# Popis WPA a WPA2, WPA-PSK a WPA Enterprise

## WPA

Что такое WPA

способ шифрования для защиты беспроводных сетей. Пришёл на смену WEP, как наиболее безопасный. На данный момент является самым надёжным способом защиты беспроводного соединения. Расшифровывается как **W**i-Fi **P**rotected **A**ccess.

<https://www.dmosk.ru/terminus.php?object=wpa>

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.

Поскольку Wi-Fi Alliance сделал переход с WEP на более продвинутый протокол WPA, они должны были сохранить некоторые элементы WEP, чтобы старые устройства все ещё были совместимы. К сожалению, это означает, что такие уязвимости как функция настройки WiFi Protected, которую можно взломать относительно легко, все ещё присутствуют в обновлённой версии WPA.

Почему кто-то выбирает WPA?

Протокол WPA имеет менее безопасный метод шифрования и требует более короткого пароля, что делает его более слабым вариантом с точки зрения безопасности. Для WPA не существует корпоративного решения, поскольку оно не является достаточно безопасным для поддержки использования в компаниях. Однако если у вас есть более старое программное обеспечение, WPA можно использовать с минимальной вычислительной мощностью и это протокол может стать более приемлемым для Вас вариантом, чем старый протокол WEP.

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

Расшифровка: **Wi-Fi Protected Access (защищенный Wi-Fi доступ)**

Подразделяется на 2 подвида:

* WPA-Personal (-Personal Key или -PSK)
* WPA-Enterprise.

[https://compfixer.info/wpa-wep/#WPA](https://compfixer.info/wpa-wep/" \l "WPA)

Технология WPA состоит из следующих компонентов[[1]](https://ru.bmstu.wiki/WPA_(Wi-Fi_Protected_Access)#cite_note-4):

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)
5. *протокол RADIUS*

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

WPA ключ содержит 256 бит данных. Это может производиться непосредственно пользователем, так и общим в виде шестнадцатеричного ключа из 64 цифр. Это довольно громоздкий способ, но обмен ключом шифрования не поддаётся легкому запоминанию пользователями. Второй вариант для распределения ключей шифрования WPA предполагает использование пароля и ключевой функции вывода. Пароли состоят из строки до 63 символов ASCII. Числовые значения, связанные с этими персонажами идут в сочетании с именем сети, известной как идентификатор набора служб (SSID) и проходят через множество итераций функции деривации. В результате 64 шестнадцатеричные цифры используются как ключ WPA. Ключ генерируется с паролем SSID но это является потенциально более уязвимым, чем по-настоящему случайных 64-значный ключ. Длинная фраза в сочетании с необычным именем SSID изготовит ключ, который является доказательством против грубой силы взлома. Короткие или общие фразы, такие как «пароль» в сочетании с единым SSID, такие как «сеть» или названием конкретной марки маршрутизатора, будут производить бесполезный ключ. Хакеры уже просчитали такие ключи, созданные из самых распространенных комбинаций и попытаются ввести такие пароли в начале любой атаки на сеть.  
Original: <http://juice-health.ru/internet/692-what-is-a-wpa-key>

|  |  |
| --- | --- |
| Свойство | WPA |
| Идентификация | Пользователь, компьютер |
| Авторизация | EAP или общий ключ |
| Целостность | 64-bit Message Integrity Code (MIC) |
| Шифрование | Попакетный ключ через TKIP |
| Распределение ключей | Производное от PMK |
| Вектор инициализации | Расширенный вектор, 65 бит |
| Алгоритм | RC4 |
| Длина ключа, бит | 128 |
| Требуемая инфраструктура | RADIUS |

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

Технология WPA, призванная временно (в ожидании перехода к 802.11i) закрыть бреши WEP, состоит из нескольких 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)
* протокол RADIUS

За шифрование данных в WPA отвечает протокол TKIP, который, хотя и использует тот же алгоритм шифрования — RC4 — что и в WEP, но в отличие от последнего, использует динамические ключи (то есть ключи часто меняются). Он применяет более длинный вектор инициализации и использует криптографическую контрольную сумму (MIC) для подтверждения целостности пакетов (последняя является функцией от адреса источника и назначения, а также поля данных)

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

Как упоминалось ранее, протокол WEP имеет ряд серьёзных недостатков и не является для взломщиков труднопреодолимым препятствием, поэтому в 2003 году был представлен следующий стандарт безопасности – WPA (WiFi Protected Access). Главной особенностью этого стандарта является технология динамической генерации ключей шифрования данных, постоянная на базе протокола TKIP (Temporal Key Integrity Protocol), представляющего собой дальнейшее развитие алгоритма шифрования RC4. По протоколу TKIP сетевые устройства работают с 48-битовым вектором инициализации (в отличие от 24-битового вектора WEP) и реализует правила изменения последовательности его битов, что исключает повторное использование ключей. В протоколе TKIP предусмотрена генерация нового 128-битового ключа для каждого передаваемого пакета. Кроме того, контрольные криптографические суммы в WPA рассчитываются по-новому методу под название MIC (Message Integrity Code). В каждый кадр здесь помещается специальный восьмибайтный код целостности сообщения, проверка которого позволяет отражать атаки с применением подложных пакетов. В итоге получается, что каждый передаваемый по сети пакет данных имеет собственный уникальный ключ, а каждое устройство беспроводной сети наделяется динамически изменяемым ключом.

