УДК 004.056.5

СОВРЕМЕННЫЕ ПРОТОКОЛЫ АУТЕНТИФИКАЦИИ И АВТОРИЗАЦИИ В БЕСПРОВОДНЫХ СЕТЯХ

Е.В. БЕГЛЯК, В.А. МАРЦИНКЕВИЧ

Белорусский государственный университет информатики и радиоэлектроники, Республика Беларусь

Поступила в редакцию 15 февраля 2025

Аннотация. Статья посвящена анализу современных протоколов аутентификации и авторизации в беспроводных сетях, их безопасности, эффективности и применимости в различных сценариях. Рассмотрены ключевые стандарты, включая WPA3, EAP, OAuth 2.0, OpenID Connect, а также методы управления доступом (RBAC, ABAC, SAML). Проведен сравнительный анализ протоколов по уровню защиты от кибератак, производительности и удобству внедрения. Выявлены основные проблемы, такие как уязвимости в устаревших системах и сложность интеграции в гетерогенные сети. Предложены рекомендации по выбору протоколов для корпоративных сетей, публичного Wi–Fi и IoT–устройств. Обзор подчёркивает необходимость адаптации существующих протоколов безопасности и разработки новых решений для эффективного противостояния современным киберугрозам.

Ключевые слова: аутентификация, авторизация, беспроводные сети, WPA3, EAP, OAuth 2.0, кибербезопасность, управление доступом, RBAC, ABAC, SAML, IoT.

Введение

Современный мир невозможно представить без беспроводных технологий. От корпоративных офисов до умных домов, от общественных пространств до промышленных IoT–систем – Wi–Fi и другие беспроводные сети стали основой цифровой коммуникации. Однако, чем больше устройств подключается к сети, тем шире становится поле для киберугроз. По данным аналитиков Fortinet, в 2023 году более 70 % компаний столкнулись с инцидентами, связанными с утечкой данных через уязвимости в системах аутентификации [1]. При этом традиционные методы защиты, такие как статичные пароли или устаревшие протоколы вроде WEP (Wired Equivalent Privacy), давно перестали быть надежным щитом. Злоумышленники применяют разнообразные методы атак, начиная с грубого перебора паролей и заканчивая использованием уязвимостей в механизмах аутентификации и протоколах обмена данными.

Эта проблема усугубляется разнородностью современных сетей. К одной точке доступа могут подключаться сотрудники с корпоративными ноутбуками, гости со смартфонами, датчики умного здания и даже автономные роботы. Каждое из этих устройств требует индивидуального подхода к управлению доступом. Например, IoT–устройства зачастую не способны поддерживать сложные методы аутентификации из-за ограниченных вычислительных ресурсов, а публичный Wi–Fi в аэропорту нуждается в балансе между безопасностью и удобством для пользователей.

Цель статьи – рассмотреть, как современные протоколы аутентификации и авторизации, такие как WPA3 (Wi–Fi Protected Access), OAuth 2.0, EAP (Extensible Authentication Protocol), OpenID Connect и IEEE 802.1X, решают конкретные задачи в различных сценариях. Анализ этих технологий помогает оценить компромиссы между удобством и безопасностью, а также определить их дальнейшие перспективы в условиях растущих требований к кибербезопасности.

Главное внимание уделено трем ключевым аспектам: эволюции протоколов, практической применимости и гибридным подходам. Новые стандарты, такие как WPA3 и EAP–TLS 1.3(Transport Layer Security), эффективно закрывают пробелы своих предшественников, обеспечивая более надёжную защиту. В то же время решения, которые идеально подходят для

корпоративных сетей, часто сталкиваются с трудностями в IoT–средах из-за ограничений ресурсов. В ответ на это сложность современных инфраструктур требует применения комбинированных методов аутентификации и авторизации, которые позволяют учитывать разнообразие устройств и сред.

Статья позволит глубже понять, как современные протоколы аутентификации и авторизации отвечают на вызовы цифровой эпохи, демонстрируя их достижения и выявляя области для дальнейшего развития.

Обзор современных протоколов аутентификации

Беспроводные сети, в силу своей открытой природы, требуют особенно тщательного подхода к аутентификации. Современные протоколы развиваются, чтобы противостоять не только традиционным угрозам, но и новым методам атак, которые становятся всё более изощрёнными. Среди множества решений выделяются несколько ключевых стандартов, каждый из которых занимает свою нишу в зависимости от требований к безопасности, масштабу сети и типу устройств.

