

Документ подписан простой электронной подписью

Информация о владельце:

ФИО: Узунов Федор Владимирович

Должность: Ректор

Дата подписания: 30.09.2026 08:54:43

Уникальный программный ключ:

fd935d10451b860e912264c0378f8458452bfdb697f94388008e29877a6bcbf5

**АВТОНОМНАЯ НЕКОММЕРЧЕСКАЯ ОРГАНИЗАЦИЯ
«ОБРАЗОВАТЕЛЬНАЯ ОРГАНИЗАЦИЯ ВЫСШЕГО ОБРАЗОВАНИЯ»**

«УНИВЕРСИТЕТ ЭКОНОМИКИ И УПРАВЛЕНИЯ»

Факультет экономики, управления и юриспруденции

Кафедра «Управление и бизнес-информатика»



УТВЕРЖДАЮ

Проректор по учебно-

методической работе

Г.П. Узунова

«02» февраля 2026 г.

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ПО ДИСЦИПЛИНЕ

БЕЗОПАСНОСТЬ БЕСПРОВОДНЫХ ЛОКАЛЬНЫХ СЕТЕЙ

Направление подготовки

10.03.01 «Информационная безопасность»

Профиль

Безопасность компьютерных систем

Квалификация выпускника: бакалавр

Для всех
форм обучения

Симферополь, 2026 г.

1. ОЦЕНОЧНЫЕ СРЕДСТВА ДЛЯ ТЕКУЩЕГО КОНТРОЛЯ

Средства оценивания в ходе текущего контроля:

- устные опросы в ходе семинарских занятий;
- рефераты;
- тестирование;
- практические и ситуационные задания, выполняемые в ходе семинарского занятия или рекомендуемые для самостоятельной работы.

Коды компетенции	Результаты освоения ОПОП	Перечень планируемых результатов обучения по дисциплине
ПК-6	Способен организовывать технологический процесс защиты информации ограниченного доступа в соответствии с нормативными правовыми актами и нормативными	ПК-6.1. Знает правовые основы организации защиты государственной тайны и конфиденциальной информации, задачи органов защиты государственной тайны и служб защиты информации на предприятиях, нормативные правовые акты и стандарты по лицензированию деятельности в области обеспечения защиты государственной тайны, технической защиты конфиденциальной информации, нормативные методические документы ФСБ России, ФСТЭК России в области защиты информации; ПК-6.2. Владеет навыками организации и обеспечения режима секретности

1.1 Вопросы к текущему контролю

1. Семейство стандартов IEEE 802.11. Сравните физические уровни стандартов 802.11a, 802.11b, 802.11g, 802.11n, 802.11ac и 802.11ax. Укажите рабочие частотные диапазоны и максимальные теоретические скорости.
2. Методы расширения спектра. Опишите принципы работы FHSS (Frequency Hopping) и DSSS (Direct Sequence). Почему DSSS стал основой для первых стандартов Wi-Fi?
3. Понятие BSS, ESS и IBSS. Различия между инфраструктурным режимом (Infrastructure BSS) и Ad-hoc (Independent BSS). Роль ESSID в роуминге клиентов.
4. Структура кадра Wi-Fi. Назначение полей Frame Control, Duration/ID и четырех адресов MAC в заголовке 802.11.
5. Канальный уровень 802.11. Механизм доступа CSMA/CA. Почему в Wi-Fi используется «слушай перед тем, как говорить» с подтверждением (ACK), в отличие от проводного CSMA/CD?
6. Уязвимости WEP (Wired Equivalent Privacy). Объясните принцип атаки на основе слабых векторов инициализации (IV) и атаки Флюрера, Шамира и Тишера (FMS).
7. WPA (TKIP). Как протокол TKIP (Temporal Key Integrity Protocol) пытался «залатать» дыры WEP без замены старого оборудования? В чем заключалась его основная слабость?
8. WPA2 и CCMP (AES). Почему режим счетчика (Counter Mode) с CBC-MAC (AES-CCMP) считается криптографически стойким по сравнению с TKIP?

9. Четырехстороннее рукопожатие (4-Way Handshake) в WPA2. Опишите процесс обмена кадрами между STA (клиент) и AP (точка доступа) для генерации и подтверждения ключей PTK и GTK.
10. Уязвимость KRACK (Key Reinstallation Attack). В чем заключалась логическая ошибка в стандарте WPA2, позволявшая злоумышленнику расшифровывать трафик путем принудительной переустановки ключа?
11. WPA3: SAE (Simultaneous Authentication of Equals). Как протокол «драконьей» кривой (Dragonfly Handshake) защищает от офлайн-атак по словарю, которые были возможны в WPA2-PSK?
12. Аутентификация в корпоративных сетях (WPA2/WPA3-Enterprise). Роль протоколов семейства IEEE 802.1X. Как работают EAP (Extensible Authentication Protocol) и RADIUS-сервер?
13. Методы EAP. Сравните EAP-TLS, PEAP и EAP-FAST с точки зрения требований к сертификатам и уровня безопасности.
14. Архитектура контроллера беспроводных сетей (WLC). Централизованная (Centralized) против распределенной (Distributed) архитектуры. Преимущества использования CAPWAP/LWAPP.
15. Изоляция клиентов и гостевой доступ. Механизмы L2 изоляции (Client Isolation) и работа Captive Portal (Web Authentication).
16. Обнаружение и предотвращение вторжений (WIDS/WIPS). Как система классифицирует «злой двойник» (Rogue AP) и ложную точку доступа (Honeypot AP)? Методы борьбы (Wireless Containment).
17. Угрозы физического уровня. Атаки типа «отказ в обслуживании» (DoS) через радиопомехи (Jamming) и истощение аккумулятора клиента (Power Consumption Attacks).
18. Безопасность управления. Риски использования протоколов HTTP, Telnet и SNMPv2 для управления точками доступа. Необходимость использования SSHv3 и HTTPS.
19. Wi-Fi Direct и P2P-GO. Специфические риски безопасности при прямом соединении устройств в обход точки доступа.
20. Методология аудита Wi-Fi. Опишите этапы: разведка (Discovery) с помощью Kismet/NetStumbler, анализ рукопожатий (Handshake capture) с Aircrack-ng, и активные атаки (Aireplay-ng). В каких случаях для перехвата рукопожатия необходимо принудительное отключение клиента (Deauthentication attack)?

