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

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)

Методы и средства криптографической защиты информации

Направление подготовки: 10.03.01 Информационная безопасность

Направленность (профиль): Безопасность 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: 5665
Подписал: заведующий кафедрой Нутович Вероника Евгеньевна
Дата: 24.05.2022

1. Общие сведения о дисциплине (модуле).

Целью освоения дисциплины (модуля) является:

- изучение основных математических подходов к решению задач компьютерной безопасности.

Задачами дисциплины являются:

- изучение стандартов в области криптографической защиты информации;
- изучение основных методов шифрования;
- изучение базовых алгоритмов, применяемых в криптосистемах.

2. Планируемые результаты обучения по дисциплине (модулю).

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

ОПК-3 - Способен использовать необходимые математические методы для решения задач профессиональной деятельности;

ОПК-9 - Способен применять средства криптографической и технической защиты информации для решения задач профессиональной деятельности .

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

Знать:

- арифметические алгоритмы, связанные с криптографическими системами
- основные задачи и понятия криптографии;
- требования к шифрам и основные характеристики шифров;
- модели шифров и математические методы их исследования;
- принципы построения криптографических алгоритмов.

Уметь:

- использовать базовые знания теории чисел для реализации арифметическихалгоритмов в криптографических системах;
- использовать частотные характеристики открытых текстов для анализа простейших шифров замены и перестановки;
- пользоваться научно-технической литературой в области криптографии.

Владеть:

- инструментами криптографической защиты информации;

- современной терминологией в области информационной безопасности.

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	Сем. №6
Контактная работа при проведении учебных занятий (всего):	44	44
В том числе:		
Занятия лекционного типа	30	30
Занятия семинарского типа	14	14

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 64 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	Квадратичные вычеты и основы теории эллиптических кривых Рассматриваемые вопросы: - квадраты в конечных полях; - символ Лежандра; - свойства символа Лежандра; - свойства символа Лежандра; - символ Якоби; - понятие эллиптической кривой.
2	История и основные понятия криптографии Рассматриваемые вопросы: - история и основы криптографии; - виды шифров. Результаты К. Шеннона. Криптостойкость шифров. Атаки; - статистический анализ шифр-текстов; - генерирование случайных подстановок. Базовые алгоритмы криптографии; - простые числа, тесты на простоту. Тест Рабина-Миллера; - построение больших простых чисел.
3	Системы шифрования Рассматриваемые вопросы: -блочное шифрование; - алгоритм шифрования Эль-Гамаля; - алгоритм шифрования Рабина.

4.2. Занятия семинарского типа.

Практические занятия

№ п/п	Тематика практических занятий/краткое содержание
1	Квадратичные вычеты и основы теории эллиптических кривых В результате работы на практичесикх занятиях студент получает навык работы с символами Лежандра, Якоби, получает навык решения задач с эллиптической кривой
2	История и основные понятия криптографии В результате работы на практических занятиях студент получает навык работы с простейшими методами шифрования, изучает криптостойкость шифров, атаки, осваивает генерирование случайных подстановок, изучает базовые алгоритмы криптографии.
3	Системы шифрования В результате работы на практическом занятии студент получает навык работы с блочным шифрованием, изучет алгоритм шифрования Эль-Гамаля и Рябина и применяет знания при при решении задач

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	Выполнение курсовой работы.

5	Подготовка к промежуточной аттестации.
6	Подготовка к текущему контролю.

4.4. Примерный перечень тем курсовых работ

Вычисление символов Лежандра и Якоби, построение больших простых чисел, алгоритмы шифрования RSA, алгоритмы шифрования Эль-Гамаля, схемы цифровой подписи на основе RSA и др. криптосистемы

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

№ п/п	Библиографическое описание	Место доступа
1	Основы современной криптографии С.Г. Баричев, В.В. Гончаров, Р.Е. Серов Однотомное издание Горячая линия - Телеком , 2002; -175 с.; - ISBN 5-93517-075-2	НТБ
2	Введение в криптографию В.В. Ященко, Н.П. Варновский, Ю.В. Нестеренко и др.; Под общ. ред. В.В. Ященко Однотомное издание МЦНМО: "ЧеРо" , 2000; - 287 с.; - ISBN 5-900916-65-0	НТБ МИИТ
3	Введение в теоретико-числовые методы криптографии М. М. Глухов, И. А. Круглов, А. Б. Пичкур, А. В. Черемушкин Однотомное издание Лань , 2010; - 394 с; - ISBN 978-5-8114-1116-0	НТБ
4	Введение в криптосистемы с открытым ключом Н. А.Введение в криптосистемы с открытым ключом Н. А.; - 286 с.; - ISBN 5-94157-563-7	НТБ МИИТ
5	Современная криптография: теория и практика Венбо Мао; - 763 с.; - ISBN 5-8459-0847-7	НТБ МИИТ
6	Классическое введение в современную теорию чисел К. Айерленд; Пер. с англ. С.П. Демушкина ; Под ред. А.Н. Паршина; Под Ред. А.Н. Паршин Однотомное издание Мир , 1987; - 415 с.	НТБ МИИТ
7	Криптография в задачах и упражнениях В.О. Осипян, К.В. Осипян Однотомное издание "Гелиос АРВ" , 2004; -143; - ISBN 5-85438-009-9	НТБ МИИТ

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

http://library.miit.ru/ - электронно-информационная система НТБ МИИТ

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

- пакет прикладных обучающих программ: MATHCAD, Maple

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

- Компьютерное и мультимедийное оборудование: компьютер, проектор, экран;

9. Форма промежуточной аттестации:

Зачет в 6 семестре.
Курсовая работа в 6 семестре.

10. Оценочные материалы.

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

Авторы:

старший преподаватель кафедры
«Цифровые технологии управления
транспортными процессами» В.П. Посвянский

Согласовано:

Заведующий кафедрой ВССиИБ Б.В. Желенков

Заведующий кафедрой ЦТУТП В.Е. Нутович

Председатель учебно-методической
комиссии Н.А.Клычева