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)

Технологии защиты конфиденциальной 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: 4196
Подписал: заведующий кафедрой Желенков Борис Владимирович
Дата: 23.04.2024

1. Общие сведения о дисциплине (модуле).

Целью освоения учебной дисциплины «Технологии защиты конфиденциальной информации» является формирование профессиональных компетенций по основным разделам дисциплины.

Основными задачами дисциплины являются:

- изучение криптографических примитивов, протоколов, систем и технологий;
- изучение криптографических методов и средств защиты конфиденциальной информации;
- изучение требований и основных документов ФСТЭК по защите информации;
- студенты должны уметь применять теорию на практике.

2. Планируемые результаты обучения по дисциплине (модулю).

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

ОПК-6 - Способен при решении профессиональных задач организовывать защиту информации ограниченного доступа в соответствии с нормативными правовыми актами, нормативными и методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю ;

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

ПК-1 - способностью выполнять работы по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации .

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

Знать:

- виды конфиденциальной информации;
- криптографические алгоритмы, протоколы, системы и технологии;
- атаки на криптографические протоколы и системы, методы противодействия атакам;
- нормативные и методические документы Федеральной службы безопасности Российской Федерации, ФСТЭК;

- подходы к построению систем защиты информации.

Уметь:

- выполнять работы по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации;
- применять на практике методы противодействия атакам;
- использовать на практике службы и механизмы безопасности;
- применять средства криптографической и технической защиты информации для решения задач профессиональной деятельности.

Владеть:

- навыками использования полученных теоретических знаний на практике;
- навыками организации защиты конфиденциальной информации ограниченного доступа в соответствии с нормативными правовыми актами, нормативными и методическими документами;
- при решении профессиональных задач организовывать защиту информации ограниченного доступа в соответствии с нормативными правовыми актами, нормативными и методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю.
- навыками по установке, настройке и обслуживанию средств защиты информации.

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):	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	ЗАЩИТА ИНФОРМАЦИИ Рассматриваемые вопросы: - требования ФСТЭК по защите информации; - рекомендации по технической защите данных; - классы средств защиты данных.
2	ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ Рассматриваемые вопросы: - меры по обеспечению информационной безопасности; - документы ФСТЭК по ИБ; - сертифицированные средства ИБ ФСТЭК; - Госреестр средств защиты информации.
3	КОНФИДЕНЦИАЛЬНАЯ ИНФОРМАЦИЯ Рассматриваемые вопросы: - основные виды конфиденциальной информации, принятые в законодательстве РФ; - законодательное регулирование; - конфиденциальность в России.
4	ЗАЩИТА КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ Рассматриваемые вопросы: - порядок обеспечения информационной безопасности; - криптографическая защита информации.
5	КРИПТОГРАФИЧЕСКИЕ МЕТОДЫ ЗАЩИТЫ ИНФОРМАЦИИ Рассматриваемые вопросы: - методы защиты виды, классификация; - шифрование, стенография, кодирование, сжатие и др..
6	КРИПТОГРАФИЧЕСКИЕ СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ

№ п/п	Тематика лекционных занятий / краткое содержание
	Рассматриваемые вопросы: - средства криптографической защиты информации (СКЗИ); - сертифицированные криптографические средства защиты информации в России.
7	КРИПТОГРАФИЧЕСКИЕ СИСТЕМЫ Рассматриваемые вопросы: - алгоритмы шифрования данных DES, Triple DES, AES, алгоритм Ривеста и др.; - криптосистема шифрования данных RSA, схемы шифрования Полига-Хеллмана, Эль Гамаля, комбинированный метод шифрования и др. - криптографические хэш-функции.
8	КРИПТОГРАФИЧЕСКИЕ ПРИМИТИВЫ Рассматриваемые вопросы: - свойства примитивов, основные примитивы, объединение примитивов; - свойства безопасности.
9	КРИПТОГРАФИЧЕСКИЕ ПРОТОКОЛЫ Рассматриваемые вопросы: - понятие протокола, отличия от криптосистем; - функции протоколов, состав, обозначения, классификация; - виды атак на криптографические протоколы.
10	БАЗОВЫЕ КРИПТОГРАФИЧЕСКИЕ ПРОТОКОЛЫ Рассматриваемые вопросы: - базовые протоколы, протокол Диффи-Хеллмана, протокол Блюма; - разделение секрета.
11	СТАНДАРТНЫЕ КРИПТОГРАФИЧЕСКИЕ ПРОТОКОЛЫ Рассматриваемые вопросы: - стандартные протоколы; - протоколы аутентификации; - электронная подпись; - протоколы электронных платежей, другие виды протоколов.
12	КВАНТОВАЯ КРИПТОГРАФИЯ Рассматриваемые вопросы: - основные понятия и определения; - квантовые сети, суть квантовой передачи данных; - квантовая телепортация и экспериментальная реализация.
13	КВАНТОВОЕ РАСПРЕДЕЛЕНИЕ КЛЮЧЕЙ Рассматриваемые вопросы: - виды ошибок при передаче информации; - протоколы подготовки и измерения, протоколы основанные на запутанности.
14	ПРОЕКТИРОВАНИЕ СИСТЕМ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ Рассматриваемые вопросы: - принципы построения систем защиты конфиденциальной информации; - основы политики безопасности (понятие политики безопасности, реализация политики безопасности, модели безопасности); - основные этапы.
15	АНАЛИЗ СИСТЕМ ОБЕСПЕЧЕНИЯ ИБ Рассматриваемые вопросы: - аудит безопасности, анализ рисков, разработка Концепции обеспечения ИБ;

