Безопасность и уязвимость Wi-Fi

Стандарт IEEE 802.11, атаки на соединения и защита от них.

[Содержание стандарта Wi-Fi и спецификаций](#_329m6px9xv75)

[Протокол безопасности](#_2ci2tgfx15d)

[Атаки на Wi-Fi. Последствия и методы защиты](#_xouk5ernnyjx)

[Утилиты для работы с Wi-Fi](#_w72hu2skmbfo)

[Практика](#_c5d9qfauyv0k)

[Задача 1. Разведать местность](#_ug3tgq2terao)

[Задача 2. Сбросить клиента с точки и поймать EAPOL-пакет](#_1s7fys4k35ys)

Практическое [задание](#_3tfrjxxltv85)

[Дополнительные материалы](#_1pj11aaentb8)

[Используемая литература](#_uvp6qax5r1ok)

#

# Содержание стандарта Wi-Fi и спецификаций

Любые действия с системой начинаются с ее изучения. Если ее использует множество людей, она обязана быть стандартизированной. Это касается и сетей Wi-Fi.

На этом уроке мы не будем разбирать весь стандарт IEEE 802.11 — вы сможете сделать это самостоятельно с помощью [методички](https://ru.bmstu.wiki/IEEE_802.11).





*Рисунок 1. Возможные архитектуры сетей AP, Ad-Hoc и Mesh*

## Протокол безопасности

Есть несколько устаревших видов настроек аутентификации, которые небезопасны, но по неизвестным причинам до сих пор поддерживаются производителями сетевого оборудования. Из их числа — открытые сети без шифрования, которые применяются в общественных местах. Устройства в них аутентифицированы по умолчанию. WEP-шифрование основано на алгоритме RC4. С ним связано множество атак.

Безопасность в сетях Wi-Fi регламентируется стандартом 802.11i и его предшественниками (WEP, WPA). Для работы по стандарту 802.11i создается иерархия ключей. После аутентификации беспроводного клиента сервер аутентификации и клиент создают общий мастер-ключ (МК). Затем он добавляет обновляемый мастер-ключ (РТК) длиной 256 бит. Для каждой сессии пары «клиент и точка доступа» создают новый ключ РМК, который усиливает защиту канала доступа и создает набор ключей РТК. Он состоит из трех ключей: ключа целостности сообщений, ключа шифрования и ключа однонаправленной связи между клиентом и точкой доступа.



*Рис. 2. Алгоритмы шифрования и дешифровки WEP*



*Рис. 3. Шифрование по протоколу TKIP*

Для метода аутентификации WPA2 существует два решения: для домашних сетей — WPA2-Personal, для корпоративных — WPA2-Enterprise. Если скомпрометирован домашний пароль, необходимо сразу его менять и доводить до всех пользователей. В корпоративной версии пароль (динамический ключ) меняется «на лету», и нет необходимости при увольнении сотрудника менять его и сообщать сотрудникам. В enterprise-версии в аутентификации участвует третья сторона — сервер аутентификации.

Рассмотрим процедуру аутентификации WPA2-Enterprise:

