# 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.

# 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:

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

# 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.

# WPA-PSK vs. WPA-Enterprise

**WPA-PSK** – этот вариант подойдет для домашнего использования. Для авторизации в сети нужен только ключ безопасности. Когда нужно задать только пароль (ключ) и потом использовать его для подключения к Wi-Fi сети. Используется один пароль для всех устройств. Сам пароль хранится на устройствах. Где его при необходимости можно посмотреть, или сменить. При использовании WPA-PSK в настройках точки доступа и профилях беспроводного соединения клиентов указывается общий ключ (Pre-Shared Key) пароль длиной от 8 до 63 символов.

Обновление в WPA3 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.

**WPA-Enterprise (WPA-802.1x, RADIUS)** – this mode provides the security needed for wireless networks in business environments. It is more complicated to set up, and it offers individualized and centralized control over access to your Wi-Fi network. When users try to connect to the network, they need to present their login credentials. This mode supports 802.1x RADIUS authentication and is appropriate in the cases where a RADIUS server is deployed. WPA-Enterprise should only be used when a RADIUS server is connected for client authentication. Users never deal with the actual encryption keys. They are securely created and assigned per user session in the background after a user presents their login credentials. This prevents people from getting the network key from computers.

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

# Slovníky

Изначально неизвестно даже из сколько символов состоит подбираемый пароль жертвы. Именно по этой причине злоумышленники крайне редко применяют общедоступные словари. Тут уже нужно использовать навыки социальной инженерии. Если говорить точнее, то просто к часто используемым вариантам добавить сведения о жертве: имя, фамилия, дата рождения и т. д. Это поможет во много раз повысить шанс на успешную атаку. Ниже будут приведены команды для реализации этого способа.

# 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.
* Запретить клиентским рабочим станциям подключаться к доступным беспроводным сетям.
* Изменить admin:admin на что-то посильнее.
* Nepoužívat veřejné otevřené sítě.

# 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.