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)

Криптографические протоколы

Направление подготовки: 10.03.01 Информационная безопасность

Направленность (профиль): Безопасность компьютерных систем

Форма обучения: Очная

1. Общие сведения о дисциплине (модуле).

Целями освоения дисциплины (модуля) являются:

- ознакомление студентов с основными понятиями теории криптографических протоколов;

- овладение основными идеями и методами современной теории криптографических протоколов;

- ознакомление студентов с основными криптографическими протокола распределения ключей, протоколами аутентификации, различными промежуточными и более развитыми протоколами;

- овладение навыком разложения любого криптографического протокола на промежуточные с целью создания программного обеспечения, обслуживающего исполнение протокола.

Задачами дисциплины являются:

- получение знаний при решении следующих профессиональных задач: применение стандартных криптопротоколов и интернет-технологий, средств и методов хранения и передачи аутентификационной информации, основных протоколов идентификации и аутентификации абонентов, протоколов дистанционного принятия решений, математических моделей шифров, использование криптографических стандартов.

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:

- основные принципы криптографии и защиты информации;
- алгоритмы шифрования RSA и Эль-Гамаля.

Уметь:

- работать с кольцами вычетов и кольцами многочленов.

Владеть:

- арифметикой конечных полей.

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 1
Контактная работа при проведении учебных занятий (всего):	50	50
В том числе:		
Занятия лекционного типа	34	34
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 94 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	Понятие протокола Рассматриваемые вопросы: - понятие протокола, отличия от криптосистем.

№ п/п	Тематика лекционных занятий / краткое содержание
2	Стандартные протоколы Рассматриваемые вопросы: - протоколы аутентификации.
3	Другие виды протоколов Рассматриваемые вопросы: - протоколы электронных платежей.
4	Базовые протоколы Рассматриваемые вопросы: - протокол Диффи-Хеллмана; - протокол Блюма.
5	Стандартные протоколы Рассматриваемые вопросы: - электронная подпись; - разделение секрета.
6	Другие виды протоколов Рассматриваемые вопросы: - криптографические хэш-функции.
7	Другие виды протоколов Рассматриваемые вопросы: - электронные деньги с купюрами разного номинала.
8	Другие виды протоколов Рассматриваемые вопросы: - протоколы аутентификации

4.2. Занятия семинарского типа.

Практические занятия

№ п/п	Тематика практических занятий/краткое содержание
1	Понятие протокола, отличия от криптосистем В результате работы на практическом занятии обучающийся получает навык работы с протоколами и отличие их от криптосистем
2	Протокол Диффи-Хеллмана В результате работы на практическом занятии обучающийся получает навык работы с протоколом Диффи-Хеллмана
3	Протокол Блюма В результате работы на практическом занятии обучающийся получает навык работы с протоколом Блюма
4	Протоколы аутентификации В результате работы на практическом занятии обучающийся получает навык работы с протоколом аутентификации
5	Электронная подпись В результате работы на практическом занятии обучающийся получает навык работы с электронной подписью
6	Разделение секрета В результате работы на практическом занятии обучающийся получает навык работы с разделением секрета

№ п/п	Тематика практических занятий/краткое содержание
7	Протоколы электронных платежей В результате работы на практическом занятии обучающийся получает навык работы с протоколами электронных платежей
8	Электронные деньги с купюрами разного номинала В результате работы на практическом занятии обучающийся получает навык работы с электроннами деньгами и купюрами разного номинала
9	Криптографические хэш-функции В результате работы на практическом занятии обучающийся получает навык работы с криптографическими хэш-функциями

4.3. Самостоятельная работа обучающихся.

№ п/п	Вид самостоятельной работы
1	Изучение дополнительной литературы
2	Подготовка к практичесим занятиям
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	С.Г. Баричев, В.В. Гончаров, Р.Е. Серов Основы современной криптографии. М. : Горячая линия - Телеком, 2002. - 175 с. - ISBN 5-93517-075-2 Однотомное издание	НТБ (фб.); НТБ (чз.1); НТБ (чз.2)
2	В.В. Ященко, Н.П. Варновский, Ю.В. Нестеренко и др. Введение в криптографию. МЦНМО, 2000. - 287 с. - ISBN 5-900916-65-0 Однотомное издание	НТБ (фб.); НТБ (чз.2)
3	М. М. Глухов, И. А. Круглов, А. Б. Пичкур, А. В. Черемушкин Введение в теоретико-числовые методы криптографии. Лань, 2022. - 396 с.; ISBN 978-5-507-45348-1 Однотомное издание	НТБ
4	Н. А. Молдовян, А.А. Молдовян Введение в криптосистемы с открытым ключом. БХВ-Петербург, 2005. - 286 с.; ISBN 5-94157-563-7	НТБ
5	Венбо Мао Гелиос Современная криптография: теория и практика. Вильямс, 2005. - 763 с.; ISBN 5-8459-0847-7	НТБ
6	В. О. Осипян, К. В. Осипян Криптография в задачах и упражнениях. Гелиос АРВ, 2004. - 143 с.; - ISBN 5-85438-009-9 Однотомное издание	НТБ

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).

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

Поисковая система Яндекс (www.yandex.ru).

Единая коллекция цифровых образовательных ресурсов (http://window.edu.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.

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 в 7 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