Кроме того, протокол WPA поддерживает шифрование по стандарту AES (Advanced Encryption Standard), то есть по усовершенствованному стандарту шифрования, который отличается более стойким криптоалгоритмом, чем это реализовано в протоколах WEP и TKIP.

При развёртывании беспроводных сетей в домашних условиях или небольших офисах обычно используется вариант протокола безопасности WPA на основе общих ключей – WPA-PSK(Pre Shared Key).

При использовании WPA-PSK в настройках точки доступа и профилях беспроводного соединения клиентов указывается пароль длинной от 8 до 63 символов.

WPA-PSK не подходит для беспроводных сетей крупных организаций, для них используется WPA-EAP, где авторизация пользователей проводится на отдельном RADIUS-сервере. Для использования 802.1х необходимо разворачивать полноценную инфраструктуру открытого ключа PKI. Сервер аутентификации, после получения сертификата от пользователя, использует 802.1х для генерации уникального базового ключа для сеанса связи. TKIP осуществляет передачу сгенерированного ключа пользователю и точке доступа, после чего выстраивает иерархию ключей плюс систему управления. Для этого используется двусторонний ключ для динамической генерации ключей шифрования данных, которые, в свою очередь, используются для шифрования каждого пакета данных. Подобная иерархия ключей TKIP заменяет один ключ WEP (статический) на 500 миллиардов возможных ключей, которые будут использованы для шифрования данного пакета данных.

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

## WPA2

В 2004 году был принят к использованию WPA2 — более безопасный, по сравнению с WPA. В большинстве устройств настройка представлена пунктом wpa/wpa2 psk (парольная фраза) или wpa/wpa2 enterprise (внешний источник ключей, например, сервер RADIUS).

Src: <https://www.dmosk.ru/terminus.php?object=wpa>

Почему лучше выбирать WPA2?

Протокол WPA2 - это обновлённая версия WPA, которая использует шифрование AES и длинные пароли для создания защищённой сети. WPA2 имеет версии для личного и корпоративного использования, что делает его идеальным вариантом как для домашних пользователей, так и для предприятий. Однако для работы этого протокола требуется больше вычислительных мощностей, поэтому, если у вас старое устройство, тот этот протокол может работать на нем медленно или вообще не работать.

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

WPA2 — более современная и улучшенная версия защиты WPA. Точно так же может работать в обоих режимах: PSK и Enterprise. Отличается тем, что поддерживает тип шифрования AES CCMP

<https://compfixer.info/wpa-wep/#WPA>

WPA2 (Wireless Protected Access ver. 2.0) – это вторая версия набора алгоритмов и протоколов обеспечивающих защиту данных в беспроводных сетях Wi-Fi. Как предполагается, WPA2 должен существенно повысить защищенность беспроводных сетей Wi-Fi по сравнению с прежними технологиями. Новый стандарт предусматривает, в частности, обязательное использование более мощного алгоритма шифрования AES (Advanced Encryption Standard) и аутентификации [802.1X](http://www.technorium.ru/cisco/802-1-x.shtml).

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

Технология WPA являлась временной мерой до ввода в эксплуатацию стандарта 802.11i. Часть производителей до официального принятия этого стандарта ввели в обращение технологию WPA2, в которой в той или иной степени используются технологии из 802.11i. Такие как использование протокола CCMP (Counter Mode with Cipher Block Chaining Message Authentication Code Protocol), взамен TKIP, 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>

Дальнейшим развитием протокола WPA является WPA2. WPA2 определяется стандартом IEEE 802.11i, принятым в июне 2004 года. В нём реализованы CCMP и шифрование AES, 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.

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

## WPA-PSK

Этот вариант подойдет для домашнего использования. Для авторизации в сети нужен только ключ безопасности

<https://compfixer.info/wpa-wep/#WPA>

WPA/WPA2 - Personal (PSK) – это обычный способ аутентификации. 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. Рекомендуется использовать именно этот вариант.

<https://help-wifi.com/nastrojka-zashhity-wi-fi-setej/tip-bezopasnosti-i-shifrovaniya-besprovodnoj-seti-kakoj-vybrat/>

WPA-Personal

Этот тип в основном используется для использования в небольших офисах и для личного пользования в домашних условиях. Для этого не требуется сервер аутентификации. Для всех подключенных беспроводных устройств используется 256-битный ключ аутентификации.