Одним из наиболее значимых шагов в эволюции безопасности Wi–Fi стало появление WPA3 в 2018 году. Новый протокол решает давние проблемы предыдущего стандарта WPA2, вызвавшие серьезную критику из-за его уязвимостей. WPA3 ввёл технологию SAE (Simultaneous Authentication of Equals), устранившую риск атак методом перебора паролей, таких как Pixie Dust. Кроме того, протокол обеспечивает механизм «совершенной прямой секретности» (Perfect Forward Secrecy), гарантируя, что даже при компрометации долгосрочного ключа злоумышленник не сможет расшифровать ранее перехваченные данные. Отдельного внимания заслуживает функция Wi–Fi Easy Connect, упрощающая подключение устройств без дисплея – от умных лампочек до промышленных датчиков. Однако, несмотря на прогрессивность WPA3, его внедрение сталкивается с рядом сложностей. Многие организации до сих пор используют оборудование, не поддерживающее новый стандарт, а массовый переход требует значительных финансовых и временных затрат [2].

Для корпоративных сред, где безопасность часто важнее удобства, остаётся актуальным EAP. Гибкость EAP позволяет выбирать из десятков методов аутентификации, адаптируясь к специфике инфраструктуры. Например, EAP–TLS, основанный на взаимной проверке сертификатов, обеспечивает высочайший уровень защиты, но требует развёртывания PKI (Public Key Infrastructure), что может быть избыточным для малого бизнеса. В таких случаях чаще применяются EAP–PEAP (Protected Extensible Authentication Protocol) или EAP–TTLS (Tunneled Transport Layer Security), которые используют туннелирование для защиты учётных данных. Эти методы особенно востребованы в образовательных учреждениях и крупных компаниях, где необходимо балансировать между безопасностью и простотой масштабирования. Для сред с повышенными требованиями к мобильности и многофакторной аутентификации отлично подходит EAP–MSCHAPv2 (Microsoft Challenge Handshake Authentication Protocol), который часто используется в комбинации с PEAP для обеспечения дополнительного уровня защиты, хотя и обладает ограничениями в контексте устойчивости к определённым видам атак. Развитие протоколов EAP продолжается, открывая новые возможности для обеспечения безопасности и повышения эффективности сетевых решений.

Интересный пример конвергенции технологий демонстрирует использование OAuth 2.0 и OpenID Connect в публичных беспроводных сетях. Изначально разработанные для авторизации в веб-приложениях, эти протоколы нашли применение в сценариях, где пользователь должен получить временный доступ к сети через стороннего провайдера. Например, при подключении к Wi–Fi в аэропорту система может перенаправить пользователя на страницу входа через Google или Facebook, используя OAuth 2.0 для делегирования прав. Это упрощает процесс для конечного пользователя и снижает нагрузку на провайдера, которому не нужно хранить пароли. Однако такая модель несёт риски, связанные с фишингом и утечкой токенов, что требует дополнительных мер, таких как обязательная многофакторная аутентификация.

Отдельного упоминания заслуживает стандарт IEEE 802.1X**,** который служит основой для контроля доступа в крупных сетях. Его архитектура, включающая три компонента – клиент,

аутентификатор и сервер аутентификации – обеспечивает централизованное управление политиками безопасности, минимизируя риск несанкционированного доступа. Например, в университетском кампусе 802.1X может использоваться для сегментирования трафика студентов, преподавателей и администрации, направляя каждую группу в отдельную VLAN (Virtual Local Area Network) для повышения уровня безопасности и оптимизации сетевых ресурсов. Ещё одним преимуществом является гибкость стандарта, позволяющая интегрировать его с различными механизмами аутентификации, такими как EAP–TLS или EAP–PEAP, что делает его универсальным инструментом для различных инфраструктур. Однако, несмотря на надёжность и эффективность, внедрение 802.1X зачастую требует значительных усилий по адаптации существующих сетей и предварительного обучения IT–специалистов, что ограничивает его применение в малых и средних сетях.

