МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное бюджетное образовательное учреждение высшего образования "Российский государственный геологоразведочный университет имени Серго Орджоникидзе"

(МГРИ)

Математические основы криптографии

рабочая программа дисциплины (модуля)

Закреплена за кафедрой **Промышленной кибербезопасности и защиты геоданных**

Учебный план s100503_25_BZO25.plx
Специальность 10.05.03 Информационная безопасность автоматизированных систем

Квалификация **Специалист по защите информации**

Форма обучения **очная**

Общая трудоемкость **3 ЗЕТ**

Часов по учебному плану 108
в том числе:
аудиторные занятия 64,25
самостоятельная работа 43,75

Виды контроля в семестрах:
зачеты 5

Распределение часов дисциплины по семестрам

Семестр (<Курс>.<Семестр на курсе>)	**5 (3.1)**		Итого	
Недель	16 4/6			
Вид занятий	УП	РП	УП	РП
Лекции	32	32	32	32
Практические	32	32	32	32
Иные виды контактной работы	0,25	0,25	0,25	0,25
В том числе инт.	4	4	4	4
Итого ауд.	64,25	64,25	64,25	64,25
Контактная работа	64,25	64,25	64,25	64,25
Сам. работа	43,75	43,75	43,75	43,75
Итого	108	108	108	108

Москва 2025

1. ЦЕЛИ ОСВОЕНИЯ ДИСЦИПЛИНЫ (МОДУЛЯ)	
1.1	Дисциплина "Математические основы криптографии" обеспечивает приобретение знаний и умений в соответствии с государственным образовательным стандартом, содействует формированию мировоззрения и системного мышления.
1.2	Целью преподавания дисциплины "Математические основы криптологии" является изложение основополагающих принципов защиты информации с помощью криптографических методов и примеров реализации этих методов на практике.
1.3	Задачи дисциплины - дать основы:
1.4	-системного подхода к организации защиты информации, передаваемой и обрабатываемой техническими средствами на основе применения криптографических методов;
1.5	-алгебраических и теоретико-числовых принципов синтеза и анализа шифров;
1.6	-математических методов, используемых в криптоанализе и криптографии.

2. МЕСТО ДИСЦИПЛИНЫ (МОДУЛЯ) В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ	
Цикл (раздел) ОП:	Б1.О
2.1	**Требования к предварительной подготовке обучающегося:**
2.1.1	Сети и системы передачи информации
2.1.2	Электроника
2.1.3	Информационные технологии
2.1.4	Линейная алгебра и аналитическая геометрия
2.1.5	Языки программирования
2.1.6	Дискретная математика
2.1.7	Инженерная и компьютерная графика
2.1.8	Высшая математика и теория вероятности
2.1.9	Математическая логика и теория алгоритмов
2.2	**Дисциплины (модули) и практики, для которых освоение данной дисциплины (модуля) необходимо как предшествующее:**
2.2.1	Технология подготовки выпускной квалификационной работы

3. КОМПЕТЕНЦИИ ОБУЧАЮЩЕГОСЯ, ФОРМИРУЕМЫЕ В РЕЗУЛЬТАТЕ ОСВОЕНИЯ ДИСЦИПЛИНЫ (МОДУЛЯ)	
ОПК-2: Способен применять программные средства системного и прикладного назначений, в том числе отечественного производства, для решения задач профессиональной деятельности	
Знать:	
Уровень 1	общие принципы построения современных компьютеров, формы и способы представления данных в персональном компьютере; логико-математические основы построения электронных цифровых устройств; состав, назначение аппаратных средств и программного обеспечения персонального компьютера; элементы компьютерного дизайна и графического отображения объектов в виде чертежей или рисунков; типовые структуры и принципы организации компьютерных сетей назначение, функции и обобщённую структуру операционных систем назначение и основные компоненты систем баз данных; общие принципы построения, области и особенности применения языков программирования высокого уровня;
Уровень 2	специализированные программные средства для моделирования режимов работы и исследования характеристик электрических цепей; основные возможности современных интегрированных сред разработки программного обеспечения на объектно-ориентированных языках программирования; возможности компиляторов программных проектов под различные операционные системы; наборы инструкций для системных утилит автоматической сборки программного обеспечения и установки программных пакетов объектно-ориентированных библиотек и фреймворков; методы коммутации и маршрутизации;
Уровень 3	основные телекоммуникационные протоколы; принципы работы элементов и функциональных узлов современной электронной аппаратуры и физические процессы, протекающие в них; типовые схемотехнические решения основных узлов и блоков электронной аппаратуры; терминологию, основные руководящие и регламентирующие документы в области ЭВМ и вычислительных систем; характеристики программных разработок, позволяющих работать с алгебраическими структурами;
Уметь:	
Уровень 1	применять типовые программные средства сервисного назначения, информационного поиска и обмена данными в сети Интернет; составлять документы, используя прикладные программы офисного назначения; пользоваться средствами пользовательских интерфейсов операционных систем; применять методы построения компьютерных моделей изделий; применять типовые программные средства сервисного назначения и пользоваться сетевыми средствами для обмена данными, в том числе с использованием глобальной информационной сети Интернет;

