Аннотация к рабочей программе дисциплины «Элементы алгебры и теории чисел»

Цель преподавания дисциплины

Цель преподавания дисциплины – формирование у студентов основных представлений о важнейших разделах алгебры и теории чисел, а также подготовка студентов к использованию полученных знаний в методах и алгоритмах криптографии и криптологии.

Задачи изучения дисциплины

Задачи преподавания дисциплины – ознакомление студентов с рядом методов, свойств и утверждений алгебры и теории чисел, которые лежат в основе некоторых разделов криптографии и криптологии.

Выпускник по направлению подготовки должен овладеть основными понятиями и методами:

– аксиоматического задания алгебраических объектов: групп, колец и полей,;

– проверки соответствия данной структуры определенным требованиям;

– методами теории чисел;

– методами решения задач линейной алгебры;

– методами решения сравнений и систем сравнений в кольце целых чисел.

Компетенции, формируемые в результате освоения дисциплины

Способен применять соответствующий математический аппарат для решения профессиональных задач (ОПК-2);

Способен принимать участие в проведении экспериментальных исследований системы защиты информации (ПК-12).

Разделы дисциплины

Введение и предмет курса. Теорема деления с остатком. Делимость и её свойства. Простые числа. Каноническое представление целых чисел. НОД. Взаимно простые числа и их свойства. НОК. Свойства НОК, НОД. Сравнения и их свойства. Системы сравнений первой степени. Сравнения второй степени. Непрерывные дроби. Группы, кольца, поля. Их свойства. Элементы теории многочленов. Эллиптические кривые над полем. Точки эллиптической кривой и их свойства. Эллиптические кривые над конечными полями. Действия над точками эллиптической кривой.

МИНОБРНАУКИ РОССИИ
Юго-Западный государственный университет

УТВЕРЖДАЮ:
Декан факультета
фундаментальной и прикладной
(наименование ф-та полностью)
информатики
Т.А. Ширабакина
(подпись, инициалы, фамилия)
«01» 02 2017 г

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Элементы алгебры и теории чисел

направление подготовки (специальность) *10.03.01*
(шифр согласно ФГОС
Информационная безопасность
и наименование направление подготовки (специальности)

Безопасность автоматизированных систем
наименование профиля, специализации или магистерской программы

форма обучения *очная*
очная, очно-заочная, заочная

Курск – 2017

Рабочая программа составлена в соответствии с Федеральным государственным образовательным стандартом высшего образования направления подготовки 10.03.01 Информационная безопасность и на основании учебного плана направления подготовки 10.03.01 Информационная безопасность, одобренного Учёным советом университета, протокол № 5 «30» 01 2017 г.

Рабочая программа обсуждена и рекомендована к применению в учебном процессе для обучения студентов по направлению подготовки 10.03.01 Информационная безопасность на заседании кафедры информационной безопасности № 9 «01» 02 2017г.

Зав. кафедрой ИБ Таныгин М.О.

Разработчик программы
профессор кафедры ИБ Добрица В.П.

Согласовано:

Директор научной библиотеки Макаровская В.Г.

Рабочая программа пересмотрена, обсуждена и рекомендована к применению в образовательном процессе на основании учебного плана направления подготовки 10.03.01 Информационная безопасность, одобренного Ученым советом университета протокол № 5 «30» 01 2017г. на заседании кафедры информационной безопасности, 28.08.2017, 01

(наименование кафедры, дата, номер протокола)

Зав. кафедрой к.т.н., доцент Таныгин М.О.

Рабочая программа пересмотрена, обсуждена и рекомендована к применению в образовательном процессе на основании учебного плана направления подготовки 10.03.01 Информационная безопасность, одобренного Ученым советом университета протокол № 9 «26» 03 2018г. на заседании кафедры информационной безопасности, 22.06.2018, 12

(наименование кафедры, дата, номер протокола)

Зав. кафедрой к.т.н., доцент Таныгин М.О.

Рабочая программа пересмотрена, обсуждена и рекомендована к применению в образовательном процессе на основании учебного плана направления подготовки 10.03.01 Информационная безопасность, одобренного Ученым советом университета протокол № « » 20 г. на заседании кафедры информационной безопасности, 27.06.2019, 11

(наименование кафедры, дата, номер протокола)

Зав. кафедрой к.т.н., доцент Таныгин М.О.

Рабочая программа пересмотрена, обсуждена и рекомендована к применению в образовательном процессе на основании учебного плана направления подготовки 10.03.01 Информационная безопасность, одобренного Ученым советом университета протокол №7 «25» 02 2020г. на заседании кафедры информационной безопасности протокол № 1 «31» 08 2020г.

Зав. кафедрой _____

Рабочая программа пересмотрена, обсуждена и рекомендована к применению в образовательном процессе на основании учебного плана направления подготовки 10.03.01 Информационная безопасность, одобренного Ученым советом университета протокол №7 «25» 02 2020г. на заседании кафедры информационной безопасности протокол №11 «28» 06 2021г.

