



РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Б1.В.ДВ.02.01 Безопасность беспроводных локальных сетей

Направление подготовки: 10.03.01 Информационная безопасность

Направленность (профиль): Безопасность компьютерных систем (по отрасли или в сфере профессиональной деятельности)

Квалификация (степень): бакалавр

Форма обучения: очная

Институт: математики, естествознания и техники

Кафедра: математического моделирования, компьютерных технологий и информационной безопасности

	очная форма	очно-заочная форма	заочная форма
Курс	4		
Семестр	7		

Лекции	10		
Лабораторные занятия	20		
Практические (семинарские) занятия	10		
в т. ч. практическая подготовка	4		
Форма(ы) промежуточной аттестации	Зачет		
Контроль			
Иные формы работы			
Самостоятельная работа	32		

Всего часов: 72

Трудоемкость: 2 зачетных единицы.

Разработчик(и) рабочей программы: кандидат педагогических наук, доцент Л.Н. Александрова

I. ОРГАНИЗАЦИОННО-МЕТОДИЧЕСКИЙ РАЗДЕЛ

Цель изучения дисциплины:

формирование компетенций по основным разделам дисциплины для целостного представления принципов построения, исследования и анализа защищенных беспроводных локальных сетей.

Задачи изучения дисциплины:

- изучение особенностей беспроводных технологий, в том числе локальных;
- изучение принципов разработки беспроводных сетей и обеспечения их безопасности;
- усвоение основных стандартов построения и защиты беспроводных локальных сетей.

Место дисциплины в структуре ОПОП: реализуется в части, формируемой участниками образовательных отношений блока Б1. Дисциплины (модули).

Планируемые результаты обучения по дисциплине:

Код компетенции	Индикаторы достижения компетенции	Планируемые результаты обучения по дисциплине
ПКС-2	Знать: <ul style="list-style-type: none">- основные виды и классификацию информационных ресурсов организации (предприятия);- сущность профессиональной деятельности по обеспечению защиты информации в процессе эксплуатации автоматизированных систем.	Знает: <ul style="list-style-type: none">- 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: <ul style="list-style-type: none">- выделять из общих информационных ресурсов предприятия информацию, подлежащую защите;- строить модели защиты информации на основе анализа структуры и содержания информационных процессов и особенностей эксплуатации автоматизированных систем.	Умеет: <ul style="list-style-type: none">- выявлять уязвимости беспроводных сетей, анализировать угрозы и предотвращать атаки на беспроводные сети;- проводить оценку безопасности беспроводных сетей.
	Владеть: <ul style="list-style-type: none">- способностью определять информационные ресурсы, подлежащие защите, угрозы безопасности информации и возможные пути их реализации на основе анализа структуры и содержания информационных процессов и особенностей эксплуатации автоматизированных систем;- навыками реализации моделей защиты информации на основе анализа структуры и содержания	Владеет: <ul style="list-style-type: none">- способами определения задач, проведения организационных и технических мероприятий по контролю (мониторингу) защищенности конфиденциальной информации, подготовки материалов по результатам контроля;- навыками разработки защищенных беспроводных сетей.

	информационных процессов и особенностей эксплуатации автоматизированных систем.	
--	---	--

II. СОДЕРЖАНИЕ И ОБЪЕМ ДИСЦИПЛИНЫ

с указанием количества часов, выделенных на контактную работу обучающихся с преподавателем (по видам учебных занятий) и на самостоятельную работу

Очная форма обучения

№	Наименование разделов и тем	Всего часов	Аудиторные занятия			Сам. Раб.
			ЛК	ПЗ	ЛБ	
Раздел 1. Основы функционирования беспроводных сетей		28	4	4	8	12
1	Тема 1. Особенности беспроводных сетей и их классификация	14	2	2	4	6
2	Тема 2. Организация беспроводных широкополосных сетей Разведка и атаки на беспроводные сети.	14	2	2	4	6
Раздел 2. Безопасность беспроводных локальных сетей		44	6	6	12	20
3	Тема 3. Подходы к проектированию системы информационной безопасности беспроводных сетей	14	2	2	4	6
4	Тема 4. Сети WI-FI. Защита в сетях WI-FI.	14	2	2	4	6
5	Тема 5. Виртуальные частные сети VPN. Технологии и алгоритмы шифрования в VPN.	16	2	2	4	8
	Зачет					
	Контроль					
	Итого за 7 семестр	72	10	10	20	32
	в т.ч. практическая подготовка	4		2	2	
	ИТОГО	72	10	10	20	32

