

МИНИСТЕРСТВО ТРАНСПОРТА РОССИЙСКОЙ ФЕДЕРАЦИИ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ
УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«РОССИЙСКИЙ УНИВЕРСИТЕТ ТРАНСПОРТА»
(РУТ (МИИТ))



Рабочая программа дисциплины (модуля),
как компонент образовательной программы
базового высшего образования
по специальности
10.05.01 Компьютерная безопасность,
утвержденной первым проректором ФГАОУ ВО
РУТ (МИИТ) Тимониным В.С.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)

Линейная алгебра

Специальность: 10.05.01 Компьютерная безопасность

Специализация: Безопасность компьютерных систем и сетей
(в сфере связи, информационных и
коммуникационных технологий)

Форма обучения: Очная

Рабочая программа дисциплины (модуля) в виде
электронного документа выгружена из единой
корпоративной информационной системы управления
университетом и соответствует оригиналу

Простая электронная подпись, выданная ФГАОУ ВО РУТ
(МИИТ)

ID подписи: 1343395

Подписал: И.о. заведующего кафедрой Тищенко Сергей
Александрович

Дата: 01.09.2026

1. Общие сведения о дисциплине (модуле).

Целью освоения дисциплины (модуля) является:

- формирование фундаментальной математической базы: системное понимание алгебраических структур и теоретико-числовых методов, которые лежат в основе современных информационных технологий;
- развитие алгоритмического мышления и навыков формализации задач: научить переводить практические задачи (например, из области криптографии или оптимизации) на язык математики, а затем — в эффективный программный код;
- подготовка к изучению и применению специализированных ИТ-дисциплин: создать прочный фундамент для дальнейшего освоения таких областей, как криптография, информационная безопасность, машинное обучение, теория кодирования и проектирование баз данных, где глубокие знания алгебры и теории чисел являются обязательными.

Задачами освоения дисциплины (модуля) являются:

- освоение ключевых понятий алгебры: изучение базовых алгебраических структур: группы, кольца, поля;
- освоение теории чисел: делимость, алгоритм Евклида, сравнения по модулю, малая теорема Ферма и теорема Эйлера;
- изучение и программная реализация алгоритмов с применением теории чисел;
- применение полученных знаний для решения прикладных ИТ-задач;
- использование элементов линейной алгебры (векторы, матрицы) для решения систем линейных уравнений, что является основой для многих алгоритмов в машинном обучении и компьютерной графике.

2. Планируемые результаты обучения по дисциплине (модулю).

Перечень формируемых результатов освоения образовательной программы (компетенций) в результате обучения по дисциплине (модулю):

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

Обучение по дисциплине (модулю) предполагает, что по его результатам обучающийся будет:

Знать:

- способы решения систем линейных алгебраических уравнений;

- понятие группы, кольца, поля; свойства операций, примеры конечных полей (в частности, поле Галуа);

- делимость целых чисел, алгоритм Евклида для нахождения НОД, основная теорема арифметики, свойства сравнений по модулю, малая теорема Ферма и теорема Эйлера.

и их применение.

Уметь:

- реализовывать и использовать ключевые алгоритмы, такие как алгоритм Евклида, быстрое возведение в степень по модулю и решето Эратосфена;

- переводить практические проблемы из области защиты информации или анализа данных на язык математических моделей;

- понимать принципы работы асимметричных криптосистем и цифровых подписей.

Владеть:

- понятиями и теоремами теории чисел, комбинаторики, теории графов, а также базовыми алгебраическими структурами: группами, кольцами и полями;

- навыками модульной арифметики, свободно оперировать понятием сравнения по модулю, выполнять все арифметические действия в кольцах вычетов $\mathbb{Z}_n$.

- инструментами формальной логики и доказательства.

3. Содержание дисциплины (модуля).

3. Объем дисциплины (модуля).

3.1. Общая трудоемкость дисциплины (модуля).

