МИНОБРНАУКИ РОССИИ

Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Российский государственный гуманитарный университет»
(ФГБОУ ВО «РГГУ»)

ИНСТИТУТ ИНФОРМАЦИОННЫХ НАУК И ТЕХНОЛОГИЙ БЕЗОПАСНОСТИ
Факультет информационных систем и безопасности
Кафедра фундаментальной и прикладной математики

ОБЩАЯ АЛГЕБРА И ТЕОРИЯ ЧИСЕЛ

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

01.03.04 Прикладная математика
Код и наименование направления подготовки/специальности

Математика информационных сред
Наименование направленности (профиля)/ специализации

Уровень высшего образования: *бакалавриат*

Форма обучения: *Очная*

РПД адаптирована для лиц
с ограниченными возможностями
здоровья и инвалидов

Москва 2024

ОБЩАЯ АЛГЕБРА И ТЕОРИЯ ЧИСЕЛ

Рабочая программа дисциплины

Составитель:

канд. пед. н., доцент, доцент кафедры фундаментальной и прикладной математики
А.А. Бастрон

УТВЕРЖДЕНО
Протокол заседания кафедры
фундаментальной и прикладной математики
№ 8 от 20.03.2024

ОГЛАВЛЕНИЕ

1. Пояснительная записка

1.1. Цель и задачи дисциплины

Цель дисциплины: ознакомить студентов с алгебраическими и теоретико-числовыми методами, используемыми в криптографии и теории кодирования, научить студентов владеть и применять эти методы.

Задачи: познакомить студентов с основными понятиями алгебры и теории чисел, показать современные приложения теории и научить решать стандартные прикладные задачи с помощью изученного материала.

1.2. Перечень планируемых результатов обучения по дисциплине, соотнесенных с индикаторами достижения компетенций

Компетенция (код и наименование)	**Индикаторы компетенций** (код и наименование)	**Результаты обучения**
ОПК-1. Способен применять знание фундаментальной математики и естественно-научных дисциплин при решении задач в области естественных наук и инженерной практике	ОПК-1.1. Знает и определяет области реализации фундаментальных понятий и владеет опытом адаптации текущих задач к формальным теориям.	*Знать:* теоретический материал, использующий современные методы и результаты из общей алгебры и теории чисел, которые используются в теории кодирования, криптографии и смежных областях; *Уметь*: решать задачи предлагаемого курса, пользоваться современными прикладными пакетами программ для решения предлагаемых в курсе специальных задач; *Владеть:* навыками формализации классических алгебраических задач, а также иметь достаточно точное представление о прикладных возможностях этого курса.
	ОПК-1.2. Осуществляет поиск математических методов и умеет использовать необходимый теоретический материал для решения поставленных проблем.	*Знать:* теоретический материал, использующий современные методы и результаты из общей алгебры и теории чисел, которые используются в теории кодирования, криптографии и смежных областях; *Уметь*: решать задачи предлагаемого курса *Владеть:* навыками формализации классических алгебраических задач

1.3. Место дисциплины в структуре образовательной программы

Дисциплина «Общая алгебра и теория чисел» относится к обязательной части блока дисциплин учебного плана.

Для освоения дисциплины необходимы знания, умения и владения, сформированные в ходе изучения следующих дисциплин: «Дискретная математика».

В результате освоения дисциплины формируются знания, умения и владения, необходимые для изучения следующих дисциплин и прохождения практик: «Квантовые вычисления и квантовая криптография», «Теория кодирования», «Теория систем и системный анализ», Учебная практика (Проектно-технологическая практика), Производственная практика (Научно-

исследовательская работа (получение первичных навыков научно-исследовательской деятельности)).

2. Структура дисциплины

Общая трудоёмкость дисциплины составляет 4 з.е., 144 академических часа.

Структура дисциплины для очной формы обучения

Объем дисциплины в форме контактной работы обучающихся с педагогическими работниками и (или) лицами, привлекаемыми к реализации образовательной программы на иных условиях, при проведении учебных занятий:

Семестр	Тип учебных занятий	Количество часов
3	Лекции	**24**
3	Практические занятия	**32**
	Всего:	**56**

Объем дисциплины в форме самостоятельной работы обучающихся составляет 88 академических часов.

