

ЮЖНО-УРАЛЬСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

УТВЕРЖДАЮ:
Руководитель направления



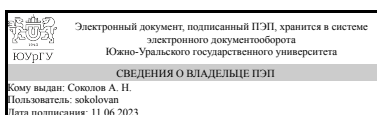
А. Н. Соколов

РАБОЧАЯ ПРОГРАММА

дисциплины 1.О.15 Математические основы криптологии
для направления 10.03.01 Информационная безопасность
уровень Бакалавриат
форма обучения очная
кафедра-разработчик Защита информации

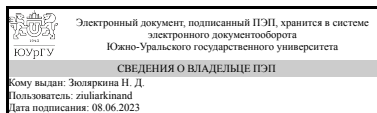
Рабочая программа составлена в соответствии с ФГОС ВО по направлению подготовки 10.03.01 Информационная безопасность, утверждённым приказом Минобрнауки от 17.11.2020 № 1427

Зав.кафедрой разработчика,
к.техн.н., доц.



А. Н. Соколов

Разработчик программы,
д.физ.-мат.н., доц., профессор



Н. Д. Зюляркина

1. Цели и задачи дисциплины

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

Краткое содержание дисциплины

В рамках данной дисциплины приводятся сведения из различных разделов алгебры и теории чисел, которые в дальнейшем используются в синтезе и анализе различных криптосистем.

2. Компетенции обучающегося, формируемые в результате освоения дисциплины

Планируемые результаты освоения ОП ВО (компетенции)	Планируемые результаты обучения по дисциплине
ОПК-2 Способен применять информационно-коммуникационные технологии, программные средства системного и прикладного назначения, в том числе отечественного производства, для решения задач профессиональной деятельности	Знает: характеристики программных разработок, позволяющих работать с алгебраическими структурами Умеет: производить вычисления с помощью пакета GAP и аналогичных программных комплексов Имеет практический опыт: программирования в пакете GAP
ОПК-3 Способен использовать необходимые математические методы для решения задач профессиональной деятельности	Знает: определения и свойства основных алгебраических структур: групп, колец и полей Умеет: производить вычисления в кольцах вычетов, матричных кольцах и в конечных полях Имеет практический опыт: работы с элементами групп, колец и полей

3. Место дисциплины в структуре ОП ВО

Перечень предшествующих дисциплин, видов работ учебного плана	Перечень последующих дисциплин, видов работ
1.О.10.01 Алгебра и геометрия, 1.О.13 Математическая логика и теория алгоритмов, ФД.04 Методы искусственного интеллекта, 1.О.25 Языки программирования, 1.О.10.02 Математический анализ, 1.О.12 Теория вероятностей и математическая статистика,	ФД.03 Технология подготовки выпускной квалификационной работы

1.О.24 Введение в графические системы общего и специализированного назначения, 1.О.14 Теория информации, 1.О.23 Информатика, 1.О.11 Дискретная математика, 1.О.26 Информационные технологии, 1.О.22 Схемотехника, 1.О.19 Электроника, 1.О.10.03 Специальные главы математики, 1.О.43 Объектно-ориентированное программирование, 1.О.17 Основы теории цепей и электротехника, 1.О.18 Сети и системы передачи информации	
--	--

Требования к «входным» знаниям, умениям, навыкам студента, необходимым при освоении данной дисциплины и приобретенным в результате освоения предшествующих дисциплин:

Дисциплина	Требования
1.О.23 Информатика	Знает: 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 Умеет: 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 Имеет практический опыт:
1.О.24 Введение в графические системы общего и специализированного назначения	Знает: элементы компьютерного дизайна и графического отображения объектов в виде чертежей или рисунков, основные положения стандартов Единой системы конструкторской документации (ЕСКД) и Единой системы программной документации (ЕСПД) Умеет: применять методы построения компьютерных моделей изделий, применять требования стандартов Единой системы конструкторской документации (ЕСКД) и Единой системы программной документации (ЕСПД) Имеет практический опыт: элементарных геометрических построений при помощи средств компьютерной графики; построения двумерных и трехмерных (3D) изображений изделий, разработки технической документации в соответствии с требованиями стандартов Единой системы конструкторской документации (ЕСКД) и Единой системы программной документации (ЕСПД)
ФД.04 Методы искусственного интеллекта	Знает: 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 Умеет: 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 искусственного интеллекта, интерпретировать полученные результаты Имеет практический опыт: 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
1.О.13 Математическая логика и теория алгоритмов	Знает: логику высказываний и предикатов; основы теории алгоритмов Умеет: применять математические методы и вычислительную технику для решения практических задач Имеет практический опыт: применения методов математической логики и теории алгоритмов
1.О.25 Языки программирования	Знает: 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 Умеет: разрабатывать и реализовывать на языке высокого уровня алгоритмы решения типовых профессиональных задач, работать с интегрированной средой разработки программного обеспечения Имеет практический опыт:
1.О.12 Теория вероятностей и математическая статистика	Знает: 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; стандартные методы получения точечных и интервальных оценок параметров вероятностных распределений; стандартные методы проверки статистических гипотез Умеет: пользоваться стандартными вероятностно-статистическими методами анализа

