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)

Теоретико-числовые методы в криптографии

Специальность: 10.05.01 Компьютерная безопасность

Специализация: Информационная безопасность объектов информатизации на базе компьютерных систем

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: 2053
Подписал: заведующий кафедрой Баранов Леонид Аврамович
Дата: 01.09.2026

1. Общие сведения о дисциплине (модуле).

Дисциплина «Теоретико-числовые методы в криптографии» реализует требования федерального государственного образовательного стандарта высшего профессионального образования по направлению подготовки 10.05.01 « Компьютерная безопасность». Дисциплина «Теоретико-числовые методы в криптографии» относится к числу профессиональных прикладных дисциплин в силу направленности материала по проблемам безопасности и его важности для подготовки специалиста. Целью преподавания дисциплины «Теоретико-числовые методы в криптографии» является изложение слушателям основных принципов и методов защиты информации, комплексного проектирования и анализа защищенных компьютерных систем КС.

Задачами изучения дисциплины являются: понятия и задачи решаемые в криптографии; видах информации, подлежащей шифрованию, о методах криптографического синтеза и анализа; применениях криптографии в решении задач аутентификации, построения систем цифровой подписи; о методах криптозащиты компьютерных систем и сетей и основных подходах к изучению криптосистем. Основной целью изучения учебной дисциплины «Теоретико-числовые методы в криптографии» является формирование у обучающегося компетенций для научно-исследовательского видав деятельности. Дисциплина предназначена для получения знаний для решения следующих профессиональных задач (в соответствии с типами задач профессиональной деятельности): научно-исследовательская деятельность: анализ состояния и динамики объектов деятельности с использованием необходимых методов и средств анализа, моделирование исследуемых явлений или процессов с использованием современных вычислительных машин и систем, а также компьютерных программ; разработка программ и методик испытаний объектов защиты информации, разработка предложений по внедрению результатов научных исследований.

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;

ПК-2 - Способен проводить анализ информационной безопасности объектов и систем, принимать участие в организации и сопровождении

аттестации объекта информатизации на предмет соответствия требованиям защиты информации.

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

Знать:

- Основные понятия и методы фундаментальных разделов математики (алгебра, математический анализ, теория вероятностей, математическая логика, дискретная математика), необходимые для решения профессиональных задач.
- Принципы построения научной гипотезы, проведения верификации и валидации полученных результатов в области компьютерной безопасности.
- Математические основы криптографической защиты информации (теория чисел, конечные поля, эллиптические кривые, сложность вычислений).
- Современные методы математического моделирования (аналитические, имитационные, статистические) применительно к задачам анализа защищенности компьютерных систем.

Уметь:

- Выбирать адекватные математические методы и алгоритмы для формализации и решения поставленных задач профессиональной деятельности.
- Применять методы статистической обработки данных и интерпретировать результаты научных исследований для создания новых или совершенствования существующих средств защиты.
- Решать прикладные задачи компьютерной безопасности (аутентификация, разграничение доступа, обнаружение аномалий) с использованием математического аппарата.
- Проводить анализ компонентов системы безопасности с использованием математических методов (например, верификация моделей, анализ достижимости, оценка производительности).

Владеть:

- Навыками применения математического аппарата для формализации прикладных задач в области информационной безопасности.
- Навыками работы с научной литературой, патентными базами и нормативной документацией.

- Навыками применения специализированного математического программного обеспечения (пакеты символьных вычислений, статистические пакеты) для решения задач безопасности.

- Навыками построения и программной реализации моделей для оценки показателей защищенности компьютерных систем.

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 №5
Контактная работа при проведении учебных занятий (всего):	64	64
В том числе:		
Занятия лекционного типа	32	32
Занятия семинарского типа	32	32

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 80 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	Основы теории чисел Рассматриваемые вопросы: - Теория делимости - Функция Эйлера
2	Теория сравнений Рассматриваемые вопросы: - Теория сравнений
3	Сравнения с одним неизвестным Рассматриваемые вопросы: - Сравнения с одним неизвестным
4	Теория квадратичных вычетов Рассматриваемые вопросы: - Теория квадратичных вычетов
5	Первообразные корни и индексы Рассматриваемые вопросы: - Первообразные корни и индексы
6	Построение доказуемо простых чисел общего и специального вида Рассматриваемые вопросы: - Построение доказуемо простых чисел общего и специального вида
7	Алгебраические основы теории чисел Рассматриваемые вопросы: - Алгебраические основы теории чисел
8	Основные понятия алгебры Рассматриваемые вопросы: - Основные понятия алгебры
9	Конечные поля и неприводимые многочлены Рассматриваемые вопросы: - Конечные поля и неприводимые многочлены
10	Кольца многочленов Рассматриваемые вопросы: - Кольца многочленов
11	Алгоритмы в криптографии и криптоанализе Рассматриваемые вопросы: - Алгоритмы в криптографии и криптоанализе
12	Элементы теории сложности Рассматриваемые вопросы: - Элементы теории сложности
13	Алгоритмы факторизации Рассматриваемые вопросы: - Алгоритмы факторизации
14	Алгоритмы дискретного логарифмирования Рассматриваемые вопросы: - Алгоритмы дискретного логарифмирования

4.2. Занятия семинарского типа.