№ п/п	Тематика лекционных занятий / краткое содержание
	- анализ архитектуры и структуры системы защиты; - анализ политик, процедур, регламентов и т.п.; - анализ программных и технических средства защиты конфиденциальной информации.
16	ЭКСПЛУАТАЦИЯ СИСТЕМ ОБЕСПЕЧЕНИЯ ИБ Рассматриваемые вопросы: - методика испытаний; - доработка системы; - организационные этапы.

4.2. Занятия семинарского типа.

Практические занятия

№ п/п	Тематика практических занятий/краткое содержание
1	ПОЛОЖЕНИЯ ISO 15408 (COMMON CRITERIA) Результат работы - получение навыков практического применения стандарта.
2	МЕЖСЕТЕВЫЕ ЭКРАНЫ Результат работы - приобретение навыков применения МЭ.
3	ЗАЩИТА АВТОМАТИЗИРОВАННЫХ СИСТЕМ Результат работы - получение навыков практического применения Руководящего документа ФСТЭК.
4	ЗАЩИТА СРЕДСТВ ВЫЧИСЛИТЕЛЬНОЙ ТЕХНИКИ Результат работы - получение навыков практического применения Руководящего документа.
5	АНАЛИЗ АТАК НА КРИПТОГРАФИЧЕСКИЕ ПРОТОКОЛЫ Результат работы – отчёт с описанием атаки, вычисленным пространством сценариев атак, указанием методов противодействия.
6	БАЗОВЫЕ АЛГОРИТМЫ КРИПТОГРАФИИ Результат работы – генерирование случайных подстановок.
7	МЕТОДЫ ШИФРОВАНИЯ. БЛОЧНЫЕ ШИФРЫ Результат работы – выбранный ключ, зашифрованное сообщение.
8	МЕТОДЫ ШИФРОВАНИЯ. ПОТОЧНЫЕ ШИФРЫ Результат работы – выбранный ключ, зашифрованное сообщение.
9	СИСТЕМЫ ШИФРОВАНИЯ Результат работы – реализация алгоритма шифрования Эль-Гамаля.
10	ПРОТОКОЛЫ КОНФИДЕНЦИАЛЬНОГО ВЫЧИСЛЕНИЯ Результат работы - вычисленная функция над конечным полем.
11	ИССЛЕДОВАНИЕ ПРИКЛАДНЫХ КРИПТОГРАФИЧЕСКИХ ПРОТОКОЛОВ Результат работы – отчет с описанием практического применения протоколов и анализом криптографических функций.
12	ИССЛЕДОВАНИЕ ПРОТОКОЛА БЛЮМА Результат работы – отлаженная программа, реализующая протокол привязки к биту (протокол Блюма - схема Блюма-Микали).
13	АЛГОРИТМ ШИФРОВАНИЯ РАБИНА Результат работы – отлаженная программа, реализующая алгоритм шифрования Рабина.

№ п/п	Тематика практических занятий/краткое содержание
14	АНАЛИЗ ПРОТОКОЛОВ КВАНТОВОГО РАСПРЕДЕЛЕНИЯ КЛЮЧЕЙ 1 ТИПА Результат работы – проведенное исследование протокола подготовки и измерения.
15	АНАЛИЗ ПРОТОКОЛОВ КВАНТОВОГО РАСПРЕДЕЛЕНИЯ КЛЮЧЕЙ 2 ТИПА Результат работы – проведенное исследование протоколов, основанных на запутанности.
16	РАЗРАБОТКА СИСТЕМЫ ИНФОРМАЦИОННОЙ ЗАШИТЫ ОБЪЕКТА ИНФОРМАТИЗАЦИИ В результате выполнения работы студентом будет подготовлен отчет с описанием системы защиты информации.

4.3. Самостоятельная работа обучающихся.

