команд для научно-исследовательских и опытно-конструкторских работ; - знать основы метода научного подхода к изучению и освоению новых профессиональных знаний; - основные теории и методы работы экономических механизмов в рыночных условиях; - знать основы действующей правовой системы в объеме необходимом для работы как по найму, так и в качестве самостоятельного хозяйствующего субъекта. <p>уметь:</p> <ul style="list-style-type: none"> - анализировать информацию и работать с большим количеством источников информации; - выявлять, согласовывать и осуществлять социальное взаимодействие; - самостоятельно определять ключевые задачи, формировать план действий с учетом общекомандных приоритетов; - эффективно использовать современные образовательные и информационные технологии для исследования заданной темы; - самостоятельно осваивать новые методы работы хозяйствующих субъектов и адаптироваться к решению новых практических задач; - самостоятельно контролировать свои действия в правовом аспекте; <p>Владеть:</p> <ul style="list-style-type: none"> - технологиями поиска решений поставленной задачи и анализа последствий возможных решений задачи; - практически средствами управления и работы в команде в различных ролях - навыками гибкой разработки в условиях высокой неопределённости окружения; - навыками формирования научных гипотез, их проверки и построения соответствующих научных выводов;

	<ul style="list-style-type: none"> - навыками быстрой адаптации к изменениям экономических условий, решения задач, требованиями должностных обязанностей. - навыками поиска решений юридических вопросов
Краткая характеристика учебной дисциплины	<ol style="list-style-type: none"> 1. Бизнес-планирование и формирование команды 2. Разработка и выведение продукта на рынок 3. Охрана интеллектуальной собственности и трансфер технологий 4. Оценка инвестиционной привлекательности и инструменты привлечения финансирования
Разработчики	Минкова Е.В., доцент, к.п.н.

АННОТАЦИЯ рабочей программы дисциплины «Философия» по специальности 10.05.01 «Компьютерная безопасность» специализация «Математические методы защиты информации» квалификация выпускника: специалист по защите информации	
Цель изучения дисциплины	Цель изучения дисциплины «Философия» - дать целостное представление о философии как самостоятельной области духовной культуры и теоретических исследований
Компетенции, формируемые в результате освоения дисциплины	УК-5. Способен анализировать и учитывать разнообразие культур в процессе межкультурного взаимодействия
Результаты освоения образовательной программы (ИДК)	УК.5.1. Имеет представление о межкультурном разнообразии общества в социально-историческом аспекте. УК.5.2. Демонстрирует знания межкультурного разнообразия общества в этическом контексте. УК.5.3. Умеет выстраивать взаимодействие с учетом национальных и социокультурных особенностей.
Знания, умения и навыки, получаемые в процессе изучения дисциплины	Знать - основные этапы развития и современное состояние философской мысли; - основные понятия и проблемы философских исследований основные концепции, родившиеся при решении наиболее значимых философских проблем Уметь: - анализировать философские тексты - ставить и решать собственные перспективные исследовательские задачи Владеть: - навыками использования фундаментальных философских категорий и знаний, необходимых для решения научно-исследовательских и практических задач
Краткая характеристика учебной дисциплины	Тема 1. Предмет и метод философии. Специфика философского знания Тема 2. Роль философии в жизни человека и общества Тема 3. От мифа к логосу: генезис и становление философии Тема 4. Основные этапы истории западной философии Тема 5. Духовные основы и особенности русской философии

	<p>Тема 6. Проблема сознания в философии</p> <p>Тема 7. Возможности и границы познания</p> <p>Тема 8. Научное познание и знание</p> <p>Тема 9. Основы онтологии</p> <p>Тема 10. Научная, философская и религиозная картины мира</p> <p>Тема 11. Природа и сущность человека</p> <p>Тема 12. Мотивы, нормы и ценности человеческой деятельности</p> <p>Тема 13. Природа и сущность социальности</p> <p>Тема 14. Общество и личность. Проблема свободы и ответственности</p> <p>Тема 15. Основы философии истории</p> <p>Тема 16. Проблемы и перспективы современной цивилизации</p>
Разработчики	доцент кафедры философии, кандидат философских наук Вячеслав Игоревич Савинцев, ассистент кафедры философии Игорь Александрович Горьков

<p>АННОТАЦИЯ</p> <p>рабочей программы дисциплины</p> <p>«Основы коммуникаций»</p> <p>по специальности 10.05.01 «Компьютерная безопасность»</p> <p>специализация «Математические методы защиты информации»</p> <p>квалификация выпускника: специалист по защите информации</p>	
Цель изучения дисциплины	Формирование научного представления о коммуникации, ее моделях, уровнях и видах, структуре коммуникационного процесса, специфике массовой коммуникации как вида деятельности, развитие умения грамотно использовать возможности коммуникации в профессиональной деятельности математика; развитие у студентов личностных качеств, направленных на создание эффективной коммуникации, а также формирование общекультурных компетенций в соответствии с требованиями образовательного стандарта.
Компетенции, формируемые в результате освоения дисциплины	<p>УК-4. Способен применять современные коммуникативные технологии, в том числе на иностранном(ых) языке(ах), для академического и профессионального взаимодействия</p> <p>УК-5. Способен анализировать и учитывать разнообразие культур в процессе межкультурного взаимодействия</p>
Результаты освоения образовательной программы (ИДК)	<p>УК.4.1. Грамотно и ясно строит диалогическую речь в рамках межличностного и межкультурного общения на русском и иностранном языках.</p> <p>УК.4.2. Демонстрирует умение осуществлять деловую переписку на русском и иностранном языках с учетом социокультурных особенностей.</p> <p>УК.4.3. Осуществляет выбор коммуникативных стратегий и тактик при ведении деловых переговоров.</p> <p>УК.5.1. Имеет представление о межкультурном разнообразии общества в социально-историческом аспекте.</p> <p>УК.5.2. Демонстрирует знания межкультурного разнообразия общества в этическом контексте.</p> <p>УК.5.3. Умеет выстраивать взаимодействие с учетом национальных и социокультурных особенностей.</p>

Знания, умения и навыки, получаемые в процессе изучения дисциплины	<ul style="list-style-type: none"> • Знать особенности деловой коммуникации как вида коммуникации, средства реализации делового общения, свойства устной и письменной деловой коммуникации как на русском языке, так и иностранных; особенности коммуникации в разных социальных группах, принципы и способы коммуникативного взаимодействия в группе, команде; • Уметь определить характер делового общения, построить деловую коммуникацию с помощью вербальных и невербальных средств; исполнять коммуникативную роль, связанную с социальным статусом коммуниканта в условиях совместной коммуникации, разрабатывать коммуникативные способы решения конфликтных ситуаций; • Владеть навыками, составляющими коммуникативную компетентность личности; навыками оценивания коммуникативной компетентности коммуникатора и коммуниканта, в том числе и в отношении собственной личности.
Краткая характеристика учебной дисциплины	<p>Тема 1. Введение в теорию коммуникации. Узкое и широкое понимание коммуникации. Структура коммуникативного акта.</p> <p>Тема 2. Современные модели коммуникации, их особенности. Виды коммуникации.</p> <p>Тема 3. Вербальная и невербальная коммуникация</p> <p>Тема 4. Коммуникативные стратегии и тактики.</p> <p>Тема 5. Успешная и эффективная коммуникация.</p> <p>Тема 6. Деловая коммуникация: особенности, формы, виды. Система деловых документов</p> <p>Тема 7. Деловое общение в сфере математики.</p>
Разработчики	Суворова Н.А., доцент, к.ф.н.

<p>АННОТАЦИЯ рабочей программы дисциплины «Математический анализ» по специальности 10.05.01 «Компьютерная безопасность» специализация «Математические методы защиты информации» квалификация выпускника: специалист по защите информации</p>	
Цель изучения дисциплины	Фундаментальная подготовка обучающихся в области алгебры.
Компетенции, формируемые в результате освоения дисциплины	ОПК-3. Способен на основании совокупности математических методов разрабатывать, обосновывать и реализовывать процедуры решения задач профессиональной деятельности.
Результаты освоения образовательной программы (ИДК)	<p>ОПК-3.1. Знает необходимые математические методы для решения задач обеспечения защиты информации.</p> <p>ОПК-3.2. Применяет совокупность необходимых математических методов для решения задач обеспечения защиты информации.</p> <p>ОПК-3.3. Разрабатывает, обосновывает и реализует на практике процедуры решения задач обеспечения защиты информации.</p>
Знания, умения и навыки, получаемые в процессе изучения дисциплины	<p><u>знать</u> корректные постановки классических задач; математический аппарат, применяемый при решении прикладных задач;</p> <p><u>уметь</u> строго доказывать математическое утверждение; определять возможности применения методов математического анализа;</p>

	<i>-владеть практическими навыками</i> использования стандартных методов и моделей математического анализа и их применения к решению прикладных задач
Краткая характеристика учебной дисциплины	<ol style="list-style-type: none"> 1. Введение в математический анализ. 2. Числовые функции одного действительного переменного. 3. Пределы числовых последовательностей 4. Предел функции и его свойства 5. Непрерывность функции в точке и на множестве 6. Дифференцирование функции одной переменной. Производная. 7. Приложение производной 8. Неопределенный интеграл и методы интегрирования 9. Определённый интеграл и способы его вычисления 10. Приложения определённого интеграла в геометрии и физике 11. Функции нескольких независимых переменных. Дифференциальное исчисление функций нескольких переменных. 12. Числовые ряды и их приложения 13. Функциональные ряды. 14. Разложение функций в степенные ряды. 15. Собственные интегралы, зависящие от параметра. 16. Несобственные интегралы, зависящие от параметра. 17. Обобщенные функции. 18. Ряды Фурье. 19. Двойные интегралы. 20. Тройной интеграл. 21. Криволинейные интегралы первого рода. 22. Криволинейные интегралы второго рода. 23. Поверхностные интегралы первого рода 24. Поверхностные интегралы второго рода 25. Элементы теории поля
Разработчики	Худенко Владимир Николаевич, к.ф.-м.н., профессор

АННОТАЦИЯ рабочей программы дисциплины «Алгебра» по специальности 10.05.01 «Компьютерная безопасность» специализация «Математические методы защиты информации» квалификация выпускника: специалист по защите информации	
Цель изучения дисциплины	Фундаментальная подготовка обучающихся в области алгебры.
Компетенции, формируемые в результате освоения дисциплины	ОПК-3. Способен на основании совокупности математических методов разрабатывать, обосновывать и реализовывать процедуры решения задач профессиональной деятельности.
Результаты освоения	ОПК-3.1. Знает необходимые математические методы для решения задач обеспечения защиты информации. ОПК-3.2. Применяет совокупность необходимых математических методов для решения задач обеспечения защиты информации.

образовательной программы (ИДК)	ОПК-3.3. Разрабатывает, обосновывает и реализует на практике процедуры решения задач обеспечения защиты информации
Знания, умения и навыки, получаемые в процессе изучения дисциплины	В результате освоения дисциплины студент должен: - знать основные понятия алгебры и основные типы задач, возникающих в алгебре; - уметь использовать полученные теоретические знания для решения конкретных прикладных задач, производить математические расчеты в стандартных постановках, производить содержательный анализ результатов вычислений; использовать полученные знания в профессиональной деятельности; - владеть практическими навыками формализации различных задач алгебраическими методами; составления алгоритмов решения, пригодных для последующего программирования; анализа оценки эффективности применяемых методов.
Краткая характеристика учебной дисциплины	Основные разделы дисциплины: 1. Матрицы и определители. 2. Поле комплексных чисел. 3. Кольцо многочленов от одного переменного. 4. Векторные пространства и системы линейных уравнений. 5. Линейные операторы векторных пространств. 6. Евклидовы пространства. 7. Квадратичные формы. 8. Основные алгебраические структуры. 9. Элементы общей алгебры.
Разработчики	Скрыдлова Елена Викторовна, к.ф.-м.н., доцент

АННОТАЦИЯ рабочей программы дисциплины «Геометрия» по специальности 10.05.01 «Компьютерная безопасность» специализация «Математические методы защиты информации» квалификация выпускника: специалист по защите информации	
Цель изучения дисциплины	Цель дисциплины: фундаментальная подготовка обучающихся в области геометрии.
Компетенции, формируемые в результате освоения дисциплины	ОПК-3. Способен на основании совокупности математических методов разрабатывать, обосновывать и реализовывать процедуры решения задач профессиональной деятельности
Результаты освоения образовательной программы (ИДК)	ОПК-3.1. Знает необходимые математические методы для решения задач обеспечения защиты информации. ОПК-3.2. Применяет совокупность необходимых математических методов для решения задач обеспечения защиты информации. ОПК-3.3. Разрабатывает, обосновывает и реализует на практике процедуры решения задач обеспечения защиты информации.
Знания, умения и навыки, получаемые	- знать основные понятия теории дифференциальных уравнений и основные типы задач, возникающие в теории геометрии; корректные постановки классических задач, возможные сферы их

