Министерство науки и высшего образования Российской Федерации
НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ
ТОМСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ (НИ ТГУ)

Институт прикладной математики и компьютерных наук

УТВЕРЖДАЮ:
Директор
_____А. В. Замятин
« 19 » мая 20 22 г.

Рабочая программа дисциплины

**Общая алгебра**

по направлению подготовки / специальности

**10.05.01 Компьютерная безопасность**

Направленность (профиль) подготовки / специализация:
**Анализ безопасности компьютерных систем**

Форма обучения
**Очная**

Квалификация
**Специалист по защите информации**

Год приема
**2022**

Код дисциплины в учебном плане: Б1.О.02.08

СОГЛАСОВАНО:
Руководитель ОП
_____В.Н. Тренькаев

Председатель УМК
_____С.П. Сущенко

Томск – 2022

**1. Цель и планируемые результаты освоения дисциплины**

Целью освоения дисциплины является формирование следующих компетенций:

– ОПК-3 – Способен на основании совокупности математических методов разрабатывать, обосновывать и реализовывать процедуры решения задач профессиональной деятельности.

Результатами освоения дисциплины являются следующие индикаторы достижения компетенций:

ИОПК-3.1 Демонстрирует навыки выполнения стандартных действий, решения типовых задач, формулируемых в рамках базовых математических дисциплин.

ИОПК-3.2 Осуществляет применение основных понятий, фактов, концепций, принципов математики и информатики для решения задач профессиональной деятельности.

ИОПК-3.3 Выявляет научную сущность проблем, возникающих в ходе профессиональной деятельности, и применяет соответствующий математический аппарат для их формализации, анализа и выработки решения.

**2. Задачи освоения дисциплины**

Обучить студентов основным методам решения алгебраических задач, необходимых для изучения последующих курсов «комбинаторика», «теория кодирования», «теоретико-числовые методы в криптографии».

**3. Место дисциплины в структуре образовательной программы**

Дисциплина относится к обязательной части образовательной программы. Дисциплина входит в модуль «Математика».

**4. Семестр(ы) освоения и форма(ы) промежуточной аттестации по дисциплине**

Первый семестр, зачет
Второй семестр, зачет с оценкой
Третий семестр, зачет с оценкой
Четвертый семестр, экзамен

**5. Входные требования для освоения дисциплины**

Для успешного освоения дисциплины требуются компетенции, сформированные в ходе освоения образовательных программ предшествующего уровня образования.

**6. Язык реализации**

Русский

**7. Объем дисциплины**

Общая трудоемкость дисциплины составляет 16 з.е., 576 часов, из которых:
-лекции: 176 ч.
-практические занятия: 160 ч.
Объем самостоятельной работы студента определен учебным планом.

**8. Содержание дисциплины, структурированное по темам**

**Тема 1. Основные алгебраические структуры. Линейная алгебра.**

Основные алгебраические структуры.

Матрицы и определители. Линейная зависимость векторов. Системы линейных уравнений. Линейные операторы.

**Тема 2. Элементы теории множеств и комбинаторики.**

Элементы теории множеств. Счётные, несчётные множества, мощность. Теорема Кантора-Бернштейна. Операции над мощностями. Упорядоченные множества.

Элементы комбинаторики. Биномиальные коэффициенты, перестановки, размещения, сочетания. Субфакториал. Числа Стирлинга, числа Белла.

**Тема 3. Числовые системы.**

Деление с остатком. Алгоритм Евклида и расширенный алгоритм Евклида. Коэффициенты Безу. Решение систем сравнений.

Комплексные числа, действия над ними. Формула Муавра.

**Тема 4. Многочлены**

Многочлены над полем. Алгоритм Евклида. Коэффициенты Безу.

Корни многочленов. Теорема Безу, схема Горнера. Методы интерполяции. Метод Кронекера разложение в произведение неприводимых.

**Тема 5. Теория групп**

Основы теории групп. Основные свойства операций. Циклическая группа. Нормальная подгруппа, факторгруппа. Гомоморфизмы групп, прямые произведения групп.

Полупрямые произведения. Голоморф. Действие группы на множестве. Нильпотентные и разрешимые группы. Теоремы Силова.

**Тема 6. Теория колец и полей**

Основные свойства операций в кольце. Идеал, факторкольцо. Прямые суммы и произведения. Китайская теорема об остатках. Теория делимости вобласти целостности. Область главных идеалов. Теорема Гильберта о базисе.

Теория полей. Основные операции. Расширение поля. Конечные поля, характеристика, порядок. Модуль над кольцом с единицей. Подмодуль, фактормодуль. Основная теорема о конечно порождённых абелевых группах.

**9. Текущий контроль по дисциплине**

Текущий контроль по дисциплине проводится путем контроля посещаемости, проведения контрольных работ и фиксируется в форме контрольной точки не менее одного раза в семестр.

**10. Порядок проведения и критерии оценивания промежуточной аттестации**

Прохождение промежуточной аттестации по дисциплине «общая алгебра» проводится в форме зачёта в 1 семестре (на основании выполненных контрольных заданий), в форме зачёта с оценкой во 2 и 3 семестрах (учитывается выполнение контрольных работ, но допускается и проведение теоретического зачёта по билетам, влияющего на часть оценки), в форме экзамена в 4 семестре.