3. Содержание дисциплины

I. Теоретико-множественные основы алгебры. Множества. Декартово произведение, соответствие, Свойства бинарных отношений. Эквивалентность. Порядок. Функциональные отношения, функция и отображение. Равномощность. Кардинальные числа. Натуральное множество чисел.

II. Элементы теории чисел. Теория делимости и кольцо целых чисел. Основная теорема арифметики. Сравнение в кольце целых чисел. Понятие о числовых системах. Кольцо классов вычетов. Китайская теорема об остатках. Некоторые теоретико-числовые функции: определения и их свойства. Формула обратимости Мебиуса. Разложение натурального числа по степеням m. m - адические позиционные системы счисления.

III. Основы теории групп:

группы, подгруппы, порядки элементов; циклические группы и их подгруппы; симметрические группы, разложения перестановок в независимые циклы; вычисление порядков перестановок; смежные классы и теорема Лагранжа; классы сопряженных элементов, нормальные подгруппы, факторгруппы, гомоморфизмы: теорема о гомоморфизмах. Автоморфизмы и эндоморфизмы групп.

IV. Основы теории колец:

кольца, поля, алгебры, характеристика поля; делители нуля и обратимые элементы; идеалы; идеалы в кольцах матриц; факторкольцо и факторалгебры; кольца вычетов: делители нуля и обратимые элементы в кольцах вычетов; построение расширений полей, в которых

заданный многочлен имеет всех корни; алгебраические элементы и их минимальные многочлены в расширениях полей.

V. Конечные поля:

порядки конечных полей; существование и единственность конечного поля заданного порядка; цикличность конечной мультипликативной группы поля; поиск порождающего и примитивного элементов; поиск минимального многочлена для элемента конечного поля; подполя конечного поля. Поля p – адических чисел.

VI. Бинарные отношения и универсальные алгебры:

операции над бинарными отношениями; моноид бинарных отношений; эквивалентности; отношения порядка; универсальная алгебра, примеры; подалгебры, гомоморфизмы, конгруэнции, теорема о гомоморфизмах; подпрямо неразложимые алгебры; теорема Биркгофа о подпрямых разложениях: примеры.

VII. Коммутативные кольца и поля. Коммутативные кольца и поля, приложение к кодированию, шифры

4. Образовательные технологии

Для проведения *занятий лекционного типа* по дисциплине применяются такие образовательные технологии как лекция-визуализация с применением слайд-проектора, проблемная лекция.
Для проведения *практических занятий* используются такие образовательные технологии как: решение типовых задач для закрепления и формирования знаний, умений, навыков.
В рамках *самостоятельной работы* студентов проводится консультирование и проверка домашних заданий посредством электронной почты.

В период временного приостановления посещения обучающимися помещений и территории РГГУ для организации учебного процесса с применением электронного обучения и дистанционных образовательных технологий могут быть использованы следующие образовательные технологии:

– видео-лекции**;**

– онлайн-лекции в режиме реального времени;

– электронные учебники, учебные пособия, научные издания в электронном виде и доступ к иным электронным образовательным ресурсам;

– системы для электронного тестирования;

– консультации с использованием телекоммуникационных средств.

5. Оценка планируемых результатов обучения

5.1 ***Система оценивания***

Форма контроля	Макс. количество баллов	
	За одну работу	Всего
Текущий контроль:		
- РГР	15 баллов	30 баллов
- контрольная работа	10 баллов	10 баллов
- доклады	12 баллов	12 баллов
- рефераты	8 баллов	8 баллов

Промежуточная аттестация - экзамен (Экзамен по билетам)		40 баллов
Итого за семестр		100 баллов

Полученный совокупный результат конвертируется в традиционную шкалу оценок и в шкалу оценок Европейской системы переноса и накопления кредитов (European Credit Transfer System; далее – ECTS) в соответствии с таблицей:

100-балльная шкала	Традиционная шкала		Шкала ECTS
95 – 100	отлично	зачтено	A
83 – 94			B
68 – 82	хорошо		C
56 – 67	удовлетворительно		D
50 – 55			E
20 – 49	неудовлетворительно	не зачтено	FX
0 – 19			F