Зав. кафедрой _____

Рабочая программа пересмотрена, обсуждена и рекомендована к применению в образовательном процессе на основании учебного плана направления подготовки 10.03.01 Информационная безопасность, одобренного Ученым советом университета протокол №7 «25» 02 2020г. на заседании кафедры информационной безопасности протокол №11 «30» 06 2022г.

Зав. кафедрой _____

Рабочая программа пересмотрена, обсуждена и рекомендована к применению в образовательном процессе на основании учебного плана направления подготовки 10.03.01 Информационная безопасность, одобренного Ученым советом университета протокол №7 «25» 02 2020г. на заседании кафедры информационной безопасности протокол № 1 «30» 08 2023г.

Зав. кафедрой _____

1. Цель и задачи дисциплины. Перечень планируемых результатов обучения, соотнесённых с планируемыми результатами освоения образовательной программы

1.1. Цель дисциплины

Цель преподавания дисциплины – формирование у студентов основных представлений о важнейших разделах алгебры и теории чисел, а также подготовка студентов к использованию полученных знаний в методах и алгоритмах криптографии и криптологии.

1.2. Задачи дисциплины

Задачи преподавания дисциплины – ознакомление студентов с рядом методов, свойств и утверждений алгебры и теории чисел, которые лежат в основе некоторых разделов криптографии и криптологии.

Выпускник по направлению подготовки должен овладеть основными понятиями и методами:

- аксиоматического задания алгебраических объектов: групп, колец и полей,
- проверки соответствия данной структуры определенным требованиям,
- методами теории чисел,
- методами решения задач линейной алгебры,
- методами решения сравнений и систем сравнений в кольце целых чисел.

1.3. Перечень планируемых результатов обучения, соотнесённых с планируемыми результатами освоения образовательной программы

Студенты должны знать:

- основные определения и теоремы теории чисел;
- определения различных типов групп, колец о полей и их основные свойства;
- методы решения сравнений первой и второй степени, а также систем сравнений первой степени;
- методы дискретного логарифмирования показательных и степенных сравнений;
- основные операции над точками эллиптических кривых;
- аппарат линейной алгебры.

уметь:

- пользоваться учебной и научной литературой;
- применять полученные знания к исследованию задач по защите информации;
- решать основные задачи криптографии;
- строить формальные алгоритмы для построения криптосистем;
- применять полученные знания в процессе изучения других дисциплин и т.д.

владеть навыками:

- проверки простоты числа, нахождения наибольшего общего делителя, наименьшего общего кратного, нахождения канонического разложения числа;
- построения конечных полей, отличных от полей типа полей Галуа;
- решения сравнений первой и второй степени, а также систем сравнений первой степени;
- решения задач линейной алгебры;
- применения стандартных методов и алгоритмов к решению прикладных задач.

Процесс изучения дисциплины направлен на формирование следующих компетенций:

ОПК-2: способностью применять соответствующий математический аппарат для решения профессиональных задач;

ПК-12: способностью принимать участие в проведении экспериментальных исследований системы защиты информации.

2. Указание места дисциплины в структуре образовательной программы

Курс «Элементы алгебра и теория чисел» относится к дисциплинам по выбору вариативной части учебного плана (Б1.В.ВД.5.1). Дисциплина изучается на 1 курсе во 2 семестре.

3. Объем дисциплины в зачетных единицах с указанием количества академических или астрономических часов, выделенных на контактную работу обучающихся с преподавателем (по видам учебных занятий) и на самостоятельную работу обучающихся

Общая трудоёмкость (объём) дисциплины составляет 2 зачётных единицы, 72 - часа.

Таблица 3.1 - Объем дисциплины

Общая трудоемкость дисциплины	72
Контактная работа обучающихся с преподавателем (по видам учебных занятий) (всего)	36,1
лекции	18
лабораторные занятия	Не предусмотрено
практические занятия	18
экзамен	Не предусмотрено
зачет	0,1
курсовая работа (проект)	Не предусмотрено
расчетно-графическая (контрольная) работа	Не предусмотрено
Аудиторная работа (всего):	36
в том числе:	
лекции	18
лабораторные занятия	Не предусмотрено

практические занятия	18
Самостоятельная работа обучающихся (всего)	35,9
Контроль/экз (подготовка к экзамену)	0

4. Содержание дисциплины, структурированное по темам (разделам) с указанием отведенного на них количества академических часов и видов учебных занятий

4.1. Содержание дисциплины

Таблица 4.1. – Содержание дисциплины, структурированное по темам (разделам)

