

СОВРЕМЕННЫЕ МЕТОДЫ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ В СЕТЯХ WI-FI

Т.С.Жалолов¹

Mas'ul muallif: Жалолов
Турсунбек Садриддинович,
Доцент Азиатского
международного университета.

Accepted: 13 Sentabr 2026

Published: 13 Sentabr 2026

Copyright: © 2026 by the
author(s). Licensee Buxoro xalqaro
universiteti ilmiy axborotnomasi.

Iqtibos uchun: Жалолов, Т. С.
СОВРЕМЕННЫЕ МЕТОДЫ
ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ
В СЕТЯХ WI-FI / Т. С. Жалолов //
Buxoro xalqaro universiteti ilmiy
axborotnomasi. — 2026. — Т. 9, №
1. — В. 165–168.

1. Доцент Азиатского международного университета

Аннотация. В статье рассматриваются актуальные подходы к защите беспроводных локальных сетей стандарта IEEE 802.11. Автор прослеживает логику смены криптографических протоколов - от скомпрометированного WEP до действующего WPA3, - раскрывает устройство механизма одновременной аутентификации равных (SAE) и оппортунистического шифрования (OWE), а также систематизирует наиболее распространённые векторы вторжения: перехват четырёхэтапного рукопожатия, подмена точки доступа, принудительное разделение клиентов. Отдельное внимание уделено организационно-техническим мерам: сегментации трафика, контролю доступа на уровне сети и применению систем обнаружения беспроводных вторжений. Предложена многоуровневая модель защиты, объединяющая криптографические, архитектурные и поведенческие средства контроля.

Ключевые слова: беспроводная сеть, IEEE 802.11, WPA3, SAE, шифрование, аутентификация, точка доступа, обнаружение вторжений, сегментация сети, информационная безопасность.

WI-FI TARMOQLARIDA XAVFSIZLIKNI TA'MINLASHNING ZAMONAVIY USULLARI

Annotatsiya. Maqolada IEEE 802.11 standartidagi simsiz mahalliy tarmoqlarni himoyalashning bugungi yondashuvlari tahlil qilinadi. Muallif kriptografik protokollarning almashinish mantiqini - buzilgan WEP dan hozirda amaldagi WPA3 ga qadar - kuzatib boradi, teng tomonlarning bir vaqtda autentifikatsiyasi (SAE) hamda opportunistik shifrlash (OWE) mexanizmlarining ishlash tartibini ochib beradi va eng ko'p tarqalgan hujum yo'nalishlarini tizimlashtiradi: to'rt bosqichli qo'l siltashni ushlab qolish, kirish nuqtasini almashtirish, mijozlarni majburan uzish. Trafikni segmentlash, tarmoq darajasida kirishni nazorat qilish va simsiz hujumlarni aniqlash tizimlarini qo'llash kabi tashkiliy-texnik choralarga alohida e'tibor qaratilgan. Kriptografik, arxitektura va xatti-harakat nazorati vositalarini birlashtiruvchi ko'p qatlamli himoya modeli taklif etiladi.

Kalit so'zlar: simsiz tarmoq, IEEE 802.11, WPA3, SAE, shifrlash, autentifikatsiya, kirish nuqtasi, hujumlarni aniqlash, tarmoq segmentatsiyasi, informatsion xavfsizlik.

MODERN METHODS FOR ENSURING SECURITY IN WI-FI NETWORKS

Abstract. The paper examines current approaches to protecting wireless local area networks based on the IEEE 802.11 standard. The author traces the rationale behind successive generations of cryptographic protocols - from the compromised WEP to the presently deployed WPA3 - explains the operation of Simultaneous Authentication of Equals (SAE) and Opportunistic Wireless Encryption (OWE), and classifies the most widespread intrusion vectors: interception of the four-way handshake, access point impersonation, and forced client disassociation. Particular attention is devoted to organisational and technical safeguards, namely traffic segmentation, network-level access control, and the deployment of wireless intrusion detection systems. A multi-layered protection model is proposed that combines cryptographic, architectural, and behavioural control mechanisms.

Keywords: wireless network, IEEE 802.11, WPA3, SAE, encryption, authentication, access point, intrusion detection, network segmentation, information security.