Результаты зачета с оценкой определяются оценками «отлично», «хорошо», «удовлетворительно», «неудовлетворительно».

Первая часть представляет собой тест из 3 вопросов, проверяющих ИУК-1.1. Ответы на вопросы первой части даются путем выбора из списка предложенных.

Вторая часть содержит один вопрос, проверяющий ИОПК-2.2. Ответ на вопрос второй части дается в развернутой форме.

Третья часть содержит 2 вопроса, проверяющих ИПК-3.3 и оформленные в виде практических задач. Ответы на вопросы третьей части предполагают решение задач и краткую интерпретацию полученных результатов.

Примерный перечень теоретических вопросов

***Кольца и поля***

Определение кольца; теорема об основных соотношениях в кольце.

Кольцо многочленов.

Определение поля; 2 примера поля.

Кольцо классов вычетов по идеалу.

Понятие делимости и алгоритм деления Евклида для целых чисел.

Кольцо классов вычетов целых чисел; доказать, что совокупность целых чисел образует идеал тогда и только тогда, когда она состоит из всех чисел, кратных некоторому целому числу.

Кольцо классов вычетов целых чисел.

Кольцо классов вычетов целых чисел. Простые поля Галуа.

Полная и приведенная система вычетов (с примерами).

Функция Эйлера. Теорема о мультипликативности функции Эйлера.

Системы сравнений. Китайская теорема об остатках.

Многочлены над полем: нормированный многочлен, неприводимый многочлен, теорема деления для многочленов, алгоритм деления Евклида для многочленов.

Теорема Безу (с доказательством).

Идеал в кольце многочленов; сформулировать три теоремы для кольца многочленов, аналогичные теоремам для идеала в кольце целых чисел. Определения расширения и характеристики поля Галуа.

Доказать, что в поле характеристики $p$ имеет место равенство $(a + b)^p = a^p + b^p$.

Минимальная функция; 2 теоремы о свойствах минимальной функции (с доказательством).

Определение системы линейных уравнений над полем; совместные и несовместные системы; однородные и неоднородные системы.

Примитивный элемент в поле Галуа. Дискретное логарифмирование в полях Галуа.

Метод решения однородной системы линейных уравнений над полем.

Примеры задач:

**1 семестр (зачёт)**

1. Решить систему уравнений в поле вычетов $Z_5$ $\begin{cases} \overline{4}\bar{x} + \overline{3}\bar{y} = \overline{1} \\ \overline{2}\bar{x} + \overline{1}\bar{y} = \overline{3} \end{cases}$

2. Дана подстановка. Найти: число инверсий, разложение в произведение циклов, декремент.

1 2 3 4 5 6

3 6 4 5 2 1

3. $A=\begin{pmatrix}1 & 2 & 5\\ 0 & 1 & 1\end{pmatrix}, B=\begin{pmatrix}1 & 4\\ 1 & 1\\ 3 & 1\end{pmatrix}$ Найти $AB, BA$.

4. Найти параметр c, при котором $\begin{vmatrix}1 & 2 & c\\ 0 & 1 & 1\\ 1 & 3 & 2\end{vmatrix}=-3$

5. Найти обратную матрицу $\begin{pmatrix}3 & 0 & 0\\ 1 & 1 & 0\\ 1 & 1 & 2\end{pmatrix}^{-1}$

6. Найти параметр $a$, такой, что ранг матрицы $\begin{pmatrix}1 & 1 & 0 & 4\\ 1 & 2 & 2 & 1\\ 3 & 4 & 2 & a\end{pmatrix}$ равен 2.

7. Решить систему уравнений. $\begin{cases}x_1 + x_2 + 2x_3 = 9\\ 3x_1 + 6x_2 + 10x_3 = 45\\ x_1 + 7x_2 + 12x_3 = 51\end{cases}$

8. Решить однородную систему уравнений, построить ФСР.

$$\begin{cases}x_1 + x_2 + 2x_3 + x_4 = 0\\ 3x_1 + 6x_2 + 10x_3 + 4x_4 = 0\\ 4x_1 + 7x_2 + 12x_3 + 5x_4 = 0\end{cases}$$

**2 семестр (зачёт с оценкой).**

1. Векторы a,b выражены через p,q: $a=p+2q$, $b=4p+3q$. $|p|=2, |q|=1$, угол между ними 60 градусов. Найти $(a,b)$.

2. Найти собственные числа и векторы для линейного оператора, заданного матрицей $\begin{pmatrix}2 & 0 & 0\\ 1 & 3 & 2\\ 0 & 2 & 3\end{pmatrix}$

3. Найти d = НОД (a,b) и разложение d = au+bv для двух чисел: 150 и 84. 4. Найти НОК двух чисел: 150 и 84.

5. Найти функцию Эйлера для числа 21.

