DOI: 10.58168/PBHT2026_217-224
УДК 004.056

МОДЕЛИРОВАНИЕ УЯЗВИМОСТЕЙ WI-FI СЕТЕЙ И СПОСОБОВ ИХ ЗАЩИТЫ

MODELING WI-FI NETWORK VULNERABILITIES AND METHODS OF THEIR PROTECTION

Тихонов Я.А., курсант, Федеральное казенное образовательное учреждение высшего образования «Воронежский институт Федеральной службы исполнения наказаний России», Воронеж, Россия

Tikhonov Y.A., cadet, Federal Treasury Educational Institution of Higher Education "Voronezh Institute of the Federal Penitentiary Service of Russia", Voronezh, Russia

Лубенцов А.В., кандидат географических наук, доцент, профессор кафедры основ радиотехники и электроники, Федеральное казенное образовательное учреждение высшего образования «Воронежский институт Федеральной службы исполнения наказаний России», Воронеж, Россия

Lubentsov A.V., PhD in Geographical Sciences, Docent, Professor of the Radio Engineering and Electronics Fundamentals Department, Federal Treasury Educational Institution of Higher Education "Voronezh Institute of the Federal Penitentiary Service of Russia", Voronezh, Russia

Аннотация. Статья посвящена обзору угроз безопасности в сетях Wi-Fi по стандарту IEEE 802.11 и стратегиям их минимизации. Прослеживается развитие защитных механизмов от WEP к WPA3, с детальным разбором типичных эксплойтов против WPA/WPA2 (захват handshake, атаки "злой близнец", KRACK), а также свежих слабостей WPA3, обусловленных протоколом SAE и семейством атак Dragonblood. Формулируются прикладные советы по укреплению защиты Wi-Fi для разных сценариев использования (бытовые сети, образовательные учреждения, предприятия малого бизнеса), охватывающие оптимальную настройку устройств, подбор надёжных учётных данных, интеграцию VPN-каналов и контроль отклонений. Подчёркивается важность системного взгляда на защиту, сочетающего технические инновации с административными процедурами.

Ключевые слова: Wi-Fi сети, WPA3 протокол, уязвимости безопасности, защита информации, криптография Wi-Fi, VPN защита.

Abstract. The paper reviews security threats in IEEE 802.11 Wi-Fi networks and strategies to mitigate them. It traces the advancement of protection mechanisms from WEP to WPA3, detailing common exploits against WPA/WPA2 (handshake interception, Evil Twin attacks, KRACK), along with recent WPA3 flaws stemming from the SAE protocol and Dragonblood attack suite. Actionable guidelines are offered to bolster Wi-Fi security across diverse settings (residential networks, academic facilities, small enterprises), encompassing device optimization, robust credential selection, VPN channel integration, and deviation surveillance. Emphasis is placed on a holistic security perspective that merges technical advancements with administrative protocols.

Keywords: Wi-Fi networks, WPA3 protocol, security vulnerabilities, information protection, Wi-Fi cryptography, and VPN protection.

© Тихонов Я. А., Лубенцов А. В., 2026

Беспроводные сети передачи данных прочно интегрированы в инфраструктуру как частных пользователей, так и организаций. Стандарты семейства IEEE 802.11 обеспечивают доступ в сеть практически повсеместно: от домашних маршрутизаторов до корпоративных сегментов и публичных точек доступа в общественных местах. Одновременно с этим повышается и интерес злоумышленников к Wi-Fi как к удобной точке входа во внутренние ресурсы. Взлом беспроводной сети зачастую открывает доступ к локальным сервисам, позволяет перехватывать чувствительную информацию и осуществлять дальнейшее продвижение по сети.

На протяжении развития Wi-Fi было предложено несколько механизмов защиты: сначала WEP, затем WPA/TKIP, далее WPA2 с использованием AES-CCMP, и, наконец, более современный стандарт WPA3 [1-3]. В теории переход от одного поколения к следующему должен был устранять известные недостатки и укреплять криптографические основы протокола. Однако практика показала, что даже новые стандарты не являются абсолютно безопасными и могут содержать как концептуальные просчёты, так и реализационные ошибки.

