# WEP

Первый протокол безопасности был назван Wired Equivalent Privacy или WEP. Этот протокол оставался стандартом безопасности с 1999 по 2004 год. Хотя эта версия протокола была создана для защиты, тем не менее, она имела достаточно посредственный уровень безопасности и была сложна в настройке. В то время импорт криптографических технологий был ограничен, а это означало, что многие производители могли использовать только 64-битное шифрование. Это очень низкое битовое шифрование по сравнению с 128-битными или 256-битными опциями, доступными сегодня. В конечном счете, протокол WEP не стали развивать дальше. Системы, которые все ещё используют WEP, не являются безопасными. Если у вас есть система с WEP, ее следует обновить или заменить. При подключении к Wi-Fi, если в заведении используется протокол WEP, то ваша Интернет-активность не будет безопасной.

# WPA

# WPA2

# WPA3

# WPA-PSK vs WPA-Enterprise

Серьезной проблемой для всех беспроводных локальных сетей является безопасность.

Хакеры легко осуществляли подключение практически к любой WiFi сети взламывая такие первоначальные версии систем безопасности, как Wired Equivalent Privacy (WEP).

Для того, чтобы WEP работала, она реализует схему шифрования данных, которая использует комбинацию и сочетание значений ключей, генерируемых пользователем и системой. 40 [бит](https://www.speedcheck.org/ru/wiki/bit/) плюс дополнительные биты системных ключей шифрования данных поддерживаются оригинальными реализациями WEP. Для повышения уровня защиты позднее эти методы шифрования были расширены и теперь полностью поддерживают более длинные ключи, такие как 104-битные (128 бит общих данных), 128-битные (152 бита общих) и 232-битные (256 бит общих) варианты. Как только WEP будет развернута через [Wi-Fi](https://www.speedcheck.org/ru/wiki/wi-fi/) соединение, она будет шифровать поток данных с помощью закодированных ключей, так что он больше не будет читаться пользователями.

<https://www.speedcheck.org/ru/wiki/wep/>

Хакеры легко осуществляли подключение практически к любой WiFi сети взламывая такие первоначальные версии систем безопасности, как Wired Equivalent Privacy (WEP). Эти события оставили свой след, и долгое время некоторые компании неохотно внедряли или вовсе не внедряли у себя беспроводные сети, опасаясь, что данные, передаваемые между беспроводными WiFi устройствами и Wi-Fi точками доступа могут быть перехвачены и расшифрованы. Таким образом, эта модель безопасности замедляла процесс интеграции беспроводных сетей в бизнес и заставляла нервничать пользователей, использующих WiFi сети дома. Тогда институт IEEE, создал рабочую группу 802.11i , которая работала над созданием всеобъемлющей модели безопасности для обеспечения 128-битного AES шифрования и аутентификации для защиты данных. Wi-Fi Альянс представил свой собственный промежуточный вариант этого спецификации безопасности 802.11i: Wi-Fi защищенный доступ (WPA – Wi-Fi Protected Access).

<https://www.getwifi.ru/psecurity.html>

Для улучшения функций WEP в 2003 году был создан протокол Wi-Fi Protected Access или WPA. Этот улучшенный протокол по-прежнему имел относительно низкую безопасность, но его легче было настроить. WPA, в отличие от WEP, использует протокол Temporary Key Integrity Protocol (TKIP) для более безопасного шифрования.

## Новые возможности WPA3

Поскольку для выпуска потребовалось 14 лет, ожидается, что WPA3 будет значительно улучшена. Хотя эти функции выделены, для сертификации WPA3 по стандарту WiFi Alliance требуется только рукопожатие стрекозы.

### рукопожатие стрекозы

[Протокол](https://www.speedcheck.org/ru/wiki/protocol/) Dragonfly Handshake или протокол одновременной аутентификации Equals (SAE) потребует ключа шифрования для новых взаимодействий в сети. Это задержит возможную атаку, а также сделает пароль более строгим и трудным для взлома. SAE также предотвращает возможное расшифровку данных в автономном режиме.

### Замена РЭС

Протокол WiFi Device Provisioning Protocol или DPP - это новый и простой способ более безопасного добавления новых устройств. Функция Easy Connect упрощает подключение к домашнему Интернету и устройствам Интернета вещей (IoT) с помощью QR-кода.

### Оппортунистическое беспроводное шифрование (OWE)

При использовании точек доступа в общественных местах пользователям предоставляется лучшая защита через [Wi-Fi](https://www.speedcheck.org/ru/wiki/wi-fi/) Enhanced Open, которая обеспечивает неаутентифицированное шифрование.