	работать с интегрированной средой разработки программного обеспечения;
Уровень 2	использовать специализированные программные средства для моделирования режимов работы и исследования характеристик электрических цепей; использовать функциональные возможности современных интегрированных сред разработки программного обеспечения на объектно-ориентированных языках программирования для разработки прикладных программ; использовать утилиты автоматической сборки и развертывания программ в операционных системах; применять знания о системах электрической связи для решения задач по созданию защищенных телекоммуникационных систем выполнять расчеты, связанные с выбором режимов работы и определением оптимальных параметров радиооборудования и устройств цифрового тракта в составе СМС; анализировать статистические параметры трафика, проводить расчет интерфейсов внутренних направлений сети, изменять параметры коммутационной подсистемы, маршрутизации трафика, прописки кодов маршрутизации, анализировать статистику основных показателей эффективности радиосистем и систем передачи данных, выполнять расчет пропускной способности сетей радио и телекоммуникаций; применять программные средства моделирования функциональных узлов современной электронной аппаратуры;
Уровень 3	применять программные средства моделирования функциональных узлов современной электронной аппаратуры; применять стандартные программные средства для решения профессиональных задач; осуществлять сбор, обработку, анализ и систематизацию научно-технической информации в области ЭВМ и систем с применением современных информационных технологий; производить вычисления с помощью пакета GAP и аналогичных программных комплексов; осуществлять подготовку документов в среде типовых офисных пакетов
Владеть:	
Уровень 1	навыком элементарного геометрического построения при помощи средств компьютерной графики; навыком построения двухмерных и трехмерных (3D) изображений изделий; проектирования, моделирования и анализа характеристик электрических цепей с помощью специализированных программных средств;
Уровень 2	навыками работы с основными современными интегрированными средами разработки программного обеспечения на объектно- ориентированных языках; разработки, отладки и развёртывания программного обеспечения в операционных системах семейства Windows и Linux; поиска и анализа возможностей современных интегрированных программных средств разработки прикладного программного обеспечения; проектирования сетей СМС различных стандартов и расчета их основных параметров в типовых ситуациях функционирования, работой на коммутационном оборудовании по обеспечению реализации новых услуг, сопровождения геоинформационных баз данных по сети радиодоступа, информационной поддержки расчетов радиопокрытия, радиорелейных и спутниковых трасс и частотно- территориального планирования в части использования картографической информации;
Уровень 3	навыками моделирования узлов современной электронной аппаратуры; использования современной измерительной аппаратуры при экспериментальном исследовании электронной аппаратуры; программирования в пакете GAP

ОПК-3: Способен использовать математические методы, необходимые для решения задач профессиональной деятельности	
Знать:	
Уровень 1	основные понятия и задачи векторной алгебры и аналитической геометрии; основные свойства алгебраических структур; основы линейной алгебры над произвольными полями; основные понятия теории пределов и непрерывности функций одной и нескольких действительных переменных; основные методы дифференциального исчисления функций одной и нескольких действительных переменных; основные методы интегрального исчисления функций одной и нескольких действительных переменных; основные методы исследования числовых и функциональных рядов; основные задачи теории функций комплексного переменного;
Уровень 2	основные типы обыкновенных дифференциальных уравнений и методы их решения; основные понятия, составляющие предмет теории поля, его дифференциальные и интегральные характеристики; основные понятия теории рядов; основные понятия и методы теории функций комплексного переменного; основные понятия теории вероятностей, числовые и функциональные характеристики распределений случайных величин и их основные свойства; классические предельные теоремы теории вероятностей; основные понятия теории случайных процессов; постановку задач и основные понятия математической статистики;