5.2 Критерии выставления оценки по дисциплине

Баллы/ Шкала ECTS	**Оценка по дисциплине**	**Критерии оценки результатов обучения по дисциплине**
100-83/ A,B	отлично	Выставляется обучающемуся, если он глубоко и прочно усвоил теоретический и практический материал, может продемонстрировать это на занятиях и в ходе промежуточной аттестации. Обучающийся исчерпывающе и логически стройно излагает учебный материал, умеет увязывать теорию с практикой, справляется с решением задач профессиональной направленности высокого уровня сложности, правильно обосновывает принятые решения. Свободно ориентируется в учебной и профессиональной литературе. Оценка по дисциплине выставляются обучающемуся с учётом результатов текущей и промежуточной аттестации. Компетенции, закреплённые за дисциплиной, сформированы на уровне – «высокий».
82-68/ C	хорошо	Выставляется обучающемуся, если он знает теоретический и практический материал, грамотно и по существу излагает его на занятиях и в ходе промежуточной аттестации, не допуская существенных неточностей. Обучающийся правильно применяет теоретические положения при решении практических задач профессиональной направленности разного уровня сложности, владеет необходимыми для этого навыками и приёмами. Достаточно хорошо ориентируется в учебной и профессиональной литературе. Оценка по дисциплине выставляются обучающемуся с учётом результатов текущей и промежуточной аттестации. Компетенции, закреплённые за дисциплиной, сформированы на уровне – «хороший».
67-50/ D,E	удовлетво-рительно	Выставляется обучающемуся, если он знает на базовом уровне теоретический и практический материал, допускает отдельные ошибки при его изложении на занятиях и в ходе промежуточной аттестации. Обучающийся испытывает определённые затруднения в применении теоретических положений при решении практических задач профессиональной направленности стандартного уровня сложности, владеет необходимыми для этого базовыми навыками и приёмами. Демонстрирует достаточный уровень знания учебной литературы по дисциплине. Оценка по дисциплине выставляются обучающемуся с учётом результатов текущей и промежуточной аттестации. Компетенции, закреплённые за дисциплиной, сформированы на уровне –

Баллы/ Шкала ECTS	Оценка по дисциплине	Критерии оценки результатов обучения по дисциплине
		«достаточный».
49-0/ F,FX	неудовлет-ворительно	Выставляется обучающемуся, если он не знает на базовом уровне теоретический и практический материал, допускает грубые ошибки при его изложении на занятиях и в ходе промежуточной аттестации. Обучающийся испытывает серьёзные затруднения в применении теоретических положений при решении практических задач профессиональной направленности стандартного уровня сложности, не владеет необходимыми для этого навыками и приёмами. Демонстрирует фрагментарные знания учебной литературы по дисциплине. Оценка по дисциплине выставляются обучающемуся с учётом результатов текущей и промежуточной аттестации. Компетенции на уровне «достаточный», закреплённые за дисциплиной, не сформированы.

5.3 Оценочные средства (материалы) для текущего контроля успеваемости, промежуточной аттестации обучающихся по дисциплине

Текущий контроль

Примерные задания для расчетно-графической работы (РГР) №1

1.1. Доказать, что нечетные числа вида $6n+1$ (1, 2, . . .) нельзя представить как разность простых чисел.

1.2. Найти все нечетные числа, представимые в виде разности простых чисел.

1.3. Доказать, что квадрат числа $N=3n+2$ (n=1, 2, . . .) не может быть представлен в виде суммы квадрата натурального числа и простого числа.

1.3. Доказать, что наименьший простой делитель составного числа *a* не превышает $\sqrt{a}$. Верна ли данная теорема в случае простого a?

1.3.1. При помощи теоремы предыдущей задачи выяснить, простыми или составными являются числа: 1) 127; 2) 919; 3) 7429.

1.4. Найти все простые числа между: 1) 100 и 110; 2) 190 и 200; 3) 200 и 220.

1.5. Доказать, что между натуральными числами *n* и $n!$, где $n>2$, содержится по крайней мере одно простое число. ,

1.6. Написать 12 последовательных составных натуральных чисел.

1.7. Доказать, что по модулю 4 множество всех простых чисел может быть разбито на два подмножества: на простые числа вида $4n+1$ и на простые числа вида $4n+2$.

1.8. Найти натуральные значения n, такие, чтобы числа n, $n+10$, $n+14$, все были простыми.