1. Точка доступа AP посылает пользователю запрос на установление соединения EAP-Request/Identity. Если пользователь начинает устанавливать соединение с точкой доступа — наоборот, посылает сообщение EAP-Start. Беспроводная точка доступа в ответ передает сообщение EAP-Request/Identity.
2. Пользователь посылает в ответ сообщение EAP-Responce/Identity с именем компьютера. Точка доступа переправляет это сообщение RADIUS-серверу в виде сообщения RADIUS Account-Request.
3. Сервер RADIUS посылает сообщение RADIUS Access-Challenger, содержащее EAP-Request и указывающее тип EAP. Это означает начало аутентификации. В данном примере тип EAP-TLS. Точка доступа перенаправляет сообщение пользователю в виде EAP-Request.
4. Пользователь подтверждает начало аутентификации по протоколу TLS, посылая сообщение EAP-Response с типом EAP-TLS. Точка доступа перенаправляет это сообщение EAP RADIUS-серверу в виде RADIUS Access-Request.
5. Сервер RADIUS посылает сообщение RADIUS Access-Challenger, содержащее сертификат сервера RADIUS или их цепочку. Точка доступа переправляет это сообщение пользователю в виде EAP-Request.
6. Пользователь посылает сообщение EAP-Response с типом EAP-TLS, содержащее свой сертификат или их цепочку. Точка доступа переправляет это сообщение серверу RADIUS.
7. Сервер RADIUS посылает сообщение о завершении обмена аутентифицирующими сообщениями по протоколу TLS. Точка доступа переправляет его пользователю.
8. Пользователь подтверждает прием сообщением, которое транслируется в RADIUS-сервер.
9. RADIUS-сервер, исходя из данных предыдущих этапов, вычисляет сессионный ключ для пользователя и ключ для обеспечения целостности сообщений. Затем сервер посылает беспроводной точке доступа сообщение об аутентификации пользователя (RADIUS Access-Accept), содержащее сообщение EAP-Success и эти зашифрованные ключи. В таком сообщении об успешном приеме ключей отсутствуют сами ключи для шифрования данных и обеспечения их целостности. Когда пользователь получает от точки доступа сообщение EAP-Success, он с опорой на данные предыдущих этапов вычисляет свой сессионный ключ и ключ для обеспечения целостности сообщений. Следовательно, и пользователь, и точка доступа имеют одинаковые ключи.
10. Точка доступа посылает пользователю сообщение EAPOL (EAP over LAN)-KEY, содержащее широковещательный/глобальный ключ. Он зашифрован сессионным ключом пользователя по протоколу RC4. Отдельные части сообщения EAPOL подписываются с помощью протокола НМАС, который не использует шифрование. При этом используется ключ пользователя, обеспечивающий целостность. После приема сообщения EAPOL-KEY пользователь проверяет его целостность и расшифровывает широковещательный/глобальный ключ.

# Атаки на Wi-Fi. Последствия и методы защиты

**Инъекция пакетов** — это атака, внедряющая фальшивые пакеты протокола управления соединением. Примеры инъекцией утилитой **aireplay-ng**:

1. **Деаутентификация.** Эта атака отправляет пакеты для разрыва соединения одному или нескольким клиентам, которые связаны с заданной точкой доступа. Деаутентификация клиентов может иметь ряд причин:
	1. восстановление скрытого ESSID, который не показывается в вещании;
	2. «маскировка», или захват рукопожатия WPA/WPA2 путем принудительной повторной аутентификации клиентов;
	3. генерация ARP-запросов — Windows-клиенты иногда очищают их ARP-кэш после разрыва соединения.

Эта атака бесполезна, если нет подключенных к беспроводной сети клиентов или аутентификация фальшивая.

1. **Задержка.** Эта атака позволяет выполнить два типа WEP-аутентификации: Open и Shared — и ассоциироваться с точкой доступа (ТД). Это полезно, если нужен ассоциированный MAC-адрес в атаках **aireplay-ng**, а ассоциированных клиентов в данный момент нет. Атака фальшивой аутентификации не генерирует ARP-пакеты. Такую аутентификацию нельзя использовать для аутентификации/ассоциации с точками доступа **WPA/WPA2**.
2. **Интерактив.** Эта атака позволяет выбрать пакет для воспроизведения и инъекции. Атака может получить пакеты для воспроизведения из двух источников: живого потока пакетов с вашей беспроводной карты и из файла **pcap**. Многие упускают в **aireplay-ng** функцию чтения из файла. Она позволяет прочитать пакеты из захваченных сессий или сгенерированных для атак файлов **pcap** и повторно использовать их.
3. **Повторение ARP.** Классическая атака повторного воспроизведения ARP-запроса — это наиболее эффективный и надежный способ сгенерировать новые векторы инициализации (**IVs**). Программа ищет ARP-пакеты и пересылает их обратно к точке доступа. Из-за этого она повторяет ARP-пакет с новыми **IV**. Программа пересылает один пакет многократно. При этом каждый ARP-пакет, повторенный точкой доступа, имеет новые **IVs**. Они позволяют определить WEP-ключ.
4. **Chopchop.** В случае успеха эта атака может расшифровать данные WEP, не зная ключа. Это может работать даже в отношении динамического WEP. Атака не восстанавливает сам WEP-ключ, а раскрывает простой текст. Но некоторые точки доступа не поддаются ей, отбрасывая пакеты данных короче 60 байт. Если точка доступа отбрасывает пакеты короче 42 байт, **aireplay** пытается предположить оставшиеся пропущенные данные, так как заголовок предсказуем. Если захвачен IP-пакет, дополнительно проверяется контрольная сумма заголовка — корректна ли она после угадывания недостающей части. Эта атака требует по крайней мере одного WEP-пакета.
5. **Фрагментирование.** Эта атака может получить 1500 байт из алгоритма псевдослучайной генерации **PRGA**. Она не раскрывает сам WEP-ключ, а получает только PRGA. Его можно использовать для генерации пакета с **packetforge-ng** и использовать его для инъекционных атак. Требуется получить по крайней мере один пакет от точки доступа, чтобы инициировать эту атаку.
6. **Caffe-latte.** Атакующий должен быть в диапазоне AP и подключенного клиента — фальшивого или реального. Эта атака позволяет собрать достаточно пакетов для взлома WEP-ключа без AP, достаточно просто клиента в диапазоне.
7. **Cfrag.** Превращает IP- или ARP-пакеты от клиента в ARP-запросы в отношении него. Эта атака работает особенно хорошо, если ее применять к сетям **ad-hoc**. Можно использовать ее для клиентов **softAP** (программной точки доступа) и нормальных клиентов ТД.
8. **Режим миграции.** Эта атака работает с точками доступа **Cisco Aironet**, настроенными в **WPA Migration Mode**. Он позволяет клиентам WPA и WEP подключаться к точке доступа, используя одинаковый **Service Set Identifier** (**SSID**). Программа прослушивает WEP-инкапсулированный широковещательный ARP-пакет и меняет биты, чтобы переделать его в ARP, приходящий с MAC-адреса атакующего. Затем переправляет к точке доступа. Из-за этого она повторяет ARP-пакет с новым IV и также переправляет ARP-ответ к атакующему с новым IV. Программа пересылает один ARP-пакет снова и снова. При этом каждый ARP-пакет, повторенный точкой доступа, имеет новый IV. ARP-ответ перенаправляется точкой доступа к атакующему. Новые IV позволяют определить WEP-ключ.