Эволюция протоколов аутентификации отражает общий тренд на персонализацию безопасности. Если раньше универсальные решения доминировали на рынке, то сегодня выбор метода зависит от конкретного контекста – от типа устройства до уровня доверия к пользователю. Это создаёт новые возможности, но и усложняет проектирование сетей, требуя от разработчиков глубокого понимания как технологий, так и бизнес-процессов.

Протоколы авторизации

Аутентификация, обеспечивающая проверку подлинности пользователя или устройства, – лишь первый рубеж защиты беспроводной сети. Следующий критически важный этап – авторизация, определяющая, какие ресурсы и в каком объёме доступны субъекту после успешной проверки. Если аутентификация отвечает на вопрос «кто вы?», то авторизация решает, «что вам разрешено делать». В условиях, когда сети становятся всё более сложными и распределёнными, методы управления доступом эволюционируют, предлагая решения для разных уровней гибкости и безопасности.

Одним из наиболее распространённых подходов остаётся RBAC (Role-Based Access Control) – управление доступом на основе ролей. Его принцип прост: каждому пользователю или устройству назначается роль (например, «сотрудник», «гость», «администратор»), которая определяет права доступа к сетевым ресурсам. В корпоративной Wi–Fi–сети – это может означать, что сотрудники отдела разработки получают доступ к серверам с исходным кодом, тогда как гости ограничены лишь выходом в интернет. Преимущество RBAC – в простоте администрирования. Добавление нового пользователя требует лишь присвоения ему соответствующей роли, а не индивидуальной настройки прав. Однако эта же простота становится недостатком в динамичных средах. Например, в университете, где студент одновременно может быть членом нескольких исследовательских групп, ручное управление ролями быстро превращается в логистический кошмар.

Альтернативой выступает ABAC (Attribute-Based Access Control) – управление доступом на основе атрибутов. Вместо жёстких ролей ABAC учитывает множество параметров: тип устройства, местоположение, время запроса, уровень безопасности соединения и даже данные из внешних систем (например, статус подписки из CRM). Представьте умное здание, где датчик температуры получает доступ к облачной платформе только при подключении через защищённую сеть, в рабочее время и, если его показания не выходят за заданный диапазон. Такая гранулярность делает ABAC идеальным для IoT–сетей, где тысячи устройств с разными функциями требуют индивидуальных политик. Однако за гибкость приходится платить: ABAC требует сложной инфраструктуры для анализа атрибутов в реальном времени, что увеличивает нагрузку на серверы авторизации [3].

Особый случай – SAML (Security Assertion Markup Language), который решает проблему федеративной авторизации в распределённых экосистемах. SAML позволяет одной организации делегировать аутентификацию и авторизацию доверенному провайдеру. Например, при подключении к партнёрской Wi–Fi–сети сотрудник компании-соискателя может использовать учётные данные своей корпоративной Active Directory, не создавая новый аккаунт. SAML–токен, подписанный поставщиком удостоверений, содержит всю необходимую информацию о правах доступа, что упрощает кросс-доменное взаимодействие. Этот подход особенно востребован в образовании и здравоохранении, где учреждения часто объединяются в консорциумы. Однако

SAML уязвим к атакам на основе подделки токенов, если не используются строгие методы шифрования и регулярная ротация ключей.

Интересно наблюдать, как эти протоколы комбинируются в реальных сценариях. В крупном университете, например, может использоваться связка EAP–TLS для аутентификации преподавательских и исследовательских устройств, ABAC для динамического управления доступом к студенческим ресурсам на основе курса обучения и текущего семестра, а SAML – для предоставления временного доступа внешним приглашённым лекторам или участникам конференции. Такая многослойность позволяет закрывать разные аспекты безопасности, но создаёт риск конфликта политик. Например, если RBAC ограничивает доступ студентов только к общедоступным библиотечным материалам, а SAML–токен от партнёрского учебного учреждения запрашивает расширенные права, система должна иметь чёткие правила приоритезации.

С учетом постоянно растущей сложности сетевых инфраструктур, комбинированный подход, включающий элементы RBAC, ABAC и SAML, становится необходимостью для обеспечения надежной защиты и гибкости управления доступом.

Сравнительный анализ протоколов

Эффективность протоколов аутентификации и авторизации невозможно оценить в отрыве от контекста их применения. С ростом числа подключённых устройств и усложнением сетевых инфраструктур выбор протоколов аутентификации и авторизации становится критически важным для обеспечения безопасности. Анализ ключевых протоколов демонстрирует, как технологии стремятся найти баланс между защитой и удобством.»