№ п/п	Раздел (тема) дисциплины	Содержание
1.	Введение и предмет курса.	Задачи и программа курса. О применение методов алгебры и теории чисел в криптографии. Литература по курсу. Самостоятельная работа студентов. Связь с другими дисциплинами.
2.	Теорема деления с остатком. Делимость и её свойства. Простые числа.	Теорема деления целых чисел с остатком. Делимость целых чисел и её свойства. Простые и составные числа. Теорема Евклида о бесконечности множества простых чисел. Решето Эратосфена.
3.	Каноническое представление целых чисел. НОД.	Каноническое представление целого числа. Критерий делимости на языке канонического разложения. Число натуральных делителей целого числа. Сумма натуральных делителей целого числа. Наибольший общий делитель целых чисел. Свойства НОД. Алгоритм Евклида нахождения НОД. Теорема о линейном представлении НОД.
4.	Взаимно простые числа и их свойства. НОК. Свойства НОК, НОД.	Взаимно простые числа и их свойства. Наименьшее общее кратное целых чисел и его свойства. Представление о распределении простых чисел. Простые числа в арифметических последовательностях. Проблема «близнецов».
5.	Сравнения и их свойства. Системы сравнений первой степени.	Сравнения и их свойства. Классы вычетов и их свойства. Функция Эйлера и её свойства. Малая теорема Ферма. Теорема Эйлера. Мультипликативно обратные по модулю элементы. Сравнения первой степени и способы их решения. Система сравнений первой степени. Китайская теорема об остатках. Первообразные корни. Дискретные логарифмы. Решение показательных и степенных сравнений.

6.	Сравнения второй степени. Непрерывные дроби.	Сравнения второй степени. Символы Лежандра и Якоби и их свойства. Квадратичные вычеты и невычеты и их свойства. Непрерывные (цепные) дроби. Разложение рационального числа в цепную дробь. Подходящие дроби и их свойства. Подходящие дроби в качестве наилучших приближений действительных чисел и их свойства.
7.	Группы, кольца, поля. Их свойства.	Группы и подгруппы. Циклические группы и подгруппы. Таблицы Кэли. Группы перестановок. Теорема Кэли. Действие группы на множестве. Транзитивные группы. Кольца и их свойства. Область целостности. Поле и его свойства. Идеалы кольца. Характеристика кольца. Центр кольца. Фактор-кольца. Гомоморфизм колец и его свойства. Евклидовы кольца и их свойства.
8.	Элементы теории многочленов.	Конечные расширения полей и их свойства. Алгебраические и трансцендентные элементы. Поле разложения многочлена и его свойства. Поля Галуа (конечные поля). Порядки неприводимых многочленов. Линейные рекуррентные последовательности. Схема Горнера. Теорема Виета. Деление многочленов над полем.
9.	Эллиптические кривые над полем. Точки эллиптической кривой и их свойства.	Эллиптические кривые над полем. Уравнение Вейерштрасса. Алгебраически замкнутое поле. Алгебраическое замыкание поля. Теорема Штейница. Аффинные, *F*-рациональные и точки эллиптической кривой. Невырожденная (гладкая) эллиптическая кривая. Дискриминант и *j*-инвариант эллиптической кривой. Изоморфизм эллиптических кривых.
10.	Эллиптические кривые над конечными полями. Действия над точками эллиптической кривой.	Проективная плоскость. Проективная точка. Бесконечно удалённая точка. Теорема Виета для кубического уравнения. Сложение точек на эллиптической кривой, его геометрический смысл. Эллиптические кривые над конечными полями. ζ – функция эллиптической кривой над полем Галуа. Теорема Хассе. Теорема Ленстры.

Таблица 4.2 – Содержание дисциплины и его методическое обеспечение

№ п/п	Раздел учебной дисциплины	Виды учебной деятельности (в часах)			Учебно-методические материалы	Формы текущего контроля успеваемости *(по неделям семестра)*	Компетенции
		лек	№ лаб	№ пр.			

						Форма промежуточной аттестации *(по семестрам)*	
1	2	3	4	5	6	7	8
1	Введение и предмет курса.	2	-	-	[1], [2], [3], [16], [18], [20]	С	ОПК – 2
2	Теорема деления с остатком. Делимость и её свойства. Простые числа.	2	-	1	[1], [2], [3], [16], [17]	КО Сдача заданий.	ОПК – 2; ПК-12
3	Каноническое представление целых чисел. НОД.	2	-	2	[1], [2], [3] [6], [13], [18]	КО Сдача заданий.	ОПК – 2; ПК-12
4	Взаимно простые числа и их свойства. НОК. Свойства НОК, НОД.	2	-	3	[1], [2], [5], [12], [16], [25]	КО Сдача заданий.	ОПК – 2; ПК-12
5	Сравнения и их свойства. Системы сравнений первой степени.	4	-	4	[1], [2], [3], [5], [11], [17]	КО Сдача заданий.	ОПК – 2; ПК-12
6	Сравнения второй степени. Непрерывные дроби.	4	-	5	[1], [12], [17], [28]	КО Сдача заданий.	ОПК – 2; ПК-12
7	Группы, кольца, поля. Их свойства.	4	-	6	[1], [12], [21], [26]	КО Сдача заданий.	ОПК – 2
8	Элементы теории многочленов.	4	-	7	[2], [4], [5], [11]	КО Сдача заданий.	ОПК – 2; ПК-12
9	Эллиптические кривые над полем. Точки эллиптической кривой и их свойства.	6	-	8	[2], [6], [10], [11]	КО Сдача заданий.	ОПК – 2; ПК-12
10	Эллиптические кривые над конечными полями. Действия над точками эллиптической кривой.	6	-	9	[2], [6], [10], [11]	КО Сдача заданий.	ОПК – 2; ПК-12
	Всего	36				З	

Э– экзамен, КР – курсовая работа; КП – курсовой проект, К – контрольная работа, З – зачет, С – собеседование, СР – семестровая работа, Кл – коллоквиум, КО – контрольный опрос, МК – автоматизированный программированный контроль (машинный контроль).