в процессе изучения дисциплины	<p>приложений;</p> <p>- уметь понять поставленную задачу и использовать аппарат геометрии в процессе ее решения; на основе анализа увидеть и корректно сформулировать результат; использовать полученные знания в профессиональной деятельности; ориентироваться в постановках задач; на основе анализа увидеть и корректно сформулировать результат; передавать результат проведенных физико-математических и прикладных исследований в виде конкретных рекомендаций, выраженных в терминах предметной области изучавшегося явления; модифицировать классические задачи геометрии для их использования в профессиональной деятельности;</p> <p>- владеть практическими навыками решения задач геометрии, векторно-координатным методом аналитической геометрии для решения геометрических и смежных задач; практическими навыками решения задач с использованием линий и поверхностей 1-го и 2-го порядков.</p>
Краткая характеристика учебной дисциплины	<p>Основные разделы дисциплины.</p> <ol style="list-style-type: none"> 1. Векторы и операции над ними 2. Системы координат на плоскости и в пространстве 3. Линии 1-го и 2-го порядка на плоскости 4. Плоскость в пространстве 5. Прямая в пространстве 6. Изучение поверхностей 2-го порядка по их каноническим уравнениям
Разработчики	Полякова Катерина Валентиновна, к.ф.-м.н., доцент

<p>АННОТАЦИЯ</p> <p>рабочей программы дисциплины</p> <p>«Информатика»</p> <p>по специальности 10.05.01 «Компьютерная безопасность»</p> <p>специализация «Математические методы защиты информации»</p> <p>квалификация выпускника: специалист по защите информации</p>	
Цель изучения дисциплины	Целью освоения дисциплины «Информатика» является формирование общей информационной культуры студентов, подготовка их к изучению других дисциплин, связанных с использованием современных информационных технологий в практической деятельности и обеспечения их информационной безопасности.
Компетенции, формируемые в результате освоения дисциплины	ОПК-2. Способен применять программные средства системного и прикладного назначений, в том числе отечественного производства, для решения задач профессиональной деятельности
Результаты освоения образовательной программы (ИДК)	<p>ОПК-2.1. Понимает современные информационные технологии и программные средства, в том числе отечественного производства, для решения задач профессиональной деятельности.</p> <p>ОПК-2.2. Выбирает современные информационные технологии и программные средства, в том числе отечественного производства, для решения задач профессиональной деятельности.</p> <p>ОПК-2.3. Обладает навыками применения современных информационных технологий и программных средств, в том числе</p>

	отечественного производства, для решения задач профессиональной деятельности.
Знания, умения и навыки, получаемые в процессе изучения дисциплины	<p><i>Знать:</i></p> <ul style="list-style-type: none"> • формы и способы представления данных в компьютере; • логико-математические основы построение электронных цифровых устройств; • состав, назначение функциональных компонентов и программного обеспечения персонального компьютера; <p><i>Уметь:</i></p> <ul style="list-style-type: none"> • применять типовые программные средства сервисного назначения; • пользоваться сетевыми средствами обмена данными, в том числе с использованием глобальной информационной сети интернет; • пользоваться возможностями интерфейса командной строки современных операционных систем; <p><i>Владеть:</i></p> <ul style="list-style-type: none"> • навыками работы с офисными приложениями. <p>навыками алгоритмизации и структурного программирования на языке высокого уровня.</p>
Краткая характеристика учебной дисциплины	<p>Раздел 1. «Алгоритмизация и программирование»</p> <p>Раздел 2. «Основы теории информации»</p> <p>Раздел 3 «Представление информации в компьютере».</p> <p>Раздел 4. «Элементы теории алгоритмов»</p> <p>Раздел 5. «Основы построения компьютера».</p> <p>Раздел 6. «Программное обеспечение компьютера».</p> <p>Раздел 7. Компьютерные сети и проблемы информационной безопасности.</p>
Разработчики	Дёмин С.А., старший преподаватель

<p>АННОТАЦИЯ</p> <p>рабочей программы дисциплины</p> <p>«Дифференциальные уравнения»</p> <p>по специальности 10.05.01 «Компьютерная безопасность»</p> <p>специализация «Математические методы защиты информации»</p> <p>квалификация выпускника: специалист по защите информации</p>	
Цель изучения дисциплины	Фундаментальная подготовка обучающихся в области дифференциальных уравнений.
Компетенции, формируемые в результате освоения дисциплины	ОПК-3. Способен на основании совокупности математических методов разрабатывать, обосновывать и реализовывать процедуры решения задач профессиональной деятельности.
Результаты освоения образовательной программы (ИДК)	<p>ОПК-3.1. Знает необходимые математические методы для решения задач обеспечения защиты информации.</p> <p>ОПК-3.2. Применяет совокупность необходимых математических методов для решения задач обеспечения защиты информации.</p> <p>ОПК-3.3. Разрабатывает, обосновывает и реализует на практике процедуры решения задач обеспечения защиты информации</p>
Знания, умения и навыки,	В результате освоения дисциплины студент должен:

получаемые в процессе изучения дисциплины	<p>- знать основные понятия теории дифференциальных уравнений и основные типы задач, возникающих в теории дифференциальных уравнений;</p> <p>- уметь ориентироваться в постановках задач; на основе анализа увидеть и корректно сформулировать результат; применять совокупность необходимых математических методов для решения задач обеспечения защиты информации;</p> <p>- владеть практическими навыками решения обыкновенных дифференциальных уравнений, систем дифференциальных уравнений, исследования решений на устойчивость.</p>
Краткая характеристика учебной дисциплины	<p>Основные разделы дисциплины:</p> <ol style="list-style-type: none"> 1. Общие понятия теории дифференциальных уравнений. 2. Дифференциальные уравнения первого порядка. 3. Приложения дифференциальных уравнений к геометрии и физике. 4. Дифференциальные уравнения высших порядков. 5. Линейные однородные уравнения. 6. Неоднородные линейные уравнения 2-го порядка. 7. Системы обыкновенных дифференциальных уравнений. <p>Устойчивость.</p> <ol style="list-style-type: none"> 8. Решение дифференциальных уравнений в окрестностях особых точек. Фазовая плоскость.
Разработчики	Шевченко Юрий Иванович, к.ф.-м.н., профессор

<p>АННОТАЦИЯ</p> <p>рабочей программы дисциплины</p> <p>«Комплексный анализ»</p> <p>по специальности 10.05.01 «Компьютерная безопасность»</p> <p>специализация «Математические методы защиты информации»</p> <p>квалификация выпускника: специалист по защите информации</p>	
Цель изучения дисциплины	Фундаментальная подготовка обучающихся в области комплексного анализа.
Компетенции, формируемые в результате освоения дисциплины	ОПК-3. Способен на основании совокупности математических методов разрабатывать, обосновывать и реализовывать процедуры решения задач профессиональной деятельности.
Результаты освоения образовательной программы (ИДК)	<p>ОПК-3.1. Знает необходимые математические методы для решения задач обеспечения защиты информации.</p> <p>ОПК-3.2. Применяет совокупность необходимых математических методов для решения задач обеспечения защиты информации.</p> <p>ОПК-3.3. Разрабатывает, обосновывает и реализует на практике процедуры решения задач обеспечения защиты информации.</p>
Знания, умения и навыки, получаемые в процессе изучения дисциплины	<p>В результате освоения дисциплины студент должен:</p> <p>- знать: основные понятия комплексного анализа; возможные сферы приложения методов решения практических задач средствами комплексного анализа, в том числе в компьютерном моделировании прикладных задач.</p> <p>- уметь: использовать полученные теоретические знания для решения конкретных прикладных задач, производить математические расчеты в стандартных постановках, производить</p>

	<p>содержательный анализ результатов вычислений; формулировать задачу, используя логический и вычислительный аппарат комплексного анализа; использовать полученные знания в профессиональной деятельности.</p> <p>- владеть: профессиональным языком предметной области; навыками применения теоретических основ комплексного анализа в практической деятельности; навыками формализации математических задач, составления алгоритмов решения, используемых для программирования.</p>
Краткая характеристика учебной дисциплины	<p>Основные разделы дисциплины:</p> <ol style="list-style-type: none"> 1. Введение в комплексный анализ. 2. Дифференцируемость функций комплексного переменного 3. Элементарные аналитические функции. 4. Интегрирование функций комплексного переменного. 5. Последовательности и ряды аналитических функций. 6. Ряд Лорана и особые точки однозначного характера. 7. Теория вычетов и ее приложения.
Разработчики	Шевченко Юрий Иванович, к.ф.-м.н., профессор

АННОТАЦИЯ рабочей программы дисциплины «Теория вероятностей и математическая статистика» по специальности 10.05.01 «Компьютерная безопасность» специализация «Математические методы защиты информации» квалификация выпускника: специалист по защите информации	
Цель изучения дисциплины	Целью освоения дисциплины «Теория вероятностей и математическая статистика» является формирование математической культуры, овладение студентами математическим аппаратом теории вероятностей и математической статистики, который используется непосредственно для решения прикладных задач и построения вероятностных моделей в различных областях практической деятельности.
Компетенции, формируемые в результате освоения дисциплины	ОПК-3 Способен на основании совокупности математических методов разрабатывать, обосновывать и реализовывать процедуры решения задач профессиональной деятельности
Результаты освоения образовательной программы (ИДК)	ОПК-1.1. Обладает фундаментальными знаниями, полученными в области математических и (или) естественных наук. ОПК-1.2. Демонстрирует умение решать задачи, формулируемые в рамках математических и (или) естественных наук. ОПК-1.3. Имеет навыки выбора методов решения задач профессиональной деятельности на основе теоретических знаний.
Знания, умения и навыки, получаемые в процессе изучения дисциплины	- знать основные методы и модели теории вероятностей и математической статистики; о возможностях, предоставляемых точными науками по интерпретации и обобщению научных исследований; знать о возможностях, предоставляемых теорией вероятностей при решении прикладных задач; - уметь применять стандартные методы и модели к решению типовых теоретико-вероятностных и статистических задач;

	- владеть практическими навыками использования математического аппарата теории вероятностей для решения конкретных задач; навыками по поиску дополнительного материала по каждой теме курса; навыками формализации задач, составления алгоритмов решения, пригодных для последующего программирования; владеть профессиональным языком предметной области знания
Краткая характеристика учебной дисциплины	<p>Основные разделы дисциплины.</p> <ol style="list-style-type: none"> 1. Пространство элементарных событий. 2. Биномиальное распределение. 3. Случайная величина. Функция распределения. 4. Многомерные случайные величины. 5. Числовые характеристики случайной величины. 6. Предельные теоремы. 7. Цепи Маркова. 8. Статистические модели. Вариационный ряд и его характеристики. 9. Статистическое оценивание неизвестных параметров распределения. 10. Методы оценивания. 11. Оценки наибольшего правдоподобия. 12. Метод наименьших квадратов. 13. Доверительные интервалы. 14. Проверка статистических гипотез.
Разработчики	Степанов Алексей Васильевич д.ф.-м.н., профессор

<p>АННОТАЦИЯ рабочей программы дисциплины «Языки программирования» по специальности 10.05.01 «Компьютерная безопасность» специализация «Математические методы защиты информации» квалификация выпускника: специалист по защите информации</p>	
Цель изучения дисциплины	Цель дисциплины: фундаментальная и практическая подготовка обучающихся в области методов программирования
Компетенции, формируемые в результате освоения дисциплины	<p>ОПК-7. Способен создавать программы на языках высокого и низкого уровня, применять методы и инструментальные средства программирования для решения профессиональных задач, осуществлять обоснованный выбор инструментария программирования и способов организации программ;</p> <p>ОПК-13. Способен разрабатывать компоненты программных и программно-аппаратных средств защиты информации в компьютерных системах и проводить анализ их безопасности;</p>
Результаты освоения образовательной программы (ИДК)	<p>ОПК-7.1. Разрабатывает программы на языках высокого и низкого уровня.</p> <p>ОПК-7.2. Применяет известные методы программирования и возможности базового языка программирования для решения типовых профессиональных задач.</p> <p>ОПК-7.3. Осуществляет обоснованный выбор инструментария программирования и способов организации программ.</p>

	<p>ОПК-13.1. Знает принципы функционирования программных и программно-аппаратных средств защиты информации в компьютерных системах, принципы и методы разработки их компонент, методики анализа их безопасности.</p> <p>ОПК-13.2. Разрабатывает компоненты программных и программно-аппаратных средств защиты информации в компьютерных системах.</p> <p>ОПК-13.3. Проводит анализ безопасности компонент программных и программно-аппаратных средств защиты информации в компьютерных системах.</p>
<p>Знания, умения и навыки, получаемые в процессе изучения дисциплины</p>	<p>Знать:</p> <ul style="list-style-type: none"> – Синтаксис языка C++ – Синтаксис основных библиотек языка C++ – Основные способы организации данных в языке C++ – Синтаксис основных библиотек языка C++, их особенности, достоинства и недостатки – Основные способы организации данных в языке C++, их особенности, достоинства и недостатки – Принципы написания безопасного кода на языке C++ – Особенности реализации обработки ошибок и работы с памятью на языке Python – Способы обезопасивания ввода на языке C++ – Основы использования криптографических библиотек в языке C++ <p>уметь:</p> <ul style="list-style-type: none"> – писать программы на языке C++ – подключать дополнительные библиотеки – находить и исправлять ошибки в коде – оптимизировать программный код – писать код на языке C++ корректно обрабатывающий пользовательский ввод, возможные ошибочные ситуации – применять стандартные криптографические библиотеки <p>владеть:</p> <ul style="list-style-type: none"> – навыками практической работы с IDE языка C++ – навыками поиска информации о библиотеках языка C++, чтения их документации – навыками идентификации небезопасного кода и исправления его средствами автоматизированного тестирования кода
<p>Краткая характеристика учебной дисциплины</p>	<p>Основные разделы дисциплины.</p> <ol style="list-style-type: none"> 1. Общее понятие о программировании. Виды языков программирования. Язык C++ 2. Базовые типы данных языка C++ 3. Условия и циклы 4. Функции. Lamda-выпажения 5. Структуры данных 6. Ввод/вывод в C и C++. Работа с файлами 7. Ссылки и указатели. Динамическое выделение памяти 8. Классы, ООП. 9. Конструкторы и деструкторы 10. Переопределение операторов 11. Наследование 12. Шаблоны