1.2. Темы рефератов

1. Протокол WEP (Wired Equivalent Privacy): анатомия краха. Анализ слабых векторов инициализации (IV) и атака Флюрера, Шамира и Тишера (FMS).
2. Сравнительный анализ атак на WEP: атака PTW (Tews, Pyshkin, Weinmann) против атаки по словарю (Aircrack-ng). Эффективность и требования к количеству пакетов.
3. WPA с протоколом TKIP: «костыль» для старого оборудования. Механизм MIC (Mikhail) и уязвимость к атакам инъекции QoS-очереди.
4. Четырехстороннее рукопожатие (4-Way Handshake) в WPA2: детальный разбор процесса обмена кадрами EAPOL и генерации парного переходного ключа (PTK).
5. Уязвимость KRACK (Key Reinstallation Attack): логические ошибки в реализации стандарта WPA2 и методы защиты на уровне клиентских ОС до выхода патчей.
6. Переход от WPA2-CCMP к WPA3-SAE: анализ рукопожатия Dragonfly и защита от офлайн-атак по словарю.
7. Архитектура Enterprise-режима Wi-Fi: роль RADIUS-сервера и протокола EAP (Extensible Authentication Protocol) в централизованной аутентификации.
8. Сравнение методов EAP: EAP-TLS, PEAP-MSCHAPv2 и EAP-FAST. Баланс между уровнем безопасности, сложностью развертывания и требованиями к сертификатам.

9. Атаки на протокол MSCHAPv2 в туннеле PEAP: почему использование слабых паролей в корпоративных сетях остается критической угрозой (инструменты ASLEAP).
10. Onboarding (подключение) IoT-устройств в корпоративную сеть: протоколы WPA3-Enterprise Easy Connect (OWE/DPP) и их безопасность.
11. Безопасность RADIUS-инфраструктуры: атаки на перехват трафика внутри туннеля (RADIUS Proxy poisoning) и защита атрибута User-Password.
12. Методология проведения аудита беспроводных сетей: этапы разведки (Discovery), анализа (Analysis) и эксплуатации (Exploitation) в соответствии с методологией PTES.
13. Атаки деаутентификации и диссоциации (Deauthentication/Disassociation): использование фреймов управления 802.11 для перехвата рукопожатий (Handshake) и проведения DoS-атак.
14. Создание «злого двойника» (Rogue Access Point): использование утилит airbase-ng и hostapd-wpe для кражи учетных данных пользователей.
15. Анализ защищенности скрытого SSID и фильтрации MAC-адресов: почему эти методы не являются реальной защитой и обходятся за считанные минуты.
16. Использование программно-определяемых радиосистем (SDR) для анализа Wi-Fi: возможности HackRF One и RTL-SDR за пределами стандартных адаптеров с режимом монитора.
17. Анализ побочных каналов (Side-Channel Attacks) в Wi-Fi: атаки по времени (timing attacks) на реализации криптографических функций в драйверах.
18. Угрозы физического уровня: постановка помех (Jamming) и создание «RF-зон тишины» как средство нарушения доступности сети.
19. Безопасность Wi-Fi Direct и P2P-соединений: риски несанкционированного доступа к файловым системам мобильных устройств и принтерам.
20. Анонимность в беспроводных сетях: уязвимости протоколов локации (802.11k/v/r) и отслеживание устройств по MAC-адресу (протоколы предотвращения: Private MAC Address в iOS/Android).
21. Протокол OWE (Opportunistic Wireless Encryption) в открытых сетях: замена незащищенного Open Wi-Fi на автоматически шифруемые соединения без пароля.
22. Безопасность Mesh-сетей Wi-Fi: механизмы маршрутизации (802.11s) и защита транзитного трафика между узлами (Mesh Peering).
23. Защита спектра в диапазоне 6 ГГц (Wi-Fi 6E / Wi-Fi 7): новые возможности и новые векторы атак на расширенном частотном поле.
24. Контроллеры беспроводного доступа (WLC): безопасность протоколов управления CAPWAP/LWAPP и риски компрометации центрального узла управления.
25. Wireless Intrusion Prevention Systems (WIPS): методы автоматического обнаружения и подавления (containment) несанкционированных точек доступа (Rogue AP).

