# WEP (Wired Equivalent Privacy)

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.

<https://www.cloudav.ru/mediacenter/security/wpa-vs-wpa2/>

# WPA

Для улучшения функций WEP в 2003 году был создан протокол Wi-Fi Protected Access (**защищенный Wi-Fi доступ**). Этот улучшенный протокол по-прежнему имел относительно низкую безопасность, но его легче было настроить.

Технология WPA состоит из следующих компонентов:

1. *протокол 802.1x* — универсальный протокол для аутентификации, авторизации и учета (AAA)
2. *протокол EAP* — расширяемый протокол аутентификации (Extensible Authentication Protocol)
3. *протокол TKIP* — протокол временнОй целостности ключей, другой вариант перевода — протокол целостности ключей во времени (Temporal Key Integrity Protocol)
4. *MIC* — криптографическая проверка целостности пакетов (Message Integrity Code)

# WPA-PSK vs. WPA-Enterprise

* WPA-Personal (-Personal Key или -PSK) - Протокол WPA-Personal используется на основе общих ключей WPA-PSK (Pre Shared Key) и считается менее безопасным режимом. Ключ PSK предназначен для домашних сетей, сетей небольших офисов или частных групп, где всем участникам группы предоставляется один ключ безопасности беспроводной сети Wi-Fi, т.е. всем абонентам выдается одна парольная фраза, которая открывает доступ. При использовании WPA-PSK в настройках точки доступа и профилях беспроводного соединения клиентов указывается общий ключ (PSK)- пароль- длиной от 8 до 63 символов. Протокол WPA-PSK позволяет беспроводному устройству Brother обмениваться данными с точками доступа при помощи способа шифрования TKIP или AES.
* WPA-Enterprise - В этом случае каждый пользователь получает уникальный пароль, который работает только для одного компьютера, т.к. авторизация пользователей проводится на отдельном [RADIUS-сервере](https://ru.bmstu.wiki/RADIUS_(Remote_Authentication_in_Dial-In_User_Service)). Именно сервер проверки подлинности 802.1X распределяет различные ключи каждому отдельному пользователю.

<https://www.cloudav.ru/mediacenter/security/wpa-vs-wpa2/>

<https://ru.bmstu.wiki/WPA_(Wi-Fi_Protected_Access)>

# WPA2

Технология WPA являлась временной мерой до ввода в эксплуатацию стандарта 802.11i.

Дальнейшим развитием этого протокола является WPA2. WPA2 определяется стандартом IEEE 802.11i, принятым в июне 2004 года. В нём реализованы CCMP и шифрование AES (Advanced Encryption Standard), за счёт чего WPA2 стал более защищённым, чем его предшественник. CCMP (Counter Mode with Cipher Block Chaining Message Authentication Code Protocol, протокол блочного шифрования с кодом аутентичности сообщения и режимом сцепления блоков и счётчика) – протокол шифрования 802.11i, созданный для замены TKIP, обязательного протокола шифрования WPA и WEP, как более надёжный вариант. В качестве алгоритма шифрования там применяется усовершенствованный стандарт шифрования AES (Advanced Encryption Standard).

А для управления и распределения ключей по-прежнему применяется протокол 802.1x.

<https://www.ixbt.com/comm/prac-wpa-eap.shtml>

БИРЮКОВ, Андрей. Информационная безопасность: защита и нападение. 2-е изд. Москва: ДМК Пресс, 2017. ISBN 978-5-94074-647-8.

# WPA2-PSK vs. WPA2-Enterprise

Протоколы WPA2 работают в двух режимах аутентификации: персональном (Personal) и корпоративном (Enterprise).

## WPA2-PSK

В режиме WPA2-Personal из введённой открытым текстом парольной фразы генерируется 256-разрядный ключ PSK (PreShared Key). Ключ PSK совместно с идентификатором SSID (Service Set Identifier) используются для генерации временных сеансовых ключей PTK (Pairwise Transient Key), для взаимодействия беспроводных устройств. Как и статическому протоколу WEP, протоколу WPA2-Personal присуще определенные проблемы, связанные с необходимостью распределения и поддержки ключей на беспроводных устройствах сети, что делает его более подходящим для применения в небольших сетях из десятка устройств, в то время как для корпоративных сетей оптимален WPA2-Enterprise.