№ п/п	Вид самостоятельной работы
1	Изучение дополнительной литературы
2	Работа с лекционным материалом.
3	Подготовка к практическим занятиям.
4	Выполнение курсовой работы.
5	Подготовка к промежуточной аттестации.
6	Подготовка к текущему контролю.

4.4. Примерный перечень тем курсовых работ

Курсовая работа «Криптографическая защита информации».

Примерный перечень тем курсовых работ:

- Реализация алгоритма Ривеста.

- Реализация алгоритма DES – режим сцепления блоков в CBC шифре.

- Реализация алгоритма DES – режим работы ECB (электронный блокнот).

- Реализация алгоритма DES – режим работы CFB – обратная связь по шифротексту.

- Реализация алгоритма DES – OFB – обратная связь по выходу.

- Алгоритм федерального стандарта x9.9.

- Алгоритм криптографического преобразования – общий.

- Алгоритм криптографического преобразования в режиме простой замены.

- Алгоритм криптографического преобразования в режиме гаммирования с обратной связью

- Алгоритм криптографического преобразования в режиме имитовставки.

- Алгоритм, основанный на схеме шифрования Эль Гамаля.

- Алгоритм, основанный на комбинированном методе шифрования

- Открытое распределение ключей Диффи-Хеллмана

- Алгоритм электронной подписи RSA.

- Алгоритм электронной подписи DSA.

- Отечественный стандарт электронной подписи.

- Алгоритм цифровой подписи с дополнительными функциями по схеме «слепой подписи».

- Алгоритм цифровой подписи с дополнительными функциями по схеме «неоспоримой подписи».

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

№ п/п	Библиографическое описание	Место доступа
1	Вострецова Е.В., Основы информационной безопасности: учебное пособие для студентов вузов. Екатеринбург: Изд-во Урал. ун-та, 2019.- 204 с. - ISBN 978-5-7996-2677-8.	https://elar.urfu.ru/bitstream/10995/73899/3/978-5-7996-2677-8_2019.pdf(дата обращения: 03.03.2024). -Текст: электронный.
2	Казарин О. В., Программно-аппаратные средства защиты информации. Защита программного обеспечения: учебник и практикум для среднего профессионального образования / О. В. Казарин, А. С. Забабурин. Москва: Издательство Юрайт,	https://e.lanbook.com/book/110336 (дата обращения: 03.03.2024). — Режим доступа: для авториз. пользователей.— Текст:электронный

	2022. 312 с. (Профессиональное образование). ISBN 978-5-534-13221-2.	
3	Голиков А. М., Защита информации в инфокоммуникационн ых системах и сетях: учебное пособие / А. М. Голиков. Москва: ТУСУР, 2015. 284 с. // Лань: электронно-библиотечная система.	https://e.lanbook.com/book/110336 (дата обращения: 03.03.2024). — Режим доступа: для авториз. пользователей. — Текст: электронный
4	Нестеров С. А., Основы информационной безопасности:учебное пособие / С. А. Нестеров. 5-е изд., стер. Санкт-Петербург: Лань, 2022. 324 с. ISBN 978-5-8114-4067-2.	https://e.lanbook.com/book/206279(дата обращения: 03.03.2024) Режим доступа: для авториз.пользователей. – Текст: электронный
5	Лось А. Б., Нестеренко, А. Ю., Рожков, М. И. Криптографические методы защиты информации для изучающих компьютерную безопасность: учебник для академического бакалавриата / А. Б. Лось, А. Ю. Нестеренко, М. И. Рожков.2-е изд., испр.М.: Издательство Юрайт, 2019. 473 с. (Серия: Бакалавр. Академический курс). ISBN 978-5-534-12474-3.	https://azon.market/image/catalog/v_1/product/pdf/378/3777079.pdf(дата обращения: 16.02.2024). Режим доступа: для авториз. пользователей.Текст:электронный

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

Форум специалистов по информационным технологиям http://citforum.ru/

Интернет-университет информационных технологий http://www.intuit.ru/

Поисковые системы: Yandex, Google, Mail.

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.

Специализированное программное обеспечение не требуется.

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:

рабочие место преподавателя с персональным компьютером, подключённым к INTERNET;

специализированная лекционная аудитория с мультимедиа аппаратурой;

рабочие места студентов в компьютерном классе, подключённые к сети INTERNET.

9. Форма промежуточной аттестации:

Курсовая работа в 6 семестре.

Экзамен в 6 семестре.

10. Оценочные материалы.

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

Авторы:

профессор, доцент, д.н. кафедры
«Вычислительные системы, сети и
информационная безопасность» И.Е. Сафонова

Согласовано:

Заведующий кафедрой ВССиИБ Б.В. Желенков

Председатель учебно-методической
комиссии Н.А. Андриянова