	экспериментальных данных, 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 Имеет практический опыт:
1.О.10.02 Математический анализ	Знает: 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;основные типы обыкновенных дифференциальных уравнений и методы их решения Умеет: 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 Имеет практический опыт:
1.О.10.01 Алгебра и геометрия	Знает: основные понятия и задачи векторной алгебры и аналитической геометрии;основные свойства алгебраических структур;основы линейной алгебры над произвольными полями Умеет: 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 Имеет практический опыт:
1.О.43 Объектно-ориентированное программирование	Знает: методы разработки алгоритмов и программ в рамках объектно-ориентированной парадигмы программирования на современном языке высокого уровня; принципы объектно-ориентированной парадигмы: абстрагирование, инкапсуляция, наследование,

	полиморфизм; основные синтаксические конструкции объектно-ориентированного языка программирования: классы, поля, свойства, методы, выражения, события; методы обобщенного программирования; методы оценки сложности алгоритмов; функциональные возможности стандартной библиотеки языка и фреймворка, 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 Умеет: 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, 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 Имеет практический опыт: разработки алгоритмов и программ; отладки, поиска и устранения ошибок программного кода; оценки сложности алгоритмов; использования возможностей стандартной библиотеки, сторонних библиотек программного кода и фреймворков, работы с основными современными интегрированными средами разработки программного обеспечения на объектно-ориентированных языках; разработки, отладки и развертывания программного обеспечения в операционных системах семейства Windows и Linux; поиска и анализа возможностей современных интегрированных программных средств разработки прикладного программного обеспечения
1.О.10.03 Специальные главы математики	Знает: основные понятия, составляющие предмет теории поля, его дифференциальные и интегральные характеристики; основные понятия теории рядов; основные понятия и методы теории функций комплексного переменного Умеет: применять методы теории поля, теории рядов, теории функций комплексного переменного для постановки и решения прикладных задач Имеет практический

	опыт: решения задач, относящихся к теории поля, теории рядов и теории функций комплексного переменного; применения изучаемого математического аппарата для решения прикладных задач
1.О.26 Информационные технологии	Знает: типовые структуры и принципы организации компьютерных сетей назначение, функции и обобщённую структуру операционных систем назначение и основные компоненты систем баз данных Умеет: применять типовые программные средства сервисного назначения и пользоваться сетевыми средствами для обмена данными, в том числе с использованием глобальной информационной сети Интернет Имеет практический опыт:
1.О.18 Сети и системы передачи информации	Знает: 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 Умеет: 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 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 Имеет практический опыт: 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 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
1.О.11 Дискретная математика	Знает: 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 Умеет: 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 Имеет практический опыт:
1.О.14 Теория информации	Знает: основные понятия и определения теории информации Умеет: определять информационные характеристики системы передачи сообщений и каналов связи Имеет практический опыт:
1.О.17 Основы теории цепей и электротехника	Знает: специализированные программные средства для моделирования режимов работы и исследования характеристик электрических цепей, 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 средства измерения физических величин; методы обработки экспериментальных данных Умеет: использовать специализированные программные средства для моделирования режимов работы и исследования характеристик электрических цепей, решать типовые задачи по следующим разделам курса физики: электростатика, электродинамика, постоянный и переменный ток, электромагнитная индукция; применять физические законы и вычислительную технику для решения практических задач; работать с измерительными приборами; выполнять физический эксперимент, обрабатывать