### Большие размеры ключа сеанса работы

Чем больше размер ключа сеанса, тем сложнее будет взломать пароли. Эта функция доступна для WPA3-Enterprise, которая поддерживает 192-битную защиту на всех этапах аутентификации.[[3]](https://www.speedcheck.org/ru/wiki/wpa3/#fn3)

### Аутентификация NFC

Связь ближнего радиуса действия также может быть включена в сертификацию WPA3. Эта технология используется при стыковке устройств для соединения на очень коротком расстоянии. Невозможно обмануть NFC с помощью междугородней связи. Нажав устройство или IoT на точку доступа, можно легко подключиться, если у вас есть WPA3-роутер. Это простое подключение может быть низким уровнем безопасности, но более удобным для пользователей, так как им больше не придется запоминать пароли, и как только устройство будет установлено, оно будет храниться там для будущих подключений.[[4]](https://www.speedcheck.org/ru/wiki/wpa3/#fn4)

### Повышенная безопасность предприятия

WPA3, в отличие от WPA2, предоставляет 192-битный [пакет](https://www.speedcheck.org/ru/wiki/packet/) безопасности, который обеспечивает более надежную систему безопасности для корпоративных сред. Более крупные ключи шифрования используются особенно на важных предприятиях, таких как оборона, промышленные предприятия и, конечно же, правительство. Чем больше размер ключа, тем выше безопасность шифрования данных. Это также затрудняет проникновение хакеров в критически важные сети.[[5]](https://www.speedcheck.org/ru/wiki/wpa3/#fn5)

<https://www.speedcheck.org/ru/wiki/wpa3/>

More info: <https://habr.com/ru/post/424925/> WPA3

# Certifikát

Certifikát slouží k ověření identity. Dá se používat i pro identifikaci osob, ale my se s ním budeme setkávat zejména jako s prostředkem pro ověření autenticity serveru, ke kterému se připojujeme.

K čemu ověření identity serveru? Například když budete chtít získat něčí heslo do systému, který není pod vaší kontrolou, můžete na svém serveru vyrobit maketu přihlašovací stránky daného systému. Ta ale bude zadané jméno a heslo posílat vám (útočníkovi). Pak stačí, aby se oběť spojila s vaší maketou místo s pravým serverem (přesměrování IP, pokud máte v moci router, případně ARP poisoning, DNS přesměrování, …) a zadala přihlašovací údaje. A máte vyhráno.

Ale vygenerovat si certifikát znějící na libovolné jméno není problém. Jak tedy poznat, že certifikát serveru je opravdu pravý? V SSL se to řeší tak, že certifikát je vždy podepsán. Buď může být podepsán sám sebou (tzv. Self-signed Certificate), nebo je podepsán jiným certifikátem, tzv. certifikační autoritou (Certificate Authority, CA).

Certifikát CA může být rovněž podepsán nějakou jinou certifikační autoritou. Filozofie je taková, že do uživatelského SW jsou nahrány certifikáty těch autorit, kterým uživatel věří.

# Bezpečnostní zásady

Сокрытие ESSID

Многие администраторы считают, что сокрытие ESSID помогает защитить их беспроводную сеть. На самом деле это не особенно хороший способ защиты. Опытный злоумышленник сможет без труда обнаружить вашу беспроводную сеть даже при отключённой трансляции ESSID. Значение ESSID не должно идентифицировать вашу беспроводную сеть, то есть оно не должно содержать названия компании или другой информации, которая может привлечь злоумышленников.

Мы уже говорили о необходимости смены ESSID, используемого по умолчанию. Причина необходимости такой замены кроется в следующем: при шифровании трафика идентификатора существуют так называемые Rainbow-таблицы, содержащие значения зашифрованных с помощью идентификаторов пакетов. По этим таблицам злоумышленник сможет буквально за несколько секунд расшифровать ключ шифрования. Для борьбы с этим необходимо использовать нестандартное (неосмысленное) значение ESSID.

# Závěr:

Безопасность беспроводной сети менялась с течением времени, чтобы стать более надёжной, но при этом и более простой с точки зрения её настройки. Но как бы не улучшались протоколы самой главной уязвимость всегда будет оставаться человек. Никто не застрахован от взлома путём фишинга или социальной инженерии, но если вы будете придерживаться выше перечисленных принципов безопасности, то это поможет защитить вашу сеть от взлома.