	13. Классы-контейнеры STL. Итераторы 14. Исключения и их обработка 15. Стандартные библиотеки языка C и C++
Разработчики	Верещагин Сергей Дмитриевич, к.ф.-м.н., доцент

АННОТАЦИЯ рабочей программы дисциплины «Дискретная математика» по специальности 10.05.01 «Компьютерная безопасность» специализация «Математические методы защиты информации» квалификация выпускника: специалист по защите информации	
Цель изучения дисциплины	Цель дисциплины: целью освоения дисциплины «Дискретная математика» является ознакомление студентов с основными разделами дискретной математики и ее применением для решения практических задач, а также обеспечение фундаментальной подготовки в одной из важнейших областей современной математики.
Компетенции, формируемые в результате освоения дисциплины	ОПК-3. Способен на основании совокупности математических методов разрабатывать, обосновывать и реализовывать процедуры решения задач профессиональной деятельности.
Результаты освоения образовательной программы (ИДК)	ОПК-3.1. Знает необходимые математические методы для решения задач обеспечения защиты информации. ОПК-3.2. Применяет совокупность необходимых математических методов для решения задач обеспечения защиты информации. ОПК-3.3. Разрабатывает, обосновывает и реализует на практике процедуры решения задач обеспечения защиты информации.
Знания, умения и навыки, получаемые в процессе изучения дисциплины	<ul style="list-style-type: none"> ● Знать: <ul style="list-style-type: none"> – основные дискретные структуры: конечные автоматы, грамматики, графы, комбинаторные структуры; – методы перечисления для основных дискретных структур; – основы комбинаторного анализа; – основные понятия и алгоритмы теории графов. ● Уметь: <ul style="list-style-type: none"> – решать задачи периодичности и эквивалентности для конечных автоматов; – применять аппарат производящих функций и рекуррентных соотношений для решения перечислительных задач; – решать оптимизационные задачи на графах; – применять стандартные методы дискретной математики для решения профессиональных задач; – грамотно применять изученные математические методы. ● Владеть: <ul style="list-style-type: none"> – навыками применения языка и средств дискретной математики; – навыками решения комбинаторных и теоретико-графовых задач; – навыками построения дискретных моделей при решении профессиональных задач; – навыками обращения с дискретными конструкциями и методами математического и алгоритмического моделирования при решении прикладных задач.
Краткая	Основные разделы дисциплины.

характеристика учебной дисциплины	16. Элементы теории множеств. 17. Теория графов. 18. Основные комбинаторные методы.
Разработчики	Белова Ольга Олеговна, к.ф.-м.н., доцент

АННОТАЦИЯ рабочей программы дисциплины «Математическая логика и теория алгоритмов» по специальности 10.05.01 «Компьютерная безопасность» специализация «Математические методы защиты информации» квалификация выпускника: специалист по защите информации	
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	ОПК-3. Способен на основании совокупности математических методов разрабатывать, обосновывать и реализовывать процедуры решения задач профессиональной деятельности.
Результаты освоения образовательной программы (ИДК)	ОПК-3.1. Знает необходимые математические методы для решения задач обеспечения защиты информации. ОПК-3.2. Применяет совокупность необходимых математических методов для решения задач обеспечения защиты информации. ОПК-3.3. Разрабатывает, обосновывает и реализует на практике процедуры решения задач обеспечения защиты информации.
Знания, умения и навыки, получаемые в процессе изучения дисциплины	- знать систему основных понятий и теорем алгебры (логики) высказываний и предикатов, теории булевых функций, аксиоматического исчисления высказываний; - уметь применять формулы алгебры высказываний и булевы функции в решении прикладных задач, а также строить формальные доказательства в рамках исчисления высказываний; - владеть практическими навыками составления алгоритмов решения типовых задач математической логики, анализа логической структуры математических утверждений
Краткая характеристика учебной дисциплины	Основные разделы дисциплины. Тема 1. Введение в математическую логику. Тема 2. Булевы функции Тема 3. Алгебра высказываний. Исчисление высказываний. Тема 4. Алгебра предикатов. Исчисление предикатов. Тема 5. Вычислимые функции. Машины Тьюринга. Тема 6. Сложность вычислений.
Разработчики	Кулешов Артур Владимирович, к.ф.-м.н., доцент

АННОТАЦИЯ рабочей программы дисциплины «Методы программирования» по специальности 10.05.01 «Компьютерная безопасность»	
---	--

специализация «Математические методы защиты информации» квалификация выпускника: специалист по защите информации	
Цель изучения дисциплины	Цель дисциплины: фундаментальная и практическая подготовка обучающихся в области методов программирования
Компетенции, формируемые в результате освоения дисциплины	<p>ОПК-7. Способен создавать программы на языках высокого и низкого уровня, применять методы и инструментальные средства программирования для решения профессиональных задач, осуществлять обоснованный выбор инструментария программирования и способов организации программ;</p> <p>ОПК-13. Способен разрабатывать компоненты программных и программно-аппаратных средств защиты информации в компьютерных системах и проводить анализ их безопасности;</p>
Результаты освоения образовательной программы (ИДК)	<p>ОПК-7.1. Разрабатывает программы на языках высокого и низкого уровня.</p> <p>ОПК-7.2. Применяет известные методы программирования и возможности базового языка программирования для решения типовых профессиональных задач.</p> <p>ОПК-7.3. Осуществляет обоснованный выбор инструментария программирования и способов организации программ.</p> <p>ОПК-13.1. Знает принципы функционирования программных и программно-аппаратных средств защиты информации в компьютерных системах, принципы и методы разработки их компонент, методики анализа их безопасности.</p> <p>ОПК-13.2. Разрабатывает компоненты программных и программно-аппаратных средств защиты информации в компьютерных системах.</p> <p>ОПК-13.3. Проводит анализ безопасности компонент программных и программно-аппаратных средств защиты информации в компьютерных системах.</p>
Знания, умения и навыки, получаемые в процессе изучения дисциплины	<p>Знать:</p> <ul style="list-style-type: none"> - Синтаксис языка Python - Синтаксис основных библиотек языка Python - Основные способы организации данных в языке Python - Синтаксис основных библиотек языка Python, их особенности, достоинства и недостатки - Основные способы организации данных в языке Python, их особенности, достоинства и недостатки - Принципы написания безопасного кода на языке Python - Особенности реализации обработки ошибок и работы с памятью на языке Python - Способы обезопасивания ввода на языке Python - Основы использования криптографических библиотек в языке Python <p>уметь:</p> <ul style="list-style-type: none"> - писать программы на языке Python - подключать дополнительные библиотеки - находить и исправлять ошибки в коде - оптимизировать программный код

	<ul style="list-style-type: none"> - писать код на языке Python корректно обрабатывающий пользовательский ввод, возможные ошибочные ситуации - применять стандартные криптографические библиотеки <p>владеть:</p> <ul style="list-style-type: none"> - навыками практической работы с IDE языка Python - навыками поиска информации о библиотеках языка Python, чтения их документации - навыками идентификации небезопасного кода и исправления его средствами автоматизированного тестирования кода
Краткая характеристика учебной дисциплины	<p>Основные разделы дисциплины.</p> <ol style="list-style-type: none"> 1. Общее понятие о программировании. Виды языков программирования. Язык Python 2. Базовые типы данных языка Python 3. Условия и циклы 4. Функции. Lambda-выражения 5. Структуры данных 6. Модули 7. Классы, ООП. 8. Исключения и их обработка 9. Стандартные библиотеки языка Python 10. Библиотеки для работы с математикой 11. Реализация GUI в языке Python 12. Работа с графическими файлами 13. Работа с компьютерными сетями 14. Параллельное программирование
Разработчики	Верещагин Сергей Дмитриевич, к.ф.-м.н., доцент

<p>АННОТАЦИЯ</p> <p>рабочей программы дисциплины «ТЕОРИЯ ПСЕВДОСЛУЧАЙНЫХ ГЕНЕРАТОРОВ» по специальности 10.05.01 «Компьютерная безопасность» специализация «Математические методы защиты информации» квалификация выпускника: специалист по защите информации</p>	
Цель изучения дисциплины	<p>Целями освоения дисциплины <i>«Теория псевдослучайных генераторов»</i> являются:</p> <ul style="list-style-type: none"> - 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	<ul style="list-style-type: none"> - ОПК-2.2. Способен разрабатывать и анализировать математические модели механизмов защиты информации
Результаты освоения образовательной	<ul style="list-style-type: none"> - ОПК-2.2.1. Знает принципы построения средств криптографической защиты информации - ОПК-2.2.2. Выявляет наиболее целесообразные подходы к обеспечению защиты информации компьютерной системы.

программы (ИДК)	– ОПК-2.2.3. Применяет методы разработки математических моделей, реализуемых в средствах защиты информации.
Знания, умения и навыки, получаемые в процессе изучения дисциплины	<p>В результате освоения дисциплины обучающийся должен знать:</p> <ul style="list-style-type: none"> – 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. <p>уметь:</p> <ul style="list-style-type: none"> – 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. <p>владеть:</p> <ul style="list-style-type: none"> – 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)	<p>Содержание основных разделов курса</p> <p>Тема 1. ЛРП, регистры сдвига и потоковые шифры. Методы статистического анализа случайных и псевдослучайных последовательностей</p> <p>Тема 2. Общие свойства ЛРП. ЛРП над конечными полями</p> <p>Тема 3 m-последовательности. Корреляционные свойства ЛРП</p> <p>Тема 4. Регистры сдвига. Методы построения потоковых шифров</p>
Разработчики	Болтнев Юрий Федорович, старший преподаватель

АННОТАЦИЯ
рабочей программы дисциплины
«Сети и системы передачи информации»
по специальности 10.05.01 «Компьютерная безопасность»
специализация «Математические методы защиты информации»

квалификация выпускника: специалист по защите информации	
Цель изучения дисциплины	Целью курса «Сети и системы передачи информации» является изучение общих принципов передачи информации
Компетенции, формируемые в результате освоения дисциплины	ОПК-9. Способен решать задачи профессиональной деятельности с учетом текущего состояния и тенденций развития методов защиты информации в операционных системах, компьютерных сетях и системах управления базами данных, а также методов и средств защиты информации от утечки по техническим каналам, сетей и систем передачи информации
Результаты освоения образовательной программы (ИДК)	ОПК-9.1. Знает методы защиты информации в операционных системах, компьютерных сетях и системах управления базами данных, а также методы и средства защиты информации от утечки по техническим каналам, сетей и систем передачи информации. ОПК-9.2. Решает задачи профессиональной деятельности с учетом текущего состояния и тенденций развития методов защиты информации в операционных системах, компьютерных сетях и системах управления базами данных, а также методов и средств защиты информации от утечки по техническим каналам, сетей и систем передачи информации. ОПК-9.3. Решает 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.
Знания, умения и навыки, получаемые в процессе изучения дисциплины	Знать основные понятия построения систем и сетей электросвязи и особенности их эксплуатации; тактико-технические характеристики основных телекоммуникационных систем, сигналов и протоколов, применяемых для передачи различных видов сообщений; перспективы развития систем и сетей связи; способы передачи информации по проводным и беспроводным каналам, основные классы систем передачи информации, отличия систем вещания спутниковых группировок на различных типах орбит, разницу в механизмах передачи радиоволн различных диапазонов, возможности использования различных проводных и кабельных линий связи. Уметь творчески применять знания о системах электрической связи для решения задач по созданию защищенных телекоммуникационных систем; отслеживать тенденции развития систем и сетей электросвязи, внедрения новых служб и услуг связи; разрабатывать структурные схемы систем связи с заданными характеристиками; читать структурные и функциональные схемы систем и сетей связи; работать с программными средствами прикладного, системного и специального назначения; проводить сбор и анализ исходных данных для проектирования систем защиты информации; разрабатывать комплексные системы структурированных систем передачи данных с детальной прорисовкой трассировки компьютерных кабелей и необходимых кабельных каналов, определения необходимых элементов сетевой инфраструктуры – коммутаторов, маршрутизаторов, патч-панелей, кроссировочных элементов,

	<p>необходимых серверов и их систем бесперебойного питания, моделировать компьютерную сеть на специальных программных комплексах.</p> <p>Владеть: основными приемами кодирования информации, основными определениями передачи информации. Владеть навыками анализа основных электрических характеристик и возможностей телекоммуникационных систем по передаче оперативных и специальных сообщений; анализа сетевых протоколов; эксплуатации программного обеспечения и программно-аппаратных средств обеспечения информационной безопасности компьютерных систем; участия в приеме, настройке, регулировке, освоении и восстановлении работоспособности оборудования защиты информации; использования языков и систем программирования, инструментальных средств для решения профессиональных, исследовательских и прикладных задач.</p>
Краткая характеристика учебной дисциплины	<p>Основные разделы дисциплины.</p> <p>Тема 1. Введение. История развития систем связи. Теория эллиптических кривых.</p> <p>Тема 2. Определения. Кодирование. Модуляция. Цифровые системы передачи информации.</p> <p>Тема 3 Кабельные системы. Антенны и фидеры. Радиосвязь.</p> <p>Тема 4 Телефония, телеграфия, телевидение.</p> <p>Тема 5 Модемы. Мобильная связь.</p> <p>Тема 6 Компьютерные сети.</p>
Разработчики	Ставицкая Е.П., старший преподаватель