Общая трудоемкость дисциплины (модуля) составляет 3 з.е. (108 академических часа(ов)).

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

Тип учебных занятий	Количество часов	
	Всего	Семестр №2
Контактная работа при проведении учебных занятий (всего):	48	48
В том числе:		
Занятия лекционного типа	32	32

Занятия семинарского типа	16	16
---------------------------	----	----

3.3. Объем дисциплины (модуля) в форме самостоятельной работы обучающихся, а также в форме контактной работы обучающихся с педагогическими работниками и (или) лицами, привлекаемыми к реализации образовательной программы на иных условиях, при проведении промежуточной аттестации составляет 60 академических часа (ов).

3.4. При обучении по индивидуальному учебному плану, в том числе при ускоренном обучении, объем дисциплины (модуля) может быть реализован полностью в форме самостоятельной работы обучающихся, а также в форме контактной работы обучающихся с педагогическими работниками и (или) лицами, привлекаемыми к реализации образовательной программы на иных условиях, при проведении промежуточной аттестации.

4. Содержание дисциплины (модуля).

4.1. Занятия лекционного типа.

№ п/п	Тематика лекционных занятий / краткое содержание
1	Матрицы. Обратная матрица. Ранг матрицы. Рассматриваемые вопросы: - определение обратной матрицы; - необходимое условие существования обратной матрицы; - способ нахождения обратной матрицы с помощью алгебраических дополнений и присоединенной матрицы; - элементарные преобразования строк; - нахождение ранга матрицы с помощью элементарных преобразований; - вычисление обратной матрицы с помощью элементарных преобразований - понятие ранга матрицы.
2	Система линейных алгебраических уравнений. Методы Крамера и обратной матрицы для решения СЛАУ. Рассматриваемые вопросы: - основные понятия: определение СЛАУ, решение СЛАУ, эквивалентные системы, запись в матричной форме; - метод Крамера; - метод обратной матрицы; - матричные уравнения.
3	Метод Гаусса для решения СЛАУ. Рассматриваемые вопросы: - теорема Кронекера – Капелли;

№ п/п	Тематика лекционных занятий / краткое содержание
	- метод Гаусса для систем размерности $n \times n$; - метод Гаусса для систем размерности $n \times m$.
4	Отношение делимости в кольце целых чисел. Рассматриваемые вопросы: - определение и базовые свойства; - делимость суммы и произведения; свойства делимости для линейных комбинаций; - простые и составные числа; основная теорема о делимости.
5	Деление с остатком. Рассматриваемые вопросы: - формулировка теоремы о делении с остатком; - алгоритм Евклида, нахождение НОД и НОК двух чисел, взаимно простые числа; - линейное представление НОД (тождество Безу).
6	Основная теорема арифметики. Рассматриваемые вопросы: - простые и составные числа; - существование и единственность разложения; - канонический вид числа и следствия.
7	Отношение сравнимости. М-арифметики. Рассматриваемые вопросы: - основные понятия; - свойства сравнений; - функция Эйлера, теорема Эйлера; - малая теорема Ферма.
8	Алгебраические операции. Группы. Подгруппа. Рассматриваемые вопросы: - понятие алгебраической операции на множестве, виды. - определение группы; примеры групп; - подгруппы. Циклические группы и порождающие элементы.
9	Группы преобразований. Подстановки. Рассматриваемые вопросы: - определение группы, примеры групп; - группа биективных отображений множества на себя, связь с симметриями геометрических фигур; - понятие подстановки; - разложение произвольной подстановки в произведение независимых циклов и транспозиций; - четность подстановок, знакопеременная подгруппа.
10	Циклические группы. Свойства. Рассматриваемые вопросы: - определение порождающего элемента группы; - порядок элемента группы, связь порядка элемента с порядком порожденной им циклической подгруппы; - теорема Лагранжа; - классификация всех подгрупп циклической группы.
11	Гомоморфизм групп. Факторгруппы. Рассматриваемые вопросы: - определение гомоморфизма групп и его ядра, изоморфизмы и автоморфизмы; - основная теорема о гомоморфизме; - нормальные подгруппы, построение факторгруппы как множества смежных классов.