	результаты измерений, строить графики и проводить графический анализ опытных данных Имеет практический опыт: проектирования, моделирования и анализа характеристик электрических цепей с помощью специализированных программных средств, 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
1.О.22 Схемотехника	Знает: основы схемотехники современной радиоэлектронной аппаратуры, типовые схемотехнические решения основных узлов и блоков электронной аппаратуры Умеет: 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, применять стандартные программные средства для решения профессиональных задач Имеет практический опыт: методами расчета типовых электронных устройств, навыками чтения принципиальных схем, навыками оценки быстродействия и оптимизации работы электронных схем на базе современной элементной базы, использования современной измерительной аппаратуры при экспериментальном исследовании электронной аппаратуры
1.О.19 Электроника	Знает: 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 Умеет: применять программные средства моделирования функциональных узлов современной электронной аппаратуры, проводить расчёты типовых аналоговых и цифровых узлов современной электронной аппаратуры Имеет практический опыт: моделирования узлов современной электронной аппаратуры, работы с современной элементной базой электронной аппаратуры

4. Объём и виды учебной работы

Общая трудоемкость дисциплины составляет 3 з.е., 108 ч., 54,25 ч.
контактной работы

Вид учебной работы	Всего часов	Распределение по семестрам в часах
		Номер семестра
		6
Общая трудоёмкость дисциплины	108	108
<i>Аудиторные занятия:</i>	48	48
Лекции (Л)	32	32
Практические занятия, семинары и (или) другие виды аудиторных занятий (ПЗ)	16	16
Лабораторные работы (ЛР)	0	0
<i>Самостоятельная работа (СРС)</i>	53,75	53,75
Подготовка к практическим занятиям	40	40
Написание программ, реализующих алгебраические и теоретико-числовые алгоритмы	13,75	13.75
Консультации и промежуточная аттестация	6,25	6,25
Вид контроля (зачет, диф.зачет, экзамен)	-	зачет

5. Содержание дисциплины

№ раздела	Наименование разделов дисциплины	Объем аудиторных занятий по видам в часах			
		Всего	Л	ПЗ	ЛР
1	Введение. Основные понятия алгебры. Группы, кольца, поля.	12	8	4	0
2	Алгебраические методы в криптологии. Поля Галуа и их основные свойства. Вычисления в полях Галуа	12	8	4	0
3	Полиномиальные функции. Построение многочлена по точкам – аппроксимационная формула Лагранжа. Кратные корни и производные	6	4	2	0
4	Линейные рекуррентные последовательности над конечным кольцом и полем	8	6	2	0
5	Эллиптические кривые	10	6	4	0

5.1. Лекции

№ лекции	№ раздела	Наименование или краткое содержание лекционного занятия	Кол-во часов
1	1	Группы. Примеры групп. Порядок элемента в группе.	4
3	1	Поля. Характеристика поля.	2
4	1	Кольца. Виды колец. Обратимые элементы кольца	2
4	2	Основная теорема о конечных полях. Алгоритм построения конечного поля.	4
5	2	Строение мультипликативной группы конечного поля. Дискретный логарифм и логарифм Якоби.	4
6	3	Кольцо многочленов. Неприводимость. Корни многочлена. Поле разложения.	2
7	3	Порядок многочлена и его свойства. Примитивный многочлен.	2
8	4	Линейные рекуррентные последовательности. Минимальный период. Характеристический многочлен и ассоциированная матрица.	6

9	5	Определение эллиптической кривой. Классификация эллиптических кривых над различными полями. Сложение точек эллиптической кривой. Группа точек эллиптической кривой	6
---	---	--	---

5.2. Практические занятия, семинары

№ занятия	№ раздела	Наименование или краткое содержание практического занятия, семинара	Кол-во часов
1	1	Группы. Порядок элемента в группе. Кольца. Обратимые элементы в кольцах вычетов и матричных кольцах.	3
2	1	Контрольная работа по теме "Алгебраические структуры"	1
3	2	Построение конечного поля. Вычисления в конечных полях	2
4	2	Контрольная работа по теме "Поля"	2
5	3	Неприводимость многочленов. Корни многочленов	1
6	3	Контрольная работа по теме "Многочлены над конечными полями"	1
7	4	Линейные рекуррентные последовательности над конечными полями.	2
8,9	5	Вычисления в группе точек эллиптической кривой. Порядок группы точек эллиптической кривой.	3
10	5	Контрольная работа по теме "Эллиптические кривые"	1