<p>АННОТАЦИЯ</p> <p>рабочей программы дисциплины</p> <p>«Системы управления базами данных»</p> <p>по специальности 10.05.01 «Компьютерная безопасность»</p> <p>специализация «Математические методы защиты информации»</p> <p>квалификация выпускника: специалист по защите информации</p>	
Цель изучения дисциплины	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	ОПК-14 - Способность проектировать базы данных, администрировать системы управления базами данных в соответствии с требованиями по защите информации;
Результаты освоения образовательной программы (ИДК)	<p>ПК-14.1. Знает методы, алгоритмы и инструменты для проектирования баз данных, администрирования систем управления базами данных в соответствии с требованиями по защите информации.</p> <p>ОПК-14.2. Проектирует базу данных, осуществляет администрирование системы управления базами данных в соответствии с требованиями по защите информации</p> <p>ОПК-14.3. Разрабатывает базы данных, осуществляет администрирование систем управления базами данных в соответствии с требованиями по защите информации.</p>

<p>Знания, умения и навыки, получаемые в процессе изучения дисциплины</p>	<p>В результате формирования данной компетенции обучающийся должен:</p> <ul style="list-style-type: none"> -знать: основы теории построения баз данных; методику анализа предметной области при построении базы данных информационной системы; современные СУБД и языки, связанные с созданием и обработкой информации в базах данных, методы и подходы к оценке эффективности баз данных и СУБД; -уметь проводить даталогическое, инфологическое проектирование базы данных, осуществлять разработку физической реализации базы данных на основе современных СУБД; обнаруживать и исправлять ошибки при работе с базами данных; администрировать СУБД; -владеть практическими навыками разработки клиент-серверных систем, проверки соответствия существующих информационных систем актуальным стандартам хранения и обработки информации, требованиям заказчика, работы в современных СУБД.
<p>Краткая характеристика учебной дисциплины</p>	<ol style="list-style-type: none"> 1. Информационные системы. Базы данных и системы управления базой данных 2. Модели данных. Инфологическое и даталогическое моделирование. Этапы проектирования БД. 3. Реляционная модель данных. Нормирование. Средства и методы проектирования БД 4. Языковые средства современных СУБД. Реляционные БД и СУБД. Язык SQL 5. Реляционные БД. Организация процессов обработки данных в БД. Запросы на языке SQL 6. Реляционные БД. Ограничения целостности 7. Реляционные БД. Особенности построение интерфейса. 8. Коммерческие БД и СУБД. 9. Обзор развития современных БД и СУБД 10. Объектно-реляционные БД и СУБД. 11. Динамический и встроенный SQL. 12. Организация многопользовательского режима работы в СУБД. 13. Распределенные БД. 14. Технология клиент - сервер 15. Технологии доступа к данным. 16. Технология реплицирования данных. 17. Анализ данных. Технология NoSQL 18. Хранилища данных. 19. Документационные информационные системы. Публикация баз данных в Интернете 20. XML-серверы 21. Интеллектуальный анализ данных (Data Mining) 22. Определение больших данных. Обзор технологий хранения больших данных
<p>Разработчики</p>	<p>Каратаева П.М., старший преподаватель</p>

АННОТАЦИЯ

рабочей программы дисциплины

«Операционные системы»

по специальности 10.05.01 «Компьютерная безопасность»

специализация «Математические методы защиты информации» квалификация выпускника: специалист по защите информации	
Цель изучения дисциплины	Цель дисциплины: целью освоения дисциплины «Операционные системы» является развитие у студентов компетенций, связанных с изучением базовых понятий, компонентов и средств взаимодействия пользователя в операционной системе Linux (ОС).
Компетенции, формируемые в результате освоения дисциплины	ОПК-12. Способен администрировать операционные системы и выполнять работы по восстановлению работоспособности прикладного и системного программного обеспечения
Результаты освоения образовательной программы (ИДК)	ОПК-12.1. Знает принципы и способы администрирования операционных систем, методы и алгоритмы восстановления работоспособности прикладного и системного программного обеспечения. ОПК-12.2. Администрирует операционные системы. ОПК-12.3. Восстанавливает работоспособность прикладного и системного программного обеспечения.
Знания, умения и навыки, получаемые в процессе изучения дисциплины	- знать понятия идентификатора и дескриптора процесса; понятия приоритета и очереди процессов; понятие событийного программирования; - уметь устанавливать иерархию процессов; задавать приоритет процессам; использовать системные прерывания; - владеть практическими навыками использования интерфейса прикладного программирования (API) для разработки прикладных приложений; разработки формальных моделей политик безопасности, политик управления доступом и информационными потоками в компьютерных системах с учетом угроз безопасности информации.
Краткая характеристика учебной дисциплины (основные блоки и темы)	<ol style="list-style-type: none"> 1. Сеанс работы в Linux 2. Терминал и командная строка 3. Структура файловой системы 4. Работа с файловой системой 5. Доступ процессов к файлам и каталогам 6. Права доступа. Особые биты атрибутов 7. Работа с текстовыми данными 8. Возможности командной оболочки 9. Пользователи и безопасность 10. Использование возможностей ACL 11. Работа с SSH. Туннелирование трафика 12. Установка ПО и сервисы 13. Резервное копирование 14. Использование LVM 15. Шифрование дисков 16. Использование виртуальных систем 17. Система инициализации systemd
Разработчики	Зубков Евгений Вячеславович, старший преподаватель

АННОТАЦИЯ рабочей программы дисциплины «Компьютерные сети» по специальности 10.05.01 «Компьютерная безопасность» специализация «Математические методы защиты информации» квалификация выпускника: специалист по защите информации	
Цель изучения дисциплины	Цель дисциплины: целью освоения дисциплины «Компьютерные сети» освоение базовых знаний по вопросам построения компьютерных сетей различной модификации.
Компетенции, формируемые в результате освоения дисциплины	ОПК-15. Способен администрировать компьютерные сети и контролировать корректность их функционирования
Результаты освоения образовательной программы (ИДК)	ОПК-15.1. Знает устройство, порядок администрирования и контроля функционирования компьютерных сетей. ОПК-15.2. Разрабатывает компьютерные сети с точки зрения защиты информации. ОПК-15.3. Администрирует и контролирует корректность функционирования компьютерных сетей
Знания, умения и навыки, получаемые в процессе изучения дисциплины	<ul style="list-style-type: none"> • Знать: базовые понятия и терминологию курса, основные характеристики сред передачи данных в компьютерных сетях; способы коммутаций компьютерных сетей; механизм реализации виртуальной памяти; принципы построения и защита от сбоев и несанкционированного доступа; • Уметь объединять компьютеры в сеть, включать и исключать узлы в сети; управлять топологией и конфигурацией сети; • Владеть навыками вычислениями маски сети, маски подсетей; вычислением диапазона адресов компьютеров, их количество;
Краткая характеристика учебной дисциплины (основные блоки и темы)	18. Эволюция и основы компьютерных сетей. Требования, предъявляемые при разработке и функционировании сети. 19. Модель взаимодействия открытых систем OSI. Стандартные стеки протоколов. Стек протоколов TCP/IP. Маршрутизация. Разработка инфраструктуры корпоративной сети. 20. Беспроводные сети и стандарты. Вызов удалённых процедур. Динамическое связывание. Нити и RPC. Виртуализация, кластеры.
Разработчики	Мищук Богдан Ростиславович, к.ф.-м.н., доцент

АННОТАЦИЯ рабочей программы дисциплины «Теория кодирования, сжатия и восстановления информации» по специальности 10.05.01 «Компьютерная безопасность» специализация «Математические методы защиты информации» квалификация выпускника: специалист по защите информации	
Цель изучения дисциплины	Цель дисциплины: изучение основных понятий, теорем и алгоритмов теории кодирования, сжатия и восстановления информации, методикой построения эффективных помехоустойчивых кодов и алгоритмов их декодирования, практической реализацией этих алгоритмов.
Компетенции, формируемые в	ОПК-7: Способен создавать программы на языках высокого и низкого уровня, применять методы и инструментальные средства

<p>результате освоения дисциплины</p>	<p>программирования для решения профессиональных задач, осуществлять обоснованный выбор инструментария программирования и способов организации программ.</p> <p>ОПК-9: Способен решать задачи профессиональной деятельности с учетом текущего состояния и тенденций развития методов защиты информации в операционных системах, компьютерных сетях и системах управления базами данных, а также методов и средств защиты информации от утечки по техническим каналам, сетей и систем передачи информации.</p> <p>ОПК-2.1: Способен разрабатывать алгоритмы, реализующие современные математические методы защиты информации.</p>
<p>Результаты освоения образовательной программы (ИДК)</p>	<p>ОПК-7.1. Разрабатывает программы на языках высокого и низкого уровня</p> <p>ОПК-7.2. Применяет известные методы программирования и возможности базового языка программирования для решения типовых профессиональных задач.</p> <p>ОПК-7.3. Осуществляет обоснованный выбор инструментария программирования и способов организации программ.</p> <p>ОПК-9.1. Знает методы защиты информации в операционных системах, компьютерных сетях и системах управления базами данных, а также методы и средства защиты информации от утечки по техническим каналам, сетей и систем передачи информации.</p> <p>ОПК-9.2. Решает 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.</p> <p>ОПК-9.3. Решает 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.</p> <p>ОПК-2.1.1. Знает алгоритмы, реализующие современные математические методы защиты информации.</p> <p>ОПК-2.1.2. Разрабатывает рекомендации и предложения по совершенствованию и повышению эффективности защиты информации.</p> <p>ОПК-2.1.3. Применяет методы отладки создаваемых средств защиты.</p>
<p>Знания, умения и навыки, получаемые в процессе изучения дисциплины</p>	<p>Знать:</p> <ul style="list-style-type: none"> – базовый синтаксис языка Python для выполнения лабораторных работ по курсу; – основные понятия дисциплины (код, линейный код, дуальный код, алгоритм декодирования по синдрому, Граница Гильберта-Варшамова. Неравенство МакЭлиса, коды Рида-Соломона, BCH коды, коды Гоппы, LDPC коды) и алгоритмы на кодирования/декодирования вышеперечисленных кодов, знать как строятся криптосистемы на кодах;

	<p>– принципы работы алгоритмов кодирования и декодирования популярных кодов (Рида-Соломона, БЧХ, кодов Гоппы, LDPC кодов).</p> <p>Уметь:</p> <p>– моделировать алгоритмическую задачу, связанную с теорией кодирования, и переносить её в машинный код языка Python;</p> <p>– вычислять порождающие/проверочные матрицы, строить таблицу синдромов, вычислять дуальный код, оценивать минимальное расстояние кода;</p> <p>– анализировать сложность алгоритмов декодирования.</p> <p>Владеть:</p> <p>– навыками программирования задач из линейной алгебры и теории кодирования;</p> <p>– методами построения линейных кодов, вычисления основных параметров кода, алгоритмами кодирования и декодирования основных линейных кодов;</p> <p>– навыками реализации алгоритмов, связанных с теорией кодирования, тестировать полученные алгоритмы.</p>
Краткая характеристика учебной дисциплины	<p>Основные разделы дисциплины:</p> <ol style="list-style-type: none"> 1. Основные понятия теории кодирования 2. Линейные коды. Декодирование по синдрому 3. Граница Гильберта-Варшамова. Неравенство МакЭлиса 4. Код Рида-Соломона 5. БЧХ-код, код Гоппы 6. Коды конкатенации 7. LDPC код 8. Списочное декодирование
Разработчики	Киршанова Е.А., PhD., доцент.

<p>АННОТАЦИЯ рабочей программы дисциплины «Теория информации» по специальности 10.05.01 «Компьютерная безопасность» специализация «Математические методы защиты информации» квалификация выпускника: специалист по защите информации</p>	
Цель изучения дисциплины	Цель дисциплины: формирование у обучающихся чёткого понимания предмета теории информации и её основных концепций, а также развитие навыков применять методы теории информации для решения проблем, связанных с хранением, обработкой и передачей информации.
Компетенции, формируемые в результате освоения дисциплины	<p>ОПК-3. Способен на основании совокупности математических методов разрабатывать, обосновывать и реализовывать процедуры решения задач профессиональной деятельности.</p> <p>ОПК-2.1. Способен разрабатывать алгоритмы, реализующие современные математические методы защиты информации.</p>
Результаты освоения образовательной программы (ИДК)	<p>ОПК-3.1. Знает необходимые математические методы для решения задач обеспечения защиты информации.</p> <p>ОПК-3.2. Применяет совокупность необходимых математических методов для решения задач обеспечения защиты информации.</p>

	<p>ОПК-3.3. Разрабатывает, обосновывает и реализует на практике процедуры решения задач обеспечения защиты информации. .</p> <p>ОПК-2.1.1. Знает алгоритмы, реализующие современные математические методы защиты информации.</p> <p>ОПК-2.1.2. Разрабатывает рекомендации и предложения по совершенствованию и повышению эффективности защиты информации.</p> <p>ОПК-2.1.3. Применяет методы отладки создаваемых средств защиты</p>
Знания, умения и навыки, получаемые в процессе изучения дисциплины	<p>- 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;</p> <p>- 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;</p> <p>- владеть основами построения математических моделей текстовой информации и моделей систем передачи информации; навыками применения математического аппарата для решения прикладных теоретико-информационных задач.</p>
Краткая характеристика учебной дисциплины	<p>Основные разделы дисциплины.</p> <ol style="list-style-type: none"> 1 Энтропия и взаимная информация. 2 Дискретные источники сообщений. 3 Кодирование дискретных источников сообщений. 4 Дискретные каналы связи. 5 Теоремы кодирования для дискретных каналов связи без памяти.
Разработчики	Колесников Никита Сергеевич , мл. науч. сотрудник лаборатория «Математические методы защиты и обработки информации»