Уровень 3	стандартные методы получения точечных и интервальных оценок параметров вероятностных распределений; стандартные методы проверки статистических гипотез; логику высказываний и предикатов; основы теории алгоритмов; свойства основных дискретных структур: конечных полей, графов, конечных автоматов, комбинаторных структур; основные понятия и методы теории графов; основные понятия и методы теории конечных автоматов; основные понятия и методы комбинаторного анализа; основные понятия и определения теории информации; определения и свойства основных алгебраических структур: групп, колец и полей; области применения основных моделей и методов построения искусственного интеллекта;
Уметь:	
Уровень 1	строить и изучать математические модели конкретных явлений и процессов для решения расчетных и исследовательских задач; решать основные задачи векторной алгебры и аналитической геометрии;: решать основные задачи линейной алгебры, системы линейных уравнений над полями; использовать методы аналитической геометрии и векторной алгебры в смежных дисциплинах и физике; использовать методы линейной алгебры для решения прикладных задач; исследовать функциональные зависимости, возникающие для решения стандартных прикладных задач; использовать типовые модели и методы математического анализа для решения стандартных прикладных задач; проводить типовые расчеты с использованием основных формул дифференциального и интегрального исчисления;
Уровень 2	пользоваться справочными материалами по математическому анализу; применять методы теории поля, теории рядов, теории функций комплексного переменного для постановки и решения прикладных задач; применять стандартные вероятностные и статистические модели для решения типовых прикладных задач; пользоваться стандартными вероятностно- статистическими методами анализа экспериментальных данных; строить стандартные процедуры принятия решений на основе имеющихся экспериментальных данных; использовать расчетные формулы и таблицы для решения стандартных вероятностно-статистических задач; применять математические методы и вычислительную технику для решения практических задач; решать задачи периодичности и эквивалентности для конечных автоматов;
Уровень 3	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; решать типовые комбинаторные и теоретико-графовые задачи; использовать язык и средства дискретной математики для решения профессиональных задач; определять информационные характеристики системы передачи сообщений и каналов связи; производить вычисления в кольцах вычетов, матричных кольцах и в конечных полях; строить модели искусственного интеллекта для решения проектных задач, декомпозировать задачи на подзадачи и решать их с помощью методов искусственного интеллекта, интерпретировать полученные результаты;
Владеть:	
Уровень 1	навыком решения задач, относящихся к теории поля, теории рядов и теории функций комплексного переменного; навыком применения изучаемого математического аппарата для решения прикладных задач;
Уровень 2	навыком применения методов математической логики и теории алгоритмов; навыком работы с элементами групп, колец и полей;
Уровень 3	навыком оформления технических заданий при решении задач с использованием методов искусственного интеллекта

В результате освоения дисциплины (модуля) обучающийся должен

3.1	**Знать:**
3.1.1	основные характеристики сигналов электросвязи, спектры и виды модуляции; эталонную модель взаимодействия открытых систем; принципы построения и функционирования систем и сетей передачи информации; методы коммутации и маршрутизации; основные телекоммуникационные протоколы , методы коммутации и маршрутизации; основные телекоммуникационные протоколы;
3.1.2	основные положения стандартов Единой системы конструкторской документации (ЕСКД) и Единой системы программной документации (ЕСПД), элементы компьютерного дизайна и графического отображения объектов в виде чертежей или рисунков;
3.1.3	язык программирования высокого уровня (основы объектно-ориентированного программирования); стандартные алгоритмы и методы организации и обработки данных, общие принципы построения, области и особенности применения языков программирования высокого уровня;