Введение. Беспроводной доступ перестал быть удобным дополнением к проводной инфраструктуре и превратился в её основной канал: значительная доля корпоративного и бытового трафика передаётся сегодня по радиointерфейсу. Такая смена роли изменила и структуру рисков. Если проводной сегмент физически ограничен пределами помещения, то радиосигнал распространяется за стены здания, а значит, потенциальный нарушитель не нуждается ни в подключении к порту коммутатора, ни в присутствии внутри охраняемого периметра. Достаточно находиться в зоне уверенного приёма и располагать адаптером, поддерживающим режим наблюдения.

Ответом на эту особенность стала последовательная смена криптографических протоколов, каждый из которых устранял слабости

предшественника. Однако практика показывает, что обновление протокола само по себе не гарантирует защищённости: значительная часть успешных вторжений опирается не на взлом шифра, а на ошибки конфигурирования, использование словарных парольных фраз и доверчивость пользователя, подключающегося к точке доступа с привычным именем сети.

Цель настоящей работы - систематизировать современные средства защиты сетей IEEE 802.11 и показать, что устойчивость беспроводного сегмента достигается лишь сочетанием криптографических, архитектурных и организационных мер. В качестве материала использованы спецификации отраслевых стандартов, публикации по анализу уязвимостей протоколов рукопожатия, а также рекомендации по построению защищённых беспроводных инфраструктур.

1. Эволюция протоколов защиты беспроводного канала. Первый механизм конфиденциальности, заложенный в исходную редакцию стандарта, носил название Wired Equivalent Privacy и опирался на потоковый шифр RC4 с коротким вектором инициализации. Уязвимость решения оказалась не столько в самом шифре, сколько в способе его применения: вектор передавался открыто и повторялся уже через несколько десятков тысяч кадров, что позволяло восстановить ключевой поток статистическими методами. Практическая скорость компрометации такой сети измеряется минутами, поэтому протокол давно исключён из перечня допустимых.

Промежуточным решением стал WPA с протоколом временной целостности ключа (TKIP). Он сохранил совместимость с существующим оборудованием, но ввёл смену ключа для каждого кадра и код проверки целостности, устраняющий возможность незаметной подмены содержимого. Тем не менее наследование архитектуры RC4 не позволило считать WPA долгосрочной мерой.

Качественный переход произошёл с принятием WPA2, где вместо потокового шифра применён блочный алгоритм AES в режиме счётчика с кодом аутентификации сообщения (CCMP). Криптографическое ядро WPA2 не скомпрометировано до настоящего времени, однако процедура согласования сеансового ключа - четырёхэтапное рукопожатие - оказалась чувствительна к повторному воспроизведению третьего сообщения, что было продемонстрировано в исследовании атак на переустановку ключа.

Действующее поколение - WPA3 - устраняет именно эту слабость. Вместо доказательства владения общим секретом через обмен зависимыми от него величинами применён протокол одновременной аутентификации равных (SAE), основанный на схеме обмена ключами с сопоставлением пароля. Ключевое следствие состоит в том, что перехваченный обмен более не содержит материала, пригодного для офлайн-словарной атаки: каждая попытка проверки пароля требует нового активного взаимодействия с точкой доступа, а значит, поддаётся ограничению по частоте.

2. Механизмы аутентификации и шифрования в актуальных решениях. Современный набор средств защиты беспроводного канала неоднороден: выбор конкретного механизма определяется характером сети. Для домашних и небольших офисных сегментов предусмотрен режим с общей парольной фразой, где роль защитника от подбора играет SAE. Корпоративная модель строится иначе - на инфраструктуре 802.1X, в которой точка доступа выполняет функцию посредника, а решение о допуске принимает сервер аутентификации по протоколу RADIUS. Учётные данные при этом передаются внутри защищённого туннеля, формируемого одним из методов расширяемого протокола аутентификации - как правило, EAP-TLS с взаимной проверкой сертификатов.

Отдельного упоминания заслуживает защита открытых сетей общественного доступа. Ранее подключение без пароля означало полное отсутствие шифрования, и любой участник радиоэфира мог читать трафик соседних устройств. Опportunистическое беспроводное шифрование (OWE) решает задачу иначе: сохраняя привычную для пользователя процедуру подключения без ввода секрета, оно выполняет анонимный обмен ключами, в результате которого каждая станция получает индивидуальный сеансовый ключ.