Изучим подробнее сведения о наиболее значимых уязвимостях беспроводных сетей, с акцентом на протокол WPA3, а также анализ практических методов повышения защищённости, включающих правильную настройку оборудования и использование виртуальных частных сетей (VPN) поверх Wi-Fi-канала.

Первое поколение защиты, протокол WEP, опиралось на использование потокового шифра RC4 и статического ключа. Накопленный опыт эксплуатации выявил фундаментальные слабости в генерации векторов инициализации и способах применения ключевого материала, что сделало возможным восстановление секретного ключа по относительно небольшому объёму перехваченного трафика с помощью статистического анализа. В результате WEP был признан устаревшим, а для повышения уровня безопасности был предложен протокол WPA с набором расширений TKIP.

Дальнейшим шагом стал стандарт WPA2, в котором основным алгоритмом шифрования стал AES в режиме CCMP. Несмотря на существенное усиление криптографической компоненты, оказалось, что безопасность сети определяется не только выбранным алгоритмом шифрования, но и механизмами аутентификации, устойчивостью пароля, защищённостью рукопожатий и корректностью реализации протокола на стороне оборудования.

Важный практический вывод, неоднократно подтверждённый в исследованиях, заключается в том, что уязвимость системы нередко проявляется не на уровне математических основ алгоритма, а в логике построения протокола и ошибках его программной реализации. Именно эта особенность наиболее ярко проявилась при анализе WPA2 и последующего стандарта WPA3.

Даже после появления WPA3 значительная часть точек доступа продолжает функционировать в режимах WPA2-Personal или комбинированного WPA2/WPA3. Поэтому классические атаки на WPA/WPA2 сохраняют практическую значимость. К числу наиболее распространённых угроз относятся:

– перехват четырёхкратного рукопожатия в режиме WPA2-PSK и последующий офлайновый подбор пароля с использованием словарей и масок;

– атаки "злой двойник" (Evil Twin), при которых создаётся поддельная точка доступа с тем же SSID и более сильным сигналом, а пользователь, не заметив подмены, передаёт трафик через контролируемый злоумышленником узел;

– эксплуатация уязвимостей типа KRACK, связанных с повторным использованием одноразовых параметров при установлении сеансового ключа;

– атаки на уязвимые реализации протокола, в том числе с использованием некорректной обработки управляющих кадров.

Первая категория атак особенно опасна в сетях с слабыми или типовыми паролями: захватив рукопожатие, атакующий может производить подбор неограниченно долго, не взаимодействуя более с сетью. Вторая категория эксплуатирует доверие пользователей к знакомым именам сетей и отсутствие криптографической аутентификации точки доступа со стороны клиента. Третья демонстрирует, что даже формально корректный алгоритм шифрования может оказаться уязвимым при определённых особенностях протокола или его реализации.

Эти примеры показывают, что переход к более современному стандарту (WPA3) не отменяет необходимость учитывать накопленный опыт атак на предыдущие поколения и по возможности исключать режимы совместимости, открывающие доступ к старым векторам атак.

Стандарт WPA3 был разработан как попытка устранить наиболее заметные недостатки WPA2. В режиме Personal он использует схему аутентификации SAE (Simultaneous Authentication of Equals), основанную на т. н. Dragonfly-рукопожатии [4]. В отличие от четырёхкратного рукопожатия WPA2, где устойчивость сети во многом определяется сложностью пароля, SAE должен затруднять офлайновый перебор за счёт того, что обе стороны участвуют в вычислении общего секрета, а информация, полезная для подбора, практически не утечёт наружу.

Однако ряд исследовательских работ показал, что реализация Dragonfly в рамках WPA3 не лишена слабых мест [5]. В частности, было продемонстрировано, что при определённых вариантах параметров (выбор групп, особенностей отображения пароля в элемент группы) и при наличии побочных каналов возможно существенно сократить пространство поиска пароля. Кроме того, выявлены сценарии, в которых атакующий может навязать клиенту переход на менее защищённый протокол, эксплуатируя режимы совместимости.