1.3 Тестовые задания

1. Какой механизм доступа к среде передачи данных используется в стандартах Wi-Fi (IEEE 802.11) для предотвращения коллизий? а) CSMA/CD (Collision Detection) б) Token Passing в) CSMA/CA (Collision Avoidance) г) Полудуплексный режим с фиксированным тайм-слотом *Правильный ответ: в (Обоснование: в беспроводной среде сложно одновременно передавать и слушать для обнаружения коллизий, поэтому используется механизм «слушай перед тем, как говорить» с подтверждением ACK).*
2. Какой протокол безопасности Wi-Fi считается полностью скомпрометированным и непригодным к использованию из-за уязвимости в векторе инициализации (IV)? а) WPA3-SAE б) WPA2-CCMP в) WEP (Wired Equivalent Privacy) г) WPA-TKIP *Правильный ответ: в*
3. Какова основная цель атаки типа «Deauthentication» (деаутентификация) в сетях WPA2? а) Полное уничтожение прошивки точки доступа. б) Принудительный разрыв

текущего соединения клиента для перехвата четырехстороннего рукопожатия (4-Way Handshake). в) Изменение пароля администратора точки доступа через веб-интерфейс. г) Создание зашифрованного туннеля до клиента. *Правильный ответ: б*

4. Какой криптографический алгоритм является основным и наиболее стойким в стандарте WPA2? а) RC4 б) TKIP в) AES-CCMP г) DES *Правильный ответ: в*

5. В чем заключается основная уязвимость, эксплуатируемая в атаке KRACK (Key Reinstallation Attack) против WPA2? а) Использование слабого пароля пользователем. б) Ошибка в логике четырехстороннего рукопожатия, позволяющая переустановить ключ и сбросить параметры шифрования (nonce). в) Перехват трафика до того, как он был зашифрован. г) Взлом центрального RADIUS-сервера. *Правильный ответ: б*

6. Какой метод аутентификации используется в корпоративных сетях (режим Enterprise) для централизованной проверки учетных данных пользователей? а) WPA2-PSK (Pre-Shared Key) б) WEP с общим ключом в) IEEE 802.1X с использованием RADIUS-сервера г) Фильтрация MAC-адресов *Правильный ответ: в*

7. Какой протокол аутентификации внутри защищенного TLS-туннеля (PEAP) часто подвергается офлайн-атакам на перебор паролей из-за слабости алгоритма хеширования? а) EAP-TLS б) MS-CHAPv2 в) EAP-FAST г) EAP-IKEv2 *Правильный ответ: б*

8. Что такое «Rogue Access Point» (Rogue AP) в контексте безопасности предприятия? а) Точка доступа, работающая на частоте 6 ГГц. б) Несанкционированная точка доступа, подключенная к корпоративной сети сотрудником или злоумышленником. в) Точка доступа с самым мощным передатчиком в здании. г) Виртуальная точка доступа, созданная на ноутбуке. *Правильный ответ: б*

9. Какой новый метод рукопожатия (Handshake) введен в стандарте WPA3 для защиты от офлайн-атак по словарю, которые были возможны в WPA2-PSK? а) 4-Way Handshake б) SAE (Simultaneous Authentication of Equals) / Dragonfly в) PSK v2 г) Diffie-Hellman Group 14 *Правильный ответ: б*

10. Почему использование скрытого SSID (Hidden SSID) и фильтрации MAC-адресов не считается надежной защитой беспроводной сети? а) Потому что эти функции не поддерживаются современными устройствами. б) Потому что SSID и MAC-адреса передаются в открытом виде в служебных пакетах (Probe Response/Association), и их легко перехватить. в) Потому что они замедляют скорость интернета в 10 раз. г) Потому что они блокируют работу Bluetooth. *Правильный ответ: б*

11. Какой режим работы Wi-Fi позволяет двум устройствам соединиться напрямую без использования точки доступа (инфраструктуры)? а) Infrastructure Mode б) Ad-Hoc (IBSS) в) Monitor Mode г) Master Mode *Правильный ответ: б*

12. Для чего в корпоративных сетях используется система WIPS (Wireless Intrusion Prevention System)? а) Для автоматического увеличения скорости Wi-Fi до максимума. б) Для автоматического обнаружения и подавления (containment) несанкционированных точек доступа и атак. в) Для очистки жестких дисков компьютеров от вирусов. г) Для печати документов с мобильных телефонов. *Правильный ответ: б*

13. Какой заголовок (Header) в стандарте 802.11 содержит информацию о типе кадра, подтипе и наличии шифрования? а) Frame Control б) Duration/ID в) Sequence Control г) FCS (Frame Check Sequence) *Правильный ответ: а*

14. В чем заключается атака «Злой двойник» (Evil Twin)? а) Установка двух одинаковых точек доступа в одной комнате для балансировки нагрузки. б) Создание поддельной точки доступа с таким же именем (SSID), как у легитимной, для перехвата трафика и кражи паролей. в) Использование двух антенн для усиления сигнала. г) Одновременная работа точки доступа в диапазонах 2.4 ГГц и 5 ГГц. *Правильный ответ: б*

15. Какой протокол был разработан для замены незащищенных открытых сетей (Open Wi-Fi) в кафе и аэропортах, обеспечивая автоматическое шифрование трафика без ввода пароля? а) WEP б) OWE (Opportunistic Wireless Encryption) в) WPA-PSK г) PEAP *Правильный ответ: б*

