УДК 004.6

2.3.6. Методы и системы защиты информации, информационная безопасность (технические науки)

БЕЗОПАСНОСТЬ WI-FI РАЗНЫХ ПОКОЛЕНИЙ

Крепышев Дмитрий Александрович
доцент, канд. экон. наук
SPIN-код: 8507-4755
e-mail krepyshev.d@kubsau.ru
ФГБОУ ВО Кубанский государственный аграрный университет имени И. Т. Трубилина, г. Краснодар, РФ

Абушкевич Юрий Сергеевич
студент
yura.abushkevich@mail.ru
Кубанский государственный аграрный университет имени И.Т. Трубилина, Россия, Краснодар 350044, Калинина 13

Ярощук Павел Александрович
студент
erioxis@vk.com
Кубанский государственный аграрный университет имени И.Т. Трубилина, Россия, Краснодар 350044, Калинина 13

В статье рассматривается эволюция защиты беспроводных сетей от 802.11 до 802.11ax (Wi-Fi 6). Анализируются уязвимости стандартов, изменения в шифровании и аутентификации, а также влияние технологий MIMO и OFDMA на безопасность. Также даются рекомендации по защите локальных и общественных Wi-Fi сетей, включая использование WPA3. Статья подчеркивает важность соблюдения современных стандартов безопасности для пользователей и организаций

Ключевые слова: WI-FI, БЕЗОПАСНОТЬ, СТАНДАРТЫ IEEE 802.11, WPA3, ШИФРОВАНИЕ, АУТЕНТИФИКАЦИЯ, УЯЗВИМОСТИ, ТЕХНОЛОГИИ MIMO, OFDMA, БЕСПРОВОДНЫЕ СЕТИ, ЗАЩИТА ДАННЫХ, ЭВОЛЮЦИЯ ТЕХНОЛОГИЙ, ОБЩЕСТВЕННЫЕ СЕТИ, РЕКОМЕНДАЦИИ ПО БЕЗОПАСНОСТИ, WI-FI 6

http://dx.doi.org/10.21515/1990-4665-205-014

UDC 004.6

2.3.6. Information protection methods and systems, information security (technical sciences)

WI-FI SECURITY ACROSS GENERATIONS

Krepyshev Dmitry Alexandrovich
Senior lecturer
RSCI SPIN-code: 8507-4755
e-mail krepyshev.d@kubsau.ru
FSAU HE Kuban State Agrarian University named after I.T. Trubilin, Krasnodar, Russia

Abushkevich Yuriy Sergeevich
student
yura.abushkevich@mail.ru
"Kuban State Agrarian University named after I.T. Trubilin", Krasnodar 350044, Kalinina 13, Russia

Yaroshuck Pavel Aleksandrovich
student
erioxis@vk.com
"Kuban State Agrarian University named after I.T. Trubilin", Krasnodar 350044, Kalinina 13, Russia

The article discusses the evolution of wireless network security from 802.11 to 802.11ax (Wi-Fi 6). It analyzes the vulnerabilities of standards, changes in encryption and authentication, as well as the impact of MIMO and OFDMA technologies on security. The article also provides recommendations for securing both local and public Wi-Fi networks, including the use of WPA3. It emphasizes the importance of adhering to modern security standards for both users and organizations

Keywords: WI-FI, SECURITY, IEEE 802.11 STANDARDS, WPA3, ENCRYPTION, AUTHENTICATION, VULNERABILITIES, MIMO TECHNOLOGIES, OFDMA, WIRELESS NETWORKS, DATA PROTECTION, TECHNOLOGY EVOLUTION, PUBLIC NETWORKS, SECURITY RECOMMENDATIONS, WI-FI 6

Постановка проблемы. Беспроводные сети стали неотъемлемой частью повседневной жизни, но их использование влечет за собой новые угрозы. Рост Wi-Fi способствовал появлению хакеров, специализирующихся на взломе сетей и атаках на пользователей. С 2004 года Gartner предупреждали, что безопасность WLAN будет одной из главных проблем.

Методы решения. Для решения поставленной проблемы в статье применяются такие методы научного исследования, как анализ, сравнение и обобщение. Источниками информации стали научные работы и технические материалы, посвященные безопасности беспроводных сетей, а также публикации отечественных и зарубежных авторов по теме эволюции стандартов IEEE 802.11. Также использованы данные открытых исследований и статистики, касающиеся современных угроз и мер безопасности для Wi-Fi сетей. В рамках работы проводится комплексный анализ основных уязвимостей различных версий протоколов 802.11, изменений в методах шифрования и аутентификации, а также воздействия новых технологий, таких как MIMO и OFDMA, на безопасность сетей.

