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 направлению подготовки
10.03.01 Информационная безопасность,
утвержденной первым проректором РУТ (МИИТ)
Тимониным В.С.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)

Дискретная математика. Алгебра и теория чисел.

Направление подготовки: 10.03.01 Информационная безопасность

Направленность (профиль): Безопасность компьютерных систем

Форма обучения: Очная

1. Общие сведения о дисциплине (модуле).

Целью освоения дисциплины (модуля) является:

- обеспечение понимания ключевых идей, методов и проблем математической логики, алгебры, теории чисел и дискретной математики, соответствующих современному уровню развития науки;

- формирование знаний и умений, необходимых для успешного использования аппарата дискретной математики, алгебры и теории чисел в различных научных, инженерных и прикладных задачах;

- создание прочной базы для дальнейшего самостоятельного изучения и углубления знаний в области дискретной математики и связанных с ней разделов.

Задачами освоения дисциплины (модуля) являются:

- формирование представлений о современном состоянии проблем математической логики, алгебры, теории чисел и дискретной математики;

- формирование знаний и умений, необходимых для освоения и использования математической логики, алгебры, теории чисел и дискретной математики в различных областях знаний;

- развитие навыков самообразования и самостоятельного углубления знаний в области математической логики, алгебры, теории чисел и дискретной математики.

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:

Владеть:

- операции над множествами, декартово произведение, отношения эквивалентности и порядка, мощность множества;

- основные логические операции (И, ИЛИ, НЕ), законы логики, нормальные формы (ДНФ, КНФ);

- 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.

Знать:

- формализовать задачи из предметной области на языке теории множеств, логики и теории графов;
- применять комбинаторные методы для подсчета вариантов, использовать теорию чисел для создания и анализа криптографических систем;
- писать программный код для реализации базовых алгоритмов дискретной математики;.
- доказывать истинность утверждений, оценивать вычислительную сложность разработанных алгоритмов.

Уметь:

- способность абстрагироваться от конкретной физической или технической задачи и представить её в виде математической модели, используя аппарат дискретной математики;
- умение строить строгие логические выводы и доказательства корректности как самих математических утверждений, так и спроектированных процедур;
- свободное выполнение арифметических операций в кольцах вычетов, работа с многочленами над конечными полями.
- уверенное использование специализированного программного обеспечения (например, систем компьютерной алгебры) для символьных вычислений, проверки гипотез и визуализации результатов.

3. Объем дисциплины (модуля).

3.1. Общая трудоемкость дисциплины (модуля).

Общая трудоемкость дисциплины (модуля) составляет 4 з.е. (144 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 96 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	Введение в дискретную математику. Множества и операции над ними. Рассматриваемые вопросы: - предмет дискретной математики, её роль в информатике и криптографии; - понятие множества, способы задания множеств, подмножества; - операции над множествами: объединение, пересечение, разность, симметрическая разность. Диаграммы
2	Бинарные отношения. Рассматриваемые вопросы: - декартово произведение множеств; определение бинарного отношения; - свойства бинарных отношений: рефлексивность, симметричность, антисимметричность, транзитивность; - отношения эквивалентности и порядка. Разбиение множества на классы эквивалентности.
3	Основы математической логики. Логика высказываний. Рассматриваемые вопросы: - высказывания и логические операции: конъюнкция, дизъюнкция, отрицание, импликация, эквиваленция; - таблицы истинности, тавтологии, противоречия, выполнимые формулы; - законы логики высказываний (дистрибутивность, де Моргана) и их применение для упрощения формул.
4	Логика предикатов и кванторные операции. Рассматриваемые вопросы:

№ п/п	Тематика лекционных занятий / краткое содержание
	- понятие предиката; кванторы всеобщности (?) и существования (?); - формулы логики предикатов; свободные и связанные переменные; - равносильные преобразования предикатных формул; построение отрицания высказывания с кванторами.
5	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.
6	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).
7	Основная теорема арифметики. Рассматриваемые вопросы: - простые и составные числа; - существование и единственность разложения; - канонический вид числа и следствия.
8	Отношение сравнимости. М-арифметики. Рассматриваемые вопросы: - основные понятия; - свойства сравнений; - функция Эйлера, теорема Эйлера; - малая теорема Ферма.
9	Алгебраические операции. Группы. Подгруппа. Рассматриваемые вопросы: - понятие алгебраической операции на множестве, виды. - определение группы; примеры групп; - подгруппы. Циклические группы и порождающие элементы.
10	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.
11	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.
12	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
13	Кольцо. Идеал. Рассматриваемые вопросы: - определение кольца; примеры колец; - кольцо вычетов по модулю n; - определение идеала кольца, главные идеалы; - понятие факторалгебры (факторкольца) по идеалу.
14	Поле. Рассматриваемые вопросы: - определение поля; характеристика поля; - простое поле характеристики 0 и простое поле характеристики p (конечное поле); - расширения полей.
15	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.
16	Отношение делимости. Неприводимые многочлены. Рассматриваемые вопросы: - делимость в кольце многочленов; - определение неприводимого и приводимого многочлена; - критерий Эйзенштейна; - основная теорема арифметики для многочленов

4.2. Занятия семинарского типа.

Практические занятия

№ п/п	Тематика практических занятий/краткое содержание
1	Операции над множествами и бинарные отношения. В результате практического занятия студент научится выполнять операции над множествами (объединение, пересечение), строить диаграммы Венна; определять свойства бинарных отношений по матрице смежности; находить классы эквивалентности для заданного отношения эквивалентности.
2	Логика высказываний. Таблица истинности. Логика предикатов и кванторы. В результате практического занятия студент научится формализовывать высказывания естественного языка в виде формул; строить таблицы истинности; упрощать логические выражения с помощью законов булевой алгебры, записывать математические утверждения с использованием кванторов; выполнять равносильные преобразования формул; корректно строить отрицание для высказываний с вложенными кванторами.
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	Изучение дополнительной литературы.
2	Подготовка к текущим занятитиям.
3	Изучение лекционного материала
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	Ерусалимский, Я. М. Дискретная математика. Теория и практикум : учебник для вузов / Я. М. Ерусалимский. — 3-е изд., стер. — Санкт-Петербург : Лань, 2025. — ISBN 978-5-507-53650-4. — Текст : электронный // Лань : электронно-библиотечная система. — Режим доступа: для авториз. пользователей. — С. 1	https://e.lanbook.com/book/493997

2	Гашков С. Б. Дискретная математика: учебник для вузов / 3-е изд., стер. — Санкт-Петербург : Лань, 2025, 520 с. ISBN 978-5-507-49866-6. — Текст: электронный/ Лань : электронно-библиотечная система.	https://reader.lanbook.com/book/451232
3	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. — С. 1.	https://e.lanbook.com/book/522111
4	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
5	Проскуряков, 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
6	Туганбаев, А. А. Алгебраические структуры : учебник для вузов / А. А. Туганбаев. — Санкт-Петербург : Лань, 2024. — ISBN 978-5-507-48163-7. — Текст : электронный // Лань : электронно-библиотечная система. — Режим доступа: для авториз. пользователей. — С. 1.	https://e.lanbook.com/book/394511
7	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. — С. 1.	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/).

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
«Высшая математика» Е.В. Родина

Согласовано:

Заведующий кафедрой ВССиИБ Б.В. Желенков

и.о. заведующего кафедрой ПМ С.А. Тищенко

Председатель учебно-методической
комиссии Н.А. Андриянова