Комплекс исследований, объединённых под названием Dragonblood [6], подробно анализирует различные варианты атак на WPA3, в том числе:

– использование утечек по времени выполнения и по потреблению ресурсов при обработке отдельных шагов протокола;

– навязывание клиентам неустойчивых параметров, облегчающих последующий подбор пароля;

– понижение уровня защиты за счёт принуждения к использованию режима WPA2 при наличии переходной конфигурации WPA2/WPA3.

Обзор публикаций и сообщений разработчиков показывает, что часть выявленных уязвимостей была устранена в обновлённых версиях прошивок и программного обеспечения точек доступа [7, 8]. Тем не менее ответственность за своевременное применение таких обновлений лежит на администраторах и владельцах устройств, а в реальных условиях именно задержка с обновлением часто становится причиной успешных атак.

Практико-ориентированные обзоры и статьи показывают, что для реализации атак на Wi-Fi злоумышленникам достаточно использовать открытые инструменты, входящие в состав популярных дистрибутивов для тестирования безопасности [9]. Типичный алгоритм действий включает несколько этапов:

1) пассивное сканирование эфира с целью выявления доступных точек доступа, типа применяемого шифрования и наличия активных клиентов;

2) инициирование процедуры деаутентификации, чтобы заставить клиента переподключиться и тем самым перехватить рукопожатие в WPA2 или обмен сообщениями в режиме переходной совместимости WPA2/WPA3;

3) последующий офлайновый анализ захваченных данных с использованием специализированного ПО для подбора паролей;

4) при необходимости – развёртывание фальшивой точки доступа и организация атак социальной инженерии для кражи учетных данных.

При работе с сетями, использующими "чистый" WPA3 без режимов совместимости, набор доступных атак существенно сужается, однако остаётся возможность эксплуатировать ошибки в конкретных реализациях протокола или в логике конфигурации. Это подчёркивает необходимость рассматривать безопасность Wi-Fi не только как криптографическую задачу, но и как комплексный вопрос конфигурирования и сопровождения инфраструктуры.

Результаты анализа литературных источников позволяют сформулировать ряд практических рекомендаций по повышению устойчивости беспроводных сетей к атакам.

Во-первых, при наличии технической возможности следует использовать режим "чистого" WPA3 без поддержки устаревших протоколов. Это снижает вероятность атак по понижению уровня защиты и повторного использования известных уязвимостей WPA2. При этом важно следить за актуальностью прошивок точек доступа и клиентских устройств, так как многие уязвимости устраняются именно на уровне обновления программного обеспечения.

Во-вторых, даже при применении современных протоколов значительную роль продолжает играть качество аутентификационных данных. Длинные случайные пароли или индивидуальные учётные записи в режиме Enterprise существенно затрудняют подбор и снижают последствия возможной утечки. Желательно также включать защиту служебного трафика (Protected Management Frames), затрудняющую подделку управляющих кадров и реализацию атак деаутентификации.

В-третьих, особенно в условиях использования публичных и мало контролируемых сетей, целесообразно добавлять поверх Wi-Fi ещё один контур защиты в виде VPN-туннеля. В этом случае даже успешная подмена точки доступа или частичный перехват трафика в пределах локального радиосегмента не позволяет злоумышленнику получить доступ к содержимому шифруемого VPN-соединения. На практике это реализуется через

использование современных протоколов (OpenVPN, WireGuard и др.), настроенных на доверенном сервере.

Наконец, важным элементом остаётся мониторинг и обучение пользователей. Технические средства могут фиксировать появление подозрительных точек доступа, а также аномальные попытки аутентификации. Пользователям следует разъяснять основные признаки небезопасных сетей и базовые правила поведения при доступе к Wi-Fi в общественных местах.

Для практического применения рассмотренных подходов полезно дифференцировать рекомендации в зависимости от типа среды: домашняя сеть, учебное заведение, малый бизнес.