4.2. Лабораторные работы и (или) практические занятия

Таблица 4.3 – Практические занятия

Номер занятия	Наименование практического (семинарского) занятия	Объем в часах
1	2	3
1	Теорема деления с остатком. Делимость и её свойства.	2
2	Каноническое представление целых чисел. НОД. Взаимно простые числа. НОК.	2
3	Сравнения и их свойства.	2
4	Системы сравнений первой степени. Сравнения второй степени.	2
5	Непрерывные дроби.	2
6	Группы, кольца, поля. Элементы теории многочленов.	2
7	Эллиптические кривые над полем. Точки эллиптической кривой и их свойства.	2
8-9	Эллиптические кривые над конечными полями. Действия над точками эллиптической кривой.	4
	Всего	18 часов

4.3 Самостоятельная работа студентов (СРС)

Таблица 4.34 – Самостоятельная работа студентов

№	Наименование раздела учебной дисциплины	Срок выполнения	Время, затрачиваемое на выполнение СРС, час.
1	2	3	4
1.	Введение и предмет курса.	1-2 неделя	4
2.	Теорема деления с остатком. Делимость и её свойства. Простые числа.	3-4 недели	6
3.	Каноническое представление целых чисел. НОД.	5-6 недели	6

4.	Взаимно простые числа и их свойства. НОК. Свойства НОК, НОД.	7-8 недели	8
5.	Сравнения и их свойства. Системы сравнений первой степени.	9-10 недели	6
6.	Сравнения второй степени. Непрерывные дроби.	11-12 недели	6
7.	Группы, кольца, поля. Их свойства.	13-14 недели	6
8.	Элементы теории многочленов.	15-16 недели	6
9.	Эллиптические кривые над полем. Точки эллиптической кривой и их свойства.	17-18 недели	6
Итого			54

5. Перечень учебно-методического обеспечения для самостоятельной работы обучающихся по дисциплине

Студенты могут при самостоятельном изучении отдельных тем и вопросов дисциплин пользоваться учебно-наглядными пособиями, учебным оборудованием и методическими разработками кафедры в рабочее время, установленное Правилами внутреннего распорядка работников.

Учебно-методическое обеспечение для самостоятельной работы обучающихся по данной дисциплине организуется:

библиотекой университета:

- библиотечный фонд укомплектован учебной, методической, научной, периодической, справочной и художественной литературой в соответствии с УП и данной РПД;
- имеется доступ к основным информационным образовательным ресурсам, информационной базе данных, в том числе библиографической, возможность выхода в Интернет.

кафедрой:

- путем обеспечения доступности всего необходимого учебно-методического и справочного материала;
- путем предоставления сведений о наличии учебно-методической литературы, современных программных средств;
- путем разработки:

– методических рекомендаций, пособий по организации самостоятельной

работы студентов;

– тем рефератов;
– вопросов к зачету;
–методических указаний к выполнению лабораторных работ и т.д.
типографией университета:
– помощь авторам в подготовке и издании научной, учебной и методической литературы;
- удовлетворение потребности в тиражировании научной, учебной и методической литературы.

6. Образовательные технологии

В соответствии с требованиями ФГОС и Приказа Министерства образования и науки РФ от 05 апреля 2017 г. №301 реализация компетентностного подхода предусматривает широкое использование в образовательном процессе активных и интерактивных форм проведения занятий в сочетании с внеаудиторной работой с целью формирования и развития профессиональных навыков студентов. Удельный вес занятий, проводимых в интерактивных формах, составляет 24.8% от аудиторных занятий согласно УП. Средствами промежуточного контроля успеваемости студентов являются защита лабораторных работ, опросы на практических занятиях по темам лекций.

Таблица 6.1 – Интерактивные образовательные технологии, используемые при проведении аудиторных занятий

№	Наименование раздела (лекции, практического или лабораторного занятия)	Используемые интерактивные образовательные технологии	Объем в часах
1	2	3	4
1	Введение в предмет «Элементы алгебры и теории чисел» (лекция)	Компьютерные симуляции. Презентация	2
2	Делимость, НОД, НОК (лекция, практика)	Разбор конкретных ситуаций. Таблицы, программы нахождения НОД, НОК, проверки простоты числа	6
3	Непрерывные дроби (лекция, практика)	Разбор конкретных ситуаций. Таблицы	4
4	Группы, кольца, поля (лекция, практика)	Разбор конкретных ситуаций. Таблицы: аксиомы, примеры.	6
Итого			18

7. Фонд оценочных средств для проведения промежуточной аттестации обучающихся по дисциплине

7.1. Перечень компетенций с указанием этапов их формирования в процессе освоения образовательной программы

