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)

Теоретические основы компьютерной безопасности

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: 17.02.2024

1. Общие сведения о дисциплине (модуле).

Целью освоения учебной дисциплины «Теоретические основы компьютерной безопасности» является формирование профессиональных компетенций по основным разделам дисциплины.

Основными задачами дисциплины являются:

- освоение студентами базовых методов и средств защиты компьютерной информации (организационных, технических, программных);
- ознакомление с законодательством и стандартами в этой области;
- студенты должны изучить теоретические основы компьютерной безопасности и 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-1.4 - Способен оценивать уровень безопасности компьютерных систем и сетей, в том числе в соответствии с нормативными и корпоративными требованиями;

ОПК-11 - Способен проводить эксперименты по заданной методике и обработку их результатов ;

ПК-5 - способностью принимать участие в организации и сопровождении аттестации объекта информатизации по требованиям безопасности информации ;

ПК-11 - способностью принимать участие в проведении экспериментальных исследований системы защиты информации.

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

Знать:

виды политик управления доступом и информационными потоками в компьютерных сетях.

Уметь:

обосновывать выбор используемых программно-аппаратных средств защиты информации в компьютерных сетях.

Владеть:

навыками разработки порядка применения программно-аппаратных средств защиты информации в компьютерных сетях.

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. №7
Контактная работа при проведении учебных занятий (всего):	48	48
В том числе:		
Занятия лекционного типа	32	32
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 96 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	

№ п/п	Тематика лекционных занятий / краткое содержание
	1. ВВЕДЕНИЕ В ДИСЦИПЛИНУ. ПРАВОВЫЕ И ОРГАНИЗАЦИОННЫЕ МЕТОДЫ ЗАЩИТЫ ИНФОРМАЦИИ. Рассматриваемые вопросы: - методы и средства защиты компьютерной информации; - законодательные меры защиты информации (нормативные правовые акты РФ в области защиты информации); - стандарты: оценочные стандарты и технические спецификации; - организации-разработчики стандартов. 2. УГРОЗЫ БЕЗОПАСНОСТИ ИНФОРМАЦИИ В КОМПЬЮТЕРНЫХ СИСТЕМАХ. Рассматриваемые вопросы: - характеристики угроз, служб и механизмов безопасности (виды; взаимосвязь между службами и реализующими их механизмами); - классификация угроз (пути их реализации; комплекс требований к системе компьютерной безопасности); - основные способы и каналы утечки информации (преодоление программных средств защиты; - способы несанкционированного доступа). 3. АППАРАТНО-ПРОГРАММНЫЕ СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ. Рассматриваемые вопросы: - основные средства защиты компьютерной информации и их функции (Zecurion Zgate; Secret Disk; КриптоПро CSP; другие разработки); - криптопроцессоры; - уровни защиты информации; - защита от изменения потока сообщений и прерывания передачи, защита от навязывания ложных сообщений в каналы связи; - способы защиты сетей (сетевые атаки и методы противодействия; связь между характеристиками развития вирусной атаки и сетевой структурой); - межсетевые экраны. 4. СИММЕТРИЧНЫЕ И АССИМЕТРИЧНЫЕ КРИПТОСИСТЕМЫ. Рассматриваемые вопросы: - стандарты шифрования данных (алгоритм шифрования данных DES; Triple DES; AES; алгоритм Ривеста); - Российский стандарт крипто- и имитозащиты сообщений; - концепция криптосистемы с открытым ключом; - криптосистема шифрования данных RSA; - схемы шифрования (Полига-Хеллмана, Эль Гамаля, комбинированный метод шифрования). 5. КРИПТОГРАФИЧЕСКИЕ КЛЮЧИ. Рассматриваемые вопросы: - управление криптографическими ключами (виды ключей, процедуры управления ключами); - генерация ключей; - хранение ключей; - распределение ключей. 6. УПРАВЛЕНИЕ ДОСТУПОМ К РЕСУРСАМ. Рассматриваемые вопросы: - требования, подходы и задачи управления доступом; - модели доступа (механизмы управления доступом, идентификация и установление подлинности); - проверка полномочий субъектов на доступ к ресурсам.