Домашний пользователь, как правило, использует одно устройство-маршрутизатор, предоставляемое провайдером или приобретённое самостоятельно. В этом случае основными мерами защиты являются: изменение заводского пароля администратора, отключение удалённого управления, включение WPA3-Personal (при поддержке клиентских устройств) либо, как минимум, WPA2-AES, использование длинной парольной фразы, регулярная проверка наличия обновлений прошивки маршрутизатора. Дополнительно рекомендуется настроить гостевую сеть для устройств, которым нельзя доверять полностью (смарт-техника, устройства гостей), и при доступе к чувствительным ресурсам (интернет-банк, личный кабинет госуслуг) использовать VPN-подключение к доверенному серверу.

В учебных заведениях (колледжи, вузы) беспроводная сеть обычно обслуживает большое количество пользователей и устройств с различным уровнем доверия. Здесь целесообразно внедрение сегментации (отдельные SSID для сотрудников и студентов), использование WPA2/WPA3-Enterprise с индивидуальными учётными записями и централизованной аутентификацией, ограничение доступа из гостевых сегментов к внутренним ресурсам. Важную роль играет мониторинг: системы обнаружения вторжений в беспроводной среде позволяют вовремя зафиксировать появление "левых" точек доступа и аномальную активность.

Для малого бизнеса (кафе, гостиницы, офисы) ключевым вопросом становится разделение служебной и клиентской сетей. Рекомендуется организовывать отдельную гостевую сеть с ограниченной полосой пропускания и доступом только в интернет, защищённую WPA2/WPA3 с простыми, но регулярно меняемыми паролями. Внутренняя сеть, используемая для работы кассового оборудования, серверов и рабочих станций, должна быть отделена на уровне VLAN и иметь более строгие политики безопасности. Для доступа сотрудников к внутренним ресурсам из внеофисных локаций целесообразно использовать VPN-каналы.

С учётом того, что тема защиты беспроводных сетей широко преподаётся в технических вузах, представляется полезным кратко описать пример методики лабораторного практикума, позволяющего студентам на практике познакомиться с основами атак и защит.

В качестве тестового стенда может использоваться отдельная точка доступа, не подключённая к производственной сети, и один-два клиентских устройства. На лабораторном компьютере устанавливается дистрибутив, содержащий инструменты анализа Wi-Fi (например, Kali Linux). В рамках работы студентам предлагается:

– провести сканирование эфира и идентифицировать тестовую сеть;

– перехватить рукопожатие WPA2-PSK и продемонстрировать принцип офлайнового подбора пароля на небольшом словаре (с использованием заранее подготовленных тестовых паролей);

– пронаблюдать попытки деаутентификации и их влияние на поведение клиента;

– настроить более стойкую конфигурацию сети (длинный пароль, отключение лишних протоколов, включение защиты управляющих кадров) и повторно оценить сложность атаки.

Отдельным этапом может быть обсуждение особенностей WPA3 и рассмотрение известных уязвимостей на теоретическом уровне без практического воспроизведения потенциально опасных сценариев. Важно подчёркивать, что подобные эксперименты допускаются только в изолированных лабораторных условиях и не могут проводиться в реальных сетях без явного разрешения владельца.

Вопросы защиты информации в беспроводных сетях в российской юрисдикции рассматриваются в более широком контексте обеспечения информационной безопасности. Ключевым документом стратегического уровня является Доктрина информационной безопасности Российской Федерации, где обозначены цели и направления государственной политики в области защиты информации и критической инфраструктуры [10].

На отраслевом уровне требования к защите информации в автоматизированных системах, в том числе использующих беспроводной доступ, формулируются в документах ФСТЭК России и ФСБ России. Для государственных информационных систем и объектов критической информационной инфраструктуры устанавливаются минимальные наборы мер защиты, включающие использование сертифицированных средств криптографической защиты, разграничение доступа, регистрацию событий безопасности. Хотя конкретные протоколы Wi-Fi не всегда перечисляются явно, при проектировании систем предусмотрено, что беспроводной сегмент должен соответствовать общим требованиям по конфиденциальности и целостности данных.

