WI-FI SECURITY

WPA2 vs WPA3

Насколько реально безопасен ваш Wi-Fi?

Пароль Wi-Fi — это лишь часть истории.
Разбираем, как современная Wi-Fi аутентификация изменила правила безопасности.



@lionsoulbatyshchikov

WI-FI SECURITY

WPA2 vs WPA3

Это стандарты безопасности — а не Wi-Fi пароли.

И WPA2, и WPA3 защищают вашу беспроводную связь, но используют разные механизмы безопасности.

WPA2
УСТОЯВШИЙСЯ СТАНДАРТ

- Появился в **2004**
- Чаще всего использует **AES-CCMP**
- Применяет **PSK** (Pre-Shared Key) в домашних сетях
- До сих пор широко используется по всему миру

WPA3
СОВРЕМЕННОЕ УЛУЧШЕНИЕ

- Появился в **2018**
- Разработан для усиления безопасности **аутентификации**
- Использует **SAE** (Simultaneous Authentication of Equals) для **WPA3-Personal**
- Добавляет более строгие **требования к безопасности**

Главный вывод: Оба стандарта защищают Wi-Fi трафик — но WPA3 меняет способ **аутентификации** устройств.



@lionsoulbatyshchikov

БОЛЬШАЯ РАЗНИЦА

PSK vs SAE

Это не просто пароль.
Это принципиально разный подход к безопасности.

Одна и та же цель — аутентифицировать ваше устройство. Но используются совершенно **разные механизмы защиты.**

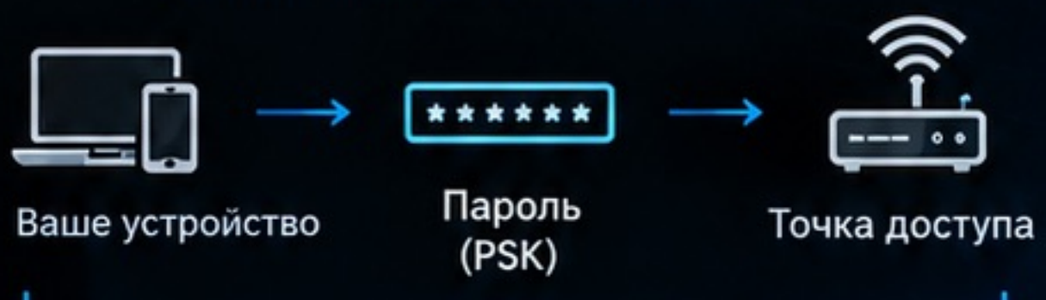
WPA2-Personal

PSK

Предварительно общий ключ

Пароль используется как часть процесса аутентификации и устанавливает доверие к сети.

Слабый пароль может сделать сеть уязвимой — атакующий может получить доступ, даже если использует нужные аутентификационные материалы.



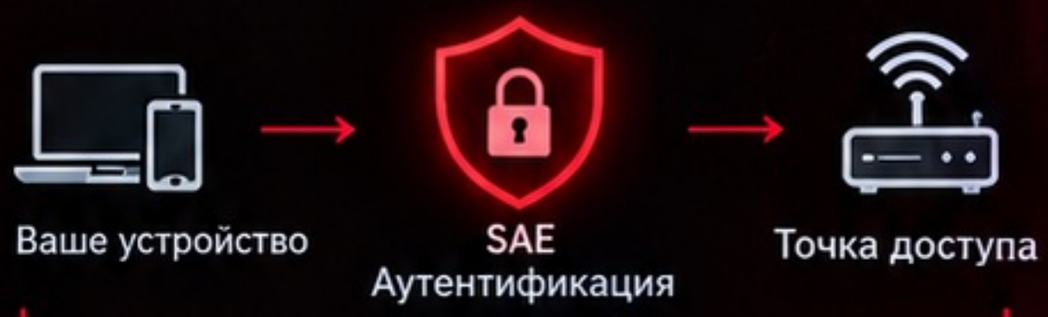
WPA3-Personal

SAE

Одновременная аутентификация равных

SAE заменяет традиционный PSK-рукопожатие на более надёжный процесс.