<p>АННОТАЦИЯ</p> <p>рабочей программы дисциплины</p> <p>«Организационное и правовое обеспечение информационной безопасности»</p> <p>по специальности 10.05.01 «Компьютерная безопасность»</p> <p>специализация «Математические методы защиты информации»</p> <p>квалификация выпускника: специалист по защите информации</p>	
Цель изучения дисциплины	<p>Целью освоения дисциплины «Организационное и правовое обеспечение информационной безопасности» является:</p> <p>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</p>

<p>Компетенции, формируемые в результате освоения дисциплины</p>	<p>Процесс изучения дисциплины «Организационно-правовое обеспечение информационной безопасности» направлен на формирование следующих компетенций:</p> <ul style="list-style-type: none"> - 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).
<p>Результаты освоения образовательной программы (ИДК)</p>	<p>ОПК-5.1. Демонстрирует знание нормативных правовых актов, нормативных и методических документов, регламентирующих деятельность по защите информации в организации; классифицирует и оценивает угрозы информационной безопасности для объекта информатизации.</p> <p>ОПК-5.2. Формулирует основные требования по защите конфиденциальной информации, персональных данных и охране результатов интеллектуальной деятельности в организации.</p> <p>ОПК-5.3. Анализирует и разрабатывает проекты локальных правовых актов, инструкций, регламентов и организационно-распорядительных документов, регламентирующих работу по обеспечению информационной безопасности в организации.</p> <p>ОПК-6.1. Понимает угрозы безопасности информации и возможные пути их реализации, нормативные правовые акты, нормативные и методические документы Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю.</p> <p>ОПК-6.2. Способен организовать защиту информации ограниченного доступа в соответствии с нормативными правовыми актами, нормативными и методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю.</p> <p>ОПК-6.3. Обладает навыками организации защиты информации ограниченного доступа в соответствии с нормативными правовыми актами, нормативными и методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю.</p>
<p>Знания, умения и навыки, получаемые в процессе изучения дисциплины</p>	<p>В результате изучения дисциплины студент должен:</p> <p>знать:</p> <ul style="list-style-type: none"> - 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; <p>уметь:</p> <ul style="list-style-type: none"> - применять нормативные правовые акты и нормативные методические документы в области обеспечения информационной безопасности;

	<ul style="list-style-type: none"> - 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; <p><u>владеть:</u></p> <ul style="list-style-type: none"> - навыками работы с нормативными правовыми актами.
Краткая характеристика учебной дисциплины (основные блоки и темы)	<p>Содержание основных разделов (тем) дисциплины:</p> <p>1. <u>Правовое обеспечение информационной безопасности.</u> 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.</p> <p>2. <u>Организационное обеспечение информационной безопасности.</u> 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.</p>
Разработчики	Ветров Игорь Анатольевич, к.т.н., доцент

<p>АННОТАЦИЯ рабочей программы дисциплины «Модели безопасности компьютерных систем» по специальности 10.05.01 «Компьютерная безопасность» специализация «Математические методы защиты информации» квалификация выпускника: специалист по защите информации</p>	
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.
Компетенции, формируемые в результате	ОПК-8. Способен применять методы научных исследований при проведении разработок в области обеспечения безопасности компьютерных систем и сетей;

освоения дисциплины	ОПК-11. Способен разрабатывать политики безопасности, политики управления доступом и информационными потоками в компьютерных системах с учетом угроз безопасности информации и требований по защите информации;
Результаты освоения образовательной программы (ИДК)	<p>ОПК-8.1. Знает принципы работы с научной литературой, методы поиска научно-технической информации.</p> <p>ОПК-8.2. Способен осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических документов.</p> <p>ОПК-8.3. Обладает навыками решения профессиональных задач с широким использованием актуальной научно-технической литературы.</p> <p>ОПК-11.1. Знает меры по обеспечению информационной безопасности и методы управления процессом их реализации на объекте защиты.</p> <p>ОПК-11.2. Способен формировать политику информационной безопасности, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности.</p> <p>ОПК-11.3. Владеет навыками управления процессом реализации политики информационной безопасности, организации и поддержки выполнения комплекса мер по обеспечению информационной безопасности на объекте защиты.</p>
Знания, умения и навыки, получаемые в процессе изучения дисциплины	<p>знать: основные формальные модели безопасности компьютерных систем; угрозы безопасности информации; основные виды политик управления доступом; основные формальные модели дискреционного, мандатного, ролевого управления доступом, модели изолированной программной среды и безопасности информационных потоков;</p> <p>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.</p> <p>владеть: навыками построения моделей защищаемых систем и систем обеспечения безопасности КС; навыками разработки и анализа моделей безопасности КС.</p>
Краткая характеристика учебной дисциплины (основные блоки и темы)	<ol style="list-style-type: none"> 1. Основные понятия 2. Модели КС с дискреционным разграничением доступа. 3. Модели КС с мандатным разграничением доступа 4. Модели безопасности информационных потоков 5. Модели КС с ролевым разграничением доступа 6. Развитие формальных моделей безопасности КС
Разработчики	Олефиренко Денис Олегович, ассистент Института физико-математических наук и информационных технологий.

АННОТАЦИЯ
рабочей программы дисциплины
«Физика»

по специальности 10.05.01 «Компьютерная безопасность» специализация «Математические методы защиты информации» квалификация выпускника: специалист по защите информации	
Цель изучения дисциплины	Цель дисциплины: фундаментальная подготовка обучающихся в общей физике
Компетенции, формируемые в результате освоения дисциплины	ОПК-4 Способность анализировать физическую сущность явлений и процессов, лежащих в основе функционирования микроэлектронной техники, применять основные физические законы и модели для решения задач профессиональной деятельности.
Результаты освоения образовательной программы (ИДК)	ОПК-4.1. Демонстрирует знание физических законов и моделей, необходимых при решении задач обеспечения защиты информации. ОПК-4.2. Применяет необходимые физические законы и модели для решения обеспечения защиты информации. ОПК-4.3. Владеет навыками моделирования для решения задач обеспечения защиты информации.
Знания, умения и навыки, получаемые в процессе изучения дисциплины	- знать фундаментальную базу теоретических знаний по физике, иметь представление о физической картине, связывающей все изучаемые явления, теории и модели их описания. - уметь понять поставленную задачу и использовать базу теоретических знаний и практических навыков по физике в процессе ее решения; на основе анализа увидеть и корректно сформулировать результат; использовать полученные знания в профессиональной деятельности; ориентироваться в постановках задач; на основе анализа увидеть и корректно сформулировать результат; передавать результат проведенных физико-математических и прикладных исследований в виде конкретных рекомендаций, выраженных в терминах предметной области изучавшегося явления. - владеть полученными знаниями и навыками при освоении других дисциплин, которые связаны с физическими явлениями и понятиями..
Краткая характеристика учебной дисциплины	Основные разделы дисциплины. 1. Кинематика материальной точки. 2. Динамика материальной точки 3. Законы сохранения в механике. 4. Статика, гидростатика 5. Вращательное движение 6. Кинематика и динамика движения твёрдого тела, 7. Относительность в классической механике. Основы СТО. 8. Молекулярно-кинетическая теория 9. Уравнение состояния идеального газа 10. Основные законы термодинамики 11. Циклы в термодинамике. Работа, совершаемая идеальным газом. 12. Электростатика. 13. Постоянный электрический ток. 14. Магнитное поле 15. Сила Лоренца. Закон Ампера. 16. Закон Био-Савара-Лапласа. 17. Теорема Остроградского-Гаусса для магнитного поля. 18. Электромагнитная индукция. 19. Уравнения Максвелла. 20. Геометрическая оптика

	21. Волновая оптика. 22. Тепловое излучение. 23. Волновые и корпускулярные свойства частиц. 24. Строение атома. Основные понятия квантовой механики атомов и молекул 25. Основные понятия и законы ядерной физики. 26. . Основы физики элементарных частиц
Разработчики	Корнев Константин Петрович, к.ф.-м.н., доцент

АННОТАЦИЯ рабочей программы дисциплины «Электроника и схемотехника» по специальности 10.05.01 «Компьютерная безопасность» специализация «Математические методы защиты информации» квалификация выпускника: специалист по защите информации	
Цель изучения дисциплины	Формирование необходимых знаний в области основ построения современной электронной техники, используемой в построении компьютерных информационных систем и технических средствах защиты информации.
Компетенции, формируемые в результате освоения дисциплины	ОПК-4 Способность анализировать физическую сущность явлений и процессов, лежащих в основе функционирования микроэлектронной техники, применять основные физические законы и модели для решения задач профессиональной деятельности.
Результаты освоения образовательной программы (ИДК)	<p>ОПК-4.1. Демонстрирует знание физических законов и моделей, необходимых при решении задач обеспечения защиты информации.</p> <p>ОПК-4.2. Применяет необходимые физические законы и модели для решения обеспечения защиты информации.</p> <p>ОПК-4.3. Владеет навыками моделирования для решения задач обеспечения защиты информации.</p>
Знания, умения и навыки, получаемые в процессе изучения дисциплины	<p>Знать: физические принципы работы базовых элементов современной радиоэлектронной аппаратуры и физические процессы, протекающие в них; основы анализа базовых элементов и устройств радиоэлектронной аппаратуры, используемых в современных информационных системах; назначение и состав основных аналоговых и цифровых устройств, используемых в современных информационных системах.</p> <p>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.</p> <p>Владеть: навыками инженерного количественного анализа узловых элементов и устройств современной радиоэлектронной аппаратуры; навыками использования СВТ для машинного анализа аналоговых и цифровых элементов и узлов радиоэлектронной аппаратуры; навыками экспериментального анализа узловых элементов и устройств радиоэлектронной аппаратуры с применением современной измерительной техники.</p>
Краткая характеристика учебной дисциплины	<ol style="list-style-type: none"> 1. Физические основы полупроводников. 2. Полупроводниковые диоды. 3. Биполярные и полевые транзисторы. 4. Оптоэлектронные полупроводниковые приборы. 5. Аналоговые устройства. 6. Основы теории логических функций.

	7. Комбинационные логические устройства. 8. Последовательностные логические устройства.
Разработчики	Горбачев Андрей Александрович, к.т.н, доцент

АННОТАЦИЯ рабочей программы дисциплины «Аппаратные средства вычислительной техники» по специальности 10.05.01 «Компьютерная безопасность» специализация «Математические методы защиты информации» квалификация выпускника: специалист по защите информации	
Цель изучения дисциплины	Изучение основных понятий архитектуры современного компьютера, устройства и принципа действия важнейших компонентов аппаратных средств компьютера, механизмов пересылки и управления информацией.
Компетенции, формируемые в результате освоения дисциплины	ОПК-4 Способность анализировать физическую сущность явлений и процессов, лежащих в основе функционирования микроэлектронной техники, применять основные физические законы и модели для решения задач профессиональной деятельности.
Результаты освоения образовательной программы (ИДК)	ОПК-4.1. Демонстрирует знание физических законов и моделей, необходимых при решении задач обеспечения защиты информации. ОПК-4.2. Применяет необходимые физические законы и модели для решения обеспечения защиты информации. ОПК-4.3. Владеет навыками моделирования для решения задач обеспечения защиты информации.
Знания, умения и навыки, получаемые в процессе изучения дисциплины	Знать: - архитектуру основных типов современных компьютерных систем; - структуру и физические принципы работы современных и перспективных микропроцессоров; - физические принципы работы элементов и функциональных узлов электронной аппаратуры; - принципы построения и работы ПЭВМ; Уметь: - определять состав компьютера: тип процессора и его параметры, тип модулей памяти и их характеристики, тип видеокарты, состав и параметры периферийных устройств; - работать с современной элементной базой электронной аппаратуры. - определять направления использования ЭВМ определенного класса для решения служебных задач; Владеть: - навыками применения технических и программных средств тестирования с целью определения исправности компьютера и оценки его производительности; - навыками устранения неисправностей и технического обслуживания СВТ и периферийного оборудования; - навыками формирования структуры СВТ и выбора режимов их функционирования.
Краткая характеристика учебной дисциплины	1. Введение. История развития и классификация ЭВМ. 2. Структурная организация ЭВМ. 3. Командное управление. 4. Микропроцессоры. 5. Организация и структура памяти. 6. ПЭВМ. 7. Рабочие станции и серверы. 8. Периферийные устройства.
Разработчики	Горбачев Андрей Александрович, к.т.н, доцент