Таким образом, можно прийти к выводу о том, что выбор и настройка протоколов WPA2/WPA3, а также внедрение дополнительных механизмов, таких как VPN, должны рассматриваться не только с точки зрения технической целесообразности, но и сквозь призму соблюдения нормативных требований. Это особенно актуально для образовательных учреждений, органов власти и предприятий, относящихся к сфере критической инфраструктуры.

Одним из перспективных направлений исследований является использование методов машинного обучения для автоматизированного выявления атак на протоколы беспроводной связи. Уже сегодня предлагаются модели, способные по косвенным признакам отличать легитимные сеансы WPA3 от попыток атак по понижению уровня защиты и других аномалий. По мере усложнения протоколов и роста объёма трафика ручной анализ становится малореалистичным, и интеллектуальные системы мониторинга могут занять ключевое место в инфраструктуре безопасности.

Другим направлением является дальнейшее совершенствование самих протоколов аутентификации и шифрования в Wi-Fi. Обсуждаются варианты использования постквантовых алгоритмов в беспроводных сетях, усиление механизмов защиты от атак через

побочные каналы, а также более тесная интеграция средств защиты в сетевую инфраструктуру, включая точки доступа и контроллеры.

В российском контексте дополнительное значение приобретают задачи сертификации оборудования и программных средств в соответствии с национальными требованиями по защите информации. Это предполагает не только формальное соответствие стандартам, но и практическое тестирование на устойчивость к известным типам атак, включая те, которые описаны в зарубежной литературе.

Проведённый анализ показал, что безопасность беспроводных сетей не может обеспечиваться исключительно выбором "правильного" протокола шифрования. Даже современные стандарты, такие как WPA3, подвержены ряду специфических уязвимостей, связанных с особенностями протокола и его реализации. При этом старые векторы атак на WPA/WPA2 сохраняют актуальность в силу широкого распространения режимов совместимости и использования слабых паролей.

Эффективная защита Wi-Fi-инфраструктуры требует многоуровневого подхода, включающего грамотное конфигурирование точек доступа, применение стойких аутентификационных данных, использование дополнительных средств защиты (VPN, сегментация сети, мониторинг аномалий) и повышение осведомлённости пользователей. В перспективе можно ожидать дальнейшего развития как стандартов шифрования беспроводного трафика, так и интеллектуальных систем анализа, способных автоматически выявлять и блокировать сложные атаки на уровне протокола.

СПИСОК ЛИТЕРАТУРЫ

1. Крепышев, Д.А. Безопасность Wi-Fi разных поколений / Д.А. Крепышев, Ю.С. Абушкевич, П.А. Ярощук // CyberLeninka : [сайт]. – 2025. – URL: https://cyberleninka.ru/article/n/bezopasnost-wi-fi-raznyh-pokoleniy (дата обращения: 03.03.2026).

2. Модель потока атак и анализ безопасности для протоколов Wi-Fi // Радиотехнические системы и комплексы : сборник трудов конференции. – Севастополь, 2022. – URL: https://rt-sevastopol.ru/conf2022/articles/067.pdf (дата обращения: 03.03.2026).

3. Анализ уязвимостей беспроводных сетей Wi-Fi и LTE // Технический вестник университета им. Шакарима. – 2025. – URL: https://tech.vestnik.shakarim.kz/jour/article/view/1766 (дата обращения: 03.03.2026).

4. Черкасова, С.А. Уязвимость рукопожатия Dragonfly протокола WPA3 / С.А. Черкасова, Д.И. Идиятова // Научная электронная библиотека eLIBRARY.RU : [сайт]. – 2020. – URL: https://elibrary.ru/item.asp?id=42832078 (дата обращения: 03.03.2026).

5. Кухта, А.И. Анализ методов защиты беспроводной сети Wi-Fi / А.И. Кухта // Международный научный журнал «Молодой исследователь Дона». – 2020. – № 2 (23). – С. 41-48. – URL: https://mid-journal.ru/upload/mid/iblock/fb1/8_1034-Kukhta_41_48.pdf (дата обращения: 03.03.2026).