1.9. Найти простое число p, чтобы число $2p^2+1$ было также простым.

1.10. Найти такое простое число p, чтобы числа $4p^2+1$ и $6p^2$-|-1 оба были простыми.

1.11. Доказать, что указанные ниже числа одновременно простыми быть не могут: 1) p+5 и p+10; 2) p, $p+2$ и p+5; 3) 2^n+1, 2^n-1, где n>2.

1.12. Если числа p и $8p^2+1$ простые, то число $8p^2+2p+1$ также простое. Доказать.

1.13. Доказать, что 3, 5 и 7 являются единственной тройкой простых чисел-близнецов (т. е. тройкой простых 10 чисел, составляющих арифметическую прогрессию с разностью 2).

1.14. При помощи таблицы простых чисел найти наименьшее значение индекса n, при котором число вида $p_1 p_2 p_3 \ldots (p_n + 1)$, где p_i — простые числа, записанные в порядке возрастания (начиная с 2), есть число составное.

Примерные задания для расчетно-графической работы (РГР) №2

2.1. По какому модулю все целые числа сравнимы между собой?

2.2. Привести примеры целых чисел, сравнимых по модулю 8.

2.3. Привести примеры целых чисел, имеющих с модулем 6 один и тот же НОД, но не сравнимых по этому модулю.

2.4. Применить понятие сравнения к доказательству того, что числа 210 и 858 имеют с модулем 12 один и тот же НОД. Применим ли этот прием относительно чисел 385 и 77 и модуля 6?

2.5. Какие из следующих сравнений являются верными: 1) $1 \equiv -5 \pmod 6$; 2) $546 \equiv 0 \pmod{13}$; 3) $2^3 \equiv 1 \pmod 4$; 4) $3m \equiv -1 \pmod m$.

2.6. Доказать, что следующие сравнения являются верными- 1) $121 \equiv 13145 \pmod 2$; 2) $121347 \equiv 92817 \pmod{10}$; 3) $31 \equiv -9 \pmod{10}$; 4) $(m-1)^2 \equiv 1 \pmod m$, 5) $2m + 1 \equiv (m+1)^2 \pmod m$.

2.7. Доказать, что следующие сравнения являются неверными: 1) $5^{18i2} \equiv 1964 \pmod{25}$; 2) $7^{103} \equiv 3 \pmod{27}$; 3) $4^{1965} \equiv 25 \pmod{10}$;

4) $30 \sqcup 17 \equiv 81 \sqcup 19 \pmod 6$; 5) $(2n+1)(2m+1) \equiv 2k \pmod 6$, где n, m и k — числа целые.

2.8. Доказать, что каждое целое число сравнимо со своим остатком по данному модулю.

2.9. Число x удовлетворяет условию $x \equiv 2 \pmod{10}$. Записать это условие в виде уравнения с параметром и найти несколько значений x.

2.10. Найти все значения x, удовлетворяющие сравнениям: 1) $x \equiv 0 \pmod 3$; 2) $x \equiv 1 \pmod 2$.

2.11. Найти значения m, удовлетворяющие условию: 1) $20 \equiv 8 \pmod m$; 2) $3p+1 \equiv p+1 \pmod m$.

2.12. Указать возможные значения модуля в сравнении $x=5 \pmod m$, если известно, что этому сравнению удовлетворяет $x = 13$.

Примерные задания для контрольной работы

1) Доказать, что сравнимым по данному модулю значениям аргументов соответствуют сравнимые значения полинома $F(x, y, z)=ax^3 + bx^2y - cxyz - dz$ с целыми коэффициентами.

2) Если $3^n \equiv -1 \pmod{10}$, где n — число натуральное, то $3^{n+4} \equiv -1 \pmod{10}$. Доказать.

3) Доказать, что $2^{5n}-1 \vdots 31$, где n — число натуральное.

4) Доказать, что $1+3^x+9^x \vdots 13$, если $x=3n+1$ ($n = 0, 1, 2, \ldots$).

5) Доказать, что $(a+b)^p \equiv a^p + b^p \pmod p$.

6) Доказать, что $a^p \equiv b^p \pmod{p^{n+1}}$, если $a \equiv b \pmod{p^n}$

7) Доказать, что сравнения по одному и тому же модулю можно почленно делить, если части сравнения-делителя являются числами взаимно простыми с модулем. Вывести отсюда правило о делении частей сравнения на число, взаимно простое с модулем.