№ п/п	Тематика лекционных занятий / краткое содержание
	7. ЭЛЕКТРОННАЯ ПОДПИСЬ. Рассматриваемые вопросы: - проблема аутентификации данных; - хэш-функции (использование в ЭП, стандарты хэш-функций); - алгоритмы электронной подписи (назначение и виды, классификация, подделка ЭП); - подписи с дополнительными функциональными свойствами (слепая ЭП, быстрая, неоспоримая). 8. ПРОЕКТИРОВАНИЕ СИСТЕМ ЗАЩИТЫ ИНФОРМАЦИИ. Рассматриваемые вопросы: - основы политики безопасности (понятие политики безопасности; реализация политики безопасности; модели безопасности); - проектирование и реализация системы защиты информации (анализ объекта защиты, этапы проектирования и реализации системы, работы по созданию и сопровождению системы, архитектура системы защиты).

4.2. Занятия семинарского типа.

Практические занятия

№ п/п	Тематика практических занятий/краткое содержание
1	1 АНАЛИЗ ИНЖЕНЕРНО-ТЕХНИЧЕСКИХ СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ. В результате выполнения работы студент получит теоретические знания о наиболее востребованных инженерно-технических средствах защиты информации. 2 ИЗУЧЕНИЕ МЕТОДОВ ШИФРОВАНИЯ. Результат работы – криптограмма. 3 СИММЕТРИЧНЫЕ КРИПТОСИСТЕМЫ. Результат работы - изучение одного из предложенных симметричных алгоритмов. 4 АССИМЕТРИЧНЫЕ КРИПТОСИСТЕМЫ. Результат работы - изучение одного из предложенных ассиметричных алгоритмов. 5 ПРОГРАММНАЯ РЕАЛИЗАЦИЯ МЕТОДОВ ШИФРОВАНИЯ. Результатом работы является отлаженная программа, реализующая предложенный студентом метод шифрования. 6 АНАЛИЗ ПРИНЦИПОВ СОЗДАНИЯ СИСТЕМ ИНФОРМАЦИОННОЙ ЗАШИТЫ СЕТЕЙ В результате выполнения работы студентом будет подготовлен отчет, включающий список необходимых документов для разработки системы информационной защиты. 7 ЭПАТЫ РАЗРАБОТКИ СИСТЕМЫ ИНФОРМАЦИОННОЙ ЗАШИТЫ СЕТИ ПРЕДПРИЯТИЯ. Результатом работы является работоспособная компьютерная сеть, в которой настроена политика безопасности в соответствии с заданием.

4.3. Самостоятельная работа обучающихся.

№ п/п	Вид самостоятельной работы
1	1. Работа с лекционным материалом. 2. Подготовка реферата. 3.Подготовка к практическим занятиям.
2	Подготовка к промежуточной аттестации.
3	Подготовка к текущему контролю.

4.4. Примерный перечень тем эссе

Стандарты обеспечения безопасности передачи данных в глобальной сети Internet.

- Особенности функционирования межсетевых экранов.

- Особенности антивирусных программ.

- Шифрующие таблицы и применение магических квадратов.

- Классификация вирусов.

- Классификация технических каналов утечки информации.

- Перехват наведенных информативных сигналов с инженерных коммуникаций.

- Технические каналы утечки акустической информации.

- Системы пространственного электромагнитного зашумления.

- Системы линейного зашумления.

- Способы и средства защиты выделенных помещений от утечки речевой информации по техническим каналам.

- Системы и средства виброакустической маскировки.

- Основные методы шифрования, используемые в традиционных симметричных криптографических системах.

- Хэширование.

- Квантовые сети.

- Этапы работ по созданию системы защиты информации.

- Особенности реализации методов криптозащиты в каналах телекоммуникаций.

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: 03.03.2023).-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, 2022. 312 с. (Профессиональное образование). ISBN 978-5-534-13221-2.	Образовательная платформа Юрайт [сайт].URL: https://urait.ru/bcode/497433 (дата обращения: 03.03.2023). - Текст: электронный
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: 03.03.2023). — 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	Лань: э.https://e.lanbook.com/book/206279 (дата обращения: 03.03.2023). Режим доступа: для авториз. пользователей.Текст: электронный

	978-5-8114-4067-2.	
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: 18.03.2023). — 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).

Для проведения аудиторных занятий и самостоятельной работы требуются:

Рабочее место преподавателя с персональным компьютером, подключённым к сетям INTERNET

Специализированная лекционная аудитория с мультимедиа аппаратурой и интерактивной доской.

Компьютерный класс с кондиционером. Рабочие места студентов в компьютерном классе, подключённые к сетям INTERNET

Для проведения практических занятий:

компьютерный класс; кондиционер; компьютеры с минимальными требованиями – Pentium 4, ОЗУ 4 ГБ, HDD 100 ГБ, USB

9. Форма промежуточной аттестации:

Экзамен в 7 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