Очно-заочная форма обучения

(не реализуется)

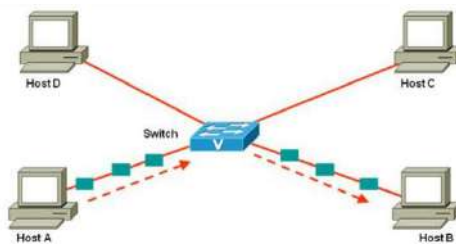
Заочная форма обучения

(не реализуется)

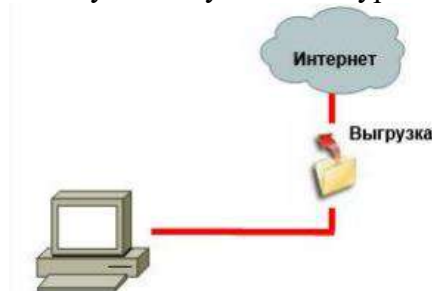
III. ОЦЕНОЧНЫЕ МАТЕРИАЛЫ ДЛЯ ПРОВЕДЕНИЯ ТЕКУЩЕЙ И ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ОБУЧАЮЩИХСЯ ПО ДИСЦИПЛИНЕ

Текущая аттестация проводится в форме контрольной работы.

Задание 1. Посмотрите на изображение. На узле HostA пользователь отправляет сообщение по электронной почте на узел HostB. Сообщение какого типа отошлет узел HostA?



Задание 2. Посмотрите на изображение. После установления соединения, пользователю Интернета необходимо выгрузить текстовый файл. При использовании модели ТСР/ІР, на прикладном уровне требуется один протокол, а на межсетевом уровне - другой. Какие два протокола будут использованы для выгрузки на двух вышеуказанных уровнях?



Задание 4. Посмотрите на изображение. Образовательное учреждение нуждается в подключении к Интернету систем ПК, использующих частную IP-адресацию. Доступ к Интернету требуется для нескольких систем, но образовательное учреждение может приобрести только один публичный IP-адрес. Что необходимо активировать на интегрированном маршрутизаторе Linksys для достижения этой цели?



Задание 5. Посмотрите на изображение. Предположим, что приведенные выходные данные поступили с узла, подключенного к интегрированному маршрутизатору Linksys. Что необходимо проверить в первую очередь, если для поиска неисправностей используется принцип "снизу вверх"?

```
C:\Documents and Settings\User> ipconfig
<<выходные данные опущены>>
IP Address . . . . .: 172.16.32.5
Subnet Mask . . . . .: 255.255.0.0
Default Gateway . . . . .: 172.16.32.1
C:\Documents and Settings\User> ping 172.16.32.1

Pinging 172.16.32.1 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Ping statistics for 172.16.32.1:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss).
```

Промежуточная аттестация обучающихся осуществляется в форме зачета с использованием следующих оценочных материалов: *перечень вопросов к зачету*.

Вопросы к зачету (7 семестр, очная форма обучения)