Он обеспечивает защиту от атак перебора паролей в автономном режиме.



Запомните:

WPA2 → PSK | WPA3 → SAE

SAE — «не взламываемый». Слабый пароль всё ещё остаётся проблемой безопасности.



@lionsoulbatyshchikov

WI-FI SECURITY

ПОЧЕМУ OFFLINE АТАКИ СТАЛИ СЛОЖНЕЕ

Разница между WPA2 и WPA3 — это не просто пароль, а то, что с ним может сделать атакующий.

В WPA2 атакующий может перехватить процесс аутентификации и подбирать пароли офлайн.

WPA3 (SAE) значительно усложняет такие атаки.

WPA2-Personal

ОФЛАЙН ПОДБОР ВОЗМОЖЕН

Атакующий захватывает Wi-Fi рукопожатие (handshake) и может подбирать миллионы паролей офлайн — без подключения к сети.



Это называется **offline dictionary attack**, и это работает, потому что в WPA2 используется **PSK** для аутентификации.

WPA3-Personal

ОФЛАЙН АТАКИ НАМНОГО СЛОЖНЕЕ

WPA3 использует **SAE** (Simultaneous Authentication of Equals) вместо классического **PSK**-рукопожатия.
Это не позволяет просто захватить обмен и так же подбирать пароли офлайн.



- Использует более безопасный механизм рукопожатия (SAE).
- Защищает от простого офлайн подбора паролей и **replay** атак.
- Атакующий не может проверить огромное количество паролей без повторного взаимодействия с сетью.

ВАЖНО ПОМНИТЬ:

WPA3 НЕЛЬЗЯ ВЗЛОМАТЬ ТАК ЖЕ, КАК WPA2.

Слабый пароль всё ещё может быть проблемой.

Вывод для защиты:

Используйте длинный уникальный Wi-Fi пароль — даже с WPA3.

@lionsoulbatyshchikov

WI-FI SECURITY

ЧТО РЕАЛЬНО ЗАЩИЩАЕТ ВАШИ ДАННЫЕ?

Шифрование: WPA2 vs WPA3

Шифрование делает ваши данные нечита емыми, поэтому даже если злоумышленник их перехватит, он не сможет легко получить к ним доступ.

WPA2-Personal

ИСПОЛЬЗУЕТ AES-CCMP

WPA2 в основном использует AES-CCMP (Advanced Encryption Standard with Counter Mode CBC-MAC) для шифрования данных.

Что это даёт:

- Конфиденциальность данных
- Целостность данных
- Защиту от replay атак

Надёжный и проверенный стандарт, но уже устаревающий по сравнению с WPA3.

WPA3-Personal

БОЛЕЕ СТРОГИЕ ТРЕБОВАНИЯ К БЕЗОПАСНОСТИ

WPA3 использует современные стандарты шифрования и протокол SAE (Simultaneous Authentication of Equals), который улучшает процесс аутентификации до установления шифрованного соединения.

Что это даёт:

- Более сильную защиту данных
- Улучшенную защиту рукопожатия (handshake)
- Повышенную устойчивость к атакам подбора паролей

Это не просто шифрование — это комплексное улучшение безопасности.

WPA3-Enterprise

РЕЖИМ 192-BIT SECURITY

Для организаций WPA3-Enterprise может использовать 192-bit security mode (например, Suite B / 192-bit encryption) для ещё более высокого уровня защиты.

Подходит для:

- Бизнеса
- Государственных организаций
- Сред с повышенными требованиями к безопасности

Обеспечивает значительно большую криптографическую стойкость.

ВАЖНО ПОНИМАТЬ:

WPA3 ≠ ПОЛНАЯ НЕУЯЗВИМОСТЬ.

Даже с WPA3 в домашних сетях по-прежнему используется режим 192-bit encryption, и слабый пароль может быть проблемой.

Главный вывод:

Реальный уровень безопасности зависит от режима WPA3 и правильной настройки роутера и устройств.

