МИНИСТЕРСТВО ТРАНСПОРТА РОССИЙСКОЙ ФЕДЕРАЦИИ

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ

«РОССИЙСКИЙ УНИВЕРСИТЕТ ТРАНСПОРТА»
(РУТ (МИИТ)

Рабочая программа дисциплины (модуля),
как компонент образовательной программы
высшего образования - программы специалитета
по специальности
10.05.01 Компьютерная безопасность,
утвержденной первым проректором 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 РУТ (МИИТ)
ID подписи: 2053
Подписал: заведующий кафедрой Баранов Леонид Аврамович
Дата: 01.06.2023

1. Общие сведения о дисциплине (модуле).

Дисциплина «Теоретико-числовые методы в криптографии» реализует требования федерального государственного образовательного стандарта высшего профессионального образования по направлению подготовки 100501 « 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 видами 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 разрабатывать, обосновывать и реализовывать процедуры решения задач профессиональной деятельности;

ОПК-8 - Способен применять методы научных исследований при проведении разработок в области обеспечения безопасности компьютерных систем и сетей;

ПК-2 - Способен применять математические методы в области компьютерной безопасности;

ПК-13 - Способен строить математические модели для оценки безопасности компьютерных систем и анализировать компоненты системы безопасности с использованием современных математических методов.

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

Знать:

- математические методы разрабатывать, обосновывать и реализовывать процедуры решения задач защиты информации
- криптографические алгоритмы и протоколы применительно к конкретным условиям
- методы в области компьютерной безопасности
- математические модели для оценки безопасности компьютерных систем и анализировать компоненты системы безопасности с использованием современных математических методов

Уметь:

- Применять систему фундаментальных знаний (математических, естественнонаучных и инженерных) для формулирования и решения проблем задач защиты информации.
- Применять методы математического моделирования для формализации содержательно отчетливо сформулированных проблем.
- Применять решения на основе специальных математических методов для обеспечения защищенной передачи данных в современных компьютерных сетях.
- Строить математические модели для оценки безопасности компьютерных систем.

Владеть:

- навыками анализа корректность комбинаторных, теоретико-числовых и криптографических алгоритмов в современных программных комплексах.
- навыками анализа компонентов системы безопасности с использованием современных математических методов.

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	Сем. №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:

№ п/п	Тематика лекционных занятий / краткое содержание
	- 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 работы студент рассматривает шифр простой замены, таблица Вижинера , обмен ключами по Диффи-Хелману Шифр RSA

№ п/п	Наименование лабораторных работ / краткое содержание
2	Сеть Фейштеля В результате выполнения работы студент рассматривает сеть Фейштеля
3	Обмен ключами по Диффи-Хелману В результате выполнения работы студент изучает особенности обмена ключами по Диффи-Хелману
4	Шифр RSA В результате выполнения лабораторной работы студент отрабатывает умение по работе с шифром RSA
5	Конечные поля и неприводимые многочлены В результате выполнения работы студент рассматривает конечные поля и неприводимые многочленытекущ.
6	Кольца многочленов В результате выполнения работы студент изучает кольца многочленов

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	Подготовка к промежуточной аттестации.
6	Подготовка к текущему контролю.

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

№ п/п	Библиографическое описание	Место доступа
1	Средства защиты информации на железнодорожном транспорте (Криптографические методы и средства) А.А. Корниенко, М.А. Еремеев, С.Е. Ададуров; Ред. А.А. Корниенко; Под Ред. А.А. Корниенко Однотомное издание Маршрут , 2006	НТБ (ЭЭ); НТБ (уч.3); НТБ (фб.); НТБ (чз.2)
2	Криптография Н. Смарт Однотомное издание Техносфера , 2006	НТБ (фб.)
1	Криптография в задачах и упражнениях В.О. Осипян, К.В. Осипян Однотомное издание "Гелиос АРВ" , 2011	НТБ (уч.3); НТБ (фб.); НТБ (чз.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/).

Электронно-библиотечная система ibooks.ru (http://ibooks.ru/).

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
«Управление и защита информации» В.М. Алексеев

Согласовано:

Заведующий кафедрой УиЗИ Л.А. Баранов

Председатель учебно-методической
комиссии С.В. Володин