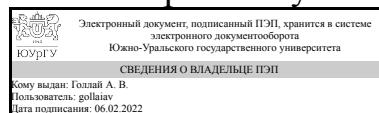


# ЮЖНО-УРАЛЬСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

УТВЕРЖДАЮ:  
Директор института  
Высшая школа электроники и  
компьютерных наук



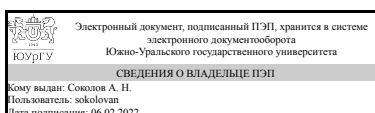
А. В. Голлай

## РАБОЧАЯ ПРОГРАММА

**дисциплины** 1.О.14 Математические основы криптологии  
**для направления** 10.03.01 Информационная безопасность  
**уровень** Бакалавриат  
**форма обучения** очная  
**кафедра-разработчик** Защита информации

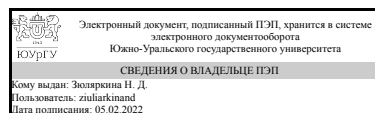
Рабочая программа составлена в соответствии с ФГОС ВО по направлению подготовки 10.03.01 Информационная безопасность, утверждённым приказом Минобрнауки от 17.11.2020 № 1427

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



А. Н. Соколов

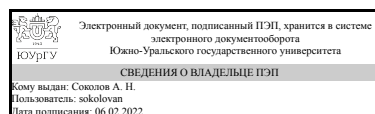
Разработчик программы,  
д.физ.-мат.н., доц., профессор



Н. Д. Зюляркина

СОГЛАСОВАНО

Руководитель направления  
к.техн.н., доц.



А. Н. Соколов

## 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<br>Умеет: производить вычисления с помощью пакета GAP и аналогичных программных комплексов<br>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<br>Умеет: производить вычисления в кольцах вычетов, матричных кольцах и в конечных полях<br>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.09.02 Математический анализ,<br>1.О.23 Введение в графические системы общего и специализированного назначения,<br>1.О.25 Информационные технологии,<br>1.О.12 Математическая логика и теория алгоритмов,<br>1.О.22 Информатика,<br>1.О.11 Теория вероятностей и математическая | ФД.03 Технология подготовки выпускной квалификационной работы |

|                                                                                                                                                                                                                                                                                                                                      |  |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--|
| статистика,<br>1.О.18 Электроника,<br>1.О.17 Сети и системы передачи информации,<br>1.О.24 Языки программирования,<br>1.О.16 Основы теории цепей и электротехника,<br>1.О.10 Дискретная математика,<br>1.О.09.03 Специальные главы математики,<br>1.О.21 Схемотехника,<br>1.О.13 Теория информации,<br>1.О.09.01 Алгебра и геометрия |  |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--|

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

| Дисциплина                                  | Требования                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|---------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1.О.16 Основы теории цепей и электротехника | <p>Знает: 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, специализированные программные средства для моделирования режимов работы и исследования характеристик электрических цепей Умеет: 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, использовать специализированные программные средства для моделирования режимов работы и исследования характеристик электрических цепей Имеет практический опыт: организации, планирования, проведения и обработки результатов экспериментов и экспериментальных исследований; работы с измерительной аппаратурой, в том числе с цифровой</p> |

|                               |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|-------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                               | измерительной техникой; обработки экспериментальных данных и оценки точности измерений, проектирования, моделирования и анализа характеристик электрических цепей с помощью специализированных программных средств                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| 1.О.24 Языки программирования | Знает: общие принципы построения, области и особенности применения языков программирования высокого уровня; язык программирования высокого уровня (объектно-ориентированное программирование), общие принципы построения, области и особенности применения языков программирования высокого уровня; язык программирования высокого уровня (объектно-ориентированное программирование)<br>Умеет: умеет работать с интегрированной средой разработки программного обеспечения; умеет разрабатывать и реализовывать на языке высокого уровня алгоритмы решения типовых профессиональных задач, работать с интегрированной средой разработки программного обеспечения; разрабатывать и реализовывать на языке высокого уровня алгоритмы решения типовых профессиональных задач<br>Имеет практический опыт: |
| 1.О.13 Теория информации      | Знает: основные понятия и определения теории информации<br>Умеет: определять информационные характеристики системы передачи сообщений и каналов связи<br>Имеет практический опыт:                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| 1.О.09.01 Алгебра и геометрия | Знает: основные понятия и задачи векторной алгебры и аналитической геометрии; основные свойства алгебраических структур; основы линейной алгебры над произвольными полями<br>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<br>Имеет практический опыт:                                                                                                                                          |
| 1.О.18 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<br>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                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| 1.О.21 Схемотехника             | <p>Знает: типовые схемотехнические решения основных узлов и блоков электронной аппаратуры, основы схемотехники современной радиоэлектронной аппаратуры Умеет: 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</p> <p>Имеет практический опыт: 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</p>                                                                 |
| 1.О.09.02 Математический анализ | <p>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:</p> |
| 1.О.22 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.25 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.11 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.17 Сети и системы передачи информации              | Знает: методы коммутации и маршрутизации; основные телекоммуникационные протоколы, 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 Умеет: енять знания о системах электрической связи для решения задач по созданию защищенных телекоммуникационных систем выполнять                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |

|                                                  |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|--------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                                                  | <p>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, проводить анализ показателей качества сетей и систем связи; анализировать тенденции развития систем и сетей электросвязи, внедрения новых служб и услуг связи Имеет практический опыт: 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, анализа основных характеристик и возможностей телекоммуникационных систем по передаче информации; использования программно-аппаратных средств обеспечения информационной безопасности автоматизированных систем</p> |
| 1.О.12 Математическая логика и теория алгоритмов | <p>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</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| 1.О.10 Дискретная математика                     | <p>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</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |

|                                                                               |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|-------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                                                                               | математики для решения профессиональных задач Имеет практический опыт:                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| 1.О.23 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 двухмерных и трехмерных (3D) изображений изделий, разработки технической документации в соответствии с требованиями стандартов Единой системы конструкторской документации (ЕСКД) и Единой системы программной документации (ЕСПД) |
| 1.О.09.03 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                                                                                                                                                                                                                                           |