3.1.4	принципы работы элементов и функциональных узлов современной электронной аппаратуры и физические процессы, протекающие в них, принципы работы элементов и функциональных узлов современной электронной аппаратуры и физические процессы, протекающие в них;
3.1.5	типовые структуры и принципы организации компьютерных сетей назначение, функции и обобщённую структуру операционных систем назначение и основные компоненты систем баз данных;
3.1.6	основные понятия и определения теории информации;
3.1.7	свойства основных дискретных структур: конечных полей, графов, конечных автоматов, комбинаторных структур; основные понятия и методы теории графов; основные понятия и методы теории конечных автоматов; основные понятия и методы комбинаторного анализа;
3.1.8	фундаментальные понятия и законы физики в области электростатики и электродинамики (закон Кулона, напряженность и потенциал электростатического поля, сила и плотность тока, законы Ома в интегральной и дифференциальной формах, закон Джоуля- Ленца, правила Кирхгофа, магнитное взаимодействие постоянных и переменных токов, закон Ампера, сила Лоренца, электромагнитная индукция, правило Ленца, явление самоиндукции индуктивность соленоида, емкость конденсатора); методы и
3.1.9	средства измерения физических величин; методы обработки экспериментальных данных, специализированные программные средства для моделирования режимов работы и исследования характеристик электрических цепей;
3.1.10	типовые схемотехнические решения основных узлов и блоков электронной аппаратуры, основы схемотехники современной
3.1.11	радиоэлектронной аппаратуры;
3.1.12	базовые принципы сбора информации для обработки и анализа при помощи методов искусственного интеллекта с учетом современных тенденций развития электроники, измерительной и вычислительной техники и информационных технологий, области применения основных моделей и методов построения искусственного интеллекта;
3.1.13	основные понятия, составляющие предмет теории поля, его дифференциальные и интегральные характеристики; основные
3.1.14	понятия теории рядов; основные понятия и методы теории функций комплексного переменного;
3.1.15	общие принципы построения современных компьютеров, формы и способы представления данных в персональном компьютере ;логико-математические основы построения электронных цифровых устройств;состав, назначение аппаратных средств и программного обеспечения;
3.1.16	основные возможности современных интегрированных сред разработки программного обеспечения на объектно-ориентированных
3.1.17	языках программирования;возможности компиляторов программных проектов под различные операционные системы;наборы
3.1.18	инструкций для системных утилит автоматической сборки программного обеспечения и установки программных пакетов объектно-ориентированных библиотек и фреймворков, методы разработки алгоритмов и программ в рамках объектно-ориентированной парадигмы программирования на современном языке высокого уровня; принципы объектно- ориентированной парадигмы: абстрагирование, инкапсуляция, наследование, персонального компьютера полиморфизм;основные синтаксические
3.1.19	конструкции объектно-ориентированного языка программирования: классы, поля, свойства, методы, выражения, события; методы
3.1.20	обобщенного программирования;методы оценки сложности алгоритмов;функциональные возможности стандартной библиотеки языка и фреймворка;
3.1.21	основные понятия и задачи векторной алгебры и аналитической геометрии;основные свойства алгебраических структур;основы
3.1.22	линейной алгебры над произвольными полями;
3.1.23	основные понятия теории пределов и непрерывности функций одной и нескольких действительных переменных;основные методы
3.1.24	дифференциального исчисления функций одной и нескольких действительных переменных;основные методы интегрального
3.1.25	исчисления функций одной и нескольких действительных переменных;основные методы исследования числовых и функциональных рядов;основные задачи теории функций комплексного переменного;основные типы обыкновенных дифференциальных уравнений и методы их решения;
3.1.26	основные понятия теории вероятностей, числовые и функциональные характеристики распределений случайных величин и их
3.1.27	основные свойства;классические предельные теоремы теории вероятностей;основные понятия теории случайных процессов; постановку задач и основные понятия математической статистики; стандартные методы получения точечных и интервальных оценок параметров вероятностных распределений;стандартные методы проверки статистических гипотез;
3.1.28	логику высказываний и предикатов; основы теории алгоритмов;
3.2	**Уметь:**

3.2.1	проводить анализ показателей качества сетей и систем связи; анализировать тенденции развития систем и сетей электросвязи, внедрения новых служб и услуг связи, применять знания о системах электрической связи для решения задач по созданию защищенных телекоммуникационных систем выполнять расчеты, связанные с выбором режимов работы определением оптимальных параметров радиооборудования и устройств цифрового тракта в составе СМС; анализировать статистические параметры трафика, проводить расчет интерфейсов внутренних направлений сети, изменять параметры коммутационной подсистемы, маршрутизации трафика, прописки кодов маршрутизации, анализировать статистику основных показателей эффективности радиосистем и систем передачи данных, выполнять расчет пропускной способности сетей радио и телекоммуникаций;
3.2.2	применять требования стандартов Единой системы конструкторской документации (ЕСКД) и Единой системы программной документации (ЕСПД), применять методы построения компьютерных моделей изделий;
3.2.3	разрабатывать и реализовывать на языке высокого уровня алгоритмы решения типовых профессиональных задач, работать с интегрированной средой разработки программного обеспечения;
3.2.4	проводить расчёты типовых аналоговых и цифровых узлов современной электронной аппаратуры, применять программные средства моделирования функциональных узлов современной электронной аппаратуры;
3.2.5	применять типовые программные средства сервисного назначения и пользоваться сетевыми средствами для обмена данными, в том числе с использованием глобальной информационной сети Интернет;
3.2.6	определять информационные характеристики системы передачи сообщений и каналов связи;
3.2.7	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; решать типовые комбинаторные и теоретико-графовые задачи; использовать язык и средства дискретной математики для решения профессиональных задач;
3.2.8	решать типовые задачи по следующим разделам курса физики: электростатика, электродинамика, постоянный и переменный ток,
3.2.9	электромагнитная индукция; применять физические законы и вычислительную технику для решения практических задач; работать с измерительными приборами; выполнять физический эксперимент, обрабатывать результаты измерений, строить графики проводить графический анализ опытных данных, использовать специализированные программные средства для моделирования режимов работы и исследования характеристик электрических цепей;
3.2.10	применять стандартные программные средства для решения профессиональных задач, применять на практике методы анализа электрических цепей; осуществлять синтез структурных и электрических схем электронных устройств; использовать стандартные методы и средства проектирования электронных узлов и устройств, в том числе для средств защиты информации;
3.2.11	модернизировать и адаптировать стандартные методы искусственного интеллекта с учетом современных тенденций развития электроники, измерительной и вычислительной техники и информационных технологий, строить модели искусственного интеллекта для решения проектных задач, декомпозировать задачи на подзадачи и решать их с помощью методов
3.2.12	искусственного интеллекта, интерпретировать полученные результаты;
3.2.13	применять методы теории поля, теории рядов, теории функций комплексного переменного для постановки и решения прикладных задач;
3.2.14	применять типовые программные средства сервисного назначения, информационного поиска и обмена данными в сети Интернет; составлять документы, используя прикладные программы офисного назначения; пользоваться средствами пользовательских интерфейсов операционных систем;
3.2.15	использовать функциональные возможности современных интегрированных сред разработки программного обеспечения на объектно-ориентированных языках программирования для разработки прикладных программ;использовать утилиты автоматической сборки и развертывания программ в операционных системах, разрабатывать алгоритмы и программы в рамках объектно-ориентированной парадигмы на современном языке программирования высокого уровня с применением основных синтаксических конструкций и функциональных возможностей стандартной библиотеки языка и фреймворка;строить и изучать математические модели конкретных явлений и процессов для решения расчетных и исследовательских задач;решать
3.2.16	основные задачи векторной алгебры и аналитической геометрии;решать основные задачи линейной алгебры, системы линейных
3.2.17	уравнений над полями;использовать методы аналитической геометрии и векторной алгебры в смежных дисциплинах и физике ;использовать методы линейной алгебры для решения прикладных задач;
3.2.18	исследовать функциональные зависимости, возникающие для решения стандартных прикладных задач;использовать типовые модели и методы математического анализа для решения стандартных прикладных задач;проводить типовые расчеты с использованием основных формул дифференциального и интегрального исчисления;пользоваться справочными материалами по математическому анализу;

