# БЕСПРОВОДНОЕ КИБЕРПРОСТРАНСТВО

**Рахимов Бахтиёржон Неъматович**
ТУИТ имени Мухаммада ал-Хоразмий DSc, профессор

**Ибрагимов Дониёр Бахтиярович**
ТУИТ имени Мухаммада ал-Хоразмий, докторант
ibra.doniyor13@gmail.com

**Алимухамедова Мадина Эркин кизи**
ТУИТ имени Мухаммада ал-Хоразмий, ассистент

***АННОТАЦИЯ***

*Беспроводные локальные сети, также известные как WLAN или сети Wi-Fi, в последние годы вошли в моду. Производители оборудования Wi-Fi и поставщики услуг быстро расширяются, чтобы удовлетворить растущий спрос на беспроводные услуги.*

*Программы настройки безопасности Wi-Fi включают в себя базовые, промежуточные и расширенные конфигурации безопасности. Предназначен для оказания помощи пользователям сети Wi-Fi в создании безопасной платформы сетевых приложений. Эта статья посвящена признанию многих опасностей и слабых мест, связанных с беспроводными сетями на базе стандарта 802.11, и этическому взлому их, чтобы сделать их более безопасными.*

*Какие настройки следует выбрать перед подключением к общедоступной сети, чтобы гарантировать, что их данные не будут потеряны? WPA3 в настоящее время считается лучшим, хотя многочисленные исследователи обнаружили недостаток безопасности в протоколе WPA3, используя метод, известный как атака KRACK. Однако на данный момент WPA3 считается самым мощным и надежным протоколом беспроводной безопасности.*

***Ключевые слова**: беспроводные сети, безопасност, Wi-Fi, WLAN, WPA 3, CRACK, WPA2.*

***ANNOTATION***

*Wireless LANs, also known as WLANs or Wi-Fi networks, have come into vogue in recent years. Wi-Fi equipment manufacturers and service providers are rapidly expanding to meet the growing demand for wireless services.*

*The Wi-Fi security setup programs include basic, intermediate, and advanced security configurations. Designed to help Wi-Fi users build a secure network application platform. This article is about recognizing the many dangers and weaknesses associated with 802.11 wireless networks and ethically hacking them to make them more secure.*

*What settings should be selected before connecting to a public network to ensure that their data is not lost? WPA 3 is currently considered the best, although numerous researchers have discovered a security flaw in the WPA 3 protocol using a technique known as the CRACK attack. However, Wpa3 is currently considered the most powerful and reliable wireless security protocol.*

***Keywords:*** *wireless networks, security, Wi-Fi, WLAN, WPA3, CRACK, WPA2*

## ВВЕДЕНИЕ

Wi-Fi - это радиосигнал, посылаемый с беспроводного маршрутизатора на близлежащее устройство, которое превращает его в данные, которые можно просматривать и использовать. Wi-Fi изначально был разработан для мобильных компьютерных устройств, таких как ноутбуки, но сейчас он широко используется в потребительских товарах, таких как телевизоры, DVD-плееры и цифровые фотоаппараты. Должно быть два способа связи с подключением Wi-Fi: через точку доступа к клиентскому соединению или через соединение клиент-клиент. Одним из видов беспроводной технологии является Wi-Fi. Технология Wi-Fi позволяет локальным сетям функционировать без использования кабелей. Он становится все более популярным для жилых и корпоративных сетей. В этой статье рассматривается одно из наиболее игнорируемых и безопасных беспроводных подключений, позволяющее пользователям успешно защищать свои данные от взлома. В этой статье рассматриваются различные виды атак, которые злоумышленник может использовать против маршрутизатора или Wi-Fi для кражи личной информации, а также симптомы, позволяющие определить, был ли взломан маршрутизатор или нет, и выбрать правильную настройку Wi-Fi. Здесь подчеркивается важность WPA3.

По сравнению с другими стандартами беспроводной связи, он в большей степени ориентирован на обеспечение безопасного соединения.

Основная цель исследования - определить необходимость беспроводного киберпространства и определить, является ли используемая нами беспроводная сеть безопасной или происходит утечка персональных данных.