@lionsoulbatyshchikov

WI-FI SECURITY

КАК ОНИ ОБХОДЯТ ЗАЩИТУ?

WPA3 — сильнее, но не идеален.

Он значительно повышает уровень безопасности,
но злоумышленники всё равно могут атаковать через
слабые пароли, устаревшие устройства и неправильные настройки.

АСПЕКТ БЕЗОПАСНОСТИ	WPA2 (старый стандарт)	WPA3 (новый стандарт)
Аутентификация пользователя	**PSK** (Pre-Shared Key)	**SAE** (Simultaneous Authentication of Equals)
Офлайн-подбор пароля	Выше риск, если перехвачен обмен данными.	**Значительно более высокая устойчивость к offline password guessing.**
Защищённые управляющие кадры (PMF)	Опционально (зависит от режима).	**Обязательно (в WPA3).**
Влияние слабого пароля	Высокое (злоумышленник может легко подобрать пароль).	**Риск всё ещё есть** (слабый пароль остаётся уязвимостью).
Современные требования к безопасности	Устаревший базовый уровень.	**Более высокий стандарт** (дополнительные улучшения и защиты).

ВАЖНО ПОМНИТЬ:

WPA3 НЕ ДЕЛАЕТ ВАС ПОЛНОСТЬЮ НЕУЯЗВИМЫМ.

Он усложняет многие атаки,
но не устраняет их полностью.

ЗЛОУМЫШЛЕННИКИ ВСЁ ЕЩЁ МОГУТ ЦЕЛИТЬСЯ В:

- Слабые пароли
- Уязвимые устройства
- Устаревшую прошивку (firmware)
- Rogue / evil-twin сети
- Неправильные настройки роутеров
- Уязвимости на стороне клиентов (client-side)

БОЛЕЕ СИЛЬНЫЕ ПРОТОКОЛЫ + ГРАМОТНЫЕ НАСТРОЙКИ = РЕАЛЬНАЯ ЗАЩИТА.

@lionsoulbatyshchikov

WI-FI SECURITY

КОГДА СТОИТ ИСПОЛЬЗОВАТЬ WPA3?

ЦЕЛЬ:
больше безопасности,
лучше защита,
меньше рисков.

Выбор зависит от ваших устройств, задач и конфигурации сети.

1. WPA3-Personal

Для современных домашних сетей.

ПОЧЕМУ?

- Более надёжная аутентификация (SAE)
- Лучше защита от offline password guessing
- Строже требования к безопасности

ЛУЧШИЙ ВЫБОР,
если ваши устройства поддерживают WPA3.

2. WPA2/WPA3 Transition Mode

Для смешанных сред с разными устройствами.

ПОЧЕМУ?

- Позволяет использовать старые устройства, не поддерживающие WPA3
- Новые устройства всё равно могут работать через WPA3
- Обеспечивает совместимость и более высокий уровень безопасности, чем чистый WPA2

ХОРОШИЙ БАЛАНС
Совместимость
+ Безопасность.

ВАЖНО ПОМНИТЬ:

Даже если роутер поддерживает WPA3, это не делает автоматически все подключённые устройства защищёнными.

- Реальный уровень безопасности зависит от поддержки WPA3 каждым устройством и от правильной настройки сети.

КАК СДЕЛАТЬ WI-FI БЕЗОПАСНЕЕ:

- Используйте WPA3, когда это возможно
- Задайте длинный и уникальный Wi-Fi пароль
- Регулярно обновляйте прошивку роутера
- Держите в актуальном состоянии телефоны, ноутбуки и IoT-устройства
- Избегайте устаревших режимов безопасности
- Отключите WPS, если он не нужен



ПРАВИЛЬНАЯ НАСТРОЙКА =
БОЛЕЕ ВЫСОКИЙ УРОВЕНЬ БЕЗОПАСНОСТИ.

Выбирайте разумно.

ЛУЧШИЙ WI-FI
БЕЗОПАСНЕЕ ДЛЯ ВАС.

@lionsoulbatyshchikov