5.3. Лабораторные работы

Не предусмотрены

5.4. Самостоятельная работа студента

Выполнение СРС			
Подвид СРС	Список литературы (с указанием разделов, глав, страниц) / ссылка на ресурс	Семестр	Кол-во часов
Подготовка к практическим занятиям	Глухов, М.М. Введение в теоретико-числовые методы криптографии. [Электронный ресурс] / М.М. Глухов, И.А. Круглов, А.Б. Пичкур, А.В. Черемушкин. — Электрон. дан. — СПб. : Лань, 2011. — 400 с. — Режим доступа: http://e.lanbook.com/book/68466 — Загл. с экрана. Глухов, М.М. Элементы теории обыкновенных представлений и характеров конечных групп с приложениями в криптографии. [Электронный ресурс] / М.М. Глухов, И.А. Круглов. — Электрон. дан. — СПб. : Лань, 2015. — 176 с. — Режим доступа: http://e.lanbook.com/book/65044 — Загл. с экрана.	6	40
Написание программ, реализующих алгебраические и теоретико-числовые алгоритмы	Глухов, М.М. Введение в теоретико-числовые методы криптографии. [Электронный ресурс] / М.М. Глухов, И.А. Круглов, А.Б. Пичкур, А.В. Черемушкин. — Электрон. дан. — СПб. : Лань, 2011. — 400 с. — Режим доступа:	6	13,75

	http://e.lanbook.com/book/68466 — Загл. с экрана. Глухов, М.М. Элементы теории обыкновенных представлений и характеров конечных групп с приложениями в криптографии. [Электронный ресурс] / М.М. Глухов, И.А. Круглов. — Электрон. дан. — СПб. : Лань, 2015. — 176 с. — Режим доступа: http://e.lanbook.com/book/65044 — Загл. с экрана.		
--	--	--	--

6. Фонд оценочных средств для проведения текущего контроля успеваемости, промежуточной аттестации

Контроль качества освоения образовательной программы осуществляется в соответствии с Положением о балльно-рейтинговой системе оценивания результатов учебной деятельности обучающихся.

6.1. Контрольные мероприятия (КМ)

№ КМ	Семестр	Вид контроля	Название контрольного мероприятия	Вес	Макс. балл	Порядок начисления баллов	Учитывается в ПА
1	6	Текущий контроль	Контрольная работа "Группы"	1	15	15 баллов - задача решена правильно 10-14 баллов - в решение есть неточности и незначительные ошибки 6-9 баллов - общий ход решения верен, но имеются серьёзные недочёты 3-5 баллов - в решении присутствует ряд серьёзных ошибок 1-2 балла - есть некоторый намёк на решение 0 баллов - задача не решалась	зачет
2	6	Текущий контроль	Контрольная работа "Кольца"	1	15	15 баллов - задача решена правильно 10-14 баллов - в решение есть неточности и незначительные ошибки 6-9 баллов - общий ход решения верен, но имеются серьёзные недочёты 3-5 баллов - в решении присутствует ряд серьёзных ошибок 1-2 балла - есть некоторый намёк на решение 0 баллов - задача не решалась	зачет
3	6	Текущий контроль	Контрольная работа "Поля"	1	15	15 баллов - задача решена правильно 10-14 баллов - в решение есть неточности и незначительные ошибки 6-9 баллов - общий ход решения верен, но имеются серьёзные недочёты 3-5 баллов - в решении присутствует ряд серьёзных ошибок 1-2 балла - есть некоторый намёк на решение	зачет

						0 баллов - задача не решалась	
4	6	Текущий контроль	Контрольная работа "Элементы теории чисел"	1	5	15 баллов - задача решена правильно 5 баллов - в решение есть неточности и незначительные ошибки 4 балла - общий ход решения верен, но имеются серьёзные недочёты 3 балла - в решении присутствует ряд серьёзных ошибок 1-2 балла - есть некоторый намёк на решение 0 баллов - задача не решалась	зачет
5	6	Текущий контроль	Конспект лекций	1	10	10 баллов - конспект представлен в полном объёме 6-9 баллов - имеется около 3/4 от всего объёма лекций 1-5 баллов - имеется 1/2 от всего объёма лекций 0 баллов - имеется менее половины объёма всех лекций	зачет
6	6	Промежуточная аттестация	Зачёт	-	40	40 баллов - задача решена правильно 30-39 баллов - в решение есть неточности и незначительные ошибки 20-29 баллов - общий ход решения верен, но имеются серьёзные недочёты 10-19 балла - в решении присутствует ряд серьёзных ошибок 1-9 балл - есть некоторый намёк на решение 0 баллов - задача не решалась	зачет