1. Беспроводная среда - инфракрасное излучение, лазер, радиопередача в узком диапазоне, радиопередача в рассеянном спектре.
2. Беспроводные мобильные сети – пакетное радиосоединение, микроволновые системы, сотовые сети, спутниковые станции. Состав и архитектурные особенности построения БС, функциональные особенности.
3. Сектор локальных интерфейсов (короткодействующие технологии беспроводной передачи данных
4. (Bluetooth, WirelessUSB), сектор локальных домашних и офисных сетей (среднедействующие технологии беспроводной передачи данных (WiFi).
5. 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).
6. Беспроводные технологии Zigbee, Z-Wave, WirelessHART, ISA100.11a, Wavenis, MESH сети и др.
7. Методы планирования зоны покрытия БПШС - статистические, детерминированные, квазидетерминированные методы.
8. Показатели качества обслуживания и факторы, определяющие их.
9. Модели пространственной организации: Эгли, Окамура, Okumura-Hata, Ли и др.
10. Классификации сетевых угроз и уязвимостей.
11. Прямые угрозы – RogueDevices, нефиксированная природа связи, уязвимости сетей и устройств, некорректно сконфигурированные точки доступа, некорректно сконфигурированные беспроводные
12. клиенты, взлом шифрования, имперсонация и Identity Theft, отказы в обслуживании.
13. Косвенные угрозы - утечки информации из проводной сети, особенности функционирования беспроводных сетей (активность в нерабочее время, скорости, интерференция, связь).
14. 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.
15. Рекомендации Р 1323565.1.012-2017 (классы защищенности); проект «Концепции создания и развития сетей 5G/IMT-2020 в Российской Федерации».
16. Меры, методы и средства защиты беспроводных сетей: технические, организационные, формальные и неформальные; аппаратные, программные, программно-аппаратные. Влияние человеческого фактора на сетевую безопасность.
17. Конфигурирование и логическая организация сети. Концепция единого входа в доменную систему и проверка подлинности.
18. Типы учетных записей.
19. Виртуализация сетей.
20. Права, привилегии и разрешения доступа. Администрирование доступа к общим ресурсам.
21. Защита ресурсов и администрирование доступа средствами файловой системы.
22. Многодоменная логическая организация сети.
23. Доверительные отношения доменов.
24. Транзитивная аутентификация. Иерархия доменов.
25. Мониторинг ресурсов и событий сети. Мониторинг сетевого трафика.
26. Оценка эффективности наборов средств, методов и мер защиты беспроводных сетей.

27. Методический подход к оптимизации выбора методов, мер и средств защиты беспроводных сетей группы стандартов IEEE 802.11.
28. Оптимизация выбора методов, мер и средств защиты. Многослойная система защиты сети - шифрования, скрытие SSID, фильтрация MAC-адресов и передача данных по VPN.
29. Сочетание между надежностью защиты и удобством использования сети. Применение. Топологии. Архитектура типичной беспроводной сенсорной сети.
30. Виды узлов и устройства сети. Стандарты беспроводных сенсорных сетей.
31. Технология ретранслируемой ближней радиосвязи 802.15.4/ZigBee - «Сенсорные сети».
32. Организация сетей Wi-Fi. Анализ методов защиты. Методы ограничения доступа – фильтрация MAC-адресов; режим скрытого идентификатора SSID.
33. 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).
34. WEP-шифрование; TKIP-шифрование, протокол Message Integrity Check для проверки целостности сообщений. SKIP-шифрование.
35. 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).
36. Преимущества и недостатки используемых шифров.
37. Преимущества VPN. Виды соединений. Построение виртуальных частных сетей. Настройка соединения через VPN-сервер. VPN-шлюз. VPN-туннель.
38. Протоколы: PPTP, L2TP, IPSec. PPTP - создание защищенных каналов для обмена данными по различным протоколам – IP, IPX, NetBEUI и др.
39. Метод шифрования, применяемый в PPTP. Установление соединения PPTP.
40. Основные настройки политика безопасности. Создание упорядоченного списка алгоритмов и Diffie-Hellman групп.
41. Ограничение IPSec, схемы применения IPSec. Установка и поддержка VPN. Обмен сообщениями в стандартном и агрессивном режимах.
42. Создании нескольких туннелей и использовании протокола NAT Traversal. Dead Peer Detection.

IV. ПЕРЕЧЕНЬ ЛИТЕРАТУРЫ, НЕОБХОДИМОЙ ДЛЯ ОСВОЕНИЯ ДИСЦИПЛИНЫ

4.1. Основная литература

1. Васяева, Н. С. Проектирование локальных вычислительных сетей : учебное пособие для курсового проектирования : [16+] / Н. С. Васяева, Е. С. Васяева ; Поволжский государственный технологический университет. – Йошкар-Ола : Поволжский государственный технологический университет, 2019. – 94 с. : ил. – Режим доступа: по подписке. – URL: <https://biblioclub.ru/index.php?page=book&id=560566> (дата обращения: 18.04.2024). – Библиогр.: с. 78-79 – ISBN 978-5-8158-2062-3. – Текст : электронный.