<https://www.speedcheck.org/ru/wiki/wpa/#%D1%82%D0%B8%D0%BF%D1%8B-wpa>

Протоколы WPA2 работают в двух режимах аутентификации: персональном (Personal) и корпоративном (Enterprise). В режиме **WPA2-Personal** из введенной 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>

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.

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

## WPA Enterprise

Это более продвинутый и замороченный вариант для корпоративных сетей для обеспечения более высокого уровня безопасности. Для авторизации требуется сервер Radius.

<https://compfixer.info/wpa-wep/#WPA>

WPA/WPA2 - Enterprise – более сложный метод, который используется в основном для защиты беспроводных сетей в офисах и разных заведениях. Позволяет обеспечить более высокий уровень защиты. Используется только в том случае, когда для авторизации устройств установлен RADIUS-сервер (который выдает пароли).

<https://help-wifi.com/nastrojka-zashhity-wi-fi-setej/tip-bezopasnosti-i-shifrovaniya-besprovodnoj-seti-kakoj-vybrat/>

Как следует из названия, он в основном используется в крупном бизнесе. Сервер аутентификации Remote Authentication Dial-in User Service (RADIUS) применяется для автоматической генерации ключей и аутентификации.[[5]](https://www.speedcheck.org/ru/wiki/wpa/#fn5)

<https://www.speedcheck.org/ru/wiki/wpa/#fn5>

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>

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.

Такой метод считается более безопасным, поэтому используется исключительно на предприятиях, требующих повышенный уровень безопасности, или в корпоративных сетях.

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

RADIUS-протокол предназначен для работы в связке с сервером аутентификации, в качестве которого обычно выступает RADIUS-сервер. В этом случае беспроводные точки доступа работают в enterprise-режиме.

Если в сети отсутствует RADIUS-сервер, то роль сервера аутентификации выполняет сама точка доступа — так называемый режим WPA-PSK (pre-shared key, общий ключ). В этом режиме в настройках всех точек доступа заранее прописывается общий ключ. Он же прописывается и на клиентских беспроводных устройствах. Такой метод защиты тоже довольно секьюрен (относительно WEP), очень не удобен с точки зрения управления. PSK-ключ требуется прописывать на всех беспроводных устройствах, пользователи беспроводных устройств его могут видеть. Если потребуется заблокировать доступ какому-то клиенту в сеть, придется заново прописывать новый PSK на всех устройствах сети и так далее. Другими словами, режим WPA-PSK подходит для домашней сети и, возможно, небольшого офиса, но не более того.

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

## WPA vs WPA2

Техническое отличие WPA от WPA2 состоит в технологии шифрования, в частности, в используемых протоколах. В WPA используется протокол TKIP, в WPA2 — проткол AES. На практике это означает, что более современный WPA2 обеспечивает более высокую степень защиты сети. К примеру, протокол TKIP позволяет создавать ключ аутентификации размером до 128 бит, AES — до 256 бит.

**Разница между WPA2 Personal и WPA2 Enterprise**

Разница между WPA2 Personal и WPA2 Enterprise состоит в том, откуда берутся ключи шифрования, используемые в механике алгоритма AES. Для частных (домашних, мелких) применений используется статический ключ (пароль, кодовое слово, PSK (Pre-Shared Key)) минимальной длиной 8 символов, которое задается в настройках точки доступа, и у всех клиентов данной беспроводной сети одинаковым. Компрометация такого ключа (проболтались соседу, уволен сотрудник, украден ноутбук) требует немедленной смены пароля у всех оставшихся пользователей, что реалистично только в случае небольшого их числа. Для корпоративных применений, как следует из названия, используется динамический ключ, индивидуальный для каждого работающего клиента в данный момент. Этот ключ может периодический обновляться по ходу работы без разрыва соединения, и за его генерацию отвечает дополнительный компонент — сервер авторизации, и почти всегда это RADIUS-сервер.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Свойство | Статический WEP | Динамический WEP | WPA | WPA 2 (Enterprise) |
| Идентификация | Пользователь, компьютер, карта WLAN | Пользователь, компьютер | Пользователь, компьютер | Пользователь, компьютер |
| Авторизация | Общий ключ | EAP | EAP или общий ключ | EAP или общий ключ |
| Целостность | 32-bit Integrity Check Value (ICV) | 32-bit ICV | 64-bit Message Integrity Code (MIC) | CRT/CBC-MAC (Counter mode Cipher Block Chaining Auth Code — CCM) Part of AES |
| Шифрование | Статический ключ | Сессионный ключ | Попакетный ключ через TKIP | CCMP (AES) |
| Распределение ключей | Однократное, вручную | Сегмент Pair-wise Master Key (PMK) | Производное от PMK | Производное от PMK |
| Вектор инициализации | Текст, 24 бита | Текст, 24 бита | Расширенный вектор, 65 бит | 48-бит номер пакета (PN) |
| Алгоритм | RC4 | RC4 | RC4 | AES |
| Длина ключа, бит | 64/128 | 64/128 | 128 | до 256 |
| Требуемая инфраструктура | Нет | RADIUS | RADIUS | RADIUS |