**Атаки на протокол контроля целостности MIC** позволяют на минуту одним пакетом выключить точку доступа. Для этого на нее досылаются неверные пакеты и активируется механизм защиты протокола.

**Атаки, основанные на методах социальной инженерии**. Эту атаку стоит заподозрить, если рядом появилась незашифрованная сеть с хорошим сигналом и заманчивым названием, или на третьем этаже стала доступна сеть **MT\_Free** с автобусной остановки. Это фальшивые точки доступа, созданные злоумышленником, чтобы перехватить персональные данные. Чтобы защититься, не ставьте на устройствах настройку «Подключаться автоматически». Если сеть ведет себя не так, как вы ее настроили, — скорее всего, она поддельная. Попробуйте сменить канал вещания и ESSID родной сети. Если старая сеть осталась, доведите до пользователей новые параметры подключения, сообщите им и начальству о компрометации данных.

Получение пароля, аутентификация в такой сети могут привести к тому, что трафик Wi-Fi перехватят и расшифруют, произойдет утечка конфиденциальной информации.

Универсальных методов борьбы с перехватом трафика или инъекцией пакетов не существует. Рекомендуется перейти на WPA2 с AES-шифрованием, уменьшить время регенерации ключей точкой доступа (вплоть до 2–3 минут) и отключить автоматическую отсылку сообщений о неверном MIC в принятом пакете. Усложните жизнь злоумышленнику: смените стандартный ESSID на нечитаемый и скройте его, смените стандартные пароли на точке доступа, поменяйте IP, логин и пароль на интерфейс администратора AP. Откажитесь от WPS: он хоть и использует восьмизначные пин-коды, но из-за ошибки в алгоритме достаточно угадать четыре цифры, а это всего десять тысяч вариантов. Не забывайте про MAC-фильтрацию и шифрование паролей. Меры защиты соизмеряйте с важностью и ценностью информации: не стоит мешать работать конечным пользователям и администраторам сети.

# Утилиты для работы с Wi-Fi

**Airbase-ng** — утилита для конфигурирования и тонкой настройки точки доступа. Зная параметры действующей точки, можно подменить ее.

**Aircrack-ng** — утилита для словарной атаки на протоколы безопасности точек доступа.

**Airdecap-ng** — для чтения **\*.pcap**-файлов дампов соединений.

**Aireplay-ng** — для инъекций Wi-Fi-пакетов в существующее соединение. От имени точки доступа отправляют пакет о разрыве соединения клиенту, чтобы он соединился, а злоумышленник поймал хендшейк — набор данных, которые точка доступа и клиент отправляют в момент соединения.

**Airmon-ng** — утилита переводит плату в режим обнаружения сетей и клиентов.

**Airodump-ng** — сканирует пространство на предмет беспроводных сетей и устройств, записывает данные обмена сетевой платы (снятия дампа). Можно записывать файлы дампа в различных форматах. Есть таблица соответствия MAC и производителей.