3.2.19	применять стандартные вероятностные и статистические модели для решения типовых прикладных задач;пользоваться стандартными вероятностно-статистическими методами анализа экспериментальных данных;строить стандартные процедуры принятия решений на основе имеющихся экспериментальных данных;использовать расчетные формулы и таблицы для решения стандартных вероятностно-статистических задач, использовать стандартные вероятностно- статистические методы анализа
3.2.20	экспериментальных данных;
3.2.21	применять математические методы и вычислительную технику для решения практических задач;
3.3	**Владеть:**
3.3.1	анализа основных характеристик и возможностей телекоммуникационных систем по передаче информации; использования программно-аппаратных средств обеспечения информационной безопасности автоматизированных систем , проектирования сетей СМС различных стандартов и расчета их основных параметров в типовых ситуациях
3.3.2	функционирования, работой на коммутационном оборудовании по обеспечению реализации новых услуг, сопровождения геоинформационных баз данных по сети радиодоступа, информационной поддержки расчетов радиопокрытия, радиорелейных и спутниковых трасс и частотно- территориального планирования в части использования картографической информации;
3.3.3	разработки технической документации в соответствии с требованиями стандартов Единой системы конструкторской документации (ЕСКД) и Единой системы программной документации (ЕСПД), элементарных геометрических построений при помощи средств компьютерной графики; построения двухмерных и трехмерных (3D) изображений изделий;
3.3.4	работы с современной элементной базой электронной аппаратуры, моделирования узлов современной электронной аппаратуры;
3.3.5	организации, планирования, проведения и обработки результатов экспериментов и экспериментальных исследований; работы с измерительной аппаратурой, в том числе с цифровой измерительной техникой; обработки экспериментальных данных и оценки точности измерений, проектирования, моделирования и анализа характеристик электрических цепей с помощью специализированных программных средств;
3.3.6	использования современной измерительной аппаратуры при экспериментальном исследовании электронной аппаратуры, методами расчета типовых электронных устройств, навыками чтения принципиальных схем, навыками оценки быстродействия и оптимизации работы электронных схем на базе современной элементной базы;
3.3.7	разработки и модернизации методов искусственного интеллекта с учетом современных тенденций развития электроники, измерительной и вычислительной техники и информационных технологий, оформления технических заданий при решении задач с использованием методов искусственного интеллекта;
3.3.8	решения задач, относящихся к теории поля, теории рядов и теории функций комплексного переменного; применения изучаемого математического аппарата для решения прикладных задач;
3.3.9	работы с основными современными интегрированными средами разработки программного обеспечения на объектно-ориентированных языках;разработки, отладки и развёртывания программного обеспечения в операционных системах семейства Windows и Linux;поиска и анализа возможностей современных интегрированных программных средств разработки прикладного
3.3.10	программного обеспечения, разработки алгоритмов и программ;отладки, поиска и устранения ошибок программного кода;оценки
3.3.11	сложности алгоритмов;использования возможностей стандартной библиотеки, сторонних библиотек программного кода и фреймворков;
3.3.12	применения методов математической логики и теории алгоритмов;

4. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

Код занятия	Наименование разделов и тем /вид занятия/	Семестр / Курс	Часов	Компетен-ции	Литература	Инте ракт.	Примечание
	Раздел 1. Введение. Основные понятия алгебры. Группы, кольца, поля.						
1.1	Группы. Примеры групп. Порядок элемента в группе. /Лек/	5	4	ОПК-2 ОПК-3	Л1.1 Л1.2Л2.1	0	
1.2	Поля. Характеристика поля. /Лек/	5	2	ОПК-2 ОПК-3	Л1.1 Л1.2Л2.1	0	
1.3	Кольца. Виды колец. Обратимые элементы кольца /Лек/	5	2	ОПК-2 ОПК-3	Л1.1 Л1.2Л2.1	0	
1.4	Группы. Порядок элемента в группе. Кольца. Обратимые элементы в кольцах вычетов и матричных кольцах. /Пр/	5	3	ОПК-2 ОПК-3	Л1.1 Л1.2Л2.1	1	

1.5	Контрольная работа по теме "Алгебраические структуры" /Пр/	5	1	ОПК-2 ОПК-3	Л1.1 Л1.2Л2.1	0	
1.6	Подготовка к практическим занятиям /Ср/	5	21	ОПК-2 ОПК-3	Л1.1 Л1.2Л2.1	0	
	Раздел 2. Алгебраические методы в криптологии. Поля Галуа и их основные свойства. Вычисления в полях Галуа						
2.1	Основная теорема о конечных полях. Алгоритм построения конечного поля. /Лек/	5	4	ОПК-2 ОПК-3	Л1.1 Л1.2Л2.1	0	
2.2	Строение мультипликативной группы конечного поля. Дискретный логарифм и логарифм Якоби. /Лек/	5	4	ОПК-2 ОПК-3	Л1.1 Л1.2Л2.1	0	
2.3	Построение конечного поля. Вычисления в конечных полях /Пр/	5	10	ОПК-2 ОПК-3	Л1.1 Л1.2Л2.1	1	
2.4	Контрольная работа по теме "Поля" /Пр/	5	10	ОПК-2 ОПК-3	Л1.1 Л1.2Л2.1	0	
	Раздел 3. Полиномиальные функции. Построение многочлена по точкам – аппроксимационная формула Лагранжа. Кратные корни и производные						
3.1	Кольцо многочленов. Неприводимость. Корни многочлена. Поле разложения. /Лек/	5	2	ОПК-2 ОПК-3	Л1.1 Л1.2Л2.1	0	
3.2	Порядок многочлена и его свойства. Примитивный многочлен. /Лек/	5	2	ОПК-2 ОПК-3	Л1.1 Л1.2Л2.1	0	
3.3	Неприводимость многочленов. Корни многочленов /Пр/	5	1	ОПК-2 ОПК-3	Л1.1 Л1.2Л2.1	0	
3.4	Контрольная работа по теме "Многочлены над конечными полями" /Пр/	5	1	ОПК-2 ОПК-3	Л1.1 Л1.2Л2.1	0	
	Раздел 4. Линейные рекуррентные последовательности над конечным кольцом и полем						
4.1	Линейные рекуррентные последовательности. Минимальный период. Характеристический многочлен и ассоциированная матрица. /Лек/	5	6	ОПК-2 ОПК-3	Л1.1 Л1.2Л2.1	0	
4.2	Линейные рекуррентные последовательности над конечными полями. /Пр/	5	2	ОПК-2 ОПК-3	Л1.1 Л1.2Л2.1	1	
4.3	Написание программ, реализующих алгебраические и теоретико-числовые алгоритмы /Ср/	5	22,75	ОПК-2 ОПК-3	Л1.1 Л1.2Л2.1	0	
	Раздел 5. Эллиптические кривые						
5.1	Определение эллиптической кривой. Классификация эллиптических кривых над различными полями.Сложение точек эллиптической кривой. Группа точек эллиптической кривой /Лек/	5	6	ОПК-2 ОПК-3	Л1.1 Л1.2Л2.1	0	
5.2	Вычисления в группе точек эллиптической кривой. Порядок группы точек эллиптической кривой. /Пр/	5	3	ОПК-2 ОПК-3	Л1.1 Л1.2Л2.1	1	
5.3	Контрольная работа по теме "Эллиптические кривые" /Пр/	5	1	ОПК-2 ОПК-3	Л1.1 Л1.2Л2.1	0	
5.4	Зачет /ИВКР/	5	0,25	ОПК-2 ОПК-3	Л1.1 Л1.2Л2.1	0	