16. Тесты «Вставьте пропущенное слово»
17. Протокол безопасности WEP (Wired Equivalent Privacy) считается скомпрометированным из-за малого размера и повторяющегося использования вектора _____ (IV) в потоке RC4. *(Правильный ответ: инициализации)*
18. Для принудительного разрыва соединения клиента с точкой доступа и перехвата четырехстороннего рукопожатия (4-Way Handshake) в атаках на WPA2 используется фрейм _____. *(Правильный ответ: деаутентификации / Deauthentication)*
19. Основным и криптографически стойким протоколом шифрования в стандарте WPA2 является _____ (основанный на AES). *(Правильный ответ: CCMP / AES-CCMP)*
20. В корпоративных сетях для централизованной аутентификации пользователей по стандарту 802.1X используется протокол _____, работающий на базе RADIUS-сервера. *(Правильный ответ: EAP / Extensible Authentication Protocol)*
21. Уязвимость KRACK (Key Reinstallation Attack) эксплуатировала ошибку в логике _____ рукопожатия (4-Way Handshake), позволяя злоумышленнику принудительно переустановить ключи шифрования. *(Правильный ответ: четырехстороннего)*
22. В стандарте WPA3 для защиты от офлайн-атак по словарю вместо Pre-Shared Key (PSK) используется метод рукопожатия _____ (SAE). *(Правильный ответ: Dragonfly / Simultaneous Authentication of Equals)*
23. Режим работы Wi-Fi адаптера, позволяющий ему перехватывать любые пакеты в радиозфере без подключения к конкретной сети, называется режимом _____. *(Правильный ответ: монитора / Monitor Mode)*
24. Несанкционированная точка доступа, подключенная к корпоративной сети (например, сотрудником в нарушение политики), называется _____ точкой доступа (Rogue AP). *(Правильный ответ: ложной / нелегитимной / несанкционированной)*
25. Механизм доступа к среде CSMA/CA, используемый в Wi-Fi, расшифровывается как Collision _____ (предотвращение коллизий), в отличие от проводного Ethernet, который их обнаруживает. *(Правильный ответ: Avoidance)*
26. Технология создания беспроводной сети напрямую между двумя устройствами без использования точки доступа (инфраструктуры) называется _____ (режим Ad-Hoc). *(Правильный ответ: IBSS / Independent Basic Service Set)*

27. Соответствие между стандартом безопасности и его характеристикой

Стандарт Характеристика / Статус

- | | |
|-------------|--|
| 1. WEP | А. Современный стандарт, использующий рукопожатие SAE для защиты от перебора паролей. |
| 2. WPA2-PSK | Б. Устаревший протокол, использующий RC4 и уязвимый из-за слабых векторов инициализации (IV). |
| 3. WPA3-SAE | В. Стандарт, использующий AES-CCMP, но уязвимый к атаке KRACK и офлайн-атакам по словарю на PSK. |
| 4. WPA-TKIP | Г. Временное решение («костыль») для замены WEP на старом оборудовании, использующее MIC. |

Правильные ответы: 1–Б, 2–В, 3–А, 4–Г.

28. Соответствие между типом атаки и ее целью

Тип атаки Цель / Механизм

- | | |
|---------------------|--|
| 1. Evil Twin | А. Принудительный разрыв соединения клиента для перехвата рукопожатия. |
| 2. Deauthentication | Б. Создание поддельной точки доступа с тем же именем для кражи учетных данных. |
| 3. Rogue AP | В. Создание помех в радиозфере для нарушения доступности сети |

Тип атаки	Цель / Механизм (DoS).
4. Jamming	Г. Несанкционированная точка доступа внутри периметра сети для обхода файрвола.

Правильные ответы: 1–Б, 2–А, 3–Г, 4–В.

29. Соответствие между протоколом EAP и его особенностью

Протокол EAP Особенность

1. EAP-TLS	А. Использует туннель PEAP для защиты обмена, но внутри использует уязвимый хеш MS-CHAPv2 и пароль.
2. PEAP-MSCHAPv2	Б. Сертификаты требуются только на сервере, клиент аутентифицируется логином/паролем внутри защищенного TLS-туннеля.
3. EAP-FAST	В. Требуется наличия цифровых сертификатов как на сервере, так и на каждом клиенте (наиболее безопасный).
4. EAP-TTLS	Г. Создает защищенный TLS-туннель с помощью «быстрого» (Flexible) метода, используя PAC (Protected Access Credential).

Правильные ответы: 1–Б, 2–А, 3–Г, 4–Б.

30. Соответствие между инструментом аудита и его функцией

Инструмент Функция

1. Airodump-ng	А. Генерация трафика и принудительная деаутентификация клиентов для ускорения перехвата рукопожатия.
2. Aircrack-ng	Б. Перехват «сырых» пакетов из эфира и сохранение рукопожатий в файл (мониторинг).
3. Aircrack-ng	В. Взлом паролей WEP/WPA из перехваченных файлов с помощью словарных атак или перебора.
4. Wireshark	Г. Графический анализ структуры кадров 802.11 и содержимого EAPOL-пакетов.

Правильные ответы: 1–Б, 2–В, 3–А, 4–Г.

