

**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.

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

| №<br>п/п | Тематика лекционных занятий / краткое содержание                                                                                                                                                                                                                                                                                                                                                                                                                     |
|----------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|          | <ul style="list-style-type: none"> <li>- метод Гаусса для систем размерности <math>n \times n</math>;</li> <li>- метод Гаусса для систем размерности <math>n \times m</math>.</li> </ul>                                                                                                                                                                                                                                                                             |
| 4        | <p>Отношение делимости в кольце целых чисел.</p> <p>Рассматриваемые вопросы:</p> <ul style="list-style-type: none"> <li>- определение и базовые свойства;</li> <li>- делимость суммы и произведения; свойства делимости для линейных комбинаций;</li> <li>- простые и составные числа; основная теорема о делимости.</li> </ul>                                                                                                                                      |
| 5        | <p>Деление с остатком.</p> <p>Рассматриваемые вопросы:</p> <ul style="list-style-type: none"> <li>- формулировка теоремы о делении с остатком;</li> <li>- алгоритм Евклида, нахождение НОД и НОК двух чисел, взаимно простые числа;</li> <li>- линейное представление НОД (тождество Безу).</li> </ul>                                                                                                                                                               |
| 6        | <p>Основная теорема арифметики.</p> <p>Рассматриваемые вопросы:</p> <ul style="list-style-type: none"> <li>- простые и составные числа;</li> <li>- существование и единственность разложения;</li> <li>- канонический вид числа и следствия.</li> </ul>                                                                                                                                                                                                              |
| 7        | <p>Отношение сравнимости. М-арифметики.</p> <p>Рассматриваемые вопросы:</p> <ul style="list-style-type: none"> <li>- основные понятия;</li> <li>- свойства сравнений;</li> <li>- функция Эйлера, теорема Эйлера;</li> <li>- малая теорема Ферма.</li> </ul>                                                                                                                                                                                                          |
| 8        | <p>Алгебраические операции. Группы. Подгруппа.</p> <p>Рассматриваемые вопросы:</p> <ul style="list-style-type: none"> <li>- понятие алгебраической операции на множестве, виды.</li> <li>- определение группы; примеры групп;</li> <li>- подгруппы. Циклические группы и порождающие элементы.</li> </ul>                                                                                                                                                            |
| 9        | <p>Группы преобразований. Подстановки.</p> <p>Рассматриваемые вопросы:</p> <ul style="list-style-type: none"> <li>- определение группы, примеры групп;</li> <li>- группа биективных отображений множества на себя, связь с симметриями геометрических фигур;</li> <li>- понятие подстановки;</li> <li>- разложение произвольной подстановки в произведение независимых циклов и транспозиций;</li> <li>- четность подстановок, знакопеременная подгруппа.</li> </ul> |
| 10       | <p>Циклические группы. Свойства.</p> <p>Рассматриваемые вопросы:</p> <ul style="list-style-type: none"> <li>- определение порождающего элемента группы;</li> <li>- порядок элемента группы, связь порядка элемента с порядком порожденной им циклической подгруппы;</li> <li>- теорема Лагранжа;</li> <li>- классификация всех подгрупп циклической группы.</li> </ul>                                                                                               |
| 11       | <p>Гомоморфизм групп. Факторгруппы.</p> <p>Рассматриваемые вопросы:</p> <ul style="list-style-type: none"> <li>- определение гомоморфизма групп и его ядра, изоморфизмы и автоморфизмы;</li> <li>- основная теорема о гомоморфизме;</li> <li>- нормальные подгруппы, построение факторгруппы как множества смежных классов.</li> </ul>                                                                                                                               |