8) Доказать, что если $ax \equiv bx \pmod m$, то $a \equiv b \left(\mod \frac{m}{(x,m)} \right)$.

9) Исходя из $p—i \equiv —i \pmod p$ где i =l, 2,…n, доказать, что: 1) $C_{n+1}^n \equiv (—1)^n \pmod p$; 2) $C_{p-2}^n \equiv (-1)^n (n+1) \pmod p$.

Примерные темы рефератов, докладов

1. Построение множества действительных чисел, преодоление иррациональности в античные времена.
2. Функция Мебиуса.
3. Решето Эрастофена.
4. Диофантовы уравнения.
5. Функция Эйлера и её свойства.
6. Необходимые и достаточные условия целочисленных решений двух уравнений с тремя неизвестными с целыми коэффициентами.
7. Группы симметрии плоскости.
8. Группа симметрии икосаэдра.
9. История возникновения групп Галуа.
10. Теорема об изоморфизме групп.

Промежуточная аттестация (экзамен)

Примерные контрольные вопросы по курсу

I. Числовые системы.

1. Простые числа. Бесконечность множества простых чисел.
2. Каноническое разложение числа на простые множители.
3. НОД и НОК чисел.
4. Непрерывные дроби. Подходящие дроби и их свойства. Разность между двумя соседними подходящими дробями.

5. Подходящие дроби как наилучшее приближение действительных чисел
6. рациональными.
7. Квадратические иррациональности. Теорема Лагранжа.
8. Алгебраические и трансцендентные числа.

П. Теория сравнений.

1. Свойства сравнений.
2. Сравнения первой степени с одним неизвестным.
3. Системы сравнений.
4. Сравнения по простому модулю.
5. Сведение сравнений $f\{x) = 0(\text{mod}/\ p^n)$ к сравнению по модулю р.
6. Квадратичные вычеты. Символ Лежандра и его свойства.
7. Классы показателей по модулю т. Классы первообразных корней.
8. Первообразные корни по модулям *p, p", 2pa.*
9. Индексы. Их свойства. Приложения теории индексов.
10. Арифметические приложения теории.
11. Вычисление порядков элементов групп, классов сопряженных элементов. Нахождение подгрупп в группах, описание всех подгрупп циклических групп, применение теоремы о гомоморфизмах.
12. Нахождения делителей нуля и обратимых элементов в заданных кольцах вычетов. Применение теоремы о гомоморфизмах для алгебр и колец. Поиск минимальных многочленов.
13. Построение конечного поля заданного порядка с помощью неприводимых многочленов. Поиск порождающих элементов мультипликативной группы для заданных полей. Описание подполей заданного конечного поля.
14. Отношения толерантности. Конгруэнции на группах и кольцах. Примеры подпрямо неразложимых алгебр, групп и колец.
15. Свойства элементов решеток. Отношения толерантности. Конгруэнции на группах и кольцах. Примеры подпрямо неразложимых алгебр, групп и колец. Свойства операции дополнения. Вычисления в булевых решетках.
16. Вычисление общего члена и производящей функции. Оценка роста элементов последовательности. Вычисление распределений элементов.

6. Учебно-методическое и информационное обеспечение дисциплины

6.1 Список источников и литературы

Литература

Основная

1. Кострикин А. И. Введение в алгебру: учебник для студентов ун-тов, обучающихся по специальностям "Математика" и "Прикл. математика" / А. И. Кострикин. - М.: Наука, Физматлит, 2000. - Ч. 3 : Основные структуры алгебры. - 2000. - 271 с.

2. Сборник задач по алгебре: Учебник для вузов / Под ред. А. И. Кострикина. - Изд. 3-е, испр. и доп. - М.: Наука, Физматлит, 2001. - 463 с.

3. Проскуряков И В. Сборник задач по линейной алгебре : учеб. пособие для студентов физ.-мат. специальностей вузов / И. В. Проскуряков. - Изд. 8-е. - М. : Юнимедиастайл : Лаб. базовых знаний, 2002. - 382 с. - (Технический университет. Математика).

4. Боревич, З.И. Теория чисел / З.И. Боревич, И.Р. Шафаревич. - М.: Ленанд, 2019. - 504 с.