АННОТАЦИЯ рабочей программы дисциплины «Защита информации от утечки по техническим каналам» по специальности 10.05.01 «Компьютерная безопасность» специализация «Математические методы защиты информации» квалификация выпускника: специалист по защите информации	
Цель изучения дисциплины	Теоретическая и практическая подготовка обучающихся к организации и проведению мероприятий по защите информации от утечки по техническим каналам на объектах информатизации и защищаемых помещениях.
Компетенции, формируемые в результате освоения дисциплины	<p>ОПК-9. Способность решать задачи профессиональной деятельности с учетом текущего состояния и тенденций развития методов защиты информации в операционных системах, компьютерных сетях и системах управления базами данных, а также методов и средств защиты информации от утечки по техническим каналам, сетей и систем передачи информации.</p> <p>ОПК-13. Способность разрабатывать компоненты программных и программно-аппаратных средств защиты информации в компьютерных системах и проводить анализ их безопасности.</p>
Результаты освоения образовательной программы (ИДК)	<p>ОПК-9.1. Знает методы защиты информации в операционных системах, компьютерных сетях и системах управления базами данных, а также методы и средства защиты информации от утечки по техническим каналам, сетей и систем передачи информации.</p> <p>ОПК-9.2. Решает 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.</p> <p>ОПК-9.3. Решает 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.</p> <p>ОПК-13.1. Знает принципы функционирования программных и программно-аппаратных средств защиты информации в компьютерных системах, принципы и методы разработки их компонент, методики анализа их безопасности.</p> <p>ОПК-13.2. Разрабатывает компоненты программных и программно-аппаратных средств защиты информации в компьютерных системах.</p> <p>ОПК-13.3. Проводит анализ безопасности компонент программных и программно-аппаратных средств защиты информации в компьютерных системах.</p>
Знания, умения и навыки, получаемые в процессе изучения дисциплины	<p>Знать: технические каналы утечки информации; возможности различных видов технической разведки; виды технических средств, используемых при защите объектов информатизации; способы и средства защиты информации от утечки по техническим каналам;</p> <p>Уметь: формировать требования по технической защите информации; применять наиболее эффективные методы и средства технической защиты информации; контролировать эффективность мер защиты информации.</p> <p>Владеть: методами технической защиты информации; навыками расчета и инструментального контроля показателей технической защиты информации; методиками проверки защищенности объектов информатизации на соответствие требованиям нормативных документов.</p>

Краткая характеристика учебной дисциплины	1. Концепция технической защиты информации. Организационные основы технической защиты информации. 3. Теоретические основы технической защиты информации. 4. Физические основы утечки информации по техническим каналам. 5. Технические средства добывания информации. 6. Технические средства защиты информации.
Разработчики	Горбачев Андрей Александрович, к.т.н, доцент

АННОТАЦИЯ рабочей программы дисциплины «Теоретико-числовые методы в криптографии» по специальности 10.05.01 «Компьютерная безопасность» специализация «Математические методы защиты информации» квалификация выпускника: специалист по защите информации	
Цель изучения дисциплины	Цель дисциплины: фундаментальная подготовка обучающихся в области дифференциальных уравнений.
Компетенции, формируемые в результате освоения дисциплины	ОПК-8. Способен применять методы научных исследований при проведении разработок в области обеспечения безопасности компьютерных систем и сетей. ОПК-10. Способен анализировать тенденции развития методов и средств криптографической защиты информации, использовать средства криптографической защиты информации при решении задач профессиональной деятельности.
Результаты освоения образовательной программы (ИДК)	ОПК-8.1. Знает принципы работы с научной литературой, методы поиска научно-технической информации. ОПК-8.2. Осуществляет подбор, изучение и обобщение научно-технической литературы, нормативных и методических документов. ОПК-8.3. Обладает навыками решения профессиональных задач с широким использованием актуальной научно-технической литературы. ОПК-10.1. Понимает целесообразность использования криптографических алгоритмов в современных программных комплексах. ОПК-10.2. Применяет методы криптоанализа к конкретным криптографическим примитивам. ОПК-10.3. Реализует алгоритмы, в том числе криптографические, в современных программных комплексах.
Знания, умения и навыки, получаемые в процессе изучения дисциплины	- 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/проблемы теории чисел в приложениях компьютерной безопасности. - уметь применять типовые теоретико-числовые алгоритмы; проводить оценку сложности алгоритмов; разрабатывать эффективные алгоритмы и программы; работать с литературой, в том числе зарубежной, касающейся задач и проблематики теории чисел в криптографических приложениях.

	- 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; практическими навыками применения стандартных алгоритмов в криптографических приложениях.
Краткая характеристика учебной дисциплины	Основные разделы дисциплины. 1. Введение. 2. Теория сложности вычислений. 3. Элементы теории чисел. 4. Быстрые вычисления. 5. Основные теоретико-числовые задачи в криптографии. 6. Криптография с открытым ключом.
Разработчики	Малыгина Екатерина Сергеевна, к.ф.-м.н., доцент

АННОТАЦИЯ рабочей программы дисциплины «Методы и средства криптографической защиты информации» по специальности 10.05.01 «Компьютерная безопасность» специализация «Математические методы защиты информации» квалификация выпускника: специалист по защите информации	
Цель изучения дисциплины	Цель дисциплины: целью освоения дисциплины «Методы и средства криптографической защиты информации» является получение студентами теоретических знаний о современных принципах и средствах защиты информации с помощью криптографических методов.
Компетенции, формируемые в результате освоения дисциплины	ОПК-10. Способен анализировать тенденции развития методов и средств криптографической защиты информации, использовать средства криптографической защиты информации при решении задач профессиональной деятельности;
Результаты освоения образовательной программы (ИДК)	ОПК-10.1. Понимает целесообразность использования криптографических алгоритмов в современных программных комплексах ОПК-10.2. Применяет методы криптоанализа к конкретным криптографическим примитивам. ОПК-10.3. Реализует алгоритмы, в том числе криптографические, в современных программных комплексах
Знания, умения и навыки, получаемые в процессе изучения дисциплины	<ul style="list-style-type: none"> ● знать математические основы криптографических алгоритмов и современное программное обеспечение; ● уметь формализовать и алгоритмизировать математические методы, моделировать криптографические алгоритмы в системах компьютерной алгебры и оценивать их эффективность. ● владеть приемами реализации алгоритмов вычислений над конечными полями, кольцами; приемами работы с программными средствами прикладного, системного и специального назначения.
Краткая характеристика учебной дисциплины	1. Основные исторические этапы развития криптографии. 2. Математические модели открытых сообщений. 3. Основные задачи криптографии. 4. Поточные шифры замены. 5. Шифры перестановки.

	6. Блочные шифры. 7. Системы шифрования с открытым ключом. 8. Криптографическая стойкость шифров. 9. Имитостойкость шифров. 10. Помехоустойчивость шифров. 11. Принципы построения алгоритмов поточного шифрования. 12. Генераторы псевдослучайных последовательностей. 13. Методы анализа криптографических алгоритмов. 14. Конструкции хеш-функций. 15. Целостность данных и аутентификация источника данных. 16. Цифровые подписи. 17. Алгоритмы идентификации. 18. Алгоритмы распределения ключей.
Разработчики	Дёмин С.А., старший преподаватель; Ставицкая Е.П., старший преподаватель

АННОТАЦИЯ рабочей программы дисциплины «Методы алгебраической геометрии в криптографии» по специальности 10.05.01 «Компьютерная безопасность» специализация «Математические методы защиты информации» квалификация выпускника: специалист по защите информации	
Цель изучения дисциплины	Цель дисциплины: целями освоения дисциплины «Методы алгебраической геометрии в криптографии» являются ознакомление студентов с основными понятиями алгебраической геометрии; ознакомление студентов с основными алгебро-геометрическими методами, применяемыми в криптографии
Компетенции, формируемые в результате освоения дисциплины	ОПК-2.2 Способен разрабатывать и анализировать математические модели механизмов защиты информации;
Результаты освоения образовательной программы (ИДК)	ОПК-2.2.1. Знает принципы построения средств криптографической защиты информации. ОПК-2.2.2. Выявляет наиболее целесообразные подходы к обеспечению защиты информации компьютерной системы. ОПК-2.2.3. Применяет методы разработки математических моделей, реализуемых в средствах защиты информации.
Знания, умения и навыки, получаемые в процессе изучения дисциплины	<ul style="list-style-type: none"> • знать основные понятия и методы алгебраической геометрии, применяемые в криптографии • уметь грамотно применять изученные математические методы, математические пакеты для обработки, детального анализа и систематизации криптографической информации; доказывать теоремы алгебраической геометрии и применять методики алгебраической геометрии при решении задач криптографического характера; • владеть навыками решения задач алгебраической геометрии; навыками применения основных понятий и теорем дисциплины при решении алгебро-геометрических задач.
Краткая характеристика	Основные разделы дисциплины. 1. Введение в алгебраическую геометрию

учебной дисциплины	2. Теория категорий 3. Многообразия 4. Локальные свойства 5. Пучки 6. Схема
Разработчики	Мельничук Евгений Михайлович, ассистент

АННОТАЦИЯ рабочей программы дисциплины «Криптографические протоколы» по специальности 10.05.01 «Компьютерная безопасность» специализация «Математические методы защиты информации» квалификация выпускника: специалист по защите информации	
Цель изучения дисциплины	Цель дисциплины: целью освоения дисциплины «Криптографические протоколы» является ознакомление студентов с существующими подходами к анализу и синтезу криптографических протоколов, изучение отечественных и международных стандартов в этой области.
Компетенции, формируемые в результате освоения дисциплины	ОПК-10. Способен анализировать тенденции развития методов и средств криптографической защиты информации, использовать средства криптографической защиты информации при решении задач профессиональной деятельности;
Результаты освоения образовательной программы (ИДК)	ОПК-10.1. Понимает целесообразность использования криптографических алгоритмов в современных программных комплексах ОПК-10.2. Применяет методы криптоанализа к конкретным криптографическим примитивам ОПК-10.3. Реализует алгоритмы, в том числе криптографические, в современных программных комплексах.
Знания, умения и навыки, получаемые в процессе изучения дисциплины	Студент должен знать: <ul style="list-style-type: none"> ● типовые протоколы, используемые в сетях связи; ● основные типы криптографических протоколов и принципов их построения с использованием различных классов криптосистем; ● основные уязвимости и свойства криптографических протоколов, характеризующие их безопасность. Студент должен уметь: <ul style="list-style-type: none"> ● использовать симметричные и асимметричные криптосистемы для построения криптографических протоколов; ● проводить анализ криптографических протоколов. Студент должен владеть: <ul style="list-style-type: none"> ● криптографической терминологией данной дисциплины; ● подходами к разработке и анализу безопасности криптографических протоколов.
Краткая характеристика учебной дисциплины	1. Введение в дисциплину. 2. Схемы цифровой подписи. 3. Криптографические протоколы идентификации. 4. Криптографические протоколы передачи ключей. 5. Криптографические протоколы открытого распределения ключей.

	6. Криптографические протоколы предварительного распределения ключей. 7. Прикладные криптографические протоколы.
Разработчики	Дёмин С.А., старший преподаватель; Ставицкая Е.П., старший преподаватель

АННОТАЦИЯ рабочей программы дисциплины «Компьютерный практикум по криптографии на эллиптических кривых» по специальности 10.05.01 «Компьютерная безопасность» специализация «Математические методы защиты информации» квалификация выпускника: специалист по защите информации	
Цель изучения дисциплины	Цель дисциплины: формирование у обучаемых способности применять современные методы и средства исследования для обеспечения информационной безопасности компьютерных систем; формирование способности ориентироваться в современных и перспективных математических методах защиты информации, оценивать возможность и эффективность их применения в конкретных задачах защиты информации; овладение методами современной алгебры, применяемыми в криптографии, теории кодирования и общих моделях безопасности компьютерных систем.
Компетенции, формируемые в результате освоения дисциплины	ОПК-2.1 Способен разрабатывать алгоритмы, реализующие современные математические методы защиты информации.
Результаты освоения образовательной программы (ИДК)	ОПК-2.1.1. Знает алгоритмы, реализующие современные математические методы защиты информации. ОПК-2.1.2. Разрабатывает рекомендации и предложения по совершенствованию и повышению эффективности защиты информации ОПК-2.1.3. Применяет методы отладки создаваемых средств защиты
Знания, умения и навыки, получаемые в процессе изучения дисциплины	Знать уравнения и основные свойства эллиптических кривых над конечными полями различной характеристики; групповой закон на множестве рациональных точек и структуру группы рациональных точек; методы подсчёта числа рациональных точек эллиптических кривых над конечными полями; Уметь определять структуру группы рациональных точек эллиптической кривой над конечным полем; моделировать алгоритмы в системах компьютерной алгебры, оценивать их работоспособность и эффективность Владеть навыками эффективных вычислений в группе точек эллиптической кривой; методами расчета параметров криптосистем на эллиптических кривых, обеспечивающих их надежность и эффективность
Краткая характеристика учебной дисциплины	1. Изоморфизм кривых. Групповой закон композиции 2. Эллиптические кривые над полем рациональных чисел и над полями различных характеристик 3. Эллиптические кривые над конечными полями. Подсчет числа точек на кривой. 4. Криптография на эллиптических кривых

Разработчики	Болтнев Ю.Ф, старший преподаватель
--------------	------------------------------------

АННОТАЦИЯ рабочей программы дисциплины «Криптография на решетках» по специальности 10.05.01 «Компьютерная безопасность» специализация «Математические методы защиты информации» квалификация выпускника: специалист по защите информации	
Цель изучения дисциплины	Цель дисциплины: изучение новых парадигм конструкций пост-квантовых асимметрических механизмов (цифровой подписи, шифрования, обмена ключами); теоретические и практические навыки криптоанализа этих механизмов, в основе которых используются евклидовы решетки.
Компетенции, формируемые в результате освоения дисциплины	<p>ОПК-8: Способность применять методы научных исследований при проведении разработок в области обеспечения безопасности компьютерных систем и сетей.</p> <p>ОПК-10: Способность анализировать тенденции развития методов и средств криптографической защиты информации, использовать средства криптографической защиты информации при решении задач профессиональной деятельности.</p> <p>ОПК-2.1: Способен разрабатывать алгоритмы, реализующие современные математические методы защиты информации.</p>
Результаты освоения образовательной программы (ИДК)	<p>ОПК-8.1. Знает принципы работы с научной литературой, методы поиска научно-технической информации.</p> <p>ОПК-8.2. Осуществляет подбор, изучение и обобщение научно-технической литературы, нормативных и методических документов.</p> <p>ОПК-8.3. Обладает навыками решения профессиональных задач с широким использованием актуальной научно-технической литературы.</p> <p>ОПК-10.1. Понимает целесообразность использования криптографических алгоритмов в современных программных комплексах</p> <p>ОПК-10.2. Применяет методы криптоанализа к конкретным криптографическим примитивам</p> <p>ОПК-10.3. Реализует алгоритмы, в том числе криптографические, в современных программных комплексах.</p> <p>ОПК-2.1.1. Знает алгоритмы, реализующие современные математические методы защиты информации.</p> <p>ОПК-2.1.2. Разрабатывает рекомендации и предложения по совершенствованию и повышению эффективности защиты информации.</p> <p>ОПК-2.1.3. Применяет методы отладки создаваемых средств защиты.</p>
Знания, умения и навыки, получаемые в процессе изучения дисциплины	<p>Знать:</p> <ul style="list-style-type: none"> – базовый синтаксис языка Python для выполнения лабораторных работ по курсу, – основные понятия дисциплины (решётка, минимумы решетки, задача нахождения короткого вектора, алгоритмы нахождения короткого вектора, алгоритмы редукции базиса, дуальная решетка,