4.2. Дополнительная литература

1. Бабицын, Л. П. Состав и характеристика сетевого оборудования ЛВС : практическое пособие / Л. П. Бабицын. – Москва : Лаборатория книги, 2012. – 155 с. – Режим доступа: по подписке. – URL: <https://biblioclub.ru/index.php?page=book&id=142475> (дата обращения: 18.04.2024). – ISBN 978-5-504-00926-1. – Текст : электронный.
2. Демидов, Л. Н. Основы эксплуатации компьютерных сетей : учебник для бакалавров / Л. Н. Демидов. – Москва : Прометей, 2019. – 799 с. : ил., табл., схем. – Режим доступа: по подписке.

– URL: <https://biblioclub.ru/index.php?page=book&id=576033> (дата обращения: 18.04.2024). – Библиогр.: с. 750 - 752. – ISBN 978-5-907100-01-5. – Текст : электронный.

3. Компьютерные телекоммуникации : учебное пособие / Ю. Ю. Громов, В. Е. Дидрих, И. В. Дидрих [и др.] ; Тамбовский государственный технический университет. – Тамбов : Тамбовский государственный технический университет (ТГТУ), 2012. – 224 с. : ил., табл., схем. – Режим доступа: по подписке. – URL: <https://biblioclub.ru/index.php?page=book&id=277792> (дата обращения: 18.04.2024). – Библиогр.: с. 220. – Текст : электронный.

4. Трофимов, В. В. Глобальные и локальные сети : учебник для вузов / В. В. Трофимов, М. И. Барабанова, В. И. Кияев. — 4-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2024. — 151 с. — (Высшее образование). — ISBN 978-5-534-20428-5. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: <https://urait.ru/bcode/558136> (дата обращения: 18.04.2024).

V. ПЕРЕЧЕНЬ РЕСУРСОВ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННОЙ СЕТИ «ИНТЕРНЕТ», НЕОБХОДИМЫХ ДЛЯ ОСВОЕНИЯ ДИСЦИПЛИНЫ

№ пп	Ссылка на информационный ресурс	Наименование разработки в электронной форме	Доступность
1.	http://edu.ru/	Российское образование: Федеральный портал. Включает ссылки на порталы и сайты образовательных учреждений; государственные образовательные стандарты; нормативные документы; каталог экскурсий и обучающих программ.	Свободный доступ
2.	http://citforum.ru/database/osbd/contents.shtml	Информационно-аналитические материалы	Свободный доступ

VI. СОВРЕМЕННЫЕ ПРОФЕССИОНАЛЬНЫЕ БАЗЫ ДАННЫХ И ИНФОРМАЦИОННЫЕ СПРАВОЧНЫЕ СИСТЕМЫ

1.	http://www.biblioclub.ru	Электронно-библиотечная система (ЭБС) Университетская библиотека онлайн	Регистрация через любой университетский компьютер. В дальнейшем предоставляется неограниченный индивидуальный доступ из любой точки, в которой имеется доступ к сети Интернет
----	---	--	---

2.	www.garant.ru	Информационно-правовой портал	Свободный доступ
3.	www.elibrary.ru	Российский информационный портал в области науки, технологии, медицины и образования	Свободный доступ
4.	www.consultant.ru	Российская компьютерная справочно-правовая система	Свободный доступ

VII. ЛИЦЕНЗИОННОЕ И СВОБОДНО РАСПРОСТРАНЯЕМОЕ ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ

При реализации учебной дисциплины применяется следующее лицензионное и свободно распространяемое программное обеспечение:

- Microsoft Windows;
- Microsoft Office;
- Libre Office и др.

VIII. ОБОРУДОВАНИЕ И ТЕХНИЧЕСКИЕ СРЕДСТВА ОБУЧЕНИЯ, НЕОБХОДИМЫЕ ДЛЯ ОСУЩЕСТВЛЕНИЯ ОБРАЗОВАТЕЛЬНОГО ПРОЦЕССА ПО ДИСЦИПЛИНЕ

Учебные занятия проводятся в аудиториях, укомплектованных специализированной мебелью, в том числе стационарными или переносными техническими средствами обучения (проектор, экран, компьютер/ноутбук).

Лабораторные занятия, групповые и индивидуальные консультации, текущая и промежуточная аттестации проводятся в специализированных компьютерных классах. Перечень основного оборудования: автоматизированные рабочие места с компьютерами, программное обеспечение общего и профессионального назначения.

Самостоятельная работа проводится в кабинетах, оснащенных компьютерной техникой с возможностью подключения к сети «Интернет» и обеспечением доступа в электронную информационно-образовательную среду университета.