5. ОЦЕНОЧНЫЕ СРЕДСТВА

5.1. Контрольные вопросы и задания

Тема 1: Группы. Примеры групп. Порядок элемента в группе
1. Что такое группа? Какие аксиомы определяют группу?
2. Приведите примеры групп (аддитивная, мультипликативная, симметрическая).
3. Что такое порядок группы и порядок элемента группы?
4. Как связаны порядок элемента и свойства циклических групп?
5. Как проверить, является ли множество с операцией группой?
Тема 2: Кольца. Виды колец. Обратимые элементы кольца
6. Что такое кольцо? Какие аксиомы определяют кольцо?
7. Чем отличается коммутативное кольцо от некоммутативного?
8. Что такое кольцо с единицей и без единицы?
9. Какие элементы называются обратимыми в кольце?
10. Что такое делители нуля и как они влияют на структуру кольца?
Тема 3: Поля. Характеристика поля
11. Что такое поле и как оно связано с кольцами?
12. Чем поле отличается от тела?
13. Какова характеристика поля и как она определяется?
14. Какие поля называются простыми?
15. Как строятся расширения полей?
Тема 4: Основная теорема о конечных полях. Алгоритм построения
16. Сформулируйте основную теорему о конечных полях.
17. Какие поля называются конечными?
18. Как определяется количество элементов в конечном поле?
19. Как построить конечное поле GF(p^n)?
20. Какие задачи решаются при построении конечного поля?
Тема 5: Мультипликативная группа конечного поля. Дискретный логарифм
21. Как устроена мультипликативная группа конечного поля?
22. Почему эта группа циклична?
23. Что такое первообразный элемент (генератор) поля?
24. Что такое дискретный логарифм и его роль в криптографии?
25. Как вычисляется логарифм Якоби и где он применяется?
Тема 6: Кольцо многочленов. Неприводимость. Корни многочлена
26. Что такое кольцо многочленов над полем?
27. Какие многочлены называются приводимыми и неприводимыми?
28. Как определить, является ли многочлен неприводимым?
29. Что такое корень многочлена и как его найти?
30. Как связаны корни многочлена и разложение на множители?
Тема 7: Поле разложения. Порядок многочлена. Примитивный многочлен
31. Что такое поле разложения многочлена?
32. Как строится поле разложения для заданного многочлена?
33. Что такое порядок многочлена?
34. Каковы свойства порядка многочлена?
35. Что такое примитивный многочлен и где он используется?
Тема 8: Линейные рекуррентные последовательности
36. Что такое линейная рекуррентная последовательность?
37. Как связаны рекуррентные последовательности и многочлены?
38. Что такое минимальный период последовательности?
39. Как определяется характеристический многочлен рекурренты?
40. Как строится ассоциированная матрица линейной рекурренты?
Тема 9: Эллиптические кривые. Классификация
41. Что такое эллиптическая кривая?
42. Как выглядит общее уравнение эллиптической кривой?
43. Как классифицируются эллиптические кривые над различными полями?
44. Что такое особенности кривых над вещественными числами, рациональными и конечными полями?
45. Какие требования предъявляются к кривым для использования в криптографии?
Тема 10: Арифметика точек эллиптической кривой
46. Как определяется операция сложения точек на эллиптической кривой?
47. Как складываются точки графически и аналитически?
48. Что такое точка на бесконечности и её роль?
49. Какие формулы используются для сложения и удвоения точек?
50. Какова структура группы точек эллиптической кривой?
Тема 11: Группа точек эллиптической кривой
51. Какова структура группы точек эллиптической кривой?
52. Как определяется порядок группы точек?
53. Что утверждает теорема Хассе?
54. Как связаны группа точек и дискретный логарифм на эллиптической кривой?
55. Как используется группа точек в криптографических протоколах?

5.2. Темы письменных работ

не предусмотрены

5.3. Оценочные средства

Рабочая программа "Математические основы криптографии" обеспечена оценочными средствами для проведения текущего контроля и промежуточной аттестации, включающими контрольные вопросы для проведения промежуточной аттестации, критерии оценивания учебной деятельности обучающихся по балльно-рейтинговой системе, примеры заданий для практических и лабораторных занятий, билеты для проведения промежуточной аттестации.
Все оценочные средства представлены в Приложении 1.