<https://ru.bmstu.wiki/WPA2_(Wi-Fi_Protected_Access_II)#.D0.A0.D0.B0.D0.B7.D0.BD.D0.B8.D1.86.D0.B0_.D0.BC.D0.B5.D0.B6.D0.B4.D1.83_WPA_.D0.B8_WPA2>

# slabiny WPA

Взломать WPA2 можно только по словарю или используя брут-форс атаку. Последний раз удавалось обойти защиту в 2010 году, используя уязвимости Hole196. WPA же взломать довольно просто — в 2009 году был представлен метод получения доступа к сети за 1 минуту.

Src: <https://www.dmosk.ru/terminus.php?object=wpa>

Поскольку Wi-Fi Alliance сделал переход с WEP на более продвинутый протокол WPA, они должны были сохранить некоторые элементы WEP, чтобы старые устройства все ещё были совместимы. К сожалению, это означает, что такие уязвимости как функция настройки WiFi Protected, которую можно взломать относительно легко, все ещё присутствуют в обновлённой версии WPA.

Единственная заметная уязвимость WPA2 заключается в том, что как только кто-то получает доступ к сети, он может атаковать другие устройства, подключённые к этой сети. Это может стать проблемой в том случае, если у компании есть внутренняя угроза, например, несчастный сотрудник, который способен взломать другие устройства в сети компании (или предоставить для этих целей своё устройства хакерам-профессионалам).

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

**Уязвимость**

23 июля 2010 года была опубликована информация об уязвимости Hole196 в протоколе WPA2. Используя эту уязвимость, авторизовавшийся в сети злонамеренный пользователь может расшифровывать данные других пользователей, используя свой закрытый ключ. Никакого взлома ключей или брут-форса не требуется[[Источник 6]](https://ru.bmstu.wiki/WPA2_(Wi-Fi_Protected_Access_II)#cite_note-6).

Тем не менее, на данный момент основными методами взлома WPA2 PSK являются атака по словарю и брутфорс. Для этого в режиме мониторинга беспроводной карты сканируется эфир и записываются необходимые пакеты. Далее проводится деавторизация клиента для захвата начального обмена пакетами (handshake), либо нужно ждать пока клиент совершит подключение. После этого уже нет необходимости находиться недалеко от атакуемой точки доступа. Атака проводится офлайн с помощью специальной программы и файла с хэндшейком.

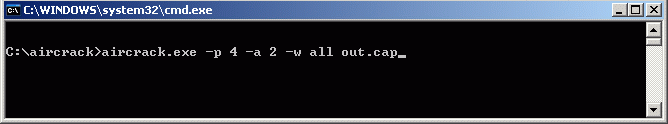
<https://ru.bmstu.wiki/WPA2_(Wi-Fi_Protected_Access_II)#.D0.A0.D0.B0.D0.B7.D0.BD.D0.B8.D1.86.D0.B0_.D0.BC.D0.B5.D0.B6.D0.B4.D1.83_WPA_.D0.B8_WPA2>

# možné metody útoku

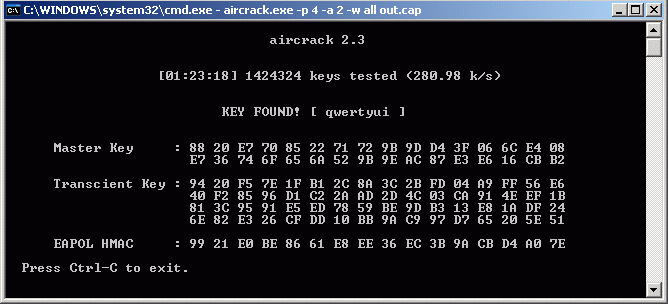
## **Как обойти шифрование WPA**

Этапы взлопа протокола WAP [[Источник 4]](https://ru.bmstu.wiki/WPA_(Wi-Fi_Protected_Access)#cite_note-6):

1. На первом этапе используется сниффер airodump. Однако в качестве выходного файла необходимо использовать именно cap-файл, а в cap-файл необходимо захватить саму процедуру инициализации клиента в сети. Если используется Linux-система, то можно провести атаку, которая заставит произвести процедуру переинициализации клиентов сети, а вот под Windows такая программка не предусмотрена.
2. После того, как в cap-файл захвачена процедура инициализации клиента сети, можно остановить программу airodump и приступить к процессу расшифровки. Для анализа полученной информации используется утилита aircrack,для который необходимо установить специальный элемент – словарь.
3. После этого запускается из командной строки программу aircrack, указывая в качестве выходного файла cap-файл и название словаря. На рисунке показан пример запуска программы aircrack.exe из командной строки:

[](https://ru.bmstu.wiki/%D0%A4%D0%B0%D0%B9%D0%BB:%D0%A0%D0%B8%D1%81_6.gif)

1. Программа перебора ключей из словаря даёт очень интенсивную нагрузку на процессор, так что если для этого используется маломощный ПК, то на эту процедуру потребуется много времени. Если же для этого используется мощный многопроцессорный сервер или ПК на базе двухъядерного процессора, то в качестве опции можно указать количество используемых процессоров, что позволит сократить время анализа и получить следующий результат:

[](https://ru.bmstu.wiki/%D0%A4%D0%B0%D0%B9%D0%BB:%D0%A0%D0%B8%D1%81_7.gif)

1. Таким образом, ключ был найден. Причём результат взлома секретного ключа никак не связан с тем, какой алгоритм шифрования (TKIP или AES) используется в сети.

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

Ключевые атаки переустановки (KRACK) являются одним из слабых мест, выявленных в реализации WPA2. Эти слабые места могут быть использованы, если злоумышленники находятся в зоне досягаемости сети. KRACK используется для сбора данных, которые ранее считались надежно зашифрованными. К таким данным и информации относятся пароли, информация о кредитных картах, сообщения электронной почты, фотографии и даже разговоры в чате. Эта атака распространена во всех современных WiFi сетях. Еще одним серьезным недостатком WPA2 является возможность манипулирования данными путем внедрения вредоносного ПО и других ошибок на веб-сайты.

Эти недостатки наблюдаются в самой конфигурации WiFi, а не в реализации и используемых продуктах (например, аппаратном и программном обеспечении). Предотвращение этих атак возможно благодаря актуальным обновлениям системы безопасности. Каждое устройство, использующее WiFi, подвержено этой уязвимости.

Первоначальные исследования показали, что почти все операционные системы и сети, такие как Apple, Windows, Android, OpenBSD, Linksys и MediaTek, в той или иной степени подвержены этому воздействию. WPA2, несмотря на свою уязвимость к подобного рода атакам, по-прежнему является наиболее надежным протоколом безопасности как для частных, так и для публичных сетей. Управление сетью должно время от времени ужесточаться и надлежащим образом обновляться, чтобы избежать любых сбоев и возможных повреждений.[[6]](https://www.speedcheck.org/ru/wiki/wpa2/#fn6)

<https://www.speedcheck.org/ru/wiki/wpa2/>

### Прямые угрозы

Радиоканал передачи данных, используемый в Wi-Fi, потенциально подвержен вмешательству с целью нарушения конфиденциальности, целостности и доступности информации. В Wi-Fi предусмотрены как аутентификация, так и шифрование, но эти элементы защиты имеют свои изъяны.

### Чужаки

Чужаками (RogueDevices, Rogues) называются устройства, предоставляющие возможность неавторизованного доступа к корпоративной сети, обычно в обход механизмов защиты, определенных политикой безопасности. Запрет на использование устройств беспроводной связи не защитит от беспроводных атак, если в сети, умышленно или нет, появится чужак. В роли чужака может выступать всё, у чего есть проводной и беспроводной интерфейсы: точки доступа (включая программные), сканеры, проекторы, ноутбуки с обоими включёнными интерфейсами и т. д.

### Нефиксированная природа связи

Беспроводные устройства могут менять точки подключения к сети прямо в процессе работы. Например, могут происходить «случайные ассоциации», когда ноутбук с Windows XP (доверительно относящейся ко всем беспроводным сетям) или просто некорректно сконфигурированный беспроводной клиент автоматически ассоциируется и подключает пользователя к ближайшей беспроводной сети. Таким образом нарушитель переключает на себя пользователя для последующего сканирования уязвимостей, фишинга или атак «человек посередине». А если пользователь при этом подключен и к проводной сети, то он становится точкой входа — чужаком. К тому же многие пользователи, подключённые к внутренней сети и имеющие Wi-Fi интерфейс, недовольные качеством и политикой работы сети, переключаются на ближайшую доступную точку доступа (или операционная система делает это автоматически при отказе проводной сети). При этом вся защита сети терпит крах.

### Взлом шифрования

О защищённости WEP и речи уже нет. Интернет полон специального и удобного в использовании ПО для взлома этого стандарта, которое собирает статистику трафика до тех пор, пока её не станет достаточно для восстановления ключа шифрования. Стандарты [WPA](https://ru.bmstu.wiki/index.php?title=WPA&action=edit&redlink=1) и [WPA2](https://ru.bmstu.wiki/index.php?title=WPA2&action=edit&redlink=1) также имеют ряд уязвимостей разной степени опасности, позволяющих их взлом.[4] Пока что нет информации об успешных атаках на WPA2-Enterprise (802.1x).

### Имперсонация и Identity Theft

Имперсонация авторизованного пользователя — серьезная угроза любой сети, не только беспроводной. Однако в беспроводной сети определить подлинность пользователя сложнее. Конечно, существуют SSID и можно пытаться фильтровать по MAC-адресам, но и то и другое передается в эфире в открытом виде, и их несложно подделать, а подделав — как минимум снизить пропускную способность сети, вставляя неправильные кадры, а разобравшись в алгоритмах шифрования — устраивать атаки на структуру сети (например, ARP-spoofing). Имперсонация пользователя возможна не только в случае MAC-аутентификации или использования статических ключей. Схемы на основе 802.1x не являются абсолютно безопасными. Некоторые механизмы (LEAP) имеют сложность взлома, схожую со взломом WEP. Другие механизмы, EAP-FAST или PEAP-MSCHAPv2, хотя и надёжнее, но не гарантируют устойчивость к комплексной атаке.

### Отказы в обслуживании

DoS атаки направлены на нарушение качества функционирования сети или на абсолютное прекращение доступа пользователей. В случае Wi-Fi сети отследить источник, заваливающий сеть «мусорными» пакетами, крайне сложно — его местоположение ограничивается лишь зоной покрытия. К тому же есть аппаратный вариант этой атаки — установка достаточно сильного источника помех в нужном частотном диапазоне.

<https://ru.bmstu.wiki/Wi-Fi#.D0.97.D0.B0.D1.89.D0.B8.D1.82.D0.B0_.D0.B2_.D1.81.D0.B5.D1.82.D1.8F.D1.85_Wi-Fi>

Можно вывести из строя всю сеть, атаковав устройства доступа по Wi-Fi. Во-вторых, он может попытаться похитить данные с доступных корпоративных серверов. Здесь речь идёт о проникновении в сеть через Wi-Fi и краже данных. В-третьих, он может осуществить атаку «Man-In-The-Middle». В этом случае злоумышленник может пропускать весь трафик через устройство, которое он контролирует и просматривать, а также при необходимости модифицировать, проходящий трафик.

Злоумышленник может украсть ключи шифрования и незаметно читать весь трафик, передаваемый по сети. Один раз украв нужные ключи шифрования, сможет совершенно незаметно читать трафик, никак не выдавая себя.

Отказ в обслуживании.

Прежде всего злоумышленник может осуществить генерацию помех на частоте работы беспроводной сети. Бороться с подобными атаками техническими средствами не так просто, потому что не шифрование, не фильтрация MAC-адресов здесь не могут.

Атака Network Allocation Vector заключается в следующем. При передаче данных в служебном фрейме, указывается сколько времени мы собираемся занимать канал. Это делается для того, чтобы избежать коллизий. На это время передача других пакетов на этом канале не ведётся. Злоумышленник может указать в служебном фрейме чрезмерно большое значение поля, в результате чего теоретически точка доступа может выйти из строя на несколько минут. Для борьбы с этим Cisco также предлагает технологию Management Frame Protection.

Взлом ключей шифрования

Злоумышленник может достаточно долго работать в режиме прослушивания, записывая трафик, а затем с помощью специальных утилит попытаться расшифровать его ключ шифрования. Технический прогресс не стоит на месте, и в последнее время большую популярность приобрёл метод перебора паролей с использованием в качестве вычислительных мощностей видеокарт. Их можно поставить до 4-х в компьютер, в результате чего, вскрытие достаточно сложного ключа шифрования может занять порядка месяца.

Уязвимость 196

Она заключается в том, что при передаче unicast-данных всегда используется уникальный ключ, а при передаче данных broadcast или multicast используется один и тот же ключ. Этот ключ знают драйвера клиентских устройств, и теоретически этот ключ можно извлечь. В результате злоумышленник сможет осуществить атаку «человек посередине» посредством использования ARP. Для этого он может подменить MAC-адрес шлюза по умолчанию на адрес своей машины. В результате весь трафик сначала будет поступать на его машину, а уже после передаваться в Интернет. Защититься от этого можно будет с помощью IPS-систем. Также можно поставить ограничение на пропуск определённых MAC-адресов.

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

RouterScan - это программа для «массового тестирования на проникновение беспроводных устройств, подключенных к всемирной или локальной сети с использованием протокола TCP/IP с включённым веб-интерфейсом администрирования по протоколу HTTP», как утверждает разработчик.  
Фактически, программа проходится по каждому IP из указанного диапазона, в надежде обнаружить там роутер и войти в его панель управления, и если у нее это получается, мы получаем достаточно много информации, а именно:

1. Собственно, сам IP адрес роутера
2. Данные для авторизации в панели управления
3. Имя устройства/модель роутера
4. **BSSID (mac-адрес или серийный номер устройства)**
5. **SSID и пароль (данные для подключения к WiFi сети)**
6. Локальный IP адрес, различные IP маски и т.д.

Самое интересное, что программа сохраняет в гуды не только роутеры, но и вообще все девайсы/сервера, где есть авторизация. То есть, если программе попадётся сервер с авторизацией, к которому она сможет подобрать пароль, он окажется в списке гудов.  
Как по мне это плюс, потому что помимо роутеров можно найти много интересных вещей. Я, например, натыкался на IP-камеры и панель управления умным домом.

<https://lolz.guru/threads/530678/>

# slovníky a jejich generování

# Certifikát

# 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.

gVxvkUK3kU4i8iM iSSDer

9XdGfvcGpXHXBbp Yandex

Для того, чтобы защитить корпоративную беспроводную сеть необходимо:

* Сменить ESSID, используемый по умолчанию, на какое-либо неосмысленное значение;
* Ограничить мощность сигнала беспроводных устройств;
* Развернуть шифрование WPA с использованием 802.1х;
* Настроить мониторинг беспроводных устройств средствами IPS;
* Запретить клиентским рабочим станциям подключаться к доступным беспроводным сетям;

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

* Не использовать WEP;
* Отключить WPS;
* Надёжный пароль;
* Изменить admin:admin на что-то посильнее;
* Изменить стандартный пин-код

<https://www.youtube.com/watch?v=K6r60hgsMSo>

# Conclusion:

Независимо от того, какой вариант лучше всего подходит для вас, важно, чтобы вы обеспечивали безопасность своему устройству, правильно защищая своё Wi-Fi-соединение. Если ваш роутер не поддерживает самый безопасный метод шифрования, рассмотрите возможность использования VPN для шифрования вашего подключения.

# Other

## Какой лучший метод обеспечения безопасности беспроводного Интернета?

Какой способ защиты вы выберете, будет зависеть от возможностей вашего роутера. Старые устройства не могут поддерживать новые протоколы безопасности, такие как WPA3.

Ниже мы приводим список протоколов безопасности, ранжированных по степени безопасности (вверху – наиболее безопасные):

1.       WPA3

2.       WPA2 Enterprise

3.       WPA2 Personal

4.       WPA + AES

5.       WPA + TKIP

6.       WEP

7.       Open Network (no security implemented)

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

## WPA против WPA2: чем они отличаются

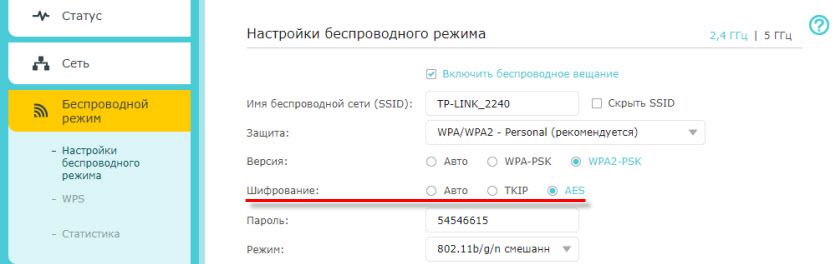
Протоколы WPA и WPA2 являются наиболее распространенными мерами безопасности, которые используются для защиты беспроводного Интернета. Учитывая это, мы сравнили разницу между WPA и WPA2, чтобы вы могли подобрать правильный вариант для вашей ситуации.

|  | **WPA** | **WPA2** |
| --- | --- | --- |
| **Год выпуска** | 2003 | 2004 |
| **Метод шифрования** | Temporal Key Integrity Protocol (TKIP) | Advanced Encryption Standard (AES) |
| **Уровень безопасности** | Выше, чем в WEP, предлагает базовый уровень безопасности | Выше, чем в WPA, предлагает повышенный уровень безопасности |
| **Поддержка устройств** | Может поддерживать более старое ПО | Совместим только с более новым ПО |
| **Длина пароля** | Допускается более короткий пароль | Требуется более длинный пароль |
| **Использование в компаниях** | Нет версии для компаний | Есть версия для компаний |
| **Требуемые вычислительные мощности** | Минимальные | Требуется больше мощностей |

При сравнении WPA и WPA2, протокол WPA2 будет лучшим вариантом, если ваше устройство может его поддерживать.



## <https://compfixer.info/tkip-aes/> **TKIP или AES**



Прежде чем станции смогут посылать кадры через точку доступа, они должны пройти аутентификацию (authenticate). В зависимости от выбора схемы безопасности аутентификация поддерживается по-разному. Если сети 802.11 ≪открыты≫, их разрешают использовать любому. Если нет — для аутентификации нужны параметры учетной записи. Рекомендуемая схема, названная WPA2 (WiFi Protected Access 2 — WiFi Защищенный Доступ 2), обеспечивает безопасность как определено стандартом 802.11i. (Просто WPA — временная схема, которая обеспечивает подмножество 802.11i. Мы пропустим ее и перейдем прямо к полной схеме.) С WPA2 точка доступа может взаимодействовать с сервером аутентификации, у которого есть имя пользователя и база данных паролей, чтобы определить, разрешено ли станции получить доступ к сети. Либо может быть сконфигурирован предустановленный ключ (pre-shared key), который является необычным названием сетевого пароля. Несколько кадров с запросом и ответом пересылаются между станцией и точкой доступа, что позволяет станции доказать, что у нее есть правильные учётные данные.

Существует два обычных сценария, в которых используется WPA2. Первый — это корпоративное использование, когда у компании есть отдельный сервер для аутентификации, хранящий имена пользователей и пароли, которые используются, чтобы определить, имеет ли право клиент получить доступ к сети. В этом случае клиенты используют стандартные протоколы для того, чтобы аутентифицировать себя и войти в сеть. Основные стандарты — это 802.1X, где точка доступа позволяет клиенту вести диалог с сервером аутентификации и наблюдать результат, и EAP (Extendable Authentication Protocol — расширенный протокол аутентификации) (RFC 3748), который описывает, как взаимодействуют клиент и аутентификационный сервер. EAP является средой, а другие стандарты определяют сообщения протокола. Мы не будем подробно рассказывать о деталях данного обмена, в кратком обзоре они не имеют значения.

Второй сценарий — домашнее использование в условиях, где нет аутентификационного сервера. Вместо него есть единый общий пароль, который используется клиентами для доступа в беспроводную сеть. Эта система менее сложная, чем в случае с аутентификационным сервером, именно поэтому она используется в домашних условиях и в маленьких фирмах, но она и менее надёжная. Основная разница состоит в том, что при наличии аутентификационного сервера каждый клиент получает ключ для шифрования трафика, неизвестный другим клиентам. При едином общем пароле для каждого клиента создаётся свой ключ, но у всех клиентов одинаковый пароль, и они могут узнать ключи друг друга, если захотят.

Наконец, мы подходим к той части, где ключи используются для обеспечения безопасности. Два протокола могут быть использованы в 802.11i для обеспечения конфиденциальности, цельности и аутентификации. Как и WPA, один из протоколов, TKIP (Temporary Key Integrity Protocol — временный протокол целостности ключа) был временным решением. Он был разработан для того, чтобы увеличить безопасность старых и медленных карт 802.11, так что безопасность у него, по крайней мере, выше, чем у WEP. Однако его сейчас тоже можно взломать, так что лучше использовать другой рекомендованный протокол — CCMP. Что означает CCMP? Это сокращение от Counter mode with Cipher block chaining message authentification code protocol — режим счётчика с протоколом аутентификации в режиме сцепления обратной связи. Мы будем называть его CCMP. Вы можете называть его как хотите.

CCMP работает довольно прямым путём. Он использует шифрование AES с помощью ключа и блоков размером 128 бит. Ключ выводится из ключа сеанса. Чтобы обеспечить конфиденциальность, сообщения зашифровываются с помощью AES в режиме счётчика. Мы обсуждали режимы шифров в разделе 8.2.3. Эти режимы предотвращают шифрование каждый раз одинаковых сообщений в одинаковые наборы бит. Режим счётчика подмешивает счётчик в процесс шифрования сообщения. Чтобы обеспечить целостность, сообщение, включая поля заголовков, кодируется шифром в режиме обратной связи, и последний блок из 128 бит сохраняется как MIC. Затем и сообщение (закодированное в режиме счётчика) и MIC высылаются. И клиент, и AP могут осуществлять данную кодировку или проверить ее при получении беспроводного пакета. Для широковещательных или групповых сообщений данная процедура применяется с использованием группового ключа.

<ftp://ftp.micronet-rostov.ru/linux-support/books/computer%20science/%D0%A2%D0%B0%D0%BD%D0%B5%D0%BD%D0%B1%D0%B0%D1%83%D0%BC%20%20-%20%D0%9A%D0%BE%D0%BC%D0%BF%D1%8C%D1%8E%D1%82%D0%B5%D1%80%D0%BD%D1%8B%D0%B5%20%D1%81%D0%B5%D1%82%D0%B8.%205-%D0%B5%20%D0%B8%D0%B7%D0%B4%D0%B0%D0%BD%D0%B8%D0%B5.pdf>

<https://3wifi.stascorp.com/>

<https://www.hackers-arise.com/creating-a-custom-wordlist-with-cru>