Код и содержание компетенции	Этапы* формирования компетенций и дисциплины (модули), при изучении которых формируется данная компетенция		
	начальный	основной	завершающий
1	2	3	4
ОПК-2: способностью применять соответствующий математический аппарат для решения профессиональных задач.	Математика; Теория вероятностей и математическая статистика; Дискретная математика; Высшая математика (спецглавы); Математическая логика и теория алгоритмов; Элементы алгебры и теории чисел; Теория графов; Ознакомительная практика	Криптографические методы защиты информации; Методы оптимизации; Вычислительные методы	Теория Информации; Преддипломная Практика; Защита выпускной квалификационной работы, включая подготовку к процедуре защиты и процедуру защиты
ПК-12: способностью принимать участие в проведении экспериментальных исследований системы защиты информации.	Психология управления коллективом; Психология; Социология; Основы управленческой деятельности; Культурология; История мировой и отечественной культуры; Проектно-технологическая практика		Техническая защита информации; Защита выпускной квалификационной работы, включая подготовку к процедуре защиты и процедуру защиты

Средствами промежуточного контроля успеваемости студентов являются защита практических заданий, опросы на практических занятиях по темам лекций. В конце семестра – зачет.

ПРИМЕРНЫЙ ПЕРЕЧЕНЬ
КОНТРОЛЬННЫХ ВОПРОСОВ

1. Последовательность расширения понятия числа.
2. Различные подходы к изучению свойств чисел.
3. Теорема деления целых чисел с остатком.
4. Делимость чисел и её свойства.
5. Простые и составные числа. Свойства.
6. Решето Эратосфена.
7. Теорема Евклида о бесконечности множества простых чисел.
8. Каноническое представление целого числа.

7.2. Описание показателей и критериев оценивания компетенций на разных этапах их формирования, описание шкал оценивания

Наименование компетенции	Показатели оценивания компетенций	Уровень сформированности компетенции		
		Удовлетворительно	Хорошо	Отлично

ОПК-2: способностью применять соответствующий математический аппарат для решения профессиональных задач.	*1.Доля освоенных обучающимся знаний, умений, навыков от общего объема ЗУН, установленных в п.1.3 РПД* *2.Качество освоенных обучающимся знаний, умений, навыков* *3.Умение применять знания, умения,* навыки *в типовых и нестандартных ситуациях*	**Знать**: основные определения и теоремы теории чисел; определения различных типов групп, колец о полей и их основные свойства; методы решения сравнений первой и второй степени, а также систем сравнений первой степени. **Уметь:** пользоваться учебной и научной литературой; решать основные задачи криптографии; применять полученные знания в процессе изучения других дисциплин и т.д. **Владеть навыками:** проверки простоты числа, нахождения наибольшего общего делителя, наименьшего общего кратного, нахождения канонического разложения числа; построения конечных полей, отличных от полей типа полей Галуа; решения сравнений первой и второй степени, а также систем сравнений первой степени.	**Знать**: основные определения и теоремы теории чисел; определения различных типов групп, колец о полей и их основные свойства; методы решения сравнений первой и второй степени, а также систем сравнений первой степени; методы дискретного логарифмирования показательных и степенных сравнений; аппарат линейной алгебры. **Уметь:** пользоваться учебной и научной литературой; применять полученные знания к исследованию задач по защите информации; решать основные задачи криптографии; строить формальные алгоритмы для построения криптосистем; применять полученные знания в процессе изучения других дисциплин и т.д. **Владеть навыками:** проверки простоты числа, нахождения наибольшего общего делителя, наименьшего общего кратного,	**Знать**: основные определения и теоремы теории чисел; определения различных типов групп, колец о полей и их основные свойства; методы решения сравнений первой и второй степени, а также систем сравнений первой степени; методы дискретного логарифмирования показательных и степенных сравнений; основные операции над точками эллиптических кривых; аппарат линейной алгебры. **Уметь:** пользоваться учебной и научной литературой; применять полученные знания к исследованию задач по защите информации; решать основные задачи криптографии; строить формальные алгоритмы для построения криптосистем; применять полученные знания в процессе изучения других дисциплин и т.д. **Владеть навыками:** проверки простоты числа, нахождения наибольшего

			нахождения канонического разложения числа; построения конечных полей, отличных от полей типа полей Галуа; решения сравнений первой и второй степени, а также систем сравнений первой степени; применения стандартных методов и алгоритмов к решению прикладных задач.	общего делителя, наименьшего общего кратного, нахождения канонического разложения числа; построения конечных полей, отличных от полей типа полей Галуа; решения сравнений первой и второй степени, а также систем сравнений первой степени; решения задач линейной алгебры; применения стандартных методов и алгоритмов к решению прикладных задач.

ПК-12: способностью принимать участие в проведении экспериментальных исследований системы защиты информации.	*1.Доля освоенных обучающимся знаний, умений, навыков от общего объема ЗУН, установленных в п.1.3 РПД* *2.Качество освоенных обучающимся знаний, умений, навыков* *3.Умение применять знания, умения,* навыки *в типовых и нестандартных ситуациях*	**Знать**: основные определения и теоремы теории чисел; определения различных типов групп, колец о полей и их основные свойства; методы решения сравнений первой и второй степени, а также систем сравнений первой степени. **Уметь:** пользоваться учебной и научной литературой; решать основные задачи криптографии; применять полученные знания в процессе изучения других дисциплин и т.д. **Владеть навыками:** проверки простоты числа, нахождения наибольшего общего делителя, наименьшего общего кратного, нахождения канонического разложения числа; построения конечных полей, отличных от полей типа полей Галуа; решения сравнений первой и второй степени, а также систем сравнений первой степени.	**Знать**: основные определения и теоремы теории чисел; определения различных типов групп, колец о полей и их основные свойства; методы решения сравнений первой и второй степени, а также систем сравнений первой степени; методы дискретного логарифмирования показательных и степенных сравнений; аппарат линейной алгебры. **Уметь:** пользоваться учебной и научной литературой; применять полученные знания к исследованию задач по защите информации; решать основные задачи криптографии; строить формальные алгоритмы для построения криптосистем; применять полученные знания в процессе изучения других дисциплин и т.д. **Владеть навыками:** проверки простоты числа, нахождения наибольшего общего делителя, наименьшего общего кратного,	**Знать**: основные определения и теоремы теории чисел; определения различных типов групп, колец о полей и их основные свойства; методы решения сравнений первой и второй степени, а также систем сравнений первой степени; методы дискретного логарифмирования показательных и степенных сравнений; основные операции над точками эллиптических кривых; аппарат линейной алгебры. **Уметь:** пользоваться учебной и научной литературой; применять полученные знания к исследованию задач по защите информации; решать основные задачи криптографии; строить формальные алгоритмы для построения криптосистем; применять полученные знания в процессе изучения других дисциплин и т.д. **Владеть навыками:** проверки простоты числа, нахождения наибольшего

			нахождения канонического разложения числа; построения конечных полей, отличных от полей типа полей Галуа; решения сравнений первой и второй степени, а также систем сравнений первой степени; применения стандартных методов и алгоритмов к решению прикладных задач.	общего делителя, наименьшего общего кратного, нахождения канонического разложения числа; построения конечных полей, отличных от полей типа полей Галуа; решения сравнений первой и второй степени, а также систем сравнений первой степени; решения задач линейной алгебры; применения стандартных методов и алгоритмов к решению прикладных задач.

7.3. Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций в процессе освоения образовательной программы

Таблица 7.3 - Паспорт комплекта оценочных средств для текущего контроля

№ п/п	Раздел (тема) дисциплины	Код контроли-руемой компе-тенции (или её части)	Технология формирования	Оценочные средства		Описание шкал оценивания
				наимено-вание	№№ заданий	
1	2	3	4	5	6	7
1	Введение и предмет курса.	ОПК – 2	Лекция, СРС	С	1-2	Согласно табл. 7.2
2	Теорема деления с остатком. Делимость и её свойства. Простые числа.	ОПК – 2	Лекция, СРС, практические задания	С, КО Защита раб №1	3-8	Согласно табл. 7.2

3	Каноническое представление целых чисел. НОД.	ОПК – 2	Лекция, СРС, практические задания	С, КО Защита раб №2	9-15	Согласно табл. 7.2
4	Взаимно простые числа и их свойства. НОК. Свойства НОК, НОД.	ОПК – 2	Лекция, СРС, практические задания	С, КО Защита раб №3	16 - 20	Согласно табл. 7.2
5	Сравнения и их свойства. Системы сравнений первой степени.	ОПК – 2	Лекция, СРС, практические задания	С, КО Защита раб №4	21 - 31	Согласно табл. 7.2
6	Сравнения второй степени. Непрерывные дроби.	ОПК – 2	Лекция, СРС, практические задания	С, КО Защита раб №5	32 - 40	Согласно табл. 7.2
7	Группы, кольца, поля. Их свойства.	ОПК – 2	Лекция, СРС, практические задания	С, КО Защита раб №6	41-63	Согласно табл. 7.2
8	Элементы теории многочленов.	ОПК – 2	Лекция, СРС, практические задания	С, КО Защита раб №7	64 - 69	Согласно табл. 7.2
9	Эллиптические кривые над полем. Точки эллиптической кривой и их свойства.	ОПК – 2	Лекция, СРС, практические задания	С, КО Защита раб №8	70 - 79	Согласно табл. 7.2
10	Эллиптические кривые над конечными полями. Действия над точками эллиптической кривой.	ОПК – 2	Лекция, СРС, практические задания	С, КО Защита раб №9	80 - 86	Согласно табл. 7.2

7.4. Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций

Процедуры оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций, регулируются следующими нормативными актами университета:

- Положение П 02.016–2015 «О балльно-рейтинговой системе оценки качества освоения образовательных программ»;
- Методические указания, используемые в образовательном процессе, указанные в списке литературы.

Для *текущего контроля* по дисциплине в рамках действующей в университете балльно-рейтинговой системы применяется следующий порядок начисления баллов

Таблица 7.4 – Порядок начисления баллов в рамках БРС

Форма контроля	Минимальный балл		Максимальный балл	
	балл	примечание	балл	примечание
Выполнение лабораторной работы №1 «Теорема деления с остатком. Делимость и её свойства»	2	Выполнил, но «не защитил»	4	Выполнил и «защитил»
Выполнение лабораторной работы №2 «Каноническое представление целых чисел. НОД. Взаимно простые числа. НОК»	2	Выполнил, но «не защитил»	4	Выполнил и «защитил»
Выполнение лабораторной работы №3 «Сравнения и их свойства»	2	Выполнил, но «не защитил»	6	Выполнил и «защитил»
Выполнение лабораторной работы №4 «Системы сравнений первой степени. Сравнения второй степени»	2	Выполнил, но «не защитил»	4	Выполнил и «защитил»
Выполнение лабораторной работы №5 «Непрерывные дроби»	2	Выполнил, но «не защитил»	4	Выполнил и «защитил»
Выполнение лабораторной работы №6 «Группы, кольца, поля. Элементы теории многочленов»	2	Выполнил, но «не защитил»	6	Выполнил и «защитил»
Выполнение лабораторной работы №7 «Эллиптические кривые над полем. Точки эллиптической кривой и их свойства»	2	Выполнил, но «не защитил»	6	Выполнил и «защитил»

Выполнение лабораторной работы №8 «Эллиптические кривые над конечными полями»	2	Выполнил, но «не защитил»	6	Выполнил и «защитил»
Выполнение лабораторной работы №9 «Действия над точками эллиптической кривой»	2	Выполнил, но «не защитил»	6	Выполнил и «защитил»
Всего	18		48	
Посещаемость			16	
Сдача зачета			36	
ИТОГО	18		100	

Для промежуточной аттестации обучающихся, проводимой в виде тестирования, используется следующая методика оценивания знаний, умений, навыков и (или) опыта деятельности. В каждом варианте КИМ - 16 заданий (15 вопросов и одна задача).

Каждый верный ответ оценивается следующим образом:
- задание в закрытой форме –2балла,
- задание в открытой форме – 2 балла,
- задание на установление правильной последовательности – 2 балла,
- задание на установление соответствия – 2 балла,
- решение компетентностно-ориентированной задачи – 6 баллов.

Максимальное количество баллов за тестирование - 36 баллов.

8. Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины

8.1. Основная учебная литература

1 Виноградов, И. М. Основы теории чисел [Текст]: учебное пособие / И. М. Виноградов. - Изд. 12-е, стер. - СПб. [и др.]: Лань, 2009. - 176 с.

2 Иванов, Б. Н. Дискретная математика. Алгоритмы и программы [Текст]: расширенный курс / Б. Н. Иванов. - Москва: Известия, 2011. - 512 с.

3 Кнауб, Л.В. Теоретико-численные методы в криптографии [Электронный ресурс]: учебное пособие / Л.В. Кнауб, Е.А. Новиков, Ю.А. Шитов; Министерство образования и науки Российской Федерации, Сибирский Федеральный университет. - Красноярск: Сибирский федеральный университет, 2011. - 160 с. // Режим доступа - http://biblioclub.ru/index.php?page=book&id=229582

8.2. Дополнительная учебная литература

4 Кострикин, А. И. Введение в алгебру. Основы алгебры [Текст]: учебник для студ. ун-тов / А. И. Кострикин. - М.: Физматлит, 1994. - 320 с.

5 Кострикин, А. И. Введение в алгебру. Основы алгебры [Текст]: учебник для студ. ун-тов / А. И. Кострикин. - М.: Физматлит, 1994. - 320 с.

6 Милых, В. А. Дискретная математика [Электронный ресурс]: учебное пособие / Курск. гос. техн. ун-т; Министерство образования и науки Российской Федерации, Курский государственный технический университет. - Курск: КурскГТУ, 2006. - 139 с.

7 Милых, В. А. Дискретная математика [Текст]: учебное пособие / В. А. Милых, И. Г. Уразбахтин; Курский государственный технический университет, Гуманитарно-технический институт (г. Курск). - Курск: КурскГТУ, 2006. - 139 с.

8 Роджерс, Х. Теория рекурсивных функций и эффективная вычислимость [Текст] / пер. с англ. В. А. Душского; под ред. В. А. Успенского. - Москва: Мир, 1972. - 624 с.

9 Панкратова, В. Г. Теория чисел [Текст]: конспект лекций / Калининский гос. ун-т. - Вып. 3. - Калинин: [б. и.], 1972. - 58 с.

10 Зуланке Р. Алгебра и геометрия [Текст]: учебник / Р. Зуланке; А. Л. Онищик. - М.: МЦНМО, 2008 - . Т. 2: Модули и алгебры. - 336 с.

11 Биркгоф, Гаррет. Современная прикладная алгебра [Текст] / пер. с англ. Ю. И. Манина. - М.: Мир, 1976. - 400 с.

8.3. Перечень методических указаний

1. Алферова, З.В. Алгебра и теория чисел [Электронный ресурс]: учебно-методический комплекс / З.В. Алферова, Э.Л. Балюкевич, А.Н. Романников. - М.: Евразийский открытый институт, 2011. – 279 с. // Режим доступа - http://biblioclub.ru/index.php?page=book&id=90645

2. Элементы алгебры и теории чисел [Текст]: методические указания по выполнению самостоятельной работы / Юго-Зап. гос. ун-т; сост.: В.П. Добрица. – Курск, 2018. – 21 с.: табл. 5. – Библиогр.: с. 20.

9. Перечень ресурсов информационно-телекоммуникационной сети ИНТЕРНЕТ, необходимых для освоения дисциплины

Электронно-библиотечная система «Лань» - http://e.lanbook.com/

Электронно-библиотечная система IQLib – http://www.iqlib.ru

Электронная библиотека «Единое окно доступа к образовательным ресурсам» - http://window.edu.ru/

10. Методические указания для обучающихся по освоению дисциплины

Основными видами аудиторной работы студента при изучении дисциплины «Элементы алгебры и теории чисел» являются лекции и практические занятия. Студент не имеет права пропускать занятия без уважительных причин.

На лекциях излагаются и разъясняются основные понятия темы, связанные с ней теоретические и практические проблемы, даются рекомендации для самостоятельной работы. В ходе лекции студент должен внимательно слушать и конспектировать материал.

Изучение наиболее важных тем или разделов дисциплины завершают практические занятия, которые обеспечивают: контроль подготовленности студента; закрепление учебного материала; приобретение опыта отстаивания своей точки зрения, устных публичных выступлений, ведения дискуссии, в том числе аргументации и защиты выдвигаемых положений и тезисов.

Практическому занятию предшествует самостоятельная работа студента, связанная с освоением материала, полученного на лекциях, и материалов, изложенных в учебниках и учебных пособиях, а также литературе, рекомендованной преподавателем.

По согласованию с преподавателем или по его заданию студенты готовят рефераты по отдельным темам дисциплины, выступают на занятиях с докладами. Основу докладов составляет, как правило, содержание подготовленных студентами рефератов.

Качество учебной работы студентов преподаватель оценивает по результатам тестирования, собеседования, защиты отчетов по лабораторным работам, а также по результатам докладов. Преподаватель уже на первых занятиях объясняет студентам, какие формы обучения следует использовать при самостоятельном изучении дисциплины «Элементы алгебры и теории чисел»: конспектирование учебной литературы и лекции, составление словарей понятий и терминов, прорешивание предлагаемых упражнений и т. п.

В процессе обучения преподаватели используют активные формы работы со студентами: чтение лекций, привлечение студентов к творческому процессу на лекциях, промежуточный контроль путем отработки студентами пропущенных лекций, участие в групповых и индивидуальных консультациях (собеседованиях). Эти формы способствуют выработке у студентов умения работать с учебником и литературой. Изучение литературы составляет значительную часть самостоятельной работы студента. Это большой труд, требующий усилий и желания студента. В самом начале работы над книгой важно определить цель и направление этой работы. Прочитанное следует закрепить в памяти. Одним из приемов закрепления освоенного материала является конспектирование, без которого немыслима серьезная работа над литературой. Систематическое конспектирование помогает научиться правильно, кратко и четко излагать своими словами прочитанный материал.

Самостоятельную работу следует начинать с первых занятий. От занятия к занятию нужно регулярно прочитывать конспект лекций, дополнять его, знакомиться с соответствующими разделами учебника, читать и конспектировать литературу по каждой теме дисциплины, прорешивать необходимые упражнения. Самостоятельная работа дает студентам возможность равномерно распределить нагрузку, способствует более

глубокому и качественному усвоению учебного материала. В случае необходимости студенты обращаются за консультацией к преподавателю по вопросам дисциплины «Элементы алгебры и теории чисел» с целью усвоения и закрепления компетенций.

Основная цель самостоятельной работы студента при изучении дисциплины «Элементы алгебры и теории чисел» - закрепить теоретические знания, полученные в процессе лекционных занятий, а также сформировать практические навыки самостоятельного анализа особенностей дисциплины.

11. Перечень информационных технологий

Microsoft Office 2016.Лицензионный договор №S0000000722 от 21.12.2015 г. с ООО «АйТи46», лицензионный договор №K0000000117 от 21.12.2015 г. с ООО «СМСКанал»,

Kaspersky Endpoint Security Russian Edition, лицензия 156A-140624-192234,

Windows 7, договор IT000012385

12. Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине

Учебная аудитория для проведения занятий лекционного и практического типа или лаборатории кафедры информационная безопасность, оснащенные мебелью: столы, стулья для обучающихся; стол, стул для преподавателя; доска, проектор для демонстрации презентаций. Помещение для самостоятельной работы Компьютер PDC2160/iC33/2*512Mb/HDD 160Gb/DVD-ROM/FDD/ATX350W/ K/m/ OFF/l 7"TFT E700 (6 шт)

13. Лист дополнений и изменений, внесенных в рабочую программу дисциплины

№ изменения	Номера страниц				Всего	Дата	Основание для изменения и подпись лица, проводившего изменения
	измененных	замененных	аннулированных	новых			
1	2	3	4	5	6	7	8