Лабораторные работы

№ п/п	Наименование лабораторных работ / краткое содержание
1	Шифр простой замены В результате выполнения практической работы студент умеет: - Реализовывать программно или вручную алгоритмы шифрования и дешифрования текста с использованием шифра простой замены (моноалфавитного шифра). - Выполнять частотный криптоанализ шифротекста для определения соответствия между символами зашифрованного и открытого текста. - Восстанавливать открытый текст по перехваченному шифротексту, используя частотные характеристики языка (например, русского или английского).
2	Сеть Фейштеля В результате выполнения работы студент умеет: - Строить схему одного раунда сети Фейштеля и объяснять принцип обратимости алгоритма независимо от используемой функции (функции шифрования). - Реализовывать упрощенную модель блочного шифра на основе сети Фейштеля с заданными параметрами (размер блока, количество раундов). - Анализировать влияние различных раундовых функций и количества раундов на лавинный эффект (изменение выходных битов при незначительном изменении входных данных или ключа).
3	Обмен ключами по Диффи-Хелману В результате выполнения работы студент умеет: - Реализовывать протокол Диффи-Хеллмана для генерации общего секретного ключа двумя абонентами через открытый канал связи. - Вычислять открытые ключи (открытые компоненты) на основе выбранных секретных ключей, простого модуля p и генератора g. - Демонстрировать уязвимость протокола к атаке "Man-in-the-Middle" (человек посередине) при отсутствии аутентификации сторон.
4	Шифр RSA В результате выполнения работы студент умеет: - Генерировать пару ключей (открытый и закрытый) для алгоритма RSA, включая выбор двух простых чисел, вычисление модуля n и функции Эйлера, а также нахождение открытой и секретной экспонент. - Выполнять операции шифрования сообщения с использованием открытого ключа и расшифрования с использованием закрытого ключа. - Оценивать стойкость RSA в зависимости от размера ключа (длины модуля n) и анализировать сложность задачи факторизации больших чисел.
5	Конечные поля и неприводимые многочлены В результате выполнения работы студент умеет: - Выполнять арифметические операции (сложение, умножение, деление) над элементами конечных полей, заданных как GF(2m), представляя элементы в виде многочленов. - Проверять многочлены на неприводимость над заданным конечным полем (например, над GF(2)) и использовать неприводимые многочлены для построения расширенных полей. - Применять свойства конечных полей для построения таблиц логарифмов (в частности, для реализации умножения через сложение степеней примитивного элемента).
6	Кольца многочленов В результате выполнения работы студент умеет: - Выполнять операции сложения, умножения и деления многочленов с коэффициентами из различных колец (например, целых чисел или по модулю простого числа). - Находить наибольший общий делитель (НОД) двух многочленов с использованием алгоритма Евклида. - Использовать свойства колец многочленов для демонстрации механизмов, лежащих в основе современных криптосистем (например, в криптографии на эллиптических кривых или в постквантовой криптографии, такой как NTRU).

4.3. Самостоятельная работа обучающихся.

№ п/п	Вид самостоятельной работы
1	Изучение дополнительной литературы.
2	Подготовка к лабораторным работам.
3	Подготовка к промежуточной аттестации.
4	Подготовка к текущему контролю.

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

№ п/п	Библиографическое описание	Место доступа
1	Криптографическая защита информации: Практикум Кунин Н. Т. Изд. МИРЭА - Российский технологический университет. - 66 с. - ISBN 978-5-7339-2447-2 , 2025	https://reader.lanbook.com/book/493382
2	Математические методы защиты информации Рацеев С.М. Учебное пособие 2-е изд., стер. - Санкт-Петербургг: Лань. - 544 с. - ISBN 978-5-507-47085-3 , 2023	https://reader.lanbook.com/book/326153#2

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

Официальный сайт РУТ (МИИТ) (https://www.miit.ru/).

Научно-техническая библиотека РУТ (МИИТ) (http:/library.miit.ru).

Образовательная платформа «Юрайт» (https://urait.ru/).

Общие информационные, справочные и поисковые системы «Консультант Плюс», «Гарант».

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).

Microsoft Internet Explorer (или другой браузер).

Операционная система Microsoft Windows.

Microsoft Office или Work 9, интегрированная среда разработки программного обеспечения для эиуляции сетевого

оборудования OmniGraffle; среда разработки программного обеспечения HTML5 и PHP.

Для проведения практических занятий необходимо иметь комплекс программ для ПЭВМ, обеспечивающих возможность выполнения работ: в области построения программных и аппаратных средств защиты информации в телекоммуникационных сетях (iOS15 Cisco и выше); программные продукты Mac OS server, XSan.

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:

Экзамен в 5 семестре.

10. Оценочные материалы.

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

Авторы:

профессор, профессор, д.н. кафедры «Интеллектуальное управление и информационная безопасность в высокоавтоматизированных транспортных системах» Института железнодорожного транспорта В.М. Алексеев

Согласовано:

Заведующий кафедрой ИУиИБ Л.А. Баранов

Председатель учебно-методической комиссии Н.А. Андриянова