6. Dragonblood: Analysing WPA3's Dragonfly Handshake : [site]. – URL: https://wpa3.mathyvanhoef.com (дата обращения: 03.03.2026).

7. A Machine Learning Approach for Detecting WPA3 Downgrade Attacks // PubMed Central : [site]. – URL: https://pmc.ncbi.nlm.nih.gov/articles/PMC12404434/ (дата обращения: 03.03.2026).

8. Опубликована технология защиты беспроводных сетей WPA3 // OpenNET : [сайт]. – 2020. – URL: https://www.opennet.ru/opennews/art.shtml?num=48854 (дата обращения: 03.03.2026).

9. Уязвимости в технологии защиты беспроводных сетей WPA3 и в EAP-pwd // OpenNET : [сайт]. – 2019. – URL: https://www.opennet.ru/opennews/art.shtml?num=50493 (дата обращения: 03.03.2026).

10. Доктрина информационной безопасности Российской Федерации : утверждена Указом Президента Российской Федерации от 5 декабря 2016 г. № 646 // Совет Безопасности РФ : [сайт]. – 2016. – URL: http://www.scrf.gov.ru/security/information/document5/ (дата обращения: 03.03.2026).

REFERENCES

1. Krepyshev, D.A. Wi-Fi Security of Different Generations / D.A. Krepyshev, Yu.S. Abushkevich, P.A. Yaroshchuk // CyberLeninka: [website]. – 2025. – URL: https://cyberleninka.ru/article/n/bezopasnost-wi-fi-raznyh-pokoleniy (date of access: 03.03.2026).

2. Attack Flow Model and Security Analysis for Wi-Fi Protocols // Radio Engineering Systems and Complexes: Conference Proceedings. – Sevastopol, 2022. – URL: https://rt-sevastopol.ru/conf2022/articles/067.pdf (date of access: 03.03.2026).

3. Analysis of Vulnerabilities of Wi-Fi and LTE Wireless Networks // Technical Bulletin of Shakarim University. – 2025. – URL: https://tech.vestnik.shakarim.kz/jour/article/view/1766 (date of access: 03.03.2026).

4. Cherkasova, S.A. Vulnerability of the Dragonfly handshake of the WPA3 protocol / S.A. Cherkasova, D.I. Idiyatova // Scientific electronic library eLIBRARY.RU: [site]. – 2020. – URL: https://elibrary.ru/item.asp?id=42832078 (date of access: 03.03.2026).

5. Kukhta, A.I. Analysis of Wi-Fi wireless network security methods / A.I. Kukhta // International scientific journal "Young researcher of the Don". – 2020. – No. 2 (23). – P. 41-48. – URL: https://mid-journal.ru/upload/mid/iblock/fb1/8_1034-Kukhta_41_48.pdf (date accessed: 03.03.2026).

6. Dragonblood: Analyzing WPA3's Dragonfly Handshake : [site]. – URL: https://wpa3.mathyvanhoef.com (date accessed: 03.03.2026).

7. A Machine Learning Approach for Detecting WPA3 Downgrade Attacks // PubMed Central : [site]. – URL: https://pmc.ncbi.nlm.nih.gov/articles/PMC12404434/ (date accessed: 03.03.2026).

8. WPA3 Wireless Network Security Technology Published // OpenNET : [site]. – 2020. – URL: https://www.opennet.ru/opennews/art.shtml?num=48854 (date of access: 03.03.2026).

9. Vulnerabilities in WPA3 wireless network security technology and in EAP-pwd // OpenNET: [date of access]. – 2019. – URL: https://www.opennet.ru/opennews/art.shtml?num=50493 (date of access: 03.03.2026).

10. Doctrine of Information Security of the Russian Federation: approved by Decree of the President of the Russian Federation of December 5, 2016, No. 646 // Security Council of the Russian Federation: [date of access]. – 2016. – URL: http://www.scrf.gov.ru/security/information/document5/ (date of access: 03.03.2026).