5.4. Перечень видов оценочных средств

Оценочные средства разработаны для всех видов учебной деятельности студента - лекций, практических занятий, самостоятельной работы и промежуточной аттестации. Оценочные средства представлены в виде:
- средства текущего контроля: проверочных работ по решению задач, дискуссии по теме;
- средств итогового контроля - промежуточной аттестации: экзамена в 5 семестре.

6. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

6.1. Рекомендуемая литература

6.1.1. Основная литература

	Авторы, составители	Заглавие	Издательство, год
Л1.1	Рацеев С. М.	Математические методы защиты информации: учебное пособие для вузов	Санкт-Петербург: Лань, 2023
Л1.2	Глухов М. М., Круглов И. А., Пичкур А. Б., Черемушкин А. В.	Введение в теоретико-числовые методы криптографии: учебное пособие для вузов	Санкт-Петербург: Лань, 2024

6.1.2. Дополнительная литература

	Авторы, составители	Заглавие	Издательство, год
Л2.1	Рацеев С. М.	Криптографические методы защиты информации и их основы. Лабораторный практикум: учебное пособие для вузов	Санкт-Петербург: Лань, 2025

6.3.1 Перечень программного обеспечения

6.3.1.1	Office Professional Plus 2019	
6.3.1.2	Windows 10	
6.3.1.3	МТС-Линк	Комплексная платформа для коммуникаций, обучения и совместной работы, разработанная с использованием современных технологий. Доступны десктопные и мобильные приложения для удобной работы с системой.

6.3.2 Перечень информационных справочных систем

6.3.2.1	База данных научных электронных журналов "eLibrary"
6.3.2.2	Электронно-библиотечная система "Лань" Доступ к коллекциям электронных изданий ЭБС "Издательство "Лань"
6.3.2.3	Электронно-библиотечная система «Книжный Дом Университета» ("БиблиоТех")

7. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

Аудитория	Назначение	Оснащение	Вид
1	Специализированная многофункциональная учебная аудитория № 1 для проведения учебных занятий лекционного и семинарского типов, групповых и индивидуальных консультаций, текущего контроля и промежуточной/ итоговой аттестации	Столы обучающихся; Стулья обучающихся; Письменный стол педагогического работника; Стул педагогического работника; Кафедра; Магнитно-маркерная доска; Мультимедийный проектор; Экран; Ноутбук с возможностью подключения к сети «Интернет» и обеспечением доступа к электронной информационно-образовательной среде	

3	Специализированная многофункциональная учебная аудитория № 3 для проведения учебных занятий семинарского типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной/ итоговой аттестации	Компьютерные столы обучающихся; Стулья обучающихся; Письменный стол педагогического работника; Стул педагогического работника; Стеллаж для учебно-методических материалов, в том числе учебно-наглядных пособий; Многофункциональное устройство (принтер, сканер, ксерокс); Интерактивная доска; Мультимедийный проектор; Ноутбуки с возможностью подключения к сети «Интернет» и обеспечением доступа к электронной информационно-образовательной среде	
5	Помещение № 5 для самостоятельной работы обучающихся	Письменный стол обучающегося; Стул обучающегося; Письменный стол обучающегося с ограниченными возможностями здоровья; Стул обучающегося с ограниченными возможностями здоровья; Ноутбук с возможностью подключения к сети «Интернет» и обеспечением доступа к электронной информационно-образовательной среде лицензиата; Моноблок (в том числе, клавиатура, мышь, наушники) с возможностью подключения к сети «Интернет» и обеспечением доступа к электронной информационно-образовательной среде	

Ауд. 8	Аудитория для научно-исследовательской работы обучающихся, курсового и дипломного проектирования № 8	Рабочие места на базе вычислительной техники с набором необходимых для проведения и оформления результатов исследований дополнительных аппаратных и/или программных средств; Письменный стол обучающегося; Стул обучающегося; Письменный стол обучающегося с ограниченными возможностями здоровья; Стул обучающегося с ограниченными возможностями здоровья; Ноутбук с возможностью подключения к сети «Интернет» и обеспечением доступа к электронной информационно-образовательной среде лицензиата; Моноблок (в том числе, клавиатура, мышь, наушники) с возможностью подключения к сети «Интернет» и обеспечением доступа к электронной информационно-образовательной среде; Многофункциональное устройство (принтер, сканер, ксерокс).	

8. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ (МОДУЛЯ)

Методические указания по изучению дисциплины "Математические основы криптографии" представлены в Приложении 2 и включают в себя:

1. Методические указания для обучающихся по организации учебной деятельности.
2. Методические указания по организации самостоятельной работы обучающихся.
3. Методические указания по организации процедуры оценивания знания, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций.