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

Цель преподавания дисциплины

Целью преподавания дисциплины «Элементы алгебры и теории чисел» является 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

- 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.

Индикаторы компетенций, формируемые в результате освоения дисциплины

ОПК-3.5 Решает задачи профессиональной области с применением дискретных моделей.

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

М.О. Таныгин
(подпись, инициалы, фамилия)
«31» августа 2021 г

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Элементы алгебры и теории чисел
(наименование дисциплины)

ОПОП ВО 10.03.01 Информационная безопасность
шифр и наименование направление подготовки (специальности)

Безопасность автоматизированных систем в сфере информационных и коммуникационных технологий
наименование направленности (профиля, специализации)

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

Курск – 2021

Рабочая программа дисциплины «Элементы алгебры и теории чисел» составлена в соответствии с ФГОС ВО – бакалавриат по направлению подготовки 10.03.01 Информационная безопасность на основании учебного плана ОПОП ВО 10.03.01 Информационная безопасность, профиль «Безопасность автоматизированных систем в сфере информационных и коммуникационных технологий», одобренного Ученым советом университета (протокол № 6 «26» 02 2021 г.).

Рабочая программа дисциплины обсуждена и рекомендована к реализации в образовательном процессе для обучения студентов по ОПОП ВО 10.03.01 Информационная безопасность, профиль «Безопасность автоматизированных систем в сфере информационных и коммуникационных технологий» на заседании кафедры информационной безопасности № 1 «30» 08 2021 г.

Зав. кафедрой _____ Таныгин М.О.

Разработчик программы
д.т.н., профессор _____ Добрица В.П.
(ученая степень и ученое звание, Ф.И.О.)

Директор научной библиотеки _____ Макаровская В.Г.

Рабочая программа дисциплины пересмотрена, обсуждена и рекомендована к реализации в образовательном процессе на основании учебного плана ОПОП ВО 10.03.01 Информационная безопасность, профиль «Безопасность автоматизированных систем в сфере информационных и коммуникационных технологий», одобренного Ученым советом университета протокол № 6 «26» 02 2021 г., на заседании кафедры информационной безопасности N11 от 30.06.2022г.
(наименование кафедры, дата, номер протокола)

Зав. кафедрой _____

Рабочая программа дисциплины пересмотрена, обсуждена и рекомендована к реализации в образовательном процессе на основании учебного плана ОПОП ВО 10.03.01 Информационная безопасность, профиль «Безопасность автоматизированных систем в сфере информационных и коммуникационных технологий», одобренного Ученым советом университета протокол № 7 «28» февраля 2022 г., на заседании кафедры ИБ от 30.08.2023 №1
(наименование кафедры, дата, номер протокола)

Зав. кафедрой _____

1. Цель и задачи дисциплины. Перечень планируемых результатов обучения по дисциплине, соотнесенных с планируемыми результатами освоения основной профессиональной образовательной программы

1.1. Цель преподавания дисциплины

Целью преподавания дисциплины «Элементы алгебры и теории чисел» является 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 изучения дисциплины

В результате изучения дисциплины студенты должны 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 по дисциплине, соотнесенных с планируемыми результатами освоения основной профессиональной образовательной программы

Таблица 1.3 – Результаты обучения по дисциплине

Планируемые результаты освоения основной профессиональной образовательной программы		*Код и наименование индикатора достижения компетенции, закрепленного за дисциплиной*	*Планируемые результаты обучения по дисциплине, соотнесенные с индикаторами достижения компетенций*
код компетенции	*наименование компетенции*		

ОПК-3	Способен использовать необходимые математические методы для решения задач профессиональной деятельности;	ОПК-3.5 Решает задачи профессиональной области с применением дискретных моделей	***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 (****или* ***Иметь опыт деятельности):*** - 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.

2. Указание места дисциплины в структуре основной профессиональной образовательной программы

Дисциплина «Элементы алгебры и теории чисел» входит в обязательную часть блока 1 «Дисциплины (модули»») основной профессиональной образовательной программы – программы бакалавриата 10.03.01 Информационная безопасность профиль «Безопасность автоматизированных систем». Дисциплина изучается на 2 курсе в 4 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 3 зачётных единицы, 108 часов

Таблица 3 – Объем дисциплины

Виды учебной работы	Всего, часов
Общая трудоемкость дисциплины	108
Контактная работа обучающихся с преподавателем по видам учебных занятий (всего)	56.1
в том числе:	
лекции	28
лабораторные занятия	0
практические занятия	28
Самостоятельная работа обучающихся (всего)	51.9
Контроль (подготовка к экзамену)	27
Контактная работа по промежуточной аттестации (всего АттКР)	0.1
в том числе:	
зачет	0.1
зачет с оценкой	не предусмотрен
курсовая работа (проект)	не предусмотрена
экзамен (включая консультацию перед экзаменом)	не предусмотрен

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

4.1. Содержание дисциплины

Таблица 4.1.1 – 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	Каноническое представление целого числа. Критерий

	представление целых чисел. НОД.	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 4.1.2 – Содержание дисциплины и её методическое обеспечение

№ п/п	Раздел учебной дисциплины	Виды учебной деятельности (в часах)			Учебно-методические материалы	Формы текущего контроля успеваемости *(по неделям семестра)* Форма промежуточной аттестации *(по семестрам)*	Компетенции
		лек	№ лаб	№ пр.			
1	2	3	4	5	6	7	8
1	Введение и предмет курса.	2	-	-	У-1,3	С,Т	ОПК-3.5
2	Теорема деления с остатком. Делимость и её свойства. Простые числа.	2	-	1	У-1-3 МУ-1	С,Т	ОПК-3.5
3	Каноническое представление целых чисел. НОД.	2	-	2	У-1-3 МУ-1	С,Т	ОПК-3.5
4	Взаимно простые числа и их свойства. НОК. Свойства НОК, НОД.	2	-	3	У-1-3 МУ-1	С,Т	ОПК-3.5
5	Сравнения и их свойства. Системы сравнений первой степени.	2	-	4	У-1-3 МУ-1	С,Т,К	ОПК-3.5
6	Сравнения второй степени. Непрерывные дроби.	4	-	5	У-4-6 МУ-1	С,Т	ОПК-3.5
7	Группы, кольца, поля. Их свойства.	2	-	6	У-1-3 МУ-1	С,Т	ОПК-3.5
8	Элементы теории многочленов.	4	-	7	У-7 МУ-1	С,Т	ОПК-3.5
9	Эллиптические кривые над полем. Точки эллиптической кривой и их свойства.	4	-	8	У-2-4 МУ-1	С,Т	ОПК-3.5
10	Эллиптические кривые над конечными полями. Действия над точками эллиптической кривой.	4	-	9	У-4-6 МУ-1	С,Т	ОПК-3.5

	Всего	28				З	

С – собеседование, Т – тест, Кейс-задача

4.2. Лабораторные работы и практические занятия

4.2.1. Практические работы

Таблица 4.2.1 – Практические работы

№	Наименование работы	Объем, час.
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.	4
4	Системы сравнений первой степени. Сравнения второй степени.	4
5	Непрерывные дроби.	4
6	Группы, кольца, поля. Элементы теории многочленов.	4
7	Эллиптические кривые над полем. Точки эллиптической кривой и их свойства.	4
8-9	Эллиптические кривые над конечными полями. Действия над точками эллиптической кривой.	4
	Итого	28

4.3. Самостоятельная работа студентов (СРС)

Таблица 4.5 – Самостоятельная работа студентов

№	Наименование раздела учебной дисциплины	Срок выполнения	Время, затрачиваемое на выполнение СРС, час.
1	2	3	4
1	Введение и предмет курса элементы алгебры и теории чисел.	1 неделя	2
2	Делимость, каноническое представление чисел, НОД, НОК, взаимно простые числа.	2-3 недели	7
3	Сравнения и их свойства. Системы сравнений первой степени. Сравнения второй степени.	4-8 недели	15
4	Непрерывные дроби.	9-10 недели	6
5	Группы, кольца, поля. Элементы теории многочленов.	11-12 недели	6
6	Эллиптические кривые над полем. Точки эллиптической кривой и их свойства.	13-16 недели	12
7	Эллиптические кривые над конечными	17-18	5.9

	полями. Действия над точками эллиптической кривой.	недели	
Итого			53.9

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 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 вопросов к экзамену, методических указаний к выполнению лабораторных и практических работ.

типографией университета:

− путем помощи авторам в подготовке и издании научной, учебной, учебно-методической литературы;

− путем удовлетворения потребностей в тиражировании научной, учебной, учебно-методической литературы.

6. Образовательные технологии. Технологии использования воспитательного потенциала дисциплины

Реализация компетентностного подхода предусматривает широкое использование в образовательном процессе активных и интерактивных форм проведения занятий в сочетании с внеаудиторной работой с целью формирования общепрофессиональных компетенций обучающихся. В рамках дисциплины предусмотрены выполнение в ходе практических работ практикоориентированных заданий.

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

№	Наименование раздела	Используемые интерактивные образовательные технологии	Объём, час.
1.	Выполнение работы «Каноническое представление целых чисел. НОД. Взаимно простые числа. НОК.»	Разбор конкретных ситуаций. Таблицы, программы нахождения НОД, НОК, проверки простоты числа	2
2.	Выполнение работы «Группы, кольца, поля. Элементы теории многочленов»	Разбор конкретных ситуаций. Таблицы: аксиомы, примеры.	2
3.	Выполнение работы «Эллиптические кривые над конечными полями. Действия над точками эллиптической кривой.»	Выполнение студентом интерактивной проверки результатов работы. Учебная дискуссия	4
	Итого		8

Технологии использования воспитательного потенциала дисциплины

Содержание дисциплины обладает значительным воспитательным потенциалом, поскольку в нем аккумулирован научный опыт человечества. Реализация воспитательного потенциала дисциплины осуществляется в рамках единого образовательного и воспитательного процесса и способствует непрерывному развитию личности каждого обучающегося. Дисциплина вносит значимый вклад в формирование общей и профессиональной культуры обучающихся. Содержание дисциплины способствует правовому, экономическому, профессионально-трудовому, воспитанию обучающихся.

Реализация воспитательного потенциала дисциплины подразумевает:

– целенаправленный отбор преподавателем и включение в лекционный материал, материал для практических и (или) лабораторных занятий содержания, демонстрирующего обучающимся образцы настоящего научного подвижничества создателей и представителей данной отрасли науки (производства, экономики, культуры), высокого профессионализма ученых (представителей производства, деятелей культуры), их ответственности за результаты и последствия деятельности для человека и общества; примеры подлинной нравственности людей, причастных к развитию науки и производства;

– применение технологий, форм и методов преподавания дисциплины, имеющих высокий воспитательный эффект за счет создания условий для взаимодействия обучающихся с преподавателем, другими обучающимися, (командная работа, разбор конкретных ситуаций)*;*

– личный пример преподавателя, демонстрацию им в образовательной деятельности и общении с обучающимися за рамками образовательного процесса высокой общей и профессиональной культуры.

Реализация воспитательного потенциала дисциплины на учебных занятиях направлена на поддержание в университете единой развивающей

образовательной и воспитательной среды. Реализация воспитательного потенциала дисциплины в ходе самостоятельной работы обучающихся способствует развитию в них целеустремленности, инициативности, креативности, ответственности за результаты своей работы – качеств, необходимых для успешной социализации и профессионального становления.

7. Фонд оценочных средств для проведения промежуточной аттестации

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

Таблица 7.1 – Этапы формирования компетенций

Код и содержание компетенции	Этапы формирования компетенций и дисциплины (модули), при изучении которых формируется данная компетенция		
	начальный	основной	завершающий
1	2	3	4
ОПК-3 Способен использовать необходимые математические методы для решения задач профессиональной деятельности	Учебно-лабораторная практика Алгебра и геометрия Математический анализ Вычислительные методы Дискретная математика Математическая логика и теория алгоритмов		Теория вероятностей и математическая статистика Подготовка к процедуре защиты и защита выпускной квалификационной работы

7.2. Описание показателей и критериев оценивания компетенций на раз- личных этапах их формирования, описание шкал оценивания

Таблица 7.2 – Показатели и критерии оценивания компетенций, шкала оценивания

Код компетенции/ этап	Показатели оценивания компетенций	Критерии и шкала оценивания компетенций		
		Пороговый уровень («удовлетворительно)	Продвинутый уровень (хорошо»)	Высокий уровень («отлично»)
ОПК - 3 / основной	ОПК-3.5 Решает задачи профессиональной области с применением дискретных	***Знать:*** - основные определения и теоремы теории чисел; - методы	***Знать:*** - определения различных типов групп, колец о полей и их основные	***Знать:*** - определения различных типов групп, колец о полей и их основные свойства;

Код компетенции/ этап	Показатели оценивания компетенций	Критерии и шкала оценивания компетенций		
		Пороговый уровень («удовлетворительно)	Продвинутый уровень (хорошо»)	Высокий уровень («отлично»)
	моделей	дискретного логарифмирования показательных и степенных сравнений; - аппарат линейной алгебры. ***Уметь:*** - пользоваться и научной литературой; - решать основные задачи криптографии; - строить формальные алгоритмы для построения криптосистем; - применять полученные знания в процессе изучения других дисциплин и т.д. ***Владеть (****или* ***Иметь опыт деятельности):*** - проверки простоты числа, нахождения наибольшего общего делителя, наименьшего общего кратного, нахождения канонического разложения числа; - решения сравнений первой и второй степени, а также систем сравнений первой степени; - решения задач	свойства; - методы решения сравнений первой и второй степени, а также систем сравнений первой степени; - основные операции над точками эллиптических кривых; - аппарат линейной алгебры. ***Уметь:*** - применять полученные знания к исследованию задач по защите информации; - решать основные задачи криптографии; - применять полученные знания в процессе изучения других дисциплин и т.д. ***Владеть (****или* ***Иметь опыт деятельности):*** - проверки простоты числа, нахождения наибольшего общего делителя, наименьшего общего кратного, нахождения канонического разложения числа; - построения конечных полей,	- 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; ***Владеть (****или* ***Иметь опыт деятельности):*** - проверки простоты числа, нахождения наибольшего общего делителя, наименьшего

Код компетенции/ этап	Показатели оценивания компетенций	Критерии и шкала оценивания компетенций		
		Пороговый уровень («удовлетворительно)	Продвинутый уровень (хорошо»)	Высокий уровень («отлично»)
		линейной алгебры;	отличных от полей типа полей Галуа; - решения задач линейной алгебры; - применения стандартных методов и алгоритмов к решению прикладных задач.	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 основной профессиональной образовательной программы

Таблица 7.3 – Паспорт комплекта оценочных средств для текущего контроля успеваемости

№ 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-3.5	Лекция, СРС	С	1-2	Согласно табл. 7.2
2	Теорема деления с остатком. Делимость и её свойства. Простые числа.	ОПК-3.5	Лекция, СРС, практические задания	С, КО Защита раб №1	3-8	Согласно табл. 7.2
3	Каноническое представление целых чисел. НОД.	ОПК-3.5	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-3.5	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-3.5	Лекция, СРС, практические задания	С, КО Защита раб №4	21 - 31	Согласно табл. 7.2
6	Сравнения второй степени. Непрерывные дроби.	ОПК-3.5	Лекция, СРС, практические задания	С, КО Защита раб №5	32 - 40	Согласно табл. 7.2
7	Группы, кольца, поля. Их свойства.	ОПК-3.5	Лекция, СРС, практические задания	С, КО Защита раб №6	41-63	Согласно табл. 7.2
8	Элементы теории многочленов.	ОПК-3.5	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-3.5	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-3.5	Лекция, СРС, практические задания	С, КО Защита раб №9	80 - 86	Согласно табл. 7.2

Примеры типовых контрольных заданий для проведения текущего контроля успеваемости

Вопросы в тестовой форме «Алгебра высказываний»

Повествовательное предложение (утверждение, суждение), о котором имеет смысл говорить, что оно истинно или ложно это:

?) высказывание

?) теорема

?) базис

Вопросы для собеседования

Тема. Формулы и подформулы алгебры высказываний

1. Понятие высказывания. Истинность высказывания.
2. Формулы и подформулы. Порядок выполнения логических операций. Сложность формулы.
3. Таблицы истинности. Выполнимые, тождественно истинные и невыполнимые формулы.
4. Основные законы логики.
5. Эквивалентные формулы, эквивалентные преобразования формул.