6. Найти остаток от деления $5^{1202}$ на 13

7. Найти остаток от деления 8559 на 11

8. Найти наименьшее натуральное число, удовлетворяющее системе сравнений: $\begin{cases} x \equiv 1(3) \\ x \equiv 2(5) \\ x \equiv 1(7) \end{cases}$

9. Умножить $(2+i)(1+2i)$

10. Вычислить $\dfrac{-6+4i}{2+3i}$

11. Вычислить $\left(1+i\sqrt{3}\right)^6$

12. Дано универсальное множество $U=\{1,2,3,4,5,6,7\}$ и множества: $A=\{2,4,6,7\}$, $B=\{1,2,6\}$, $C=\{1,3,4,5\}$. Найти $(A\cup B)\cap C$.

13. Есть 3 множества по 10 элементов, пересечение каждой пары содержит 3 элемента. Пересечение всех трёх - один элемент. Сколько всего элементов в объединении трёх множеств?

14. Поделить с помощью схемы Горнера в поле R: $f(x)=x^3+2x^2+8x+12$ на $g(x)=x-3$

15. Поделить с помощью схемы Горнера в поле $Z_5$: $f(x)=x^3+2x^2+3x+4$ на $g(x)=x+3$

16. Найти НОД двух многочленов $f(x)=x^3+11x^2+34x+24$, $g(x)=x^2+8x+12$.

17. Найти НОД и коэффициенты Безу для $f(x)=x^3+6x^2+13x+10$, $g(x)=x^2+5x+7$.

18. Устраните иррациональность в знаменателе дроби $\dfrac{1}{g(x)}=\dfrac{1}{x^2+5x+7}$, если $f(x)=x^3+6x^2+13x+10=0$.

19. Найти многочлен 3-й степени с помощью интерполяции, если
$f(-1)=3,\quad f(0)=3,\quad f(1)=7,\quad f(2)=21$.

(метод неопределённых коэффициентов либо Лагранжа).

20 .Выполните разложение $f(x)=x^4+5x^3+9x^2+7x+2$ на неприводимые многочлены с помощью метода Кронекера.

21. Найдите кратные корни и выполните разложение на неприводимые многочлены в поле R с помощью НОД многочлена и его производной (либо с помощью матрицы Сильвестра):
$f(x)=x^3-4x^2+5x-2$.

22. Найти результант двух многочленов с помощью определителя Сильвестра $f(x) = x^2 + x + 5$ $g(x) = x^2 + 2$

23. При каком минимально возможном натуральном параметре C многочлен $f(x) = x^3 + Cx^2 + 21x + 21$ неприводим над полем Q согласно признаку Эйзенштейна?

24. Сколько есть способов выбрать 2 объекта из 5 (без учёта порядка)?

25. Есть большое множество шаров 3 разных цветов. Сколько есть различных способов составить наборы из 6 шаров, где k одного цвета, m второго n третьего, k+m+n=6.

26. Есть 6 шаров: 4 белых, 1 красный, 1 чёрный. Сколько способов расположить их по порядку, если шары одного цвета можно не различать?

Результаты экзамена определяются оценками «отлично», «хорошо», «удовлетворительно», «неудовлетворительно».

## 11. Учебно-методическое обеспечение

а) Электронный учебный курс по дисциплине в электронном университете «Moodle» - https://moodle.tsu.ru/course/view.php?id=5439
https://moodle.tsu.ru/course/view.php?id=5440

б) Оценочные материалы текущего контроля и промежуточной аттестации по дисциплине (Приложение 1).

## 12. Перечень учебной литературы и ресурсов сети Интернет

| | | | | |
|---|---|---|---|---|
| Основная литература | | | | |
| 1. | Глухов М.М, Елизаров В.П, Нечаев А.А. | Алгебра | Лань | 2015, 608 с. |
| 2. | Кострикин А.И. | Введение в алгебру (в 3 томах) | Лань | 2012, 368 с. |
| Дополнительная литература | | | | |
| 3. | Курош А.Г. | Курс высшей алгебры | Лань | 2022, 432 с. |
| 4. | Фаддеев Д.К. | Лекции по алгебре | Лань | 2007, 416 с. |

## 13. Перечень информационных технологий

а) лицензионное и свободно распространяемое программное обеспечение:
MS Windows; MS Office.

б) информационные справочные системы:
– Электронный каталог Научной библиотеки ТГУ – http://chamo.lib.tsu.ru/search/query?locale=ru&theme=system
– Электронная библиотека (репозиторий) ТГУ – http://vital.lib.tsu.ru/vital/access/manager/Index
– ЭБС Лань – http://e.lanbook.com/
– ЭБС Консультант студента – http://www.studentlibrary.ru/

## 14. Материально-техническое обеспечение

Аудитории для проведения занятий лекционного типа.

Аудитории для проведения занятий семинарского типа, индивидуальных и групповых консультаций, текущего контроля и промежуточной аттестации.

Помещения для самостоятельной работы, оснащенные компьютерной техникой и доступом к сети Интернет, в электронную информационно-образовательную среду и к информационным справочным системам.

## 15. Информация о разработчиках

Приходовский Михаил Анатольевич, доцент кафедры компьютерной безопасности ТГУ.
Шерстнёва Анна Игоревна, доцент кафедры компьютерной безопасности ТГУ.