5. Босс, В. Лекции по математике: Теория чисел / В. Босс. - М.: Ленанд, 2019. - 224 с.

Дополнительная

1.Фаддеев Д.К. Задачи по высшей алгебре: учеб. пособие для студентов вузов, обучающихся по мат. специальностям / Д. К. Фаддеев, И. С. Соминский. - Изд. 17-е, стер. - СПб.; М.; Краснодар: Лань, 2008. - 287 с.

2. *Фоменко, Т. Н.* Высшая математика. Общая алгебра. Элементы тензорной алгебры : учебник и практикум для вузов / Т. Н. Фоменко. — Москва : Издательство Юрайт, 2024. — 121 с. — (Высшее образование). — ISBN 978-5-534-08097-1. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/539823

3. *Ларин, С. В.* Алгебра и теория чисел. Группы, кольца и поля : учебное пособие для вузов / С. В. Ларин. — 2-е изд., испр. и доп. — Москва : Издательство Юрайт, 2024. — 160 с. — (Высшее образование). — ISBN 978-5-534-05567-2. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/540008

6.2 Перечень ресурсов информационно-телекоммуникационной сети «Интернет».

1. А. П. Пожидаев, С. Р. Сверчков, И. П. Шестаков, Лекции по алгебре: В 2 ч.: Учеб. пособие / Новосиб. гос. ун-т. Новосибирск, 2011. 102 с. - http://www.math.nsc.ru/LBRT/a1/sotr/lections_1.pdf
2. Невский М.В. Лекции по алгебре : Учеб. пособие / Яросл. гос. ун-т. Ярославль, 2002. 265 с. - http://www.lib.uniyar.ac.ru/edocs/iuni/20020230.pdf

Национальная электронная библиотека (НЭБ) www.rusneb.ru
ELibrary.ru Научная электронная библиотека www.elibrary.ru

6.3 Профессиональные базы данных и информационно-справочные системы

Доступ к профессиональным базам данных: https://liber.rsuh.ru/ru/bases

Информационные справочные системы:
1. Консультант Плюс
2. Гарант

7. Материально-техническое обеспечение дисциплины

Для обеспечения дисциплины используется материально-техническая база образовательного учреждения: учебные аудитории, оснащённые доской, компьютером или ноутбуком, проектором (стационарным или переносным) для демонстрации учебных материалов.

Состав программного обеспечения:
1. Windows
2. Microsoft Office
3. Kaspersky Endpoint Security

8. Обеспечение образовательного процесса для лиц с ограниченными возможностями здоровья и инвалидов

В ходе реализации дисциплины используются следующие дополнительные методы обучения, текущего контроля успеваемости и промежуточной аттестации обучающихся в зависимости от их индивидуальных особенностей:

- для слепых и слабовидящих: лекции оформляются в виде электронного документа, доступного с помощью компьютера со специализированным программным обеспечением; письменные задания выполняются на компьютере со специализированным программным обеспечением или могут быть заменены устным ответом; обеспечивается индивидуальное равномерное освещение не менее 300 люкс; для выполнения задания при необходимости предоставляется увеличивающее устройство; возможно также использование собственных увеличивающих устройств; письменные задания оформляются увеличенным шрифтом; экзамен и зачёт проводятся в устной форме или выполняются в письменной форме на компьютере.
- для глухих и слабослышащих: лекции оформляются в виде электронного документа, либо предоставляется звукоусиливающая аппаратура индивидуального пользования; письменные задания выполняются на компьютере в письменной форме; экзамен и зачёт проводятся в письменной форме на компьютере; возможно проведение в форме тестирования.
- для лиц с нарушениями опорно-двигательного аппарата: лекции оформляются в виде электронного документа, доступного с помощью компьютера со специализированным программным обеспечением; письменные задания выполняются на компьютере со

специализированным программным обеспечением; экзамен и зачёт проводятся в устной форме или выполняются в письменной форме на компьютере.

При необходимости предусматривается увеличение времени для подготовки ответа.

Процедура проведения промежуточной аттестации для обучающихся устанавливается с учётом их индивидуальных психофизических особенностей. Промежуточная аттестация может проводиться в несколько этапов.