Кейс – задачи

Определите, является ли данное выражение формулой. Если это формула, то выпишите последовательность построения формулы.

Выражение $(A \vee B)(C \to A)$ формулой не является, т.к. выражения $(A \vee B)$ и $(C \to A)$ формулами являются в соответствии с определением, но между ними нет никакой операции.

Типовые задания для проведения промежуточной аттестации обучающихся

Промежуточная аттестация по дисциплине проводится в форме зачета. Зачет проводится в виде компьютерного тестирования.

Для тестирования используются контрольно-измерительные материалы (КИМ) – вопросы и задания в тестовой форме, составляющие банк тестовых заданий (БТЗ) по дисциплине, утвержденный в установленном в университете порядке.

Проверяемыми на промежуточной аттестации элементами содержания являются темы дисциплины, указанные в разделе 4 настоящей программы. Все темы дисциплины отражены в КИМ в равных долях (%). БТЗ включает в себя не менее 100 заданий и постоянно пополняется. БТЗ хранится на бумажном носителе в составе УММ и электронном виде в ЭИОС университета.

Для проверки *знаний* используются вопросы и задания в различных формах:

- закрытой (с выбором одного или нескольких правильных ответов),

- открытой (необходимо вписать правильный ответ),
- на установление правильной последовательности,
- на установление соответствия.

Умения, навыки (или опыт деятельности) и компетенции проверяются с помощью компетентностно-ориентированных задач (ситуационных, производственных или кейсового характера) и различного вида конструкторов.

Все задачи являются многоходовыми. Некоторые задачи, проверяющие уровень сформированности компетенций, являются многовариантными. Часть умений, навыков и компетенций прямо не отражена в формулировках задач, но они могут быть проявлены обучающимися при их решении.

В каждый вариант КИМ включаются задания по каждому проверяемому элементу содержания во всех перечисленных выше формах и разного уровня сложности. Такой формат КИМ позволяет объективно определить качество освоения обучающимися основных элементов содержания дисциплины и уровень сформированности компетенций.

Примеры типовых заданий для проведения
промежуточной аттестации обучающихся

Задание в закрытой форме:

Функция называется *булевой*, если она сама и ее переменные могут принимать значения ____.

Задание в открытой форме:

Произвольная дизъюнкция элементарных конъюнкций называется
ДНФ
КНФ
DNS

Задание на установление правильного приоритета логических операций:

конъюнкция, дизъюнкция, инверсия, импликация.

Задание на установление соответствия:

Установите соответствие, что не прибегая к таблице истинности, что следующая формула не является тождественно истинной: $(Y \vee Z) \Rightarrow ((X \vee Y) \Rightarrow (X \wedge Z))$.

Компетентностно-ориентированная задача:

Построить СДНФ (от трех переменных), которая равна 1 тогда и только тогда, когда ровно две переменные равны 1.

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 «О балльно-рейтинговой системе оценивания результатов обучения по дисциплинам (модулям) и практикам при освоении обучающимися образовательных программ»;

– методические указания, используемые в образовательном процессе, указанные в списке литературы.

Для *текущего контроля успеваемости* 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 работы №1 «Теорема деления с остатком. Делимость и её свойства»	2	Выполнил, но «не защитил»	4	Выполнил и «защитил»
Выполнение работы №2 «Каноническое представление целых чисел. НОД. Взаимно простые числа. НОК»	2	Выполнил, но «не защитил»	4	Выполнил и «защитил»
Выполнение работы №3 «Сравнения и их свойства»	2	Выполнил, но «не защитил»	6	Выполнил и «защитил»
Выполнение работы №4 «Системы сравнений первой степени. Сравнения второй степени»	2	Выполнил, но «не защитил»	4	Выполнил и «защитил»
Выполнение работы №5 «Непрерывные дроби»	2	Выполнил, но «не защитил»	4	Выполнил и «защитил»
Выполнение работы №6 «Группы, кольца, поля. Элементы теории многочленов»	2	Выполнил, но «не защитил»	6	Выполнил и «защитил»
Выполнение работы №7 «Эллиптические кривые над полем. Точки эллиптической кривой и их свойства»	2	Выполнил, но «не защитил»	6	Выполнил и «защитил»
Выполнение работы №8 «Эллиптические кривые над конечными полями»	2	Выполнил, но «не защитил»	6	Выполнил и «защитил»

Выполнение 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.