	<p>задачи «в среднем» (SIS, LWE), дискретное Гауссово распределение) и алгоритмы на решетках,</p> <p>– принципы работы алгоритма редукции базиса, его асимптотический анализ, а также принципы построения схемы цифровой подписи и схемы шифрования на решетке, методы доказательства безопасности этих примитивов.</p> <p>Уметь:</p> <p>– строить схему цифровой подписи на решетке и оценивать её криптографическую стойкость, строить схему шифрования на решетке и оценивать её криптографическую стойкость;</p> <p>– находить короткий вектор решетки и, в общем, моделировать задачи на решетках используя готовые библиотеки (fpylll, Sage);</p> <p>– строить основные ассиметричные криптографические примитивы, сложность которых основана на “задачах в среднем” на решетках.</p> <p>Владеть:</p> <p>– навыками криптоанализа ассиметричных протоколов, основанных на евклидовых решетках;</p> <p>– методами криптоанализа, основанного на алгоритмах редукции базиса решетки;</p> <p>– навыками реализации алгоритмов, связанных с криптографией на решетках (генерация выборки, декодирование относительно решетки, редукция базиса), и их использования.</p>
Краткая характеристика учебной дисциплины	<p>Основные разделы дисциплины:</p> <ol style="list-style-type: none"> 1. Основные понятия теории решеток 2. LLL алгоритм 3. Алгоритмы для задачи SVP. BKZ алгоритм 4. Задачи CVP и SVP 5. Задачи BDD, approxSVP, uSVP 6. Гауссово распределение на решётке 7. Задача SIS, алгоритм цифровой подписи на решетках 8. Задача LWE, метод шифрования
Разработчики	Киршанова Е.А., PhD., доцент.

<p>АННОТАЦИЯ</p> <p>рабочей программы дисциплины</p> <p>«Основы построения защищенных компьютерных сетей»</p> <p>по специальности 10.05.01 «Компьютерная безопасность»</p> <p>специализация «Математические методы защиты информации»</p> <p>квалификация выпускника: специалист по защите информации</p>	
Цель изучения дисциплины	<p>Целью освоения дисциплины является теоретическая и практическая подготовка специалистов к деятельности, связанной с построением защищенных сетевых автоматизированных систем, а также обучение принципам и методам защиты информации в компьютерных сетях.</p>
Компетенции, формируемые в результате освоения дисциплины	<p>ОПК-9. Способен решать задачи профессиональной деятельности с учетом текущего состояния и тенденций развития методов защиты информации в операционных системах, компьютерных сетях и системах управления базами данных, а также методов и средств защиты информации от утечки по техническим каналам, сетей и систем передачи информации;</p>

	ОПК-16. Способен проводить мониторинг работоспособности и анализ эффективности средств защиты информации в компьютерных системах и сетях
Результаты освоения образовательной программы (ИДК)	<p>ОПК-9.1. Знает методы защиты информации в операционных системах, компьютерных сетях и системах управления базами данных, а также методы и средства защиты информации от утечки по техническим каналам, сетей и систем передачи информации.</p> <p>ОПК-9.2. Решает 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.</p> <p>ОПК-9.3. Решает 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.</p> <p>ОПК-16.1. Знает устройство, принципы функционирования, порядок настройки, мониторинга работоспособности и анализа эффективности средств защиты информации в компьютерных системах и сетях</p> <p>ОПК-16.2. Планирует проведение мониторинга работоспособности и анализа эффективности средств защиты информации в компьютерных системах и сетях.</p> <p>ОПК-16.3. Осуществляет мониторинг работоспособности и анализ эффективности средств защиты информации в компьютерных системах и сетях</p>
Знания, умения и навыки, получаемые в процессе изучения дисциплины	<p>Знать теоретические основы дисциплин защиты информации, основные угрозы безопасности сетей, средства и методы хранения и передачи аутентификационной информации, основные протоколы идентификации и аутентификации абонентов сети, защитные механизмы и средства обеспечения сетевой безопасности, средства и методы предотвращения и обнаружения вторжений; механизмы реализации атак в сетях TCP/IP, современные методы выявления уязвимостей компьютерных сетей, основные современные отечественные и зарубежные стандарты в области компьютерной безопасности; знать средства и методы хранения и передачи аутентификационной информации, основные протоколы идентификации и аутентификации абонентов сети, защитные механизмы и средства обеспечения сетевой безопасности, средства и методы предотвращения и обнаружения вторжений</p> <p>Уметь использовать полученные теоретические знания для решения конкретных прикладных задач, формулировать политику безопасности компьютерных сетей, уметь применять защищенные</p>

	<p>протоколы, межсетевые экраны и средства обнаружения вторжений для защиты информации в сетях, осуществлять меры противодействия нарушениям сетевой безопасности с использованием различных программных и аппаратных средств защиты; проводить аудит безопасности компьютерных сетей, грамотно проводить анализ безопасности систем на соответствие стандартам, уметь выявлять уязвимости компьютерных систем и проводить их классификацию.</p> <p>Владеть практическими навыками настройки политики безопасности основных операционных систем, а также локальных компьютерных сетей, построенных на их основе; навыками настройки межсетевых экранов, методиками анализа сетевого трафика, методиками анализа результатов работы средств обнаружения вторжений; практическими навыками и методиками, по оценке безопасности компьютерных сетей.</p>
Краткая характеристика учебной дисциплины	<p>1.1. Сетевые атаки 1.2 Механизмы реализации атак в сетях TCP/IP 1.3. Примеры сетевых атак в сетях TCP/IP. Технические меры защиты от сетевых атак 1.4. Выявление сетевых атак путем анализа трафика 2.1. Криптографические протоколы обеспечения безопасности 2.2. Защита виртуальных частных сетей (VPN) 3.1. Средства и методы обеспечения целостности и конфиденциальности 3.2. Средства защиты локальных сетей при подключении к Интернет. 3.3. Защита серверов и рабочих станций. Средства и методы предотвращения и обнаружения вторжений.</p>
Разработчики	Новоселов Семен Александрович, старший преподаватель

<p>АННОТАЦИЯ рабочей программы дисциплины «Защита программ и данных» по специальности 10.05.01 «Компьютерная безопасность» специализация «Математические методы защиты информации» квалификация выпускника: специалист по защите информации</p>	
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 недеklarированных возможностей.
Компетенции, формируемые в результате освоения дисциплины	ОПК-13. Способен разрабатывать компоненты программных и программно-аппаратных средств защиты информации в компьютерных системах и проводить анализ их безопасности

Результаты освоения образовательной программы (ИДК)	<p>ОПК-13.1. Знает принципы функционирования программных и программно-аппаратных средств защиты информации в компьютерных системах, принципы и методы разработки их компонент, методики анализа их безопасности.</p> <p>ОПК-13.2. Разрабатывает компоненты программных и программно-аппаратных средств защиты информации в компьютерных системах.</p> <p>ОПК-13.3. Проводит анализ безопасности компонент программных и программно-аппаратных средств защиты информации в компьютерных системах.</p>
Знания, умения и навыки, получаемые в процессе изучения дисциплины	<p>ЗНАТЬ:</p> <ul style="list-style-type: none"> • 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; <p>УМЕТЬ:</p> <ul style="list-style-type: none"> • строить теоретические модели политик безопасности, политик управления доступом и информационными потоками в компьютерных системах с учётом различных факторов; <p>ВЛАДЕТЬ:</p> <p>навыками по реализации формальных моделей безопасности на практике.</p>
Краткая характеристика учебной дисциплины	<p>Тема 1. Анализ программных реализаций</p> <p>Тема 2. Защита программ от анализа</p> <p>Тема 3. Программные закладки</p> <p>Тема 4. Внедрение программных закладок</p> <p>Тема 5. Противодействие программным закладкам</p> <p>Тема 6. Компьютерные вирусы</p>
Разработчики	Олефиренко Денис Олегович, ассистент

<p>АННОТАЦИЯ</p> <p>рабочей программы дисциплины «Защита в операционных системах» по специальности 10.05.01 «Компьютерная безопасность» специализация «Математические методы защиты информации» квалификация выпускника: специалист по защите информации</p>	
Цель изучения дисциплины	Цель дисциплины: целями освоения дисциплины «Защита в операционных системах» являются обучить студентов принципам построения и обслуживания защищенных операционных систем, анализа безопасности защищенных операционных систем; формированию научного мировоззрения и развитию системного мышления.
Компетенции, формируемые в результате освоения дисциплины	ОПК-11. Способен разрабатывать политики безопасности, политики управления доступом и информационными потоками в компьютерных системах с учетом угроз безопасности информации и требований по защите информации;

	ОПК-13. Способен разрабатывать компоненты программных и программно-аппаратных средств защиты информации в компьютерных системах и проводить анализ их безопасности;
Результаты освоения образовательной программы (ИДК)	<p>ОПК-11.1. Знает меры по обеспечению информационной безопасности и методы управления процессом их реализации на объекте защиты.</p> <p>ОПК-11.2. Формирует политику информационной безопасности, организывает и поддерживает выполнение комплекса мер по обеспечению информационной безопасности.</p> <p>ОПК-11.3. Управляет процессом реализации политики информационной безопасности, организации и поддержки выполнения комплекса мер по обеспечению информационной безопасности на объекте защиты.</p> <p>ОПК-13.1. Знает принципы функционирования программных и программно-аппаратных средств защиты информации в компьютерных системах, принципы и методы разработки их компонент, методики анализа их безопасности.</p> <p>ОПК-13.2. Разрабатывает компоненты программных и программно-аппаратных средств защиты информации в компьютерных системах.</p> <p>ОПК-13.3. Проводит анализ безопасности компонент программных и программно-аппаратных средств защиты информации в компьютерных системах</p>
Знания, умения и навыки, получаемые в процессе изучения дисциплины	<ul style="list-style-type: none"> ● знать защитные механизмы и внутренние средства обеспечения безопасности в различных операционных системах; принципы хранения и передачи используемой при аутентификации информации; требования к подсистеме аудита и политике аудита; ● уметь применять специализированные средства для поиска и устранения проблем безопасности в различных операционных системах; настраивать политику безопасности и аудита для основных операционных систем, а также локальных вычислительных сетей, построенных на их основе; ● владеть навыками администрирования основных операционных систем; навыками по использованию сторонних программных и программно-аппаратных средств защиты информации от несанкционированного доступа для усиления процедуры аутентификации.
Краткая характеристика учебной дисциплины	<p>Основные разделы дисциплины.</p> <ol style="list-style-type: none"> 1. Введение и основные понятия 2. Базовые механизмы защиты операционных систем 3. Управление доступом 4. Идентификация, аутентификация и авторизация 5. Аудит 6. Домены Windows
Разработчики	Мельничук Евгений Михайлович, ассистент

АННОТАЦИЯ
рабочей программы дисциплины
«Основы построения защищенных баз данных»
по специальности 10.05.01 «Компьютерная безопасность»
специализация «Математические методы защиты информации»

квалификация выпускника: специалист по защите информации	
Цель изучения дисциплины	Целью освоения дисциплины является формирование навыков и умений по обеспечению безопасности информации в автоматизированных системах, основу которых составляют базы данных, дать навыки работы со встроенными в Системы управления базами данных (далее – СУБД) средствами защиты, а также показать возможные пути построения собственных механизмов защиты информации в АИС с СУБД.
Компетенции, формируемые в результате освоения дисциплины	ОПК-14. Способен проектировать базы данных, администрировать системы управления базами данных в соответствии с требованиями по защите информации; ОПК-2.2 Способен разрабатывать и анализировать математические модели механизмов защиты информации
Результаты освоения образовательной программы (ИДК)	ОПК-14.1. Знает методы, алгоритмы и инструменты для проектирования баз данных, администрирования систем управления базами данных в соответствии с требованиями по защите информации. ОПК-14.2. Проектирует базу данных, осуществляет администрирование системы управления базами данных в соответствии с требованиями по защите информации. ОПК-14.3. Разрабатывает базы данных, осуществляет администрирование систем управления базами данных в соответствии с требованиями по защите информации. ОПК-2.2.1. Знает принципы построения средств криптографической защиты информации. ОПК-2.2.2. Выявляет наиболее целесообразные подходы к обеспечению защиты информации компьютерной системы. ОПК-2.2.3. Применяет методы разработки математических моделей, реализуемых в средствах защиты информации.
Знания, умения и навыки, получаемые в процессе изучения дисциплины	Знать требования отечественных и зарубежных стандартов в области безопасности баз данных, методы защиты, принципы защиты баз данных, принципы работы механизмов защиты СУБД; методы разработки и анализа математических моделей механизмов защиты информации в СУБД. Уметь использовать встроенные механизмы СУБД, в части разграничения доступа и управления пользователями, аудита, резервирования информации, а также проектировать собственные элементы механизмов безопасности, администрировать СУБД в соответствии с требованиями по защите информации; провести анализ механизмов защиты СУБД на основе построения математической модели механизмов защиты СУБД, как встроенных, так и разработанных самостоятельно Владеть методами проектирования баз данных и механизмов защиты баз данных; методами и средствами оценки защищенности информационной системы, содержащей СУБД.
Краткая характеристика учебной дисциплины	Тема 1. Теоретические основы обеспечения безопасности в СУБД. Тема 2. Обеспечение целостности баз данных. Тема 3. Механизмы обеспечения конфиденциальности в СУБД. Тема 4. Обеспечение высокой доступности баз данных.
Разработчики	старший преподаватель Института физико-математических наук и информационных технологий Козьминых Е.В.