Не менее важен механизм защиты управляющих кадров (PMF). Именно неаутентифицированные служебные сообщения долгое время оставались основой атак принудительного разъединения: злоумышленнику достаточно было отправить поддельный кадр разрыва соединения от имени точки доступа. В WPA3 подписывание управляющих кадров переведено в разряд обязательных требований, что закрывает данный канал воздействия.

Таблица 1.

Сравнительная характеристика протоколов защиты сетей IEEE 802.11

Протокол	Алгоритм шифрования	Согласование ключа	Текущий статус
WEP	RC4, 40/104 бита	Статический ключ	Скомпрометирован
WPA	RC4 + TKIP	Четырёхэтапное рукопожатие	Не рекомендуется
WPA2	AES-CCMP, 128 бит	Четырёхэтапное рукопожатие	Допустим с оговорками
WPA3-Personal	AES-CCMP / GCMP	SAE	Рекомендуется
WPA3-Enterprise	AES-GCMP, 256 бит	802.1X / EAP-TLS	Рекомендуется

3. Векторы вторжения и противодействие им

Классификация угроз беспроводному сегменту удобно строится по признаку объекта воздействия. Первую группу образуют атаки на криптографическую процедуру: перехват рукопожатия с последующим офлайн-выбором парольной фразы, а также описанная выше переустановка сеансового ключа. Вторую группу

составляют атаки на доверие пользователя - развёртывание точки доступа с именем легитимной сети, вынуждающее устройство подключиться к оборудованию нарушителя и передать трафик через подконтрольный ему узел. Третья группа направлена на доступность: массовая рассылка кадров разъединения либо намеренная загрузка канала помехами.

Показательно, что переход на WPA3 не устраняет угрозы второй и третьей групп автоматически. Реализации SAE в первые годы эксплуатации содержали дефекты, допускавшие понижение уровня защиты при работе в смешанном режиме совместимости с WPA2, а также утечку информации через различия во времени обработки запросов. Отсюда следует практический вывод: смешанный режим следует рассматривать как временную меру периода миграции, а не как штатную конфигурацию.

Противодействие подмене точки доступа лежит преимущественно за пределами шифрования канала. Действенными оказываются взаимная аутентификация на основе сертификатов, при которой клиент проверяет подлинность сервера прежде, чем передать учётные данные, и запрет автоматического подключения к сохранённым открытым сетям. Для инфраструктуры общественного доступа целесообразно сочетание OWE с принудительным туннелированием трафика.

Защита от воздействия на доступность требует иных инструментов. Подписывание управляющих кадров нейтрализует поддельные сообщения о разъединении, однако не спасает от подавления сигнала на физическом уровне. Здесь применяются средства радиомониторинга, фиксирующие аномальный уровень шума и внезапное падение отношения сигнала к помехе, с последующим переключением на резервный частотный канал.

4. Организационно-технические меры и непрерывный контроль

Криптография защищает содержимое кадра, но не определяет, какие ресурсы окажутся доступны подключившемуся устройству. Эту задачу решает сегментация: беспроводные клиенты помещаются в отдельные виртуальные сети с отдельными политиками маршрутизации, гостевой сегмент изолируется от корпоративного, а взаимодействие между сегментами разрешается только по явно описанным правилам. Дополнительным контуром выступает контроль доступа к сети, при котором допуск устройства обусловлен не только успешной аутентификацией, но и соответствием его состояния заданным требованиям - наличием актуальных обновлений и работающих средств защиты.

Развитием этого подхода служит модель нулевого доверия, отказывающаяся от представления о внутреннем периметре как о доверенной зоне. Подключение к корпоративной беспроводной сети в такой модели не даёт никаких прав само по себе: каждый запрос к прикладному ресурсу проверяется отдельно, с учётом личности пользователя, состояния устройства и контекста обращения.