**Airolib-ng** — утилита для создания и манипулирования базами данных, содержащими библиотеки хешей. Может работать с файлами **cowpatty**.

**Airserv-ng** — утилита, позволяющая открыть порт для прослушивания и настроить сетевую карту для работы с беспроводными приложениями.

**Airtun-ng** — создает виртуальный туннель для инъекции пакетов в соединение.

Кроме перечисленных утилит семейства Air есть ряд вспомогательных, которые генерируют словари, радужные таблицы, проводят атаки по ним — например, **Cowpatty**.

# Практика

## Задача 1. Разведать местность

Перевести карту в режим монитора с помощью утилиты **Airmon-ng**.

Разведать обстановку, используя **Airodump-ng**

|  |
| --- |
| airmon-ng start wlan0 #выбрать свой интерфейс беспроводной сетиairodump-ng wlan0 |

Первая команда переводит беспроводную сетевую карту в режим обзора пространства. В таком режиме технологически возможно узнать **BSSID** сети — MAC-точки доступа. Также можно выяснить **ESSID** — ее наименование, оно же — соль для алгоритмов блочного шифрования. Установить, на каком канале и с какой мощностью сеть есть в пространстве.

Вторая команда выводит параметры сетей и клиентов, подключенных к ним. Имея на руках эту информацию, мы можем проводить инъекции пакетов.

Сейчас необходимо выбрать сеть и клиента в ней с вашего стенда.

## Задача 2. Сбросить клиента с точки и поймать EAPOL-пакет

Провести деаутентификацию клиента с помощью утилиты **Aireplay-ng**.

Разведать обстановку с помощью **Airodump-ng**.

|  |
| --- |
| airodump-ng wlan0 --channel 12 -w eapol1 #на 12 канале находится целевая сеть. В файл с именем eapol1 будем писать дамп.Далее в новом окне терминала:aireplay-ng -0 1 -a 00:40:48:7E:4A:6C -c 00:AF:H4:A3:1E:91 wlan0 #первый адрес - точки доступа, второй - клиента, -0 - вид пакета (разрыв), 1 - количество посланных пакетов. |

Первой командой запускаем запись эфира в файл **eapol1** с 12 канала, с интерфейса **wlan0**. Прерывание записи дампа в нашем случае противоречит поставленным целям, поэтому вторую команду выполняем из нового окна терминала. Посылаем через интерфейс **wlan0** один пакет о том, что точка доступа с адресом **00:40:48:7E:4A:6C** упраздняет аутентификацию (-0) клиента с адресом **00:AF:H4:A3:1E:91**. Количество пакетов можно увеличить — так успех вероятнее.

Скорее всего, сброшенное устройство попробует переподключиться. В этот момент в дамп запишется EAPOL-пакет. Имея его на руках, можно расшифровать пароль для доступа в сеть.

# Практическое задание

1. Изучить утилиты для работы с Wi-Fi.
2. Снять дамп соединения утилитой **Airodump-ng**. Для этого войти в незащищенную сеть — создайте ее специально, чтобы не допустить утечки своих персональных данных. Ввести логин и пароль на несколько сайтов. Найти сайт с незащищенным соединением (**http**), войти в аккаунт. Найти в дампе cookies от незащищенного сайта. Подготовить скриншоты с результатами исследований.
3. \* Найти хендшейк в предложенных дампах. Назвать **ESSID**, **BSSID** и канал атакованной сети, имя файла с EAPOL-пакетами.
4. \* Разработать bash-скрипт для диверсии в Wi-Fi сети. Цель — сделать неработоспособным соединение с точкой для конкретного клиента. Подготовить отчет с исходным кодом скрипта.

# Дополнительные материалы

1. [Статья про Wi-Fi роуминг](https://habr.com/post/340140/).
2. [Методичка по IEEE 802.11](https://ru.bmstu.wiki/IEEE_802.11).
3. [Методичка по AES](https://ru.bmstu.wiki/AES_%28Advanced_Encryption_Standard%29).

# Используемая литература

Для подготовки данного методического пособия были использованы следующие ресурсы:

1. [Методичка по IEEE 802.11](https://ru.bmstu.wiki/IEEE_802.11).
2. [Методичка про самоорганизующиеся сети](https://ru.bmstu.wiki/%D0%A1%D0%B5%D1%82%D0%B8_SON).