31. Соответствие между термином архитектуры Wi-Fi и определением

Термин	Определение
1. BSS (Basic Service Set)	А. Одна точка доступа и все связанные с ней клиенты (базовая ячейка).
2. ESS (Extended Service Set)	Б. Прямое соединение устройств друг с другом без точки доступа.
3. SSID	В. Набор из нескольких точек доступа, соединенных распределительной системой, представляющий одну сеть.
4. IBSS	Г. Текстовое имя беспроводной сети, используемое для идентификации.

Правильные ответы: 1–А, 2–В, 3–Г, 4–Б.

1.4 Практические и ситуационные задания

Задание 1. Сравните физические уровни стандартов IEEE 802.11a, 802.11g и 802.11n. Укажите рабочие частотные диапазоны и ключевые технологии (OFDM, MIMO), позволившие увеличить скорость передачи данных.

Задание 2. Опишите механизм доступа к среде CSMA/CA. Почему в беспроводных сетях подтверждение получения кадра (ACK) является критически важным элементом протокола, в отличие от проводного Ethernet?

Задание 3. Уязвимости протокола WEP. Объясните роль вектора инициализации (IV) в алгоритме RC4 и покажите, как его малый размер (24 бита) приводит к коллизиям и возможности взлома ключа.

Задание 4. Протокол TKIP (WPA). Опишите, как он пытался обеспечить безопасность на старом оборудовании (после WEP). В чем заключалась слабость механизма MIC (Mikhael) и атака на него?

Задание 5. WPA2-CCMP (AES). Почему режим счетчика (Counter Mode) с аутентификацией сообщения (CBC-MAC) считается криптографически стойким? Сравните его структуру с режимом потокового шифрования RC4 в WEP.

Задание 6. Четырехстороннее рукопожатие (4-Way Handshake) в WPA2. Опишите процесс генерации и подтверждения парного переходного ключа (PTK) и группового ключа (GTK) между STA и AP.

Задание 7. Протокол SAE (Simultaneous Authentication of Equals) в WPA3. Объясните принцип «драконьей» кривой (Dragonfly Handshake) и то, как он защищает от офлайн-атак по словарю, которые были возможны в WPA2-PSK.

Задание 8. Opportunistic Wireless Encryption (OWE). Как этот стандарт обеспечивает шифрование в открытых (Public) Wi-Fi сетях без использования пароля (PSK)?

Задание 9. Аутентификация Enterprise (802.1X). Опишите роли Supplicant (клиент), Authenticator (точка доступа) и Authentication Server (RADIUS) в процессе проверки учетных данных.

Задание 10. Сравнение методов EAP. В чем разница между EAP-TLS, PEAP-MSCHAPv2 и EAP-FAST с точки зрения требований к инфраструктуре открытых ключей (PKI) и уровня безопасности?

Задание 11. Уязвимость KRACK (Key Reinstallation Attack). Опишите механизм атаки на этапе 3 четырехстороннего рукопожатия. Почему это была уязвимость стандарта, а не конкретной реализации?

Задание 12. Атака «Злой двойник» (Evil Twin). Опишите этапы развертывания поддельной точки доступа с использованием утилиты hostapd и dnsmasq для кражи учетных данных пользователей.

Задание 13. Атаки деаутентификации (Deauthentication Attack). Почему фреймы управления 802.11, такие как Deauth, передаются в открытом виде и как это используется для проведения атак типа «отказ в обслуживании» (DoS) и перехвата рукопожатий?

Задание 14. Методология аудита Wi-Fi (Penetration Testing). Опишите этапы: разведка (Discovery) с помощью Kismet, захват рукопожатия (Handshake capture) и брутфорс PSK с использованием Hashcat.

Задание 15. Угрозы физического уровня. Что такое Jamming (радиопомехи)? Опишите разницу между постоянным шумом и реактивным подавлением сигнала.

Задание 16. Безопасность скрытого SSID и фильтрации MAC-адресов. Объясните, почему эти методы считаются «безопасностью через неясность» (Security through Obscurity) и как легко они обходятся.

Задание 17. Архитектура контроллера беспроводных сетей (WLC). Опишите протокол CAPWAP и разницу между режимами Split MAC и Local MAC.

Задание 18. Системы предотвращения вторжений (WIPS). Как система классифицирует «злой двойник» (Rogue AP) и какие методы «сдерживания» (Containment) она применяет (например, отправка Deauth пакетов)?

Задание 19. Безопасность Mesh-сетей (802.11s). Опишите механизм Mesh Peering Management (MPM) и риски компрометации транзитного трафика в ячеистой топологии.

Задание 20. Безопасность управления точками доступа. Сравните риски использования протоколов Telnet, HTTP и SNMPv2c против SSHv3 и HTTPS для администрирования инфраструктуры. Опишите типичные векторы атак на незащищенные интерфейсы управления.