6.2. Процедура проведения, критерии оценивания

Вид промежуточной аттестации	Процедура проведения	Критерии оценивания
зачет	При оценивании результата мероприятия используется балльно-рейтинговая система оценивания результатов учебной деятельности обучающихся (утверждена приказом ректора от 24.05.19 N 179). На зачёте происходит оценивание учебной деятельности на основе оценок за мероприятия текущего контроля. Студент может улучшить свой рейтинг пройдя мероприятие текущей аттестации, которое не является обязательным.	В соответствии с пп. 2.5, 2.6 Положения

6.3. Паспорт фонда оценочных средств

Компетенции	Результаты обучения	№ КМ					
		1	2	3	4	5	6
ОПК-2	Знает: характеристики программных разработок, позволяющих работать с алгебраическими структурами	+	+	+	+		+
ОПК-2	Умеет: производить вычисления с помощью пакета GAP и аналогичных программных комплексов	+	+	+	+		+
ОПК-2	Имеет практический опыт: программирования в пакете GAP	+	+	+	+		+
ОПК-3	Знает: определения и свойства основных алгебраических структур: групп,	+	+	+	+	+	+

	колец и полей								
ОПК-3	Умеет: производить вычисления в кольцах вычетов, матричных кольцах и в конечных полях	+	+	+					+
ОПК-3	Имеет практический опыт: работы с элементами групп, колец и полей	+	+	+					+

Типовые контрольные задания по каждому мероприятию находятся в приложениях.

7. Учебно-методическое и информационное обеспечение дисциплины

Печатная учебно-методическая документация

а) основная литература:

Не предусмотрена

б) дополнительная литература:

1. Ван-дер-Варден, Б. Л. Алгебра Б. Л. ван дер Варден; Пер. с нем. А. А. Бельский. - 3-е изд., стер. - СПб.: Лань, 2004. - 623 с.

в) отечественные и зарубежные журналы по дисциплине, имеющиеся в библиотеке:

Не предусмотрены

г) методические указания для студентов по освоению дисциплины:

1. Зюляркина Н. Д. Криптографические методы защиты информации. Методические указания по проведению практических занятий

из них: учебно-методическое обеспечение самостоятельной работы студента:

Электронная учебно-методическая документация

№	Вид литературы	Наименование ресурса в электронной форме	Библиографическое описание
1	Основная литература	Электронно-библиотечная система издательства Лань	Глухов, М.М. Введение в теоретико-числовые методы криптографии. [Электронный ресурс] / М.М. Глухов, И.А. Круглов, А.Б. Пичкур, А.В. Черемушкин. — Электрон. дан. — СПб. : Лань, 2011. — 400 с. — Режим доступа: http://e.lanbook.com/book/68466 — Загл. с экрана.
2	Дополнительная литература	Электронно-библиотечная система издательства Лань	Глухов, М.М. Элементы теории обыкновенных представлений и характеров конечных групп с приложениями в криптографии. [Электронный ресурс] / М.М. Глухов, И.А. Круглов. — Электрон. дан. — СПб. : Лань, 2015. — 176 с. — Режим доступа: http://e.lanbook.com/book/65044 — Загл. с экрана.

Перечень используемого программного обеспечения:

Нет

Перечень используемых профессиональных баз данных и информационных справочных систем:

Нет

8. Материально-техническое обеспечение дисциплины

Вид занятий	№ ауд.	Основное оборудование, стенды, макеты, компьютерная техника, предустановленное программное обеспечение, используемое для различных видов занятий
Практические занятия и семинары	913 (36)	Комплект компьютерного оборудования; Локальная вычислительная сеть; Коммутатор, Программное обеспечение: ОС Windows XP , MS Office 2007, Matlab, WinRar, Mozilla Firefox, Консультант+; Локальные СЗИ: Secret Net 6.5 (автономный вариант), Страж 3.0; Межсетевые экраны: ViPNet Custom 3.1, User Gate 5.2
Лекции	912 (36)	Комплект компьютерного оборудования, LCD Проектор, Экран проекционный, настенные стенды по защите информации (5 шт.), программное обеспечение: ОС Windows XP , MS Office 2007, Matlab, WinRar, Mozilla Firefox, Консультант+.