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

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)

Защищенные беспроводные сети

Направление подготовки: 10.04.01 Информационная безопасность

Направленность (профиль): Безопасность компьютерных систем и сетей

Форма обучения: Очная

1. Общие сведения о дисциплине (модуле).

Целью освоения учебной дисциплины «Защищенные беспроводные сети» является формирование компетенций по основным разделам дисциплины для целостного представления принципов построения, исследования и анализа защищенных беспроводных сетей.

Задачи:

- изучение особенностей беспроводных технологий;
- изучение принципов разработки беспроводных сетей и обеспечения их безопасности;
- усвоение основных стандартов построения и защиты беспроводных сетей.

2. Планируемые результаты обучения по дисциплине (модулю).

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

ОПК-1 - Способен обосновывать требования к системе обеспечения информационной безопасности и разрабатывать проект технического задания на ее создание;

ОПК-2 - Способен разрабатывать технический проект системы (подсистемы либо компонента системы) обеспечения информационной безопасности ;

ПК-3 - Способность анализировать направления развития информационных (телекоммуникационных) технологий, прогнозировать эффективность функционирования, оценивать затраты и риски, формировать политику безопасности объектов защиты.

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

Знать:

- показатели качества работы беспроводных сетей;
- стандарты современных и перспективных систем мобильной связи и беспроводного Интернета;
- требования и стандарты по обеспечению безопасности сетей беспроводного доступа.

Уметь:

- выявлять уязвимости беспроводных сетей, анализировать угрозы и предотвращать атаки на беспроводные сети;

- проводить оценку безопасности беспроводных сетей.

Владеть:

- навыками разработки защищенных беспроводных сетей.

3. Объем дисциплины (модуля).

3.1. Общая трудоемкость дисциплины (модуля).

Общая трудоемкость дисциплины (модуля) составляет 5 з.е. (180 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 №2
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 132 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	ОСОБЕНЫНОСТИ БЕСПРОВОДНЫХ СЕТЕЙ Рассматриваемые вопросы: - беспроводная среда; - беспроводные мобильные сети; - состав и архитектурные особенности построения БС, функциональные особенности.
2	КЛАССИФИКАЦИЯ БЕСПРОВОДНЫХ ТЕХНОЛОГИЙ Рассматриваемые вопросы: - сектор локальных интерфейсов, сектор локальных домашних и офисных сетей; - сектор региональных городских сетей и сектор глобальных сетей; - беспроводные технологии.
3	ОРГАНИЗАЦИЯ БЕСПРОВОДНЫХ ШИРОКОПОЛОСНЫХ СЕТЕЙ (БПШС) Рассматриваемые вопросы: - методы планирования зоны покрытия БПШС; - показатели качества обслуживания и факторы, определяющие их; - модели пространственной организации.
4	УГРОЗЫ И УЯЗВИМОСТИ БЕСПРОВОДНЫХ СЕТЕЙ Рассматриваемые вопросы: - классификации сетевых угроз и уязвимостей; - прямые угрозы; - косвенные угрозы.
5	РАЗВЕДКА И АТАКИ НА БЕСПРОВОДНЫЕ СЕТИ Рассматриваемые вопросы: - классификации сетевых атак; - разведка.
6	ЗАЩИТА БЕСПРОВОДНЫХ СЕТЕЙ Рассматриваемые вопросы: - стандарты и нормативные документы; - меры, методы и средства защиты беспроводных сетей.
7	ПОЛИТИКА БЕЗОПАСНОСТИ Рассматриваемые вопросы: - конфигурирование и логическая организация сети; - мониторинг ресурсов и событий сети, сетевого трафика.
8	ПОДХОДЫ К ПРОЕКТИРОВАНИЮ СИСТЕМЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ БЕСПРОВОДНЫХ СЕТЕЙ Рассматриваемые вопросы: - оценка эффективности наборов средств, методов и мер защиты беспроводных сетей; - оптимизация выбора методов, мер и средств защиты; - многослойная система защиты сети.
9	БЕСПРОВОДНЫЕ СЕНСОРНЫЕ СЕТИ Рассматриваемые вопросы: - применение, топологии, архитектура; - стандарты беспроводных сенсорных сетей.
10	ЗАЩИТА ИНФОРМАЦИИ В БЕСПРОВОДНЫХ СЕНСОРНЫХ СЕТЯХ Рассматриваемые вопросы: - БСС, стандарт IEEE 802.15.4 - формат кадров; - защита информации в БСС.
11	ЗАЩИТА В СЕТЯХ WI-FI Рассматриваемые вопросы: - организация сетей Wi-Fi;