2. КРИТЕРИИ ОЦЕНИВАНИЯ ПРИ ПРОВЕДЕНИИ ТЕКУЩЕГО КОНТРОЛЯ

Вид контроля	Наименование работы	Наименование оценочных средств	Шкала оценивания
Текущий контроль	Вопросы для обсуждения на занятиях; Устные опросы по ранее изученному материалу; Письменные работы: рефераты, тестовые задания; Ситуационные и практические задания; Рефераты и доклады по темам (вопросам), вынесенным на самостоятельную работу.	Оценка выступлений на практическом (семинарском) занятии, проверка заданий и аудиторных работ, устный опрос, оценивание докладов, рефератов	отлично хорошо удовлетворительно неудовлетворительно

Критерии оценивания устных ответов обучающихся

Шкала оценивания	Характеристика оценивания
отлично	оценивается ответ, который показывает прочные знания основных процессов изучаемой предметной области, отличается глубиной и полнотой раскрытия темы; владение терминологическим аппаратом; умение объяснять сущность, явлений, процессов, событий, делать выводы и обобщения, давать аргументированные ответы, приводить примеры; свободное владение монологической речью, логичность и последовательность ответа.
хорошо	оценивается ответ, обнаруживающий прочные знания основных процессов изучаемой предметной области, отличается глубиной и полнотой раскрытия темы; владение терминологическим аппаратом; умение объяснять сущность, явлений, процессов, событий, делать выводы и обобщения, давать аргументированные ответы, приводить примеры; свободное владение монологической речью, логичность и последовательность ответа. Однако допускается одна - две неточности в ответе.
удовлетворительно	оценивается ответ, свидетельствующий в основном о знании процессов изучаемой предметной области, отличающийся недостаточной глубиной и полнотой раскрытия темы; знанием основных вопросов теории; слабо сформированными навыками анализа явлений, процессов, недостаточным умением давать аргументированные ответы и приводить примеры; недостаточно свободным владением монологической речью, логичностью и последовательностью ответа. Допускается несколько ошибок в содержании ответа.
неудовлетворительно	оценивается ответ, обнаруживающий незнание процессов изучаемой предметной области, отличающийся неглубоким раскрытием темы; незнанием основных вопросов теории, несформированными навыками анализа явлений, процессов; неумением давать аргументированные ответы, слабым владением монологической речью, отсутствием логичности и последовательности. Допускаются серьезные ошибки в содержании ответа.

Критерии оценивания работы обучающихся на практических и семинарских занятиях

Шкала оценивания	Показатели	Критерии
Отлично	1. Полнота выполнения практического и тестового задания (полнота ответа); 2. Своевременность выполнения задания; 3. Последовательность и рациональность выполнения практического задания (логичность и четкость ответа);	Задание решено самостоятельно. При этом составлен правильный алгоритм решения задания, в логических рассуждениях, в выборе формул и решении нет ошибок, получен верный ответ, задание решено рациональным способом. Дан правильный и исчерпывающий ответ на поставленные теоретические и тестовые вопросы, в которых обучающийся показал всестороннее системное знание программного материала, усвоение основной и дополнительной литературы, четкое владение понятийным аппаратом.
Хорошо	4. Правильность ответов на вопросы; 5. Самостоятельность решения (владение дополнительным материалом); 6. Знание нормативно-законодательной базы и терминологии курса	Задание решено с помощью преподавателя. При этом составлен правильный алгоритм решения задания, в логическом рассуждении и решении нет существенных ошибок; правильно сделан выбор формул для решения; есть объяснение решения, но задание решено нерациональным способом или допущено не более двух несущественных ошибок, получен верный ответ. На поставленные теоретические и тестовые вопросы, при которых обучающийся показал достаточный уровень знаний основного программного материала: освоение информации лекционного курса и учебных пособий, овладение понятийным аппаратом, методикой исследований при попытке анализа различных ситуаций.
Удовлетворительно		Задание решено с подсказками преподавателя. Задание решено в общем виде. Обучающийся показал средний уровень знаний основного программного материала, но не мог убедительно аргументировать свой ответ, ошибся в использовании понятийного аппарата, показал недостаточные знания литературных источников.
Неудовлетворительно		Задание не решено. Обучающийся продемонстрировал значительные пробелы в знаниях основного программного материала, не аргументировал свой ответ, показал неудовлетворительные знания понятийного аппарата и специальной литературы.

Критерии оценивания рефератов

Форам контроля	Критерии оценивания	Шкала оценивания
Реферат	Выполнены все методические требования к написанию реферата: определена тема, актуальность; содержание соответствует теме и плану реферата; сделан краткий анализ различных точек зрения по рассматриваемой проблеме;	зачтено

	грамотно использованы первоисточники при анализе содержания; выводы сформулированы лаконично с логическими доказательствами; соблюдены требования по внешнему оформлению. Тема реферата раскрыта в полном объеме.	
	Нарушены требования по написанию и оформлению реферата. Несоответствие темы реферата. В тексте не отражены существенные моменты. Тема реферата не раскрыта до конца. Сделаны необоснованные выводы.	не зачтено

Критерии оценивания тестов

Средство контроля	Критерии оценивания – процент положительных ответов	Шкала оценивания
Тестирование	90-100	отлично
	70-89	хорошо
	40-69	удовлетворительно
	< 39	неудовлетворительно

3. ОЦЕНОЧНЫЕ СРЕДСТВА ДЛЯ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ

Средства оценивания в ходе промежуточной аттестации:

– вопросы для зачета;

–практические задания для зачета.

Коды компетенции	Результаты освоения ОПОП	Перечень планируемых результатов обучения по дисциплине
ПК-6	Способен организовывать технологический процесс защиты информации ограниченного доступа в соответствии с нормативными правовыми актами и нормативными	ПК-6.1. Знает правовые основы организации защиты государственной тайны и конфиденциальной информации, задачи органов защиты государственной тайны и служб защиты информации на предприятиях, нормативные правовые акты и стандарты по лицензированию деятельности в области обеспечения защиты государственной тайны, технической защиты конфиденциальной информации, нормативные методические документы ФСБ России, ФСТЭК России в области защиты информации; ПК-6.2. Владеет навыками организации и обеспечения режима секретности

3.1. Вопросы к зачету

1. Структура кадра 802.11. Назначение полей Frame Control, Duration/ID и четырех MAC-адресов. В каких сценариях используются все четыре адреса?