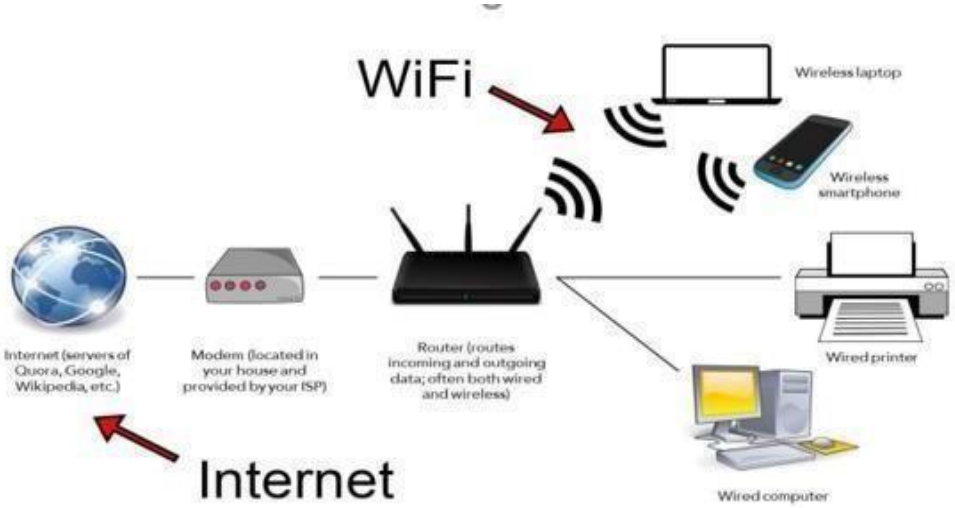


Рис. 1. Работа Wi-Fi

**Проблемы безопасности в WPA2**

CRACK - это проблема безопасности, которая влияет на WPA2, который обычно используется в современных устройствах Wi-Fi. По словам Мати Ванхофа из KU Leuven, исследователя, обнаружившего уязвимость WPA, хакер может использовать CRACK для внедрения вредоносных программ, таких как программы-вымогатели, на веб-сайты в некоторых ситуациях.

"Это может быть использовано для кражи конфиденциальной информации, таких как номера кредитных карт, пароли, сообщения чата, электронные письма, изображения и так далее", - отметил исследователь Мати Ванхеф из Католического университета Левен в Бельгии. Также возможно внедрить программы-вымогатели или другие вирусы на веб-сайты, в зависимости от расположения сети.

"CRACK" означает "Переустановка ключа". Стороннее подслушивание в сети, получившее название атаки, подразумевает, что частные переговоры при некоторых обстоятельствах могут больше не быть такими приватными, поскольку трафик Wi-Fi, проходящий между ноутбуками и точками доступа, может быть перехвачен хакерами в пределах досягаемости Wi-Fi потенциальной жертвы.

*Предлагаемые рабочие планы* на случай непредвиденных обстоятельств - Мы можем повысить уровень безопасности собственной системы защиты беспроводной сети, высокую безопасность и высокую надежность для домашнего и коммерческого Wi-Fi за счет улучшения уровня политики безопасности сети, развертывания оборудования и системы защиты безопасности, выбора сетевого оборудования.

Атаки с помощью сниффера. Методы защиты различаются в зависимости от дома и бизнеса, из-за различий в доступе к Wi-Fi и механизмах аутентификации.

Персональный предварительно разделяемый ключ (PSK) больше не используется в WPA3 и заменен одновременной аутентификацией равных (SAE). Этот подход использует обмен ключами и невосприимчив к атакам по словарю в автономном режиме, которые используют ранее сохраненные данные для подбора пароля. Этот метод защищает данные, даже если пароль является слабым, имеет краткое значение или использует общие термины.

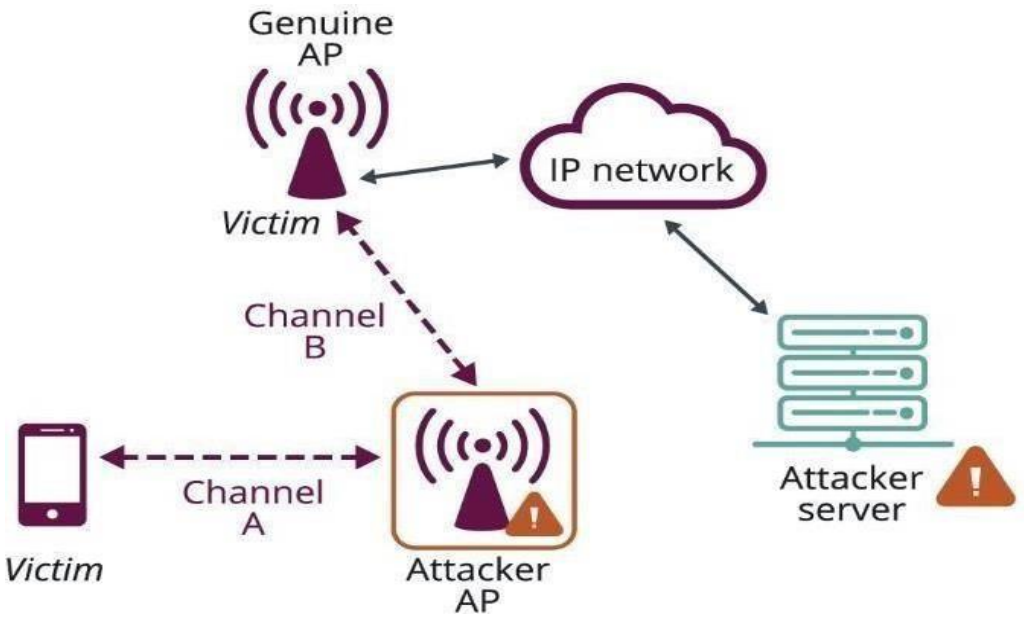


Рис. 2. Ориентация атаки WPA3 WPA3-Enterprise

WPA 3 построен на базе WPA2, но он обеспечивает ряд улучшений:

• 256-битный протокол режима Галуа/счетчика обеспечивает аутентифицированное шифрование (GCM-256);

• Режим аутентификации хэшированных сообщений (HMAC) с использованием защищенного алгоритма хэширования 384-битного ключа (SHA);

• Обмен эллиптической кривой Диффи-Хеллмана (ECDH) и алгоритм цифровой подписи эллиптической кривой используются для создания ключей (ECDSA);

• 256-битный протокол целостности широковещательной/многоадресной рассылки Galois Message Authentication Code frame protection (BIP-GMAC-256).

Необходимые изменения должны быть сделано на маршрутизаторе, чтобы оставаться в безопасности:

• Измените пароль администратора на вашем маршрутизаторе
• Включите шифрование с помощью WPA2 (или WPA 3)
• Измените сетевое имя на вашем маршрутизаторе (SSID)
• Отключить WPS
• Отключите беспроводное/удаленное управление

| | WEP | WPA | WPA2 | WPA3 |
|---|---|---|---|---|
| Brief description | Ensure wired-like privacy in wireless | Based on 802.11i without requirement for new hardware | All mandatory 802.11i features and a new hardware | Announced by Wi-Fi Alliance |
| Encryption | RC4 | TKIP + RC4 | CCMP/AES | GCMP-256 |
| Authentication | WEP-Open WEP-Shared | WPA-PSK WPA-Enterprise | WPA2-Personal WPA2-Enterprise | WPA3-Personal WPA3-Enterprise |
| Data integrity | CRC-32 | MIC algorithm | Cipher Block Chaining Message Authentication Code (based on AES) | 256-bit Broadcast/Multicast Integrity Protocol Galois Message Authentication Code (BIP-GMAC-256) |
| Key management | none | 4-way handshake | 4-way handshake | Elliptic Curve Diffie-Hellman (ECDH) exchange and Elliptic Curve Digital Signature Algorithm (ECDSA) |

Рис. 3. Сравнение алгоритмов безопасности Wi-Fi

## Заключение

В этой статье мы подчеркивали важность развития безопасного и стабильного беспроводного киберпространства, которое является наиболее насущной проблемой безопасности в условиях растущей потребности взаимосвязанного мира. Сегодня все подключено через Интернет, и Wi-Fi настолько широко распространился среди людей, что его можно найти практически в каждом доме. В результате защита этой зоны так же важна, как и защита данных, поступающих в организацию.

Использование самых мощных и актуальных настроек маршрутизатора поможет защитить ценную информацию от кражи хакерами. В этой статье рассматриваются различные атаки, которые хакер может использовать против вашего маршрутизатора, а также альтернативные методы преодоления и избежания таких атак.

WPA3 в настоящее время считается лучшим, хотя многочисленные исследователи обнаружили недостаток безопасности в протоколе WPA3, используя метод, известный как атака CRACK. Однако на данный момент WPA3 считается самым мощным и надежным протоколом беспроводной безопасности. В результате при хранении паролей и подключении к другим устройствам следует использовать алгоритм WPA3. Использование самых мощных и современных настроек маршрутизатора поможет защитить вашу ценную информацию от кражи хакерами. В этой статье рассматриваются различные атаки, которые хакер может использовать против вашего маршрутизатора, а также альтернативные методы преодоления и избежания таких атак. В настоящее время предпринимаются усилия по преодолению одного недостатка безопасности в методе WPA3, чтобы создать более безопасный алгоритм беспроводного шифрования, который может быть использован для создания безопасной беспроводной зоны.

## Список литературы:

1. С. Винджош Редди, К. Сай Рамани, К. Риджута, С. Мохаммад Али и К. Прадип Редди, "Беспроводной взлом - взлом Wi-Fi путем взлома WEP", 2010, 2-я международная конференция по образовательным технологиям и компьютерам, 2010, стр.V1-189-V1-193, doi:10.1109/ICETC.2010.5529269.
2. Х. Пэн, "Исследование анализа информационной безопасности сети Wi-Fi", 2012, 2-я международная конференция по потребительской электронике, коммуникациям и сетям (CECNet), 2012, стр. 2243-2245, Doi: 10.1109/CECNet.2012.6201786.
3. Маймон, Дэвид, Майкл Беккер, Сушант Патил и Джонатан Кац. "Самозащитное поведение в общедоступных сетях Wi-Fi". На семинаре {LASER}: Изучение результатов эксперимента по авторитарной безопасности ({LASER} 2017), стр.69-76. 2017.
4. Голдсборо, Рид. "Будьте в безопасности при использовании Wi-Fi". Учитель-библиотекарь 42, № 4 (2015): 65
5. С. Нила, М. Преда, И. Апостол и В. -В.Патрисиу, "Реактивный Wi-Fi honeypot", 2021 13-я Международная конференция по электронике, компьютерам и искусственному интеллекту (ECAI), 2021, стр. 1-6, Doi: 10.1109/ECAI52376.2021.9515048.
6. Джон С. Аткинсон, Джон Э. Митчелл, Мигель Рио, Джордж Матич, Ваш Wi-Fi протекает: что ваши мобильные приложения сплетничают о вас? Компьютерные системы будущего поколения, Том 80, 2018, страницы 546-557, ISSN 0167-739X.