#### 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                                  |



|                                                                               |       |       |
|-------------------------------------------------------------------------------|-------|-------|
| Самостоятельная работа (СРС)                                                  | 53,75 | 53,75 |
| с применением дистанционных образовательных технологий                        | 0     |       |
| Написание программ, реализующих алгебраические и теоретико-числовые алгоритмы | 13,75 | 13.75 |
| Подготовка к практическим занятиям                                            | 40    | 40    |
| 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 |
| 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: <a href="http://e.lanbook.com/book/68466">http://e.lanbook.com/book/68466</a> — 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: <a href="http://e.lanbook.com/book/65044">http://e.lanbook.com/book/65044</a> — Загл. с экрана. | 6       | 13,75        |
| 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: <a href="http://e.lanbook.com/book/68466">http://e.lanbook.com/book/68466</a> — 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: <a href="http://e.lanbook.com/book/65044">http://e.lanbook.com/book/65044</a> — Загл. с экрана. | 6       | 40           |

### 6. Текущий контроль успеваемости, промежуточная аттестация

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 | Се-местр | 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<br>10-14 баллов - в решение есть неточности и незначительные ошибки<br>6-9 баллов - общий ход решения верен, но имеются серьёзные недочёты<br>3-5 баллов - в решении присутствует ряд серьёзных ошибок<br>1-2 балла - есть некоторый намёк на решение<br>0 баллов - задача не решалась | зачет            |
| 2    | 6        | Текущий контроль | Контрольная работа "Кольца"                | 1   | 15         | 15 баллов - задача решена правильно<br>10-14 баллов - в решение есть неточности и незначительные ошибки<br>6-9 баллов - общий ход решения верен, но имеются серьёзные недочёты<br>3-5 баллов - в решении присутствует ряд серьёзных ошибок<br>1-2 балла - есть некоторый намёк на решение<br>0 баллов - задача не решалась | зачет            |
| 3    | 6        | Текущий контроль | Контрольная работа "Поля"                  | 1   | 15         | 15 баллов - задача решена правильно<br>10-14 баллов - в решение есть неточности и незначительные ошибки<br>6-9 баллов - общий ход решения верен, но имеются серьёзные недочёты<br>3-5 баллов - в решении присутствует ряд серьёзных ошибок<br>1-2 балла - есть некоторый намёк на решение<br>0 баллов - задача не решалась | зачет            |
| 4    | 6        | Текущий контроль | Контрольная работа "Элементы теории чисел" | 1   | 5          | 15 баллов - задача решена правильно<br>5 баллов - в решение есть неточности и незначительные ошибки<br>4 балла - общий ход решения верен, но имеются серьёзные недочёты<br>3 балла - в решении присутствует ряд серьёзных ошибок<br>1-2 балла - есть некоторый намёк на решение<br>0 баллов - задача не решалась           | зачет            |
| 5    | 6        | Текущий контроль | Конспект лекций                            | 1   | 10         | 10 баллов - конспект представлен в полном объёме<br>6-9 баллов - имеется около 3/4 от всего объёма лекций                                                                                                                                                                                                                  | зачет            |

|   |   |                          |       |   |    |                                                                                                                                                                                                                                                                                                                              |       |
|---|---|--------------------------|-------|---|----|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------|
|   |   |                          |       |   |    | 1-5 баллов - имеется 1/2 от всего объёма лекций<br>0 баллов - имеется менее половины объёма всех лекций                                                                                                                                                                                                                      |       |
| 6 | 6 | Промежуточная аттестация | Зачёт | - | 40 | 40 баллов - задача решена правильно<br>30-39 баллов - в решение есть неточности и незначительные ошибки<br>20-29 баллов - общий ход решения верен, но имеются серьёзные недочёты<br>10-19 балла - в решении присутствует ряд серьёзных ошибок<br>1-9 балл - есть некоторый намёк на решение<br>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. Оценочные материалы

| Компетенции | Результаты обучения                                                                              | № KM |   |   |   |   |   |
|-------------|--------------------------------------------------------------------------------------------------|------|---|---|---|---|---|
|             |                                                                                                  | 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                                | +    | + | + |   |   | + |

Фонды оценочных средств по каждому контрольному 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: <a href="http://e.lanbook.com/book/68466">http://e.lanbook.com/book/68466</a> — 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: <a href="http://e.lanbook.com/book/65044">http://e.lanbook.com/book/65044</a> — 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                                                                                                                                                           |
|---------------------------------|-------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Лекции                          | 912<br>(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+.                                                                             |
| Практические занятия и семинары | 913<br>(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 |

