Лекция 7

Информационная безопасность корпоративных WLAN

Аутентификация, защита радиоканала и контроль доступа

А.А. Хохлов • Алматы, 2026

Цель лекции

- Сформировать системное представление об угрозах информационной безопасности корпоративных беспроводных сетей и методах защиты передаваемых данных и сетевых ресурсов.
- Рассмотреть особенности уязвимостей радиоканала, угрозы несанкционированного подключения, перехвата информации и подмены беспроводной инфраструктуры.
- Изучить принципы аутентификации пользователей, шифрования беспроводного трафика и разграничения сетевого доступа.
- Проанализировать эволюцию механизмов WEP, WPA, WPA2 и WPA3, а также особенности применения современных средств безопасности в корпоративной среде.

Результаты обучения

По завершении лекции обучающийся сможет:

- Выявлять основные угрозы безопасности корпоративных WLAN и объяснять возможные последствия их реализации.
- Характеризовать механизмы аутентификации, шифрования и контроля доступа в беспроводных сетях.
- Сравнивать стандарты безопасности WEP, WPA, WPA2 и WPA3 и обосновывать выбор механизмов защиты для корпоративной WLAN.

Безопасность WLAN: многоуровневая задача

Защита радиоканала

WPA2/WPA3, шифрование данных и защищённые управляющие кадры.

Контроль подключения

IEEE 802.1X, EAP, RADIUS, AAA и политики допуска устройств.

Сетевая инфраструктура

VLAN, ACL, межсетевые экраны, журналы и защищённое администрирование.

Конфиденциальность • Целостность • Доступность

Типовые угрозы корпоративной беспроводной сети

Постороннее подключение

Компрометация общего PSK и избыточные права доступа.

Перехват и подмена

Приём радиотрафика, поддельные кадры и ошибки защиты.

Rogue AP / Evil Twin

Ложная точка с корпоративным SSID; риск похищения учётных данных.

Отказ и ошибки

Радиопомехи, недоступный RADIUS, ошибочные VLAN и ACL.

Эволюция защиты: от WEP к WPA3

WEP	RC4, криптографически устарел
WPA / TKIP	Переходная защита, устарела
WPA2	AES-CCMP, режим Enterprise
WPA3	SAE, современные режимы защиты

WEP и TKIP не следует использовать в новых корпоративных WLAN.

Режимы Personal и Enterprise

Personal: PSK / SAE

Доступ по общему секрету или SAE в WPA3-Personal. Удобно для небольших сетей.

Enterprise: IEEE 802.1X

Индивидуальные идентификаторы, EAP, сервер AAA и централизованный отзыв доступа.

PPSK: индивидуальные ключи для отдельных клиентов или устройств IoT

IEEE 802.1X и RADIUS: участники обмена



- Проверка подлинности - аутентификация.
- Назначение прав - авторизация; фиксация событий - учёт (AAA).
- RADIUS: UDP 1812 (доступ) и 1813 (учёт) в классическом варианте.

Процесс подключения защищённого клиента

01 Обнаружение SSID / Beacon → **02** Аутентификация и ассоциация → **03** 802.1X / EAP через RADIUS → **04** Ключи и политика доступа → **05** VLAN / DHCP и ресурсы

Успешная ассоциация с AP ещё не означает разрешённый IP-доступ.

EAP-TLS, сертификаты и ключи

EAP-TLS

Проверка подлинности на основе сертификатов и инфраструктуры доверия.

Проверка сервера

Клиент должен проверять доверенный центр сертификации и имя сервера.

Парные ключи

Защищают обмен между конкретной STA и точкой доступа.

Групповые ключи

Используются для определённого группового трафика.

Шифрование кадров и PMF

AES-CCMP

Защита полезной нагрузки и криптографическая проверка целостности.

PMF

Защита определённых управляющих кадров IEEE 802.11 от подделки.

Границы защиты

CRC проверяет случайные ошибки; PMF не устраняет радиопомехи.

HTTPS дополняет безопасность WLAN, но не заменяет шифрование радиоканала.

NAC: способы допуска пользователей и устройств

802.1X / EAP	Управляемые сотрудники и рабочие станции
PPSK	IoT без полноценной поддержки 802.1X
MAC-аутентификация	Ограниченные сценарии; MAC можно подменить
Captive Portal	Временный гостевой доступ через веб-портал

Портал не обеспечивает сам по себе шифрование Wi-Fi.

Сегментация WLAN: роли, VLAN и политики



VLAN отделяет сегменты; межсетевые экраны и ACL контролируют обмен между ними.

Мониторинг угроз и безопасное управление

WIDS

Выявление незнакомых AP, подозрительных событий и радиочастотных аномалий.

WIPS

Реагирование в рамках утверждённой политики и правовых ограничений.

- Сбор журналов, единое время (NTP), разбор отказов RADIUS.
- Изолированная сеть управления; SSH и HTTPS вместо открытых протоколов.
- Резервные копии, обновления и аудит действий администраторов.

Практический сценарий: безопасная WLAN университета

Сотрудники	WPA2/3-Enterprise, EAP-TLS, доступ по роли
Студенты	Собственная политика AAA, учебные сервисы
Гости	Изолированный сегмент, ограниченный срок доступа
Лабораторные IoT	PPSK / ограниченные разрешённые направления

Тестируйте как положительные, так и отрицательные сценарии доступа.

Итоги и вопросы для самопроверки

- WEP и TKIP устарели; современные сети используют WPA2/WPA3.
- IEEE 802.1X, EAP и RADIUS обеспечивают управляемую аутентификацию.
- NAC и AAA назначают права по ролям и типам устройств.
- VLAN необходимо дополнять ACL, межсетевыми экранами и аудитом.
- Безопасность WLAN - непрерывные проверки, мониторинг и обновления.

Вопрос: почему хороший сигнал и успешная ассоциация не гарантируют доступ?