№ п/п	Тематика лекционных занятий / краткое содержание
12	Кольцо. Идеал. Рассматриваемые вопросы: - определение кольца; примеры колец; - кольцо вычетов по модулю n; - определение идеала кольца, главные идеалы; - понятие факторалгебры (факторкольца) по идеалу.
13	Поле. Рассматриваемые вопросы: - определение поля; характеристика поля; - простое поле характеристики 0 и простое поле характеристики p (конечное поле); - расширения полей.
14	Кольцо многочленов над полем. Рассматриваемые вопросы: - определение кольца многочленов от одной переменной над полем; - деление с остатком в кольце многочленов; НОД двух многочленов и алгоритм Евклида. - корни многочленов, теорема Безу, связь между корнями многочлена и его линейными множителями.
15	Отношение делимости. Неприводимые многочлены. Рассматриваемые вопросы: - делимость в кольце многочленов; - определение неприводимого и приводимого многочлена; - критерий Эйзенштейна; - основная теорема арифметики для многочленов.
16	Обзорная лекция. Рассматриваемые вопросы: - иерархия алгебраических структур: от групп до полей; - понятие изоморфизма: когда структура важнее носителя; - алгебраические структуры как фундамент современных IT-технологий.

4.2. Занятия семинарского типа.

Практические занятия

№ п/п	Тематика практических занятий/краткое содержание
1	Матрицы. Обратная матрица. Ранг матрицы. В результате практического занятия студент сможет находить обратную матрицу с помощью алгебраических дополнений и присоединенной матрицы, с помощью элементарных преобразований, решать СЛАУ методом обратной матрицы.
2	Метод Гаусса для решения СЛАУ. В результате практического занятия студент сможет исследовать СЛАУ и решать её методом Гаусса.
3	Отношение делимости в кольце целых чисел. В результате практического занятия студент научится находить НОД двух или более чисел с помощью алгоритма Евклида, сможет использовать расширенный алгоритм Евклида для представления НОД в виде линейной комбинации исходных чисел.
4	Основная теорема арифметики. Отношение сравнения. В результате практического занятия студент будет понимать, что любое натуральное число больше 1 можно единственным образом представить в виде произведения простых чисел; научится выполнять базовые операции со сравнениями и решать простейшие линейные сравнения.

№ п/п	Тематика практических занятий/краткое содержание
5	Группа. Подгруппа. Группа преобразований. Подстановки. В результате практического занятия студент научится определять, является ли заданное множество с операцией группой, научится находить подгруппы в известных группах, научится описывать симметрии геометрических фигур с помощью теории групп, будет иметь представление, что множество всех подстановок является ключевой моделью для изучения конечных групп.
6	Циклические группы. Гомоморфизм групп. Факторгруппа. В результате практического занятия студент сможет определять и конструировать циклические группы, будет иметь представление о связи трёх понятий: гомоморфизм, ядро и образ.
7	Кольцо. Поле. Идеал. В результате практического занятия студент сможет проверять выполнение аксиом кольца на заданном множестве, отличать коммутативные кольца от некоммутативных, выделять кольца с единицей, сможет доказывать является ли данное множество полем.
8	Кольцо многочленов. В результате практического занятия студент сможет применять алгоритм Евклида для нахождения НОД двух многочленов, использовать алгоритм для представления НОД в виде линейной комбинации исходных многочленов (тождество Безу), проверять многочлены на взаимную простоту, разлагать многочлены на неприводимые множители, применять теорему Безу и следствия из неё.

4.3. Самостоятельная работа обучающихся.