2. Механизм доступа к среде CSMA/CA. Почему в беспроводных сетях используется «прослушивание перед передачей» с подтверждением (ACK), в отличие от обнаружения коллизий (CD) в проводном Ethernet?
3. Топологии беспроводных сетей. Различия между BSS (Basic Service Set), ESS (Extended Service Set) и IBSS (Independent BSS). Роль SSID и BSSID.
4. Канальный уровень и фрагментация. Как механизм RTS/CTS (Request to Send / Clear to Send) решает проблему «скрытого узла» (Hidden Node)?
5. Сравнение физических уровней. Ключевые отличия стандартов 802.11a/b/g/n/ac/ax (частотные диапазоны, модуляции, технологии OFDM/MIMO).
6. Протокол WEP. Объясните роль вектора инициализации (IV) и почему его малый размер (24 бита) делает протокол уязвимым к атакам типа FMS и PTW.
7. Механизм Integrity Algorithm (ICV) в WEP. Почему контроль целостности не защитил WEP от модификации пакетов?
8. WPA с протоколом TKIP. Как TKIP обеспечил обратную совместимость с оборудованием WEP и в чем заключалась главная слабость механизма MIC (Mikhael)?
9. Четырехстороннее рукопожатие (4-Way Handshake) в WPA2. Опишите процесс генерации парного переходного ключа (PTK) из PMK, ANonce и SNonce.
10. Уязвимость KRACK (Key Reinstallation Attack). В чем заключалась логическая ошибка стандарта WPA2, позволявшая злоумышленнику переустанавливать ключи шифрования?
11. SAE (Simultaneous Authentication of Equals). Опишите принцип «драконьего» рукопожатия (Dragonfly Handshake) и объясните, как он защищает от офлайн-атак по словарю, возможных в WPA2-PSK.
12. WPA3-Enterprise (192-битная безопасность). Какие дополнительные криптографические требования (GCM-256, SHA-384) предъявляются к этому режиму?
13. Opportunistic Wireless Encryption (OWE). Как OWE обеспечивает конфиденциальность в открытых (Open) Wi-Fi сетях без использования общего пароля?
14. Wi-Fi Enhanced Open. В чем разница между традиционным открытым Wi-Fi и сетью с использованием OWE с точки зрения пассивного перехвата трафика?
15. Forward Secrecy в WPA3. Как использование протокола SAE гарантирует, что компрометация пароля в будущем не позволит расшифровать ранее записанный трафик?
16. Архитектура Enterprise-режима. Роли Supplicant (клиент), Authenticator (точка доступа) и Authentication Server (RADIUS) в процессе 802.1X.
17. Протокол EAP-MD5. Почему данный метод не подходит для аутентификации в беспроводных сетях (отсутствие взаимной аутентификации и защиты от MITM)?
18. PEAP (Protected EAP). Как создается защищенный TLS-туннель и почему использование MS-CHAPv2 внутри этого туннеля остается рискованным при слабых паролях?
19. EAP-TLS. Почему этот метод считается наиболее безопасным? Какие требования к инфраструктуре (PKI) он предъявляет?
20. EAP-FAST. Какова роль PAC (Protected Access Credential) в создании защищенного туннеля без использования сертификатов на стороне клиента?
21. Атака «Злой двойник» (Evil Twin). Опишите этапы развертывания поддельной точки доступа для кражи учетных данных (Captive Portal) или перехвата трафика.
22. Атаки деаутентификации (Deauthentication Attack). Почему фреймы управления 802.11 передаются без шифрования и как это используется для проведения DoS-атак и форсированного захвата рукопожатий?
23. Инструментарий аудита (Aircrack-ng suite). Назовите функции утилит airodump-ng, aircrack-ng и aircrack-ng в процессе взлома WPA2-PSK.
24. Rogue Access Point (Несанкционированная ТД). Классификация типов «ложных» точек доступа (подключенная сотрудником, хакерская, неправильная настройка) и методы их обнаружения (WIPS).

25. Атаки на конфиденциальность местоположения. Как отслеживание MAC-адресов (даже случайных) и анализ Probe Request кадров позволяют проводить слежку за перемещением пользователей?
26. Беспроводные контроллеры (WLC). Принципы работы протоколов CAPWAP/LWAPP. Риски централизованной архитектуры (единая точка отказа/взлома).
27. Системы предотвращения вторжений (WIPS). Методы автоматического «подавления» (Containment) несанкционированных точек доступа и этические/правовые ограничения этих методов.
28. Безопасность Mesh-сетей (802.11s). Механизмы Mesh Peering и шифрования транзитного трафика (SAE в mesh).
29. Безопасность управления. Сравнение рисков использования Telnet/HTTP и SSH/HTTPS для администрирования точек доступа. Защита протоколов SNMP (v1/v2c vs v3).
30. Угрозы физического уровня (RF Jamming). Различие между постоянным шумом (Barrage Jamming) и точечным подавлением (Protocol-aware Jamming). Способы противодействия.