| №<br>п/п | Тематика лекционных занятий / краткое содержание                                                                                                                                                                                                                                                                                                                                            |
|----------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 12       | <p>Кольцо. Идеал.</p> <p>Рассматриваемые вопросы:</p> <ul style="list-style-type: none"> <li>- определение кольца; примеры колец;</li> <li>- кольцо вычетов по модулю <math>n</math>;</li> <li>- определение идеала кольца, главные идеалы;</li> <li>- понятие факторалгебры (факторкольца) по идеалу.</li> </ul>                                                                           |
| 13       | <p>Поле.</p> <p>Рассматриваемые вопросы:</p> <ul style="list-style-type: none"> <li>- определение поля; характеристика поля;</li> <li>- простое поле характеристики 0 и простое поле характеристики <math>p</math> (конечное поле);</li> <li>- расширения полей.</li> </ul>                                                                                                                 |
| 14       | <p>Кольцо многочленов над полем.</p> <p>Рассматриваемые вопросы:</p> <ul style="list-style-type: none"> <li>- определение кольца многочленов от одной переменной над полем;</li> <li>- деление с остатком в кольце многочленов; НОД двух многочленов и алгоритм Евклида.</li> <li>- корни многочленов, теорема Безу, связь между корнями многочлена и его линейными множителями.</li> </ul> |
| 15       | <p>Отношение делимости. Неприводимые многочлены.</p> <p>Рассматриваемые вопросы:</p> <ul style="list-style-type: none"> <li>- делимость в кольце многочленов;</li> <li>- определение неприводимого и приводимого многочлена;</li> <li>- критерий Эйзенштейна;</li> <li>- основная теорема арифметики для многочленов.</li> </ul>                                                            |
| 16       | <p>Обзорная лекция.</p> <p>Рассматриваемые вопросы:</p> <ul style="list-style-type: none"> <li>- иерархия алгебраических структур: от групп до полей;</li> <li>- понятие изоморфизма: когда структура важнее носителя;</li> <li>- алгебраические структуры как фундамент современных IT-технологий.</li> </ul>                                                                              |

## 4.2. Занятия семинарского типа.

### Практические занятия

| №<br>п/п | Тематика практических занятий/краткое содержание                                                                                                                                                                                                                                                                                     |
|----------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1        | <p>Матрицы. Обратная матрица. Ранг матрицы.</p> <p>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.</p>                                                        |
| 2        | <p>Метод Гаусса для решения СЛАУ.</p> <p>В результате практического занятия студент сможет исследовать СЛАУ и решать её методом Гаусса.</p>                                                                                                                                                                                          |
| 3        | <p>Отношение делимости в кольце целых чисел.</p> <p>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.</p>                                         |
| 4        | <p>Основная теорема арифметики. Отношение сравнения.</p> <p>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.</p> |

| №<br>п/п | Тематика практических занятий/краткое содержание                                                                                                                                                                                                                                                                                                                                                                          |
|----------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 5        | Группа. Подгруппа. Группа преобразований. Подстановки.<br>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.<br>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.<br>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.<br>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.

| №<br>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).

| №<br>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. | <a href="https://reader.lanbook.com/book/210983">https://reader.lanbook.com/book/210983</a> |
| 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-                        | <a href="https://reader.lanbook.com/book/513621">https://reader.lanbook.com/book/513621</a> |

|   |                                                                                                                                                                                                                                                                                      |                                                                                   |
|---|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------|
|   | 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.             | <a href="https://e.lanbook.com/book/507517">https://e.lanbook.com/book/507517</a> |
| 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. | <a href="https://e.lanbook.com/book/507388">https://e.lanbook.com/book/507388</a> |
| 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.    | <a href="https://e.lanbook.com/book/522111">https://e.lanbook.com/book/522111</a> |
| 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                                            | <a href="https://e.lanbook.com/book/269906">https://e.lanbook.com/book/269906</a> |

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](http://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:

доцент, доцент, к.н. кафедры  
«Математическое моделирование  
сложных систем» Института  
железнодорожного транспорта

Е.В. Родина

Согласовано:

Заведующий кафедрой ВССиИБ  
и.о. заведующего кафедрой ММСС  
Председатель учебно-методической  
комиссии

Б.В. Желенков

С.А. Тищенко

Н.А. Андриянова