№ п/п	Вид самостоятельной работы
1	Работа с лекционным материалом.
2	Работа с литературой.
3	Текущая подготовка к занятиям.
4	Подготовка к промежуточной аттестации.
5	Подготовка к текущему контролю.

5. Перечень изданий, которые рекомендуется использовать при освоении дисциплины (модуля).

№ п/п	Библиографическое описание	Место доступа
1	Горлач Б. А. Линейная алгебра. Издательство "Лань", 2022, - 480 с. Учебное пособие для вузов. ISBN 978-5-8114-1427-7— Текст: электронный / Лань : электронно-библиотечная система.	https://reader.lanbook.com/book/210983
2	Туганбаев А. А. Основы высшей математики»: учебное пособие для вузов / А. А. Туганбаев. — 2-е изд., стер. — Санкт-Петербург : Лань, 2026. — ISBN 978-5-507-	https://reader.lanbook.com/book/513621

	56099-8. — Текст: электронный/ Лань : электронно-библиотечная система.	
3	Курош А. Г. Курс высшей алгебры: учебник для вузов / А. Г. Курош. — 27-е изд., стер. — Санкт-Петербург : Лань, 2026. — ISBN 978-5-507-54342-7. — Текст : электронный // Лань : электронно-библиотечная система. — Режим доступа: для авториз. пользователей. — С. 83.	https://e.lanbook.com/book/507517
4	Проскураков, И. В. Сборник задач по линейной алгебре : учебное пособие для вузов. — 18-е изд., стер. — Санкт-Петербург : Лань, 2026. — ISBN 978-5-507-54308-3. — Текст : электронный // Лань : электронно-библиотечная система. — Режим доступа: для авториз. пользователей. — С. 1.	https://e.lanbook.com/book/507388
5	Глухов, М. М. Алгебра : учебник для вузов / М. М. Глухов, В. П. Елизаров, А. А. Нечаев. — 7-е изд., стер. — Санкт-Петербург : Лань, 2026. — ISBN 978-5-507-56965-6. — Текст : электронный // Лань : электронно-библиотечная система. — Режим доступа: для авториз. пользователей.	https://e.lanbook.com/book/522111
6	Тропин, М. П. Теория чисел / М. П. Тропин. — 2-е изд., стер. — Санкт-Петербург : Лань, 2023. — ISBN 978-5-507-45436-5. — Текст : электронный // Лань : электронно-библиотечная система. — Режим доступа: для авториз. пользователей. 2023	https://e.lanbook.com/book/269906

6. Перечень современных профессиональных баз данных и информационных справочных систем, которые могут использоваться при освоении дисциплины (модуля).

- Научно-техническая библиотека РУТ (МИИТ) (<http://library.miit.ru>);
- Информационный портал Научная электронная библиотека eLIBRARY.RU (www.elibrary.ru);
- Образовательная платформа «Юрайт» (<https://urait.ru/>);
- Электронно-библиотечная система издательства «Лань» (<http://e.lanbook.com/>);
- Интернет-университет информационных технологий (<http://www.intuit.ru/>).

7. Перечень лицензионного и свободно распространяемого программного обеспечения, в том числе отечественного производства, необходимого для освоения дисциплины (модуля).

Операционная система Windows;

Microsoft Office;

MS Teams;

Поисковые системы.

.

8. Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине (модулю).

Учебные аудитории для проведения учебных занятий, оснащенные компьютерной техникой и наборами демонстрационного оборудования.

9. Форма промежуточной аттестации:

Зачет во 2 семестре.

10. Оценочные материалы.

Оценочные материалы, применяемые при проведении промежуточной аттестации, разрабатываются в соответствии с локальным нормативным актом РУТ (МИИТ).

Авторы:

Е.В. Родина

Согласовано:

Заведующий кафедрой ВССиИБ

Б.В. Желенков

и.о. заведующего кафедрой ММСС

С.А. Тищенко

Председатель учебно-методической
комиссии

Н.А. Андриянова