3.2. Практические задания к зачету с оценкой

Задание 1. Сравните физические уровни стандартов IEEE 802.11a, 802.11g и 802.11n. Укажите рабочие частотные диапазоны и ключевые технологии (OFDM, MIMO), позволившие увеличить скорость передачи данных.

Задание 2. Опишите механизм доступа к среде CSMA/CA. Почему в беспроводных сетях подтверждение получения кадра (ACK) является критически важным элементом протокола, в отличие от проводного Ethernet?

Задание 3. Уязвимости протокола WEP. Объясните роль вектора инициализации (IV) в алгоритме RC4 и покажите, как его малый размер (24 бита) приводит к коллизиям и возможности взлома ключа.

Задание 4. Протокол TKIP (WPA). Опишите, как он пытался обеспечить безопасность на старом оборудовании (после WEP). В чем заключалась слабость механизма MIC (Mikhael) и атака на него?

Задание 5. WPA2-CCMP (AES). Почему режим счетчика (Counter Mode) с аутентификацией сообщения (CBC-MAC) считается криптографически стойким? Сравните его структуру с режимом потокового шифрования RC4 в WEP.

Задание 6. Четырехстороннее рукопожатие (4-Way Handshake) в WPA2. Опишите процесс генерации и подтверждения парного переходного ключа (PTK) и группового ключа (GTK) между STA и AP.

Задание 7. Протокол SAE (Simultaneous Authentication of Equals) в WPA3. Объясните принцип «драконьей» кривой (Dragonfly Handshake) и то, как он защищает от офлайн-атак по словарю, которые были возможны в WPA2-PSK.

Задание 8. Opportunistic Wireless Encryption (OWE). Как этот стандарт обеспечивает шифрование в открытых (Public) Wi-Fi сетях без использования пароля (PSK)?

Задание 9. Аутентификация Enterprise (802.1X). Опишите роли Supplicant (клиент), Authenticator (точка доступа) и Authentication Server (RADIUS) в процессе проверки учетных данных.

Задание 10. Сравнение методов EAP. В чем разница между EAP-TLS, PEAP-MSCHAPv2 и EAP-FAST с точки зрения требований к инфраструктуре открытых ключей (PKI) и уровня безопасности?

Задание 11. Уязвимость KRACK (Key Reinstallation Attack). Опишите механизм атаки на этапе 3 четырехстороннего рукопожатия. Почему это была уязвимость стандарта, а не конкретной реализации?

Задание 12. Атака «Злой двойник» (Evil Twin). Опишите этапы развертывания поддельной точки доступа с использованием утилиты hostapd и dnsmasq для кражи учетных данных пользователей.

Задание 13. Атаки деаутентификации (Deauthentication Attack). Почему фреймы управления 802.11, такие как Deauth, передаются в открытом виде и как это используется для проведения атак типа «отказ в обслуживании» (DoS) и перехвата рукопожатий?

Задание 14. Методология аудита Wi-Fi (Penetration Testing). Опишите этапы: разведка (Discovery) с помощью Kismet, захват рукопожатия (Handshake capture) и брутфорс PSK с использованием Hashcat.

Задание 15. Угрозы физического уровня. Что такое Jamming (радиопомехи)? Опишите разницу между постоянным шумом и реактивным подавлением сигнала.

Задание 16. Безопасность скрытого SSID и фильтрации MAC-адресов. Объясните, почему эти методы считаются «безопасностью через неясность» (Security through Obscurity) и как легко они обходятся.

Задание 17. Архитектура контроллера беспроводных сетей (WLC). Опишите протокол CAPWAP и разницу между режимами Split MAC и Local MAC.

Задание 18. Системы предотвращения вторжений (WIPS). Как система классифицирует «злой двойник» (Rogue AP) и какие методы «сдерживания» (Containment) она применяет (например, отправка Deauth пакетов)?

Задание 19. Безопасность Mesh-сетей (802.11s). Опишите механизм Mesh Peering Management (MPM) и риски компрометации транзитного трафика в ячеистой топологии.

Задание 20. Безопасность управления точками доступа. Сравните риски использования протоколов Telnet, HTTP и SNMPv2c против SSHv3 и HTTPS для администрирования инфраструктуры. Опишите типичные векторы атак на незащищенные интерфейсы управления.

4. КРИТЕРИИ ОЦЕНИВАНИЯ ПРИ ПРОВЕДЕНИИ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ

**Шкала оценивания уровня сформированности компетенции
(по пятибалльной системе) (зачет с оценкой)**

Шкала оценивания	Уровень освоение компетенции	Критерии оценивания
Зачет	Базовый уровень освоения компетенции	Дан правильный и исчерпывающий ответ на вопрос с отражением дополнительного материала. Обучающийся демонстрирует глубокое знание теоретического материала, умение грамотно, логично и аргументировано излагать свои мысли.
Незачет	Неудовлетворительный уровень	Отсутствует ответ или в ответе есть грубые ошибки в изложении материала, свидетельствующие о незнании и непонимании соответствующего программного материала, отсутствует понимание сути вопроса.

Текущий контроль и промежуточная аттестация осуществляются в соответствии с «Положением о текущем контроле успеваемости и промежуточной аттестации обучающихся в Автономной некоммерческой организации «Образовательная организация высшего образования» «Университет экономики и управления».

Вид промежуточной аттестации – зачет.

Форма проведения промежуточной аттестации – письменный зачет.