При проведении процедуры оценивания результатов обучения предусматривается использование технических средств, необходимых в связи с индивидуальными особенностями обучающихся. Эти средства могут быть предоставлены университетом, или могут использоваться собственные технические средства.

Проведение процедуры оценивания результатов обучения допускается с использованием дистанционных образовательных технологий.

Обеспечивается доступ к информационным и библиографическим ресурсам в сети Интернет для каждого обучающегося в формах, адаптированных к ограничениям их здоровья и восприятия информации:

- для слепых и слабовидящих: в печатной форме увеличенным шрифтом, в форме электронного документа, в форме аудиофайла.
- для глухих и слабослышащих: в печатной форме, в форме электронного документа.
- для обучающихся с нарушениями опорно-двигательного аппарата: в печатной форме, в форме электронного документа, в форме аудиофайла.

Учебные аудитории для всех видов контактной и самостоятельной работы, научная библиотека и иные помещения для обучения оснащены специальным оборудованием и учебными местами с техническими средствами обучения:

- для слепых и слабовидящих: устройством для сканирования и чтения с камерой SARA CE; дисплеем Брайля PAC Mate 20; принтером Брайля EmBraille ViewPlus;
- для глухих и слабослышащих: автоматизированным рабочим местом для людей с нарушением слуха и слабослышащих; акустический усилитель и колонки;
- для обучающихся с нарушениями опорно-двигательного аппарата: передвижными, регулируемыми эргономическими партами СИ-1; компьютерной техникой со специальным программным обеспечением.

9. Методические материалы

9.1 Планы практических занятий

Тема №1. Теоретико-множественные основания алгебры.

Цель занятия: познакомить слушателей с основными понятиями теории множеств.

Форма проведения – решение задач.

Примерные задачи для решения в аудитории:

задачи из книги [3, осн. лит.]:

Проскуряков И В. Сборник задач по линейной алгебре : учеб. пособие для студентов физ.-мат. специальностей вузов / И. В. Проскуряков. - Изд. 8-е. - М. : Юнимедиастайл : Лаб. базовых знаний, 2002. - 382 с. - (Технический университет. Математика).

№№: 123-128,139,145,167,169,178,161,536.

Контрольные вопросы: операции над множествами и их подмножествами, перестановки, рекуррентные соотношения, суммирования.

Тема №2. Элементы теории чисел.

Цель занятия: познакомить учащихся с элементами теории чисел.

Форма проведения – решение задач.

Примерные задачи для решения в аудитории:

задачи из книги [3, осн. лит.]:

Проскуряков И В. Сборник задач по линейной алгебре: учеб. пособие для студентов физ.-мат. специальностей вузов / И. В. Проскуряков. - Изд. 8-е. - М.: Юнимедиастайл: Лаб. базовых знаний, 2002. - 382 с. - (Технический университет. Математика).

№№: 1756,1760,1761, 1763,1766,1769, 1776.

Контрольные вопросы: деление с остатком, алгоритм Евклида, НОД и НОК, сравнения, полная система вычетов, приведенная система вычетов, первообразные корни и индексы, многочлены, корни многочленов.

Тема №3. Основы теории групп.

Цель занятий: основные понятия теории групп, примеры, типовые задачи.

Форма проведения – решение задач.

Примерные задачи для решения в аудитории:

задачи из [3, осн. лит.]:

Проскуряков И В. Сборник задач по линейной алгебре: учеб. пособие для студентов физ.-мат. специальностей вузов / И. В. Проскуряков. - Изд. 8-е. - М. : Юнимедиастайл : Лаб. базовых знаний, 2002. - 382 с. - (Технический университет. Математика).

№№: 1634, 1640,1645,1648,1655,1667,1674,1685,1689.

Контрольные вопросы: определение группы, свойства, отношение сопряженности, гомоморфизмы и нормальные подгруппы, абелевы групп: определение, примеры, порождающие элементы.

Тема №4. Основы теории колец.

Цель занятия: определение кольца, свойства, примеры колец, алгебры.

Форма проведения – решение задач.

Примерные задачи для решения в аудитории:

задачи из [3, осн. лит.]:

Проскуряков И В. Сборник задач по линейной алгебре учеб. пособие для студентов физ.-мат. специальностей вузов / И. В. Проскуряков. - Изд. 8-е. - М.: Юнимедиастайл: Лаб. базовых знаний, 2002. - 382 с. - (Технический университет. Математика).