Наконец, статическая настройка требует поддержки средствами наблюдения. Системы обнаружения и предотвращения беспроводных вторжений ведут постоянный учёт радиообстановки, выявляя посторонние точки доступа, несанкционированные подключения и характерные последовательности служебных кадров, свидетельствующие о попытке разъединения клиентов. Применение методов машинного обучения к профилю трафика позволяет фиксировать отклонения от типичного поведения - нехарактерное время активности, аномальный объём передачи, обращения к нетипичным адресам - то есть обнаруживать инциденты, для которых сигнатурное описание отсутствует.

Существенным, хотя нередко недооцениваемым элементом остаётся работа с персоналом. Наиболее совершенная конфигурация обесценивается, если пользователь подключается к сети с привычным именем в общественном месте и вводит корпоративные учётные данные по запросу поддельного портала авторизации. Регулярное обучение и отработка типовых сценариев вторжения дают эффект, сопоставимый с внедрением технических средств.

Заключение. Проведённый анализ позволяет утверждать, что безопасность беспроводной сети не сводится к выбору версии протокола. Смена WEP на WPA2, а затем на WPA3 закрыла принципиальные криптографические изъяны, и на сегодняшний день корректно настроенный WPA3 с обязательным подписыванием управляющих кадров следует считать базовым требованием, а не желательной опцией. Однако устойчивость системы определяется её наиболее слабым элементом, и таким элементом чаще всего оказывается не шифр, а конфигурация или человек.

Практическая модель защиты, вытекающая из рассмотренного материала, имеет четыре уровня. Криптографический уровень обеспечивает конфиденциальность и целостность кадров средствами SAE и AES-GCMP. Уровень идентификации устанавливает подлинность сторон через инфраструктуру 802.1X с взаимной проверкой сертификатов. Архитектурный уровень ограничивает область возможного ущерба посредством сегментации и принципа нулевого доверия. Наблюдательный уровень обеспечивает своевременное выявление отклонений средствами радиомониторинга и поведенческого анализа. Изъятие любого из уровней делает остальные существенно менее эффективными.

Дальнейшие направления исследования связаны, во-первых, с адаптацией перечисленных механизмов к устройствам с ограниченными вычислительными ресурсами, для которых полноценная сертификатная аутентификация затруднительна, и, во-вторых, с подготовкой беспроводных протоколов к условиям постквантовой криптографии.

Список использованной литературы

- [1] IEEE Standard for Information Technology - Telecommunications and Information Exchange between Systems. IEEE Std 802.11-2020. - New York: IEEE, 2021. - 4379 p.
- [2] IEEE Standard for Local and Metropolitan Area Networks - Port-Based Network Access Control. IEEE Std 802.1X-2020. - New York: IEEE, 2020. - 289 p.
- [3] Wi-Fi Alliance. WPA3 Specification, Version 3.0. - Austin: Wi-Fi Alliance, 2020. - 32 p.
- [4] Vanhoef M., Piessens F. Key Reinstallation Attacks: Forcing Nonce Reuse in WPA2 // Proceedings of the ACM SIGSAC Conference on Computer and Communications Security. - Dallas, 2017. - P. 1313-1328.
- [5] Vanhoef M., Ronen E. Dragonblood: Analysing the Dragonfly Handshake of WPA3 and EAP-pwd // IEEE Symposium on Security and Privacy. - San Francisco, 2020. - P. 517-533.
- [6] Fluhrer S., Mantin I., Shamir A. Weaknesses in the Key Scheduling Algorithm of RC4 // Selected Areas in Cryptography. - Berlin: Springer, 2001. - P. 1-24.
- [7] Harkins D., Kumari W. Opportunistic Wireless Encryption. RFC 8110. - IETF, 2017. - 12 p.
- [8] Souppaya M., Scarfone K. Guidelines for Securing Wireless Local Area Networks (WLANs). NIST SP 800-153. - Gaithersburg: NIST, 2012. - 26 p.
- [9] Rose S., Borchert O., Mitchell S., Connelly S. Zero Trust Architecture. NIST SP 800-207. - Gaithersburg: NIST, 2020. - 59 p.
- [10] Kohlios C., Hayajneh T. A Comprehensive Attack Flow Model and Security Analysis for Wi-Fi and WPA3 // Electronics. - 2018. - Vol. 7, No. 11. - P. 284.