8.3 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

9. Перечень ресурсов информационно-телекоммуникационной сети Интернет

1) Электронно-библиотечная система «Лань» - http://e.lanbook.com/
2) Электронно-библиотечная система IQLib – http://www.iqlib.ru
3) 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 лабораторные 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 лабораторные и практические занятия, которые обеспечивают: контроль подготовленности студента; закрепление учебного материала; приобретение опыта 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.

Качество учебной работы студентов преподаватель оценивает по результатам тестирования, собеседования, защиты отчетов по лабораторным

и практическим работам.

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 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 лекции, участие в групповых и индивидуальных консультациях (собеседовании). Эти формы способствуют выработке у студентов умения работать с учебником и литературой. Изучение литературы и справочной документации 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 закрепление 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, знакомиться с соответствующими разделами учебника, читать и конспектировать литературу по каждой теме дисциплины. 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, используемых при осуществлении образовательного процесса по дисциплине, включая перечень программного обеспечения и информационных справочных систем (при необходимости)

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 типа и лаборатории кафедры информационной безопасности, оснащенные учебной мебелью: столы, стулья для обучающихся; стол, стул для преподавателя; доска. Компьютеры (10 шт) CPU AMD-Phenom, ОЗУ 16 GB, HDD 2 Tb, монитор Aok 21”. Проекционный экран на штативе; Мультимедиацентр: ноут- букASUSX50VLPMD-T2330/14"/1024Mb/160Gb/сумка/ проектор inFocusIN24+

13. Особенности реализации дисциплины для инвалидов и лиц с ограниченными возможностями здоровья

При обучении лиц с ограниченными возможностями здоровья учитываются их индивидуальные психофизические особенности. Обучение инвалидов осуществляется также в соответствии с индивидуальной программой реабилитации инвалида (при наличии).

Для лиц с нарушением слуха возможно предоставление учебной информации в визуальной форме (краткий конспект лекций; тексты заданий, напечатанные увеличенным шрифтом), на аудиторных занятиях допускается присутствие ассистента, а также сурдопереводчиков и тифлосурдопереводчиков. Текущий контроль успеваемости осуществляется в письменной форме: обучающийся письменно отвечает на вопросы, письменно выполняет практические задания. Доклад (реферат) также может быть представлен в письменной форме, при этом требования к содержанию остаются теми же, а требования к качеству изложения материала (понятность, качество речи, взаимодействие с аудиторией и т. д.) заменяются на соответствующие требования, предъявляемые к письменным работам (качество оформления текста и списка литературы, грамотность, наличие иллюстрационных материалов и т.д.). Промежуточная аттестация для лиц с нарушениями слуха проводится в письменной форме, при этом используются общие критерии оценивания. При необходимости время подготовки к ответу может быть увеличено.

Для лиц с нарушением зрения допускается аудиальное предоставление информации, а также использование на аудиторных занятиях звукозаписывающих устройств (диктофонов и т.д.). Допускается присутствие на занятиях ассистента (помощника), оказывающего обучающимся необходимую техническую помощь. Текущий контроль успеваемости осуществляется в устной форме. При проведении промежуточной аттестации для лиц с нарушением зрения тестирование может быть заменено на устное собеседование по вопросам.

Для лиц с ограниченными возможностями здоровья, имеющих нарушения опорно-двигательного аппарата, на аудиторных занятиях, а

также при проведении процедур текущего контроля успеваемости и промежуточной аттестации могут быть предоставлены необходимые технические средства (персональный компьютер, ноутбук или другой гаджет); допускается присутствие ассистента (ассистентов), оказывающего обучающимся необходимую техническую помощь (занять рабочее место, передвигаться по аудитории, прочитать задание, оформить ответ, общаться с преподавателем).