№ п/п	Тематика лекционных занятий / краткое содержание
	- методы защиты.
12	СЕТИ WI-FI. МЕТОДЫ ШИФРОВАНИЯ Рассматриваемые вопросы: - режимы доступа; - шифрование; - протоколы.
13	ВИРТУАЛЬНЫЕ ЧАСТНЫЕ СЕТИ VPN (VIRTUAL PRIVATE NETWORK) Рассматриваемые вопросы: - виды соединений; - построение; - настройка соединения.
14	ТЕХНОЛОГИИ И АЛГОРИТМЫ ШИФРОВАНИЯ В VPN Рассматриваемые вопросы: - протоколы; - создание защищенных каналов для обмена данными по различным протоколам; - метод шифрования в PPTP, установление соединения.
15	VIRTUAL PRIVATE NETWORK (VPN). СТРУКТУРЫ ДАННЫХ ПЕРЕДАЧИ Рассматриваемые вопросы: - структура данных для пересылки по туннелю; - механизмы, компоненты, схемы IPSec; - протоколы, туннельный и транспортный режим протоколов.
16	ВИРТУАЛЬНЫЕ ЧАСТНЫЕ СЕТИ. НАСТРОЙКИ ПОЛИТИКА БЕЗОПАСНОСТИ Рассматриваемые вопросы: - основные настройки политика безопасности; - создание упорядоченного списка алгоритмов и групп. - установка и поддержка; - обмен сообщениями в стандартном и агрессивном режимах.

4.2. Занятия семинарского типа.

Лабораторные работы

№ п/п	Наименование лабораторных работ / краткое содержание
1	ШИФРОВАНИЕ ДАННЫХ С ПОМОЩЬЮ ADVANCED ENCRYPTION STANDARD – AES Результат выполнения лабораторной работы – отлаженная программа на языке программирования высокого уровня, реализующую AES (часть AES).
2	АНАЛИЗ БЕСПРОВОДНЫХ ТЕХНОЛОГИЙ И МОДЕЛЕЙ ПРОСТРАНСТВЕННОЙ ОРГАНИЗАЦИИ БЕСПРОВОДНЫХ ШИРОКОПОЛОСНЫХ СЕТЕЙ Результат выполнения работы – отчет с проведенным исследованием и сравнительным анализом характеристик беспроводных технологий (стандартов), и моделей пространственной организации БПШС.
3	АНАЛИЗ УГРОЗ, УЯЗВИМОСТЕЙ И АТАК НА БЕСПРОВОДНЫЕ СЕТИ В результате выполнения работы студент научится анализировать угрозы, уязвимости и атаки на беспроводные сети.
4	ТЕХНОЛОГИИ IPSEC В результате выполнения работы студент изучит возможностей защиты передаваемого трафика на сетевом уровне модели OSI.

№ п/п	Наименование лабораторных работ / краткое содержание
5	МЕХАНИЗМЫ БЕЗОПАСНОСТИ СЕТЕЙ WI-FI В результате выполнения работы студент изучит механизмы обеспечения безопасности беспроводной Wi-Fi сети на базе Windows-клиентов.
6	МЕХАНИЗМЫ БЕЗОПАСНОСТИ СЕТЕЙ WI-FI (ТОПОЛОГИЯ СЕТИ С ИСПОЛЬЗОВАНИЕМ RADIUS-СЕРВЕРА) В результате работы будет настроена защищенная сеть.
7	ИССЛЕДОВАНИЕ МЕТОДОВ И СРЕДСТВ ЗАЩИТЫ БЕСПРОВОДНОЙ СЕНСОРНОЙ СЕТИ Результат работы – отчет с разработанной структурой сети, и описанием комплексной системы защиты беспроводной сенсорной сети, включая технические, программные, программно-технические средства и организационные меры защиты сети.
8	СЕТИ VPN. ПРОТОКОЛ PPTP В результате выполнения работы студент научится настраивать PPTP соединение между MFS и PM.

4.3. Самостоятельная работа обучающихся.

№ п/п	Вид самостоятельной работы
1	Изучение дополнительной литературы
2	Подготовка к лабораторным работам.
3	Работа с лекционным материалом.
4	Подготовка к промежуточной аттестации.
5	Подготовка к текущему контролю.

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: 24.04.2024). - Текст: электронный.
2	Голиков А. М. Защита информации в инфокоммуникационных системах и сетях:	https://e.lanbook.com/book/110336 (дата обращения: 24.04.2024). — Режим доступа: для авториз. пользователей. — Текст: электронный

	учебное пособие / А. М. Голиков. — Москва: ТУСУР, 2015. — 284 с. // Лань: электронно-библиотечная система.	
3	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: 24.04.2024).Режим доступа: для авториз.пользователей.Текст: электронный
4	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: 24.04.2024). — 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.

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.
В случае проведении занятий с применением электронного обучения и дистанционных образовательных технологий необходимо наличие компьютерной техники, для организации коллективных и индивидуальных форм общения педагогических работников со студентами, посредством используемых средств коммуникации. Допускается замена оборудования его виртуальными аналогами.

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 лабораторных занятий:

• компьютерный класс; кондиционер; компьютеры с минимальными требованиями – Pentium 4, ОЗУ 4 ГБ, HDD 100 ГБ, USB 2.0.

9. Форма промежуточной аттестации:

Зачет во 2 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