Анализ достижений. Вопросам безопасности беспроводных сетей и эволюции стандартов IEEE 802.11 посвящено множество отечественных исследований. В работе И.В. Степановой и А.Н. Данилова рассматриваются подходы к проектированию Wi-Fi сетей и их безопасности [1]. И.С. Поздняк и соавторы анализируют методы обеспечения безопасности в беспроводных сетях [2]. А.В. Пролетарский и соавторы исследуют развитие сетей Wi-Fi и их защиту [3], а Е.В. Смирнова с коллегами — технологии современных Wi-Fi сетей [4].

Результаты и обсуждения. WEP (Wired Equivalent Privacy), выпущенный в 1997 году, был первым стандартом безопасности для беспроводных сетей. Он использовал алгоритм шифрования RC4, который на тот момент считался надежным. В 1999 году WEP был

стандартизирован IEEE в рамках 802.11b и стал основным протоколом безопасности для Wi-Fi, хотя со временем был признан уязвимым.

Уязвимость WEP заключается в использовании одного постоянного ключа для всех устройств и ограничении на шифрование только до 1500 байт, что создает риски при передаче больших пакетов. WEP был заменен WPA в 2003 году, который использует TKIP, MIC и обновленный EAP для повышения безопасности, а также централизованную архитектуру для защиты сети. Однако WPA не идеален, так как предварительный ключ уязвим, а некоторые фреймы управления не шифруются.

WPA2, выпущенный в 2004 году, использует AES для шифрования, поддерживает PSK и WPA2-Enterprise, обеспечивая высокий уровень безопасности с сильным шифрованием и аутентификацией.

WPA3, выпущенный в 2018 году, улучшает безопасность Wi-Fi, предлагая индивидуальное шифрование сессий, защиту от атак перехвата и DoS, а также новую схему аутентификации для лучшей защиты в общественных сетях. Сравнение протоколов приведено в таблице 1.

Таблица 1. Сравнение WEP, WPA, WPA2, WPA3

Параметр	**WEP**	**WPA**	**WPA2**	**WPA3**
Алгоритм шифрования	RC4	TKIP,RC4	AES-CCMP	AES-CCMP
Защита от атак	Уязвим к атаке с повтором и слабым ключам	Защита от атак с повтором, но уязвим к атаке на TKIP	Защита от атак с повтором, улучшенная безопасность	Защита от атак с повтором, улучшенная защита от подбора пароля
Поддержка 802.11n/ac/ax	Нет	Нет	Да	Да
Поддержка MiMO	Нет	Нет	Да	Да
Поддержка нового криптоалгоритма	Нет	Нет	Да	Да

Стандарт Wi-Fi был установлен в 1998 году на основе спецификаций IEEE 802.11 (Институт инженеров по электротехнике и электронике) и

быстро завоевал популярность для создания внутренних широкополосных сетей, которые формируют обширные инфраструктуры для предоставления беспроводного доступа в Интернет. В настоящее время Wi-Fi-сети могут обеспечить охват даже больших городских территорий.

Стандарты IEEE 802.11 — это набор спецификаций для беспроводных локальных сетей (WLAN), определяющий протоколы и технологии обмена данными. Со временем эти стандарты значительно изменились и улучшились. Основные версии IEEE 802.11 включают:

1. Стандарт 802.11b, работающий на 2.4 ГГц с максимальной скоростью 11 Мбит/с, стал первым популярным стандартом Wi-Fi. Однако его защита была уязвима из-за использования статических ключей шифрования, легко перехватываемых и расшифровываемых, что снижало безопасность.

2. Стандарт 802.11g, выпущенный в 2003 году, сочетал преимущества 802.11b и 802.11a, работая на 2.4 ГГц с максимальной скоростью 54 Мбит/с. Он стал популярным благодаря совместимости с 802.11b. 802.11g поддерживал WEP, но рекомендовал переход на WPA и WPA2, использующие AES для шифрования и обеспечивающие высокий уровень безопасности.

3. Стандарт 802.11n, внедренный в 2009 году, обеспечивал скорость до 600 Мбит/с с использованием MIMO (multiple-input and multiple-output) и поддержкой частот 2.4 ГГц и 5 ГГц. Он улучшил производительность и защиту от помех, поддерживал WPA, WPA2 и WPS, хотя последний был уязвим. WPA2 с AES обеспечивал высокий уровень безопасности.