№№: 1709-1718,1731,1732, 1735,1742, 1744,1747,1760.1777.

Контрольные вопросы: кольцо: определение, свойства, примеры, понятие алгебры, специальные классы алгебр.

Тема №5. Конечные поля.

Цель занятия: конечные поля: определение, примеры, применение.

Форма проведения – решение задач.

Примерные задачи для решения в аудитории:

задачи из книги [3, осн. лит.]:

Проскуряков И В. Сборник задач по линейной алгебре : учеб. пособие для студентов физ.-мат. специальностей вузов / И. В. Проскуряков. - Изд. 8-е. - М. : Юнимедиастайл : Лаб. базовых знаний, 2002. - 382 с. - (Технический университет. Математика).

№№ 1783,1784,1789,1794.

Контрольные вопросы: поля Галуа, основные примеры, свойства

Тема №6. Бинарные отношения и универсальные алгебры.

Цель занятия: определение отношения: свойства, примеры, модели кортежей, основные задачи, решаемые с помощью этих понятий.

Форма проведения – решение задач.

Примерные задачи для решения в аудитории:

задачи из книги [3, осн. лит.]:

Проскуряков И В. Сборник задач по линейной алгебре : учеб. пособие для студентов физ.-мат. специальностей вузов / И. В. Проскуряков. - Изд. 8-е. - М. : Юнимедиастайл : Лаб. базовых знаний, 2002. - 382 с. - (Технический университет. Математика).

№№ 1688, 1689,1691,1704.

Контрольные вопросы: что такое универсальная алгебра, как она связана с понятием отношение, что такое бинарное отношение и каковы его приложения в действительности?

Тема №7. Коммутативные кольца и поля.

Цель занятия: применение теории поля к криптографии, основные примеры, пропедевтика $p-$ адических чисел.

Форма проведения – решение задач.

Примерные задачи для решения в аудитории:

задачи из книги [3, осн. лит.]:

Проскуряков И В. Сборник задач по линейной алгебре : учеб. пособие для студентов физ.-мат. специальностей вузов / И. В. Проскуряков. - Изд. 8-е. - М. : Юнимедиастайл : Лаб. базовых знаний, 2002. - 382 с. - (Технический университет. Математика).

№№: 1774, 1776,1777, 1779, 1788.

Контрольные вопросы: что такое код, как он может быть связан с конечными полями, основные примеры коммутативных колец, понятие идеала, понятие примарного разложения.

Приложение 1. Аннотация
рабочей программы дисциплины

АННОТАЦИЯ РАБОЧЕЙ ПРОГРАММЫ ДИСЦИПЛИНЫ

Дисциплина «Общая алгебра и теория чисел» реализуется на факультете информационных систем и безопасности кафедрой фундаментальной и прикладной математики.

Цель дисциплины: ознакомить студентов с алгебраическими и теоретико-числовыми методами, используемыми в криптографии и теории кодирования, научить студентов владеть и применять эти методы.

Задачи: познакомить студентов с основными понятиями алгебры и теории чисел, показать современные приложения теории и научить решать стандартные прикладные задачи с помощью изученного материала.

Дисциплина направлена на формирование следующих компетенций:

ОПК-1. Способен применять знание фундаментальной математики и естественно-научных дисциплин при решении задач в области естественных наук и инженерной практике.

В результате освоения дисциплины обучающийся должен:

Знать: теоретический материал, использующий современные методы и результаты из общей алгебры и теории чисел, которые используются в теории кодирования, криптографии и смежных областях;

Уметь: решать задачи предлагаемого курса, пользоваться современными прикладными пакетами программ для решения предлагаемых в курсе специальных задач;

*Владеть**:*** навыками формализации классических алгебраических задач**,** а также иметь достаточно точное представление о прикладных возможностях этого курса.

По дисциплине предусмотрена промежуточная аттестация в форме экзамена.

Общая трудоемкость освоения дисциплины составляет 4 зачетные единицы.

Приложение 2

ЛИСТ ИЗМЕНЕНИЙ[1]

№	Текст актуализации или прилагаемый к РПД документ, содержащий изменения	Дата	№ протокола

[1] Для ОП ВО магистратуры изменения только за 2020 г.