WPA3, безусловно, задаёт новый стандарт безопасности для Wi–Fi–сетей. Его механизм SAE и совершенная прямая секретность делают его практически неуязвимым к атакам, которые успешно эксплуатировали слабости WPA2. Однако эти преимущества теряют смысл, если в сети остаются устройства, поддерживающие только старые протоколы. Например, в гетерогенной среде, где к одной точке доступа подключаются современные смартфоны и устаревшие IoT–датчики, администратор вынужден либо поддерживать смешанный режим (WPA3–Transition Mode), либо жертвовать безопасностью ради совместимости. Это ярко иллюстрирует ключевую дилемму: даже самый прогрессивный протокол бесполезен без массового внедрения.

На этом фоне EAP демонстрирует удивительную гибкость. Методы вроде EAP–TLS, требующие инфраструктуры PKI, идеальны для банков или государственных учреждений, где безопасность превалирует над стоимостью внедрения. В то же время EAP–PEAP, использующий туннелирование поверх MSCHAPv2, подходит для университетов или стартапов, где важно быстро развернуть защиту без сложных настроек. Однако универсальность не исключает проблем, связанных с конфигурацией и управлением, которые становятся критическим фактором для обеспечения надёжности сети. Исследования показывают, что до 40 % утечек в корпоративных сетях связаны с ошибками в настройке RADIUS-серверов, которые часто используются вместе с EAP.

Не менее важно, чтобы протоколы не только обеспечивали защиту и гибкость, но также способствовали улучшению пользовательского взаимодействия. OAuth 2.0 и OpenID Connect, перенесённые из веб-сферы в мир беспроводных сетей, решают принципиально иную задачу – упрощение пользовательского опыта. Их сила – в способности интегрироваться с внешними провайдерами аутентификации, такими как социальные сети или корпоративные SSO-системы. Это делает их незаменимыми для публичных Wi–Fi–сетей в аэропортах, торговых центрах или гостиницах, где посетители ожидают мгновенного доступа без регистрации. Однако обратная сторона медали – уязвимость к фишингу и атакам на токены. Если злоумышленник перехватывает OAuth-токен, он может получить доступ не только к сети, но и к связанным сервисам (например, почте пользователя). Это требует дополнительных слоёв защиты, таких как ограничение времени жизни токенов или привязка к MAC–адресу устройства.

Сравнение методов авторизации – RBAC, ABAC и SAML – раскрывает ещё один пласт противоречий. RBAC, несмотря на простоту, становится узким местом в динамичных средах. Например, в стартапе, где сотрудники часто меняют роли, постоянное обновление политик превращается в рутину. ABAC, напротив, справляется с такими сценариями, но требует

значительных вычислительных ресурсов для анализа атрибутов в реальном времени. В IoT–сетях, где тысячи датчиков генерируют запросы одновременно, это может привести к задержкам авторизации. SAML, будучи идеальным для федеративных систем, сталкивается с проблемой доверия между организациями. Если университет-партнёр не обеспечивает должный уровень защиты своих учётных данных, это ставит под угрозу всю экосистему.

Интересный кейс – использование 802.1X в промышленных IoT–сетях. Стандарт обеспечивает централизованное управление доступом, но его реализация на заводах, где оборудование работает в экстремальных условиях (высокая температура, вибрация), часто приводит к сбоям в работе RADIUS–серверов (Remote Authentication Dial-In User Service). Это вынуждает инженеров идти на компромисс, заменяя 802.1X на упрощённые протоколы вроде Pre-Shared Key (PSK), что снижает общий уровень безопасности.

Общая тенденция такова: не существует «серебряной пули», способной закрыть все сценарии. Выбор протокола напоминает сборку пазла – необходимо совместить требования безопасности, ограничения инфраструктуры и ожидания пользователей. Например, в умном городе, где тысячи устройств от уличных камер до систем освещения объединены в единую сеть, может использоваться гибридная модель: WPA3 для шифрования данных, EAP–TLS для аутентификации критически важных узлов и ABAC для динамического управления доступом на основе данных с датчиков. Таким образом, внедрение протоколов аутентификации и авторизации требует не только технической точности, но и стратегического подхода, где безопасность, производительность и удобство объединяются для создания интегрированных сетевых решений будущего.