<http://www.technorium.ru/cisco/wireless/wpa2.shtml>

## WPA2-Enterprise

В режиме **WPA2-Enterprise** решаются проблемы, касающиеся распределения статических ключей и управления ими, а его интеграция с большинством корпоративных сервисов аутентификации обеспечивает контроль доступа на основе учетных записей. Для работы в этом режиме требуются такие регистрационные данные, как имя и пароль пользователя, сертификат безопасности или одноразовый пароль, аутентификация же осуществляется между рабочей станцией и центральным сервером аутентификации. Точка доступа или беспроводной контроллер проводят мониторинг подключений и направляют аутентификационные запросы на соответствующий сервер аутентификации (как правило, это сервер RADIUS, например [Cisco ACS](http://www.technorium.ru/cisco/secure-acs.shtml)). Базой для режима WPA2-Enterprise служит стандарт [802.1X](http://www.technorium.ru/cisco/802-1-x.shtml), поддерживающий аутентификацию пользователей и устройств, пригодную как для проводных коммутаторов, так и для беспроводных точек доступа.

<http://www.technorium.ru/cisco/wireless/wpa2.shtml>

# WPA3

WPA3 is the next generation of Wi-Fi security and provides cutting-edge security protocols to the market. Building on the widespread success and adoption of Wi-Fi CERTIFIED WPA2™, WPA3 adds new features to simplify Wi-Fi security, enable more robust authentication, deliver increased cryptographic strength for highly sensitive data markets, and maintain resiliency of mission critical networks.

## Типы WPA3

### WPA3-Personal

Этот тип отличается более простым выбором пароля, чтобы пользователи могли легко запомнить его. Он также обладает более высоким уровнем безопасности, при котором сохраненные данные и трафик данных в сети не будут скомпрометированы, даже если пароль взломан и данные уже были переданы. Обновление также позволило осуществить одновременную аутентификацию Equals (SAE), которая заменила Pre-shared Keys (PSK) в [WPA2](https://www.speedcheck.org/ru/wiki/wpa2/)-Personal.

### WPA3-Enterprise

Этот тип был построен в основном для более жесткого и последовательного применения протоколов безопасности в сетях правительств, учреждений, предприятий и финансовых учреждений. Предлагая дополнительную 192-разрядную минимальную защиту, WPA3 сделает криптографические инструменты лучше. Следовательно, более надежная защита конфиденциальных данных.[[2]](https://www.speedcheck.org/ru/wiki/wpa3/#fn2)

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.

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

### WPA3-Personal

WPA3-Personal brings better protections to individual users by providing more robust password-based authentication, even when users choose passwords that fall short of typical complexity recommendations. This capability is enabled through Simultaneous Authentication of Equals (SAE), which replaces Pre-shared Key (PSK) in WPA2-Personal. The technology is resistant to offline dictionary attacks where an adversary attempts to determine a network password by trying possible passwords without further network interaction.

* **Natural password selection:** Allows users to choose passwords that are easier to remember
* **Ease of use:** Delivers enhanced protections with no change to the way users connect to a network
* **Forward secrecy:** Protects data traffic even if a password is compromised after the data was transmitted

### WPA3-Enterprise

Enterprise, governments, and financial institutions have greater security with WPA3-Enterprise. WPA3-Enterprise builds upon WPA2 and ensures the consistent application of security protocols across the network.

WPA3-Enterprise also offers an optional mode using 192-bit minimum-strength security protocols and cryptographic tools to better protect sensitive data:

* **Authenticated encryption:** 256-bit Galois/Counter Mode Protocol (GCMP-256)
* **Key derivation and confirmation**: 384-bit Hashed Message Authentication Mode (HMAC) with Secure Hash Algorithm (HMAC-SHA384)
* **Key establishment and authentication:** Elliptic Curve Diffie-Hellman (ECDH) exchange and Elliptic Curve Digital Signature Algorithm (ECDSA) using a 384-bit elliptic curve
* **Robust management frame protection:** 256-bit Broadcast/Multicast Integrity Protocol Galois Message Authentication Code (BIP-GMAC-256)

The 192-bit security mode offered by WPA3-Enterprise ensures the right combination of cryptographic tools are used and sets a consistent baseline of security within a WPA3 network.

<https://www.wi-fi.org/discover-wi-fi/security>

# Bezpečnostní zásady

Для того, чтобы защитить корпоративную беспроводную сеть необходимо:

* Сменить ESSID, используемый по умолчанию, на какое-либо неосмысленное значение;
* Ограничить мощность сигнала беспроводных устройств;
* Не использовать WEP а развернуть шифрование WPA/WPA2 с использованием 802.1х;
* Настроить мониторинг беспроводных устройств средствами IPS;
* Запретить клиентским рабочим станциям подключаться к доступным беспроводным сетям;
* Отключить WPS;
* Изменить admin:admin на что-то посильнее;

БИРЮКОВ, Андрей. Информационная безопасность: защита и нападение. 2-е изд. Москва: ДМК Пресс, 2017. ISBN 978-5-94074-647-8

# Conclusion:

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.