АННОТАЦИЯ рабочей программы дисциплины «Защита данных в государственных информационных системах» по специальности 10.05.01 «Компьютерная безопасность» специализация «Математические методы защиты информации» квалификация выпускника: специалист по защите информации	
Цель изучения дисциплины	<p>Целью изучения дисциплины «Защита данных в государственных информационных системах» является теоретическая и практическая подготовка специалистов к деятельности, связанной с комплексным анализом возможных угроз и созданием адекватной модели нарушителя, постановкой конкретных задач заданной степени сложности в рамках модели для обеспечения информационной безопасности автоматизированных систем, относящихся к категории государственных информационных систем, а также содействие фундаментализации образования и развитию системного мышления.</p>
Компетенции, формируемые в результате освоения дисциплины	<p>ОПК-1. Способен оценивать роль информации, информационных технологий и информационной безопасности в современном обществе, их значение для обеспечения объективных потребностей личности, общества и государства</p> <p>ОПК-5. Способен применять нормативные правовые акты, нормативные и методические документы, регламентирующие деятельность по защите информации;</p> <p>ОПК-6. 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</p> <p>ОПК-2.3 Способен проводить сравнительный анализ и осуществлять обоснованный выбор программных и программно-аппаратных средств защиты информации с учетом реализованных в них математических методов</p>
Результаты освоения образовательной программы (ИДК)	<p>ОПК.1.1. Демонстрирует знания понятия информации, информационной безопасности, место и роль информационной безопасности в системе национальной безопасности Российской Федерации, основы государственной информационной политики;</p> <p>ОПК.1.2. Демонстрирует знание основных средств и способов обеспечения информационной безопасности, принципов построения систем защиты информации;</p> <p>ОПК.1.3. Классифицирует защищаемую информацию по видам тайны и степеням конфиденциальности; классифицирует и оценивает угрозы информационной безопасности для объекта информатизации;</p> <p>ОПК-5.1. Демонстрирует знание нормативных правовых актов, нормативных и методических документов, регламентирующих деятельность по защите информации в организации; классифицирует и оценивает угрозы информационной безопасности для объекта информатизации.</p>

	<p>ОПК-5.2. Формулирует основные требования по защите конфиденциальной информации, персональных данных и охране результатов интеллектуальной деятельности в организации</p> <p>ОПК-5.3. Анализирует и разрабатывает проекты локальных правовых актов, инструкций, регламентов и организационно-распорядительных документов, регламентирующих работу по обеспечению информационной безопасности в организации.</p> <p>ОПК-6.1. Понимает угрозы безопасности информации и возможные пути их реализации, нормативные правовые акты, нормативные и методические документы Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю.</p> <p>ОПК-6.2. Способен организовать защиту информации ограниченного доступа в соответствии с нормативными правовыми актами, нормативными и методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю.</p> <p>ОПК-6.3. Обладает навыками организации защиты информации ограниченного доступа в соответствии с нормативными правовыми актами, нормативными и методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю.</p> <p>ОПК-2.3.1. Знает теоретико-числовые методы и алгоритмы, применяемые в средствах защиты информации.</p> <p>ОПК-2.3.2. Выбирает программные и программно-аппаратные средства защиты информации с учетом реализованных в них математических методов.</p> <p>ОПК-2.3.3. Применяет методы анализа существующих методов и средств для контроля и защиты информации.</p>
<p>Знания, умения и навыки, получаемые в процессе изучения дисциплины</p>	<p>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 документы 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</p> <p>Уметь: классифицировать защищаемую информацию по видам тайны и степеням конфиденциальности; систематизировать информацию, формулировать требования к защищаемым системам на основе требований нормативных и правовых документов;</p>

	<p>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; средствами поиска, обобщения научно-технической информации, нормативных и методических материалов, опыта в сфере своей профессиональной деятельности, разработки инструкций администраторам и пользователям государственных информационных систем; 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</p> <p>Владеть: профессиональной терминологией в области информационной безопасности; средствами поиска, методами обобщения нормативных и методических материалов в сфере своей профессиональной деятельности; практическими умениями разработки и ведения технической документации информационных систем, настройки средств защиты информации применительно в установленном классу системы</p>
Краткая характеристика учебной дисциплины	<p>Тема 1. Информационная безопасность в системе национальной безопасности Российской Федерации. Стандарты в области защиты информации государственных информационных систем</p> <p>Тема 2. Классификация государственных информационных систем. Угрозы безопасности информационных систем. Модели угроз и нарушителя.</p> <p>Тема 3. Защита информации в государственных информационных системах от утечки по техническим каналам.</p> <p>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.</p> <p>Тема 5. Порядок аттестации государственных информационных систем по требованиям безопасности информации. Ведение технической документации.</p>
Разработчики	старший преподаватель Института физико-математических наук и информационных технологий Козьминых Е.В.

<p>АННОТАЦИЯ рабочей программы дисциплины «Стратегии личностно-профессионального развития» по специальности 10.05.01 «Компьютерная безопасность» специализация «Математические методы защиты информации» квалификация выпускника: специалист по защите информации</p>	
Цель изучения дисциплины	<p>Цели освоения дисциплины:</p> <ul style="list-style-type: none"> – сформировать осознанное понимание собственных жизненных планов, их реалистичность и возможность реализации в современных условиях;

	<p>– показать возможности как личностного, так и профессионального роста;</p> <p>– акцентировать внимание на роли самообразования при реализации собственных жизненных планов.</p>
Компетенции, формируемые в результате освоения дисциплины	УК-1. Способен осуществлять критический анализ проблемных ситуаций на основе системного подхода, вырабатывать стратегию действий
Результаты освоения образовательной программы (ИДК)	<p>УК.1.1. Выбирает источники информации и осуществляет поиск информации для решения поставленных задач</p> <p>УК.1.2. Демонстрирует умение рассматривать различные точки зрения и выявлять степень доказательности на поставленную задачу</p> <p>УК.1.3. Определяет рациональные идеи для решения поставленных задач</p>
Знания, умения и навыки, получаемые в процессе изучения дисциплины	<p>Знать: стимулы, мотивы и цели карьерного роста; технологии формирования стратегии личностного и профессионального развития на основе роста самооценки; этапы формирования самооценки и технологии ее коррекции.</p> <p>Уметь: применять систему знаний о технологиях личностного роста для повышения личной эффективности и карьерного роста; определять стимулы для повышения эффективности личностного роста; управлять собственной самооценкой для корректирования стратегии личностного и профессионального развития; объективно находить сильные и слабые стороны в самооценке и корректировать их по необходимости.</p> <p>Владеть: понятийно-категориальным аппаратом, технологиями личностного роста, самооценки и эффективно применять свой потенциал для карьерного роста; технологиями личностного роста для повышения личной эффективности и карьерного роста</p>
Краткая характеристика учебной дисциплины	<p>Тема 1. Понятие личностного роста. Взаимосвязь личностного роста с этапами формирования личности.</p> <p>Тема 2. Типы личностного роста: по признаку индивидуальной профессионализации; по направлениям движения работника в структуре организации; по направленности содержанию происходящих в процессе профессионального развития изменений; по возможности времени осуществления.</p> <p>Тема 3. Мотивы личностного роста: профессиональная компетентность, менеджмент, автономия (независимость), стабильность (места жительства и работы), служение, вызов, интеграция стилей жизни, предпринимательская креативность.</p> <p>Тема 4. Особенности карьерной самореализации.</p> <p>Тема 5. Роль профессионального становления личности в личностном росте</p> <p>Тема 6. Кризисы личностного роста и технологии их преодоления</p>
Разработчики	Савкин Дмитрий Александрович, доцент

АННОТАЦИЯ

рабочей программы дисциплины

«Основы военной подготовки»

по специальности 10.05.01 «Компьютерная безопасность»

специализация «Математические методы защиты информации»

квалификация выпускника: специалист по защите информации	
Цель изучения дисциплины	формирование знаний, умений и навыков, необходимых для становления обучающихся образовательных организаций высшего образования в качестве граждан способных и готовых к выполнению воинского долга и обязанности по защите своей Родины в соответствии с законодательством Российской Федерации.
Компетенции, формируемые в результате освоения дисциплины	УК 8 - 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.
Результаты освоения образовательной программы (ИДК)	УК 8.4 - Применяет положения общевоинских уставов в повседневной деятельности подразделения, управляет строями, применяет штатное стрелковое оружие. УК 8.5 - Ведет общевойсковой бой в составе подразделения. УК 8.6 - Выполняет поставленные задачи в условиях РХБ заражения. УК 8.7 - Пользуется топографическими картами. УК 8.8 - Оказывает первую медицинскую помощь при ранениях и травмах. УК 8.9 - Имеет высокое чувство патриотизма, считает защиту Родины своим долгом и обязанностью.
Знания, умения и навыки, получаемые в процессе изучения дисциплины	Знать: основные положения общевоинских уставов ВС РФ; организацию внутреннего порядка в подразделении; основные положения Курса стрельб из стрелкового оружия; устройство стрелкового оружия, боеприпасов и ручных гранат; предназначение, задачи и организационно-штатную структуру общевойсковых подразделений (мотострелкового отделения, взвода, роты); основные факторы, определяющие характер, организацию и способы ведения современного общевойскового боя; общие сведения о ядерном, химическом и биологическом оружии, средствах его применения; правила поведения и меры профилактики в условиях заражения радиоактивными, отравляющими веществами и бактериальными средствами; тактические свойства местности, их влияние на действия подразделений в боевой обстановке; назначение, номенклатуру и условные знаки топографических карт; основные способы и средства оказания первой медицинской помощи при ранениях и травмах; тенденции и особенности развития современных международных отношений, место и роль России в многополярном мире, основные направления социально-экономического, политического и военно-технического развития страны; основные положения Военной доктрины РФ; правовое положение и порядок прохождения военной службы. Уметь: правильно применять и выполнять положения общевоинских уставов ВС РФ; осуществлять разборку и сборку автомата (АК-74) и пистолета (ПМ), подготовку к боевому применению ручных гранат; оборудовать позицию для стрельбы из стрелкового оружия; выполнять мероприятия радиационной, химической и биологической защиты; читать топографические карты различной номенклатуры; давать оценку международным

	<p>военно-политическим и внутренним событиям и фактам с позиции патриота своего Отечества; применять положения нормативно-правовых актов.</p> <p>Владеть: строевыми приемами на месте и в движении; навыками управления строями взвода; первичными навыками стрельбы из стрелкового оружия; первичными навыками подготовки к ведению общевойскового боя; навыками применения индивидуальных средств РХБ защиты; первичными навыками ориентирования на местности по карте и без карты; навыками применения индивидуальных средств медицинской защиты и подручных средств для оказания первой медицинской помощи при ранениях и травмах; навыками работы с нормативно-правовыми документами.</p>
<p>Краткая характеристика учебной дисциплины</p>	<ol style="list-style-type: none"> 1.Общевоинские уставы Вооруженных Сил Российской Федерации, их основные требования и содержание. 2.Внутренний порядок и суточный наряд. 3.Общие положения Устава гарнизонной и караульной службы. 4.Строевые приемы и движение без оружия. 5.Основы, приемы и правила стрельбы из стрелкового оружия. 6.Назначение, боевые свойства, материальная часть и применение стрелкового оружия, ручных противотанковых гранатометов и ручных гранат. 7.Выполнение упражнений учебных стрельб из стрелкового оружия. 8.Вооруженные Силы Российской Федерации их состав и задачи. Тактико-технические характеристики (ТТХ) основных образцов вооружения и техники ВС РФ. 9.Основы общевойскового боя. 10.Основы инженерного обеспечения. 11.Организация воинских частей и подразделений, вооружение, боевая техника вероятного противника. 12.Ядерное, химическое, биологическое, зажигательное оружие. 13.Радиационная, химическая и биологическая защита. 14.Местность как элемент боевой обстановки. Измерения и ориентирование на местности без карты, движение по азимутам. 15.Топографические карты и их чтение, подготовка к работе. 16.Медицинское обеспечение войск (сил), первая медицинская помощь при ранениях, травмах и особых случаях. 17.Россия в современном мире. Основные направления социально-экономического, политического и военно-технического развития страны. 18.Военная доктрина Российской Федерации. Законодательство Российской Федерации о прохождении военной службы.
<p>Разработчики</p>	<p>Балыко Сергей Владимирович, к.п.н.; Кужелев Александр Александрович, к.т.н.; Рак Евгений Николаевич; Жуков Борис Валерьевич</p>