4. Стандарт 802.11ac, выпущенный в 2013 году, использовал MIMO и работал на 5 ГГц с максимальной скоростью 1.3 Гбит/с. Он стал основным для высокоскоростных сетей, поддерживая множество пользователей. 802.11ac продолжал поддерживать WPA2 и начал внедрять WPA3 с улучшенной безопасностью и сильными шифровальными протоколами.

5. Стандарт 802.11ax (Wi-Fi 6), выпущенный в 2019 году, обеспечивал скорость до 9.6 Гбит/с, улучшив производительность в многопользовательских сетях. Он оптимизировал использование спектра и масштабируемость, а также адаптировал WPA3 для улучшенной безопасности и аутентификации в условиях высокой плотности подключений.

Стандарты IEEE 802.11 продолжают развиваться, обеспечивая скорость, надежность и безопасность. Совместимость между версиями и технологиями остается ключевым фактором их распространения и удобства использования.

На рисунке 1 изображено сравнение уязвимостей по поколениям Wi-Fi.

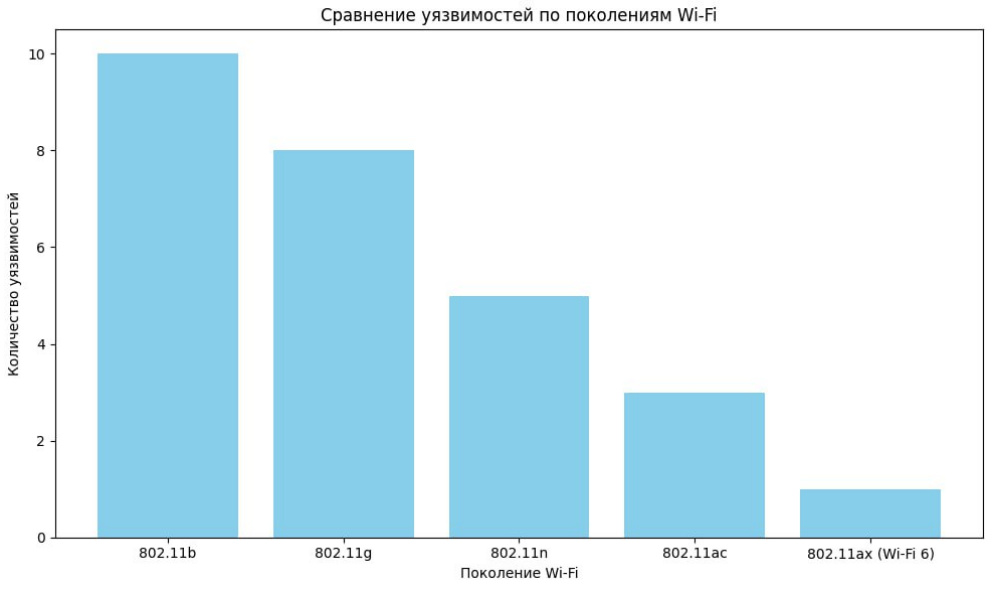

Рисунок 1. Сравнение уязвимостей по поколениям Wi-Fi

Как видно на рисунке 1 у с каждым новым поколением становилось всё меньше и меньше уязвимостей, разберём представленные в диаграмме стандарты Wi-Fi по уязвимостям:

- 802.11b:

1. Слабые стороны шифрования WEP: WEP имеет множество уязвимостей, включая использование статических ключей шифрования и недостаточное количество бит аутентификации, что делает его уязвимым

для «атак половинной силы» и атак взлома ключей.

2. Отсутствие защиты от повторной передачи: WEP не может предотвратить атаки повторного воспроизведения (Replay Attacks), что позволяет злоумышленникам перехватывать и повторно отправлять пакеты данных, ставя под угрозу целостность и подлинность данных.

3. Уязвимость к атакам «человек посередине» (MitM): из-за недостатков аутентификации и шифрования злоумышленник может выступать в качестве посредника между клиентом и точкой доступа, перехватывать и изменять данные, а также ставить под угрозу конфиденциальность данные.

4. Снижение производительности, вызванное помехами: 802.11b работает в диапазоне частот 2,4 ГГц, и ему могут создаваться помехи со стороны других устройств (например, микроволновых печей, беспроводных телефонов), что может привести к ухудшению качества связи и потере данных.

5. Сеть легко обнаружить: беспроводные сети 802.11b активно транслируют SSID, что облегчает злоумышленникам обнаружение сети, тем самым увеличивая риск атаки на сеть и получения доступа.

6. Проблемы аутентификации. WEP использует статическую аутентификацию и не может обеспечить надежную аутентификацию пользователя. Злоумышленники могут легко взломать систему с помощью различных методов, таких как подмена ARP.

7. Ограниченное количество сетей. Стандарт 802.11b поддерживает лишь относительно небольшое количество каналов (всего 11), что может вызвать проблемы с перегрузкой сети.

8. Уязвимость к атакам методом перебора паролей. Из-за слабых механизмов аутентификации сети уязвимы к атакам методом перебора, когда злоумышленники могут использовать автоматизированные инструменты, чтобы попытаться угадать сетевые пароли.

9. Отсутствие механизма контроля доступа: 802.11b не обеспечивает эффективный механизм контроля доступа для предотвращения доступа неавторизованных пользователей к сети. Некоторые устройства могут «случайно» подключиться к открытым сетям.

- 802.11g:

1. WEP имеет слабое шифрование. Хотя 802.11g поддерживает WPA и WPA2, многие старые устройства по-прежнему используют уязвимый WEP, что увеличивает риск перехвата и подделки данных.

2. Уязвимость к атакам «человек посередине» (MitM). Из-за недостатков аутентификации в WEP и некоторых реализациях WP A злоумышленники могут легко перехватывать и подделывать данные между клиентом и точкой доступа.

3. Проблемы с WPA и TKIP. В WPA используется протокол целостности временного ключа TKIP, который уязвим для определенных атак, например атаки с подделкой IV.

4. Количество каналов ограничено: 802.11g работает в диапазоне частот 2,4 ГГц. В нем имеется только три непересекающихся канала (1, 6, 11). Это может привести к помехам и перегрузкам, особенно в местах с плотной сетью.

5. Уязвимость для атак перебором: при использовании слабых паролей и статических ключей.

6. Сеть легко обнаружить. Как и 802.11b, сеть 802.11g активно транслирует SSID, из за чего злоумышленникам проще обнаружить и использовать сеть, особенно в незащищенных сетях.

7. Отсутствует механизм управления доступом. 802.11g не позволяет эффективно контролировать доступ. Это значит, что неавторизованные пользователи могут попытаться подключиться к открытым сетям со слабой защитой.

- 802.11n:

1. Слабости шифрования WPA/WPA2. Правильная настройка играет решающую роль в безопасности. Ненадёжные пароли, которые обычно используются пользователями, делают их уязвимыми для перебора, поэтому необходимо постоянно менять пароли.

2. Уязвимость к атакам MitM. Хотя 802.11n поддерживает WPA и WPA2, неправильная настройка или использование устаревших алгоритмов может привести к тому что злоумышленники смогут проводить атаки «человек посередине», перехватывать и редактировать данные. В открытых сетях данная уязвимость имеет большую актуальность

3. Проблема перегрузки в диапазоне 2,4 ГГц. Также, как и стандарты до 802.11n, работает в частотах 2,4 ГГц, что делает 802.11n чувствительным к помехам от других беспроводных устройств, что ухудшает производительность и целостность данных.

4. Уязвимости через точки доступа без защиты. Подключение к открытому Wi-Fi в публичных местах увеличивает вероятность перехвата информации злоумышленниками, которые могут создать поддельные точки доступа с тем же SSID, что и в настоящей сети.

5. Отсутствие защиты от повторной передачи. Хотя в 802.11n имеются улучшения, многие устройства могут быть недостаточно защищены от повторной передачи пакетов, что дает возможность злоумышленникам скомпрометировать сеть или получить доступ к защищенным ресурсам.

- 802.11ac:

1. Несмотря на повышенную безопасность WPA3, некорректная настройка или использование устаревшего WPA2 могут привести к тому, что сеть станет уязвима. Например, «открытые» сети и слабые пароли существенно повышают риск, что злоумышленники получат несанкционированный доступ.

2. Атаки на фрейм управления 802.11ac могут привести к разъединению устройства с точкой доступа. Несмотря на то, что WPA3 обеспечивает защиту, эта защита отсутствует в сетях, которые используют WPA2, что делает их уязвимыми для атак.

3. Устройства использующие стандарт 802.11ac уязвимы для атак, нацеленных на точки доступа. Злоумышленники способны создавать фальшивые точки доступа для перехвата данных, перенаправления пользователей на ложные веб-сайты или кражи данных.

- 802.11ax:

1. 802.11ax (Wi-Fi 6) уязвим для атак деаутентификации и диссоциации, которые могут привести к отключению пользователей от точки доступа. Многие сети по-прежнему уязвимы для атак «человек посередине» (MitM) из-за небезопасных точек доступа и неправильных конфигураций, особенно в общедоступных сетях, где этот риск более значителен.

Заключение. Безопасность Wi-Fi улучшалась с каждым стандартом, от WEP до WPA3, но старые протоколы остаются уязвимыми. Важно использовать актуальные протоколы, обновлять пароли и прошивки маршрутизаторов для защиты данных.

Список литературы

1. Степанова, И. В. Варианты и подходы к проектированию систем мобильного доступа технологии Wi-Fi: учебное пособие. Для бакалавров, направление подготовки 11.03.02 Инфокоммуникационные технологии и системы связи, профиль подготовки Сети связи и системы коммутации. Для магистров, направление подготовки 11.04.02 Инфокоммуникационные технологии и системы связи : учебное пособие / И. В. Степанова, А. Н. Данилов. — Москва : МТУСИ, 2024. — 56 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/439124 (дата обращения: 15.12.2024). — Режим доступа: для авториз. пользователей.

2. Поздняк, И. С. Обеспечение безопасности в беспроводных сетях : методические указания / И. С. Поздняк, Н. В. Киреева, О. А. Караулова. — Самара : ПГУТИ, 2019. — 22 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/223310 (дата обращения: 15.12.2024). — Режим доступа: для авториз. пользователей.

3. Пролетарский, А. В., Баскаков, И. В., Федотов, Р. А., Бобков, А. В.

Беспроводные сети Wi-Fi. — [Электронный ресурс]. — URL: https://e.lanbook.com/book/100578 (дата обращения: 15.12.2024). — Режим доступа: для авториз. пользователей.

4. Смирнова, Е. В., Пролетарский, А. В., Ромашкина, Е. А., Балюк, С. А., Суровов, А. М. Технологии современных беспроводных сетей Wi-Fi. — [Электронный ресурс]. — URL: https://e.lanbook.com/book/106534 (дата обращения: 15.12.2024). — Режим доступа: для авториз. пользователей.

References:

1. Stepanova, I. V. Varianty i podhody k proektirovaniju sistem mobil'nogo dostupa tehnologii Wi-Fi: uchebnoe posobie. Dlja bakalavrov, napravlenie podgotovki 11.03.02 Infokommunikacionnye tehnologii i sistemy svjazi, profil' podgotovki Seti svjazi i sistemy kommutacii. Dlja magistrov, napravlenie podgotovki 11.04.02 Infokommunikacionnye tehnologii i sistemy svjazi : uchebnoe posobie / I. V. Stepanova, A. N. Danilov. — Moskva : MTUSI, 2024. — 56 s. — Tekst : jelektronnyj // Lan' : jelektronno-bibliotechnaja sistema. — URL: https://e.lanbook.com/book/439124 (data obrashhenija: 15.12.2024). — Rezhim dostupa: dlja avtoriz. pol'zovatelej.

2. Pozdnjak, I. S. Obespechenie bezopasnosti v besprovodnyh setjah : metodicheskie ukazanija / I. S. Pozdnjak, N. V. Kireeva, O. A. Karaulova. — Samara : PGUTI, 2019. — 22 s. — Tekst : jelektronnyj // Lan' : jelektronno-bibliotechnaja sistema. — URL: https://e.lanbook.com/book/223310 (data obrashhenija: 15.12.2024). — Rezhim dostupa: dlja avtoriz. pol'zovatelej.

3. Proletarskij, A. V., Baskakov, I. V., Fedotov, R. A., Bobkov, A. V. Besprovodnye seti Wi-Fi. — [Jelektronnyj resurs]. — URL: https://e.lanbook.com/book/100578 (data obrashhenija: 15.12.2024). — Rezhim dostupa: dlja avtoriz. pol'zovatelej.

4. Smirnova, E. V., Proletarskij, A. V., Romashkina, E. A., Baljuk, S. A., Surovov, A. M. Tehnologii sovremennyh besprovodnyh setej Wi-Fi. — [Jelektronnyj resurs]. — URL: https://e.lanbook.com/book/106534 (data obrashhenija: 15.12.2024). — Rezhim dostupa: dlja avtoriz. pol'zovatelej.