Проблемы и вызовы

Несмотря на прогресс в разработке протоколов, их внедрение в реальных условиях сталкивается с рядом системных сложностей. Эти проблемы часто носят не технический, а организационный или инфраструктурный характер, что делает их особенно устойчивыми к быстрому решению.

Унаследованные системы и инерция внедрения. Даже самые совершенные стандарты, такие как WPA3, не могут мгновенно вытеснить устаревшие протоколы. По данным исследования Avast (2023), 58 % роутеров в домашних сетях до сих пор используют WPA2, а 7 % – критически уязвимый WEP [4]. В корпоративном секторе ситуация ненамного лучше: переход на новые стандарты требует замены оборудования, переобучения сотрудников и временных простоев. Например, больница не может позволить себе отключить сеть на время миграции с WPA2 на WPA3, так как это парализует работу подключённых медицинских устройств. Это создаёт порочный круг: уязвимости старых систем остаются неисправленными, а новые технологии внедряются фрагментарно.

Сложность управления в гетерогенных средах. Современные сети объединяют устройства с радикально разными возможностями: от мощных серверов до датчиков с микроконтроллерами на 8–битной архитектуре. Протокол, идеально подходящий для аутентификации смартфонов, может быть неприменим к IoT–устройствам из-за ограничений по энергопотреблению или вычислительной мощности. Например, EAP–TLS, требующий обработки X.509–сертификатов, недоступен для дешёвых RFID–меток, что вынуждает использовать менее безопасные методы вроде статических ключей. Такая «лоскутная» безопасность создаёт точки входа для атак, особенно когда злоумышленник целенаправленно атакует самое слабое звено в системе.

Конфликт между удобством и безопасностью. Публичные Wi–Fi–сети – наглядный пример этого противоречия. С одной стороны, провайдеры заинтересованы в максимально простом подключении пользователей: вход через соцсети, одноразовые SMS–коды, гостевые доступы. С другой – упрощение процессов открывает двери для злоупотреблений. В 2022 году компания Kaspersky зафиксировала рост фишинговых атак через поддельные страницы входа в публичные Wi–Fi, где пользователи добровольно вводили свои учётные данные OAuth. Попытки усилить безопасность (например, ввести обязательную двухфакторную аутентификацию) часто приводят к снижению числа подключений, что экономически невыгодно для бизнеса.

Юридические и регуляторные барьеры. Развитие стандартов безопасности часто опережает законодательство. Это приводит к ситуациям, когда компании формально соблюдают

правила, используя устаревшие, но сертифицированные решения. Более того, в глобальных сетях приходится учитывать противоречивые требования разных юрисдикций. Китайский стандарт WAPI (WLAN Authentication and Privacy Infrastructure), обязательный для устройств, продающихся в стране, несовместим с WPA3, что усложняет создание универсальных продуктов для международного рынка [5].

Человеческий фактор. Даже самая продуманная система безопасности может быть скомпрометирована из-за ошибок пользователей или администраторов. Классический пример – повторное использование паролей. Согласно статье Enzoic, исследование Google показало, что 65 % людей повторно используют пароли на нескольких сайтах, что создает значительные риски для безопасности [6]. В случае утечки это позволяет злоумышленникам получать доступ к критически важным ресурсам. С другой стороны, администраторы часто оставляют настройки по умолчанию (например, стандартные учётные записи RADIUS–серверов), что упрощает проведение атак типа brute force.

Эти вызовы подчёркивают, что безопасность беспроводных сетей не просто техническая задача, а комплексная проблема, требующая координации между разработчиками, регуляторами и конечными пользователями. Успешное внедрение современных протоколов невозможно без учёта экономических, социальных и юридических аспектов.

Рекомендации по выбору протоколов

Выбор протоколов аутентификации и авторизации напоминает подбор инструментов для сложного ремонта: универсальных решений нет, но есть чёткие принципы, которые помогают избежать критических ошибок. Эти принципы основаны на балансе между рисками, ресурсами и требованиями конкретной экосистемы.

Для корпоративных сетей, где утечка данных может привести к катастрофическим последствиям, приоритетом становится многоуровневая защита. Здесь оптимальна комбинация WPA3 и EAP–TLS, дополненная ABAC для управления доступом. WPA3 обеспечивает современное шифрование и защиту от офлайн–атак, в то время как EAP–TLS, использующий сертификаты, исключает риски, связанные с утечкой паролей. ABAC в такой среде позволяет гибко настраивать политики: например, доступ к финансовым системам может предоставляться только с устройств, подключённых через VPN, и только в рабочее время. Однако такая связка требует значительных инвестиций: развёртывание PKI для EAP–TLS, обновление инфраструктуры для поддержки WPA3 и внедрение систем анализа атрибутов для ABAC. Для среднего бизнеса альтернативой может стать EAP–PEAP с Active Directory-интеграцией – менее безопасный, но более простой в настройке вариант.

Публичные Wi–Fi–сети – зона повышенного риска, где безопасность часто приносится в жертву удобству. В таких сценариях OAuth 2.0 с многофакторной аутентификацией становится компромиссным решением. Например, кафе может предложить гостям вход через Google или Apple ID, что сокращает риски хранения паролей и ускоряет подключение. Для дополнительной защиты стоит ограничить сессию по времени (например, 2 часа) и использовать изоляцию клиентов (Client Isolation), чтобы предотвратить атаки между устройствами в одной сети. Интересный пример – аэропорты, где OAuth 2.0 комбинируют с геолокацией: доступ к Wi–Fi автоматически отключается, когда пользователь покидает зону терминала, что снижает риск удалённых атак.

IoT–сети – пожалуй, самый сложный кейс. Устройства вроде умных датчиков или камер часто неспособны выполнять ресурсоёмкие операции. Здесь на помощь приходят специализированные протоколы, такие как WPA3 Easy Connect, который использует QR–коды или NFC для безопасной передачи ключей без ввода данных пользователем. Для авторизации в IoT–экосистемах эффективен Lightweight ABAC, где политики упрощены до базовых атрибутов (например, «разрешённые IP–адреса» или «временные окна активности»). В умных домах это может выглядеть так: умный замок получает доступ к облаку только при подключении через защищённый канал и только для отправки уведомлений, но не для изменения настроек. Для промышленного IoT, где задержки недопустимы, применяют преаутентификацию – устройство получает временный токен до запуска, сокращая время подключения.

Особняком стоят гибридные сети, объединяющие корпоративные, публичные и IoT-устройства, где сегментация становится эффективным решением. Например, больница может настроить три виртуальных сегмента (VLAN): первый предназначен для медицинского оборудования с использованием WPA3 и EAP–TLS для доступа исключительно к локальным серверам; второй создан для пациентов и гостей, где применяется OAuth 2.0 с перенаправлением на портал и изоляцией от внутренних ресурсов; третий используется для администрации, обеспечивая комбинацию EAP–PEAP и RBAC для доступа к системам управления медицинскими данными (EHR).

Ключевое правило – резервирование. Даже идеальные протоколы, такие как WPA3, требуют альтернативных методов (например, динамических PSK) для критически важных устройств, особенно если обновления невозможны.

Мониторинг и адаптация остаются основой безопасности. Аудит, анализ журналов и тесты на проникновение помогают своевременно устранить уязвимости. Например, частые попытки подбора EAP–PEAP – сигнал к переходу на EAP–TLS или усилению блокировок.

Заключение

Беспроводные сети перестали быть просто каналом передачи данных – они превратились в сложные экосистемы, где пересекаются интересы пользователей, устройств и бизнеса. Современные протоколы аутентификации и авторизации, такие как WPA3, EAP–TLS или ABAC, демонстрируют, что безопасность больше не может быть шаблонной. Каждый протокол решает конкретную задачу: WPA3 закрывает вековые уязвимости Wi–Fi, EAP обеспечивает гибкость для корпоративных сред, а OAuth 2.0 балансирует между удобством и рисками в публичных сетях. Однако их эффективность зависит не только от технического совершенства, но и от контекста, в котором они применяются.

Главный урок, который можно извлечь из эволюции этих стандартов, – безопасность требует постоянной адаптации. Угрозы, которые казались теоретическими пять лет назад (например, атаки на IoT через поддельные точки доступа), сегодня стали повседневной реальностью. При этