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

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: 19.10.2022

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	Сем. №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	1. ОСОБЕНЫНОСТИ БЕСПРОВОДНЫХ СЕТЕЙ. Рассматриваемые вопросы: - беспроводная среда (инфракрасное излучение, лазер, радиопередача в узком диапазоне, радиопередача в рассеянном спектре); - беспроводные мобильные сети (пакетное радиосоединение, микроволновые системы, сотовые сети, спутниковые станции); - состав и архитектурные особенности построения БС, функциональные особенности, стандарты. 2. КЛАССИФИКАЦИЯ БЕСПРОВОДНЫХ ТЕХНОЛОГИЙ. Рассматриваемые вопросы: - сектор локальных интерфейсов (короткодействующие технологии беспроводной передачи данных (Bluetooth, WirelessUSB); - сектор локальных домашних и офисных сетей (среднедействующие технологии беспроводной передачи данных (WiFi); - сектор региональных городских сетей (среднедействующие технологии беспроводной передачи данных (WiMAX, Mobile Broadband Wireless Access); - сектор глобальных сетей (дальнедействующие технологии беспроводной передачи данных на базе радиорелейных, сотовых и спутниковых технологий); - беспроводные технологии Zigbee, Z-Wave, WirelessHART, ISA100.11a, Wavenis, MESH сети и др. 3. ОРГАНИЗАЦИЯ БЕСПРОВОДНЫХ ШИРОКОПОЛОСНЫХ СЕТЕЙ (БПШС). Рассматриваемые вопросы: - методы планирования зоны покрытия БПШС (статистические, детерминированные, квазидетерминированные методы); - показатели и факторы качества обслуживания; - модели пространственной организации (Эгли, Окамура, Okumura-Hata, Ли и др.). 4. УГРОЗЫ И УЯЗВИМОСТИ БЕСПРОВОДНЫХ СЕТЕЙ. Рассматриваемые вопросы: - классификации сетевых угроз и уязвимостей; - прямые угрозы - RogueDevices, нефиксированная природа связи, уязвимости сетей и устройств, некорректно сконфигурированные точки доступа, некорректно сконфигурированные беспроводные клиенты, взлом шифрования, Identity Theft, отказы в обслуживании; - косвенные угрозы - утечки информации из проводной сети, особенности функционирования беспроводных сетей (активность в нерабочее время, скорости, интерференция, связь). 5. РАЗВЕДКА И АТАКИ НА БЕСПРОВОДНЫЕ СЕТИ. Рассматриваемые вопросы: - классификации сетевых атак; - разведка, атаки на сети с WEP-шифрованием, пассивные сетевые атаки, активные сетевые атаки, повторное использование вектора инициализации (Initialization Vector Replay Attacks), манипуляция битами (Bit-Flipping Attacks), атаки на сети с WPA/WPA2-шифрованием, атака по словарю на WPA/WPA2 PSK, атака переустановки ключа в WPA и WPA2 (KRACK); - сниффинг, атака MitM (Man in the Middle), ARP-спуфинг, использование переносной точки доступа и др. 6. ЗАЩИТА БЕСПРОВОДНЫХ СЕТЕЙ. Рассматриваемые вопросы: - рекомендации Р 1323565.1.012-2017 (классы защищенности); - «Концепции создания и развития сетей 5G/IMT-2020 в Российской Федерации»;

№ п/п	Тематика лекционных занятий / краткое содержание
	- меры, методы и средства защиты беспроводных сетей: технические, организационные, формальные и неформальные; аппаратные, программные, программно-аппаратные; - влияние человеческого фактора на сетевую безопасность. 7. ПОЛИТИКА БЕЗОПАСНОСТИ. Рассматриваемые вопросы: - конфигурирование и логическая организация сети; - концепция единого входа в доменную систему и проверка подлинности, типы учетных записей; - виртуализация сетей; - права, привилегии и разрешения доступа, администрирование доступа к общим ресурсам, защита ресурсов и администрирование доступа средствами файловой системы; - многодоменная логическая организация сети, доверительные отношения доменов, транзитивная аутентификация, иерархия доменов; - мониторинг ресурсов и событий сети, - мониторинг сетевого трафика. 8. ПОДХОДЫ К ПРОЕКТИРОВАНИЮ СИСТЕМЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ БЕСПРОВОДНЫХ СЕТЕЙ. Рассматриваемые вопросы: - оценка эффективности наборов средств, методов и мер защиты беспроводных сетей; - методический подход к оптимизации выбора методов, мер и средств защиты беспроводных сетей группы стандартов IEEE 802.11; - оптимизация выбора методов, мер и средств защиты; - многослойная система защиты сети (шифрования, скрытие SSID, фильтрация MAC-адресов и передача данных по VPN); - сочетание между надежностью защиты и удобством использования сети. 9. БЕСПРОВОДНЫЕ СЕНСОРНЫЕ СЕТИ. Рассматриваемые вопросы: - применение; - топологии; - архитектура типичной беспроводной сенсорной сети, виды узлов и устройства сети; - стандарты беспроводных сенсорных сетей; - технология ретранслируемой ближней радиосвязи 802.15.4/ZigBee - «Сенсорные сети». 10. ЗАЩИТА ИНФОРМАЦИИ В БЕСПРОВОДНЫХ СЕНСОРНЫХ СЕТЯХ. Рассматриваемые вопросы: - БСС, стандарт IEEE 802.15.4 - формат кадров; - защита информации в БСС; - технология расширения спектра DSSS для защиты информации от прослушивания, и др. 11. ЗАЩИТА В СЕТЯХ WI-FI. Рассматриваемые вопросы: - организация сетей Wi-Fi; - анализ методов защиты; - методы ограничения доступа (фильтрация MAC-адресов, режим скрытого идентификатора SSID); - методы аутентификации (открытая аутентификация (Open Authentication), аутентификация с общим ключом (Shared Key Authentication), аутентификация по MAC-адресу, Wi-Fi Protected Access (WPA), WI-FI Protected Access2 (WPA2, 801.11I), Cisco Centralized Key Managment (CCKM). 12. СЕТИ WI-FI. МЕТОДЫ ШИФРОВАНИЯ. Рассматриваемые вопросы: - WEP-шифрование;

№ п/п	Тематика лекционных занятий / краткое содержание
	- TKIP-шифрование, протокол Message Integrity Check для проверки целостности сообщений; - CKIP-шифрование; - WPA-шифрование, алгоритмы RC4, AES, EAP, расширяемый протокол аутентификации, режимы: Pre-Shared Key (WPA-PSK) - каждый узел вводит пароль для доступа к сети, Enterprise - проверка серверами RADIUS, WPA2-шифрование (IEEE 802.11i); - преимущества и недостатки используемых шифров. 13. ВИРТУАЛЬНЫЕ ЧАСТНЫЕ СЕТИ VPN (VIRTUAL PRIVATE NETWORK). Рассматриваемые вопросы: - преимущества VPN, виды соединений; - построение виртуальных частных сетей; - настройка соединения через VPN-сервер; - VPN-шлюз; - VPN-туннель. 14. ТЕХНОЛОГИИ И АЛГОРИТМЫ ШИФРОВАНИЯ В VPN. Рассматриваемые вопросы: - протоколы: PPTP, L2TP, IPSec; - PPTP - создание защищенных каналов для обмена данными по различным протоколам – IP, IPX, NetBEUI и др.; - метод шифрования, применяемый в PPTP; - установление соединения PPTP. 15. VIRTUAL PRIVATE NETWORK (VPN). СТРУКТУРЫ ДАННЫХ ПЕРЕДАЧИ. Рассматриваемые вопросы: - структура данных для пересылки по туннелю PPTP; - GRE-туннели; - структура данных для пересылки по туннелю L2TP; - IPSec; - документы RFC: RFC 2401, RFC 2402, RFC 2402, RFC 2404, RFC 2405, RFC 2406, RFC 2407, RFC 2408, RFC 2409, RFC 2410, RFC 2411, RFC 2412; - механизмы, компоненты IPSec; - протоколы AH, ESP, IKE, туннельный и транспортный режим протоколов. 16. ВИРТУАЛЬНЫЕ ЧАСТНЫЕ СЕТИ. НАСТРОЙКИ ПОЛИТИКА БЕЗОПАСНОСТИ. Рассматриваемые вопросы: - основные настройки политика безопасности; - создание упорядоченного списка алгоритмов и Diffie-Hellman групп; - ограничение IPSec, схемы применения IPSec; - установка и поддержка VPN; - обмен сообщениями в стандартном и агрессивном режимах; - создании нескольких туннелей и использовании протокола NAT Traversal. Dead Peer Detection.

4.2. Занятия семинарского типа.

Лабораторные работы

№ п/п	Наименование лабораторных работ / краткое содержание
1	1 ШИФРОВАНИЕ ДАННЫХ С ПОМОЩЬЮ ADVANCED ENCRYPTION STANDARD – AES. Результат выполнения лабораторной работы – программа, реализующая соответствующий алгоритм

№ п/п	Наименование лабораторных работ / краткое содержание
	(часть алгоритма). 2 АНАЛИЗ БЕСПРОВОДНЫХ ТЕХНОЛОГИЙ И МОДЕЛЕЙ ПРОСТРАНСТВЕННОЙ ОРГАНИЗАЦИИ БЕСПРОВОДНЫХ ШИРОКОПОЛОСНЫХ СЕТЕЙ. Результат выполнения лабораторной работы - сравнительный анализ характеристик беспроводных технологий и моделей пространственной организации БПШС. 3 АНАЛИЗ УГРОЗ, УЯЗВИМОСТЕЙ И АТАК НА БЕСПРОВОДНЫЕ СЕТИ. Результат выполнения лабораторной работы – описание угроз, уязвимостей и атаки на беспроводные сети. 4 ТЕХНОЛОГИИ IPSEC. Результат выполнения лабораторной работы – перечень обнаруженных неисправностей в конфигурации IPSec-менеджера racoon и возможные способы их устранения. 5 МЕХАНИЗМЫ БЕЗОПАСНОСТИ СЕТЕЙ WI-FI. Результат выполнения лабораторной работы – настроенная защищенная беспроводная сеть необходимой топологии. 6 МЕХАНИЗМЫ БЕЗОПАСНОСТИ СЕТЕЙ WI-FI (ТОПОЛОГИЯ СЕТИ С ИСПОЛЬЗОВАНИЕМ RADIUS-СЕРВЕРА). Результат выполнения лабораторной работы – работоспособная защищенная сеть с использованием RADIUS-сервера. 7 ИССЛЕДОВАНИЕ МЕТОДОВ И СРЕДСТВ ЗАЩИТЫ БЕСПРОВОДНОЙ СЕНСОРНОЙ СЕТИ. Результат выполнения лабораторной работы – описание разработанной и защищенной беспроводной сенсорной сети. 8 СЕТИ VPN. ПРОТОКОЛ PPTP. Результат выполнения лабораторной работы – 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	https://elar.urfu.ru/bitstream/10995/73899/3/978-5-7996-2677-

	информационной безопасности: учебное пособие для студентов вузов. Екатеринбург: Изд-во Урал. ун-та, 2019.- 204 с. - ISBN 978-5-7996-2677-8.	8_2019.pdf(дата обращения: 29.01.2022). - 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: 10.10.2022) - Текст: электронный
3	Голиков, А. М. Защита информации в инфокоммуникационных 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: 04.10.2022). — 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. (дата обращения: 04.10.2022)	Лань: электронно-библиотечная система.https://e.lanbook.com/book/206279.Режим доступа:для авториз.пользователей.Текст: электронный
5	Девянин П. Н. Модели безопасности компьютерных систем. Управление доступом и информационными	Сайт издательства «Горячая линия Телеком»http://www.techbook.ru/book.php?id_book=1137(дата обращения: 10.10.2022).Текст : непосредственный.

	потоками. М.: Горячая линия – Телеком. 2020. – 352с. - ISBN 978-5-9912-0866-6.	
6	Буренин П.В., Девянин П.Н., Лебеденко Е.В. Безопасность операционной системы специального назначения Astra Linux Special Edition. версия 1.6: учебное пособие / П. В. Буренин, П. Н. Девянин, Е. В. Лебеденко [и др.]; под ред. П. Н. Девянина. - 2-е изд., перераб. и доп. - М.: Горячая линия - Телеком, 2021. - 404 с.: ил. - Библиогр.: с. 390-398. - ISBN 978-5-9912-0807-9	Библиотека РУТhttp://library.miit.ru/catalog/(дата обращения: 10.10.2022).Текст: непосредственный.
7	.Г.Олифер, Н.А.Олифер. Компьютерные сети. Принципы, технологии, протоколы: учебное пособие для вузов. - 4-е изд. - СПб.: Питер, 2015. - 944 с. : ил. - ("Учебники для вузов"). - Библиогр.: с. 917. - ISBN 978-5-496-00004-8	Библиотека РУТ (дата обращения: 04.10.2022) полочный шифр 004 О-54.
8	Мэйволд Эрик Безопасность сетей: курс лекций / Мэйволд Эрик - Москва: Интуит НОУ, 2016. - 571 с. - ISBN 978-5-9570-0046-9.	https://book.ru/book/917577(дата обращения: 04.10.2022). 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/).

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

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.

В случае проведении занятии с применением электронного обучения и дистанционных образовательных технологии необходимо наличие компьютернои техники, для организации коллективных и индивидуальных форм общения педагогических работников со студентами, посредством

используемых средств коммуникации. Допускается замена оборудования его виртуальными аналогами.

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»	Сафонова Ирина Евгеньевна

Лист согласования

Заведующий кафедрой ВССиИБ	Б.В. Желенков
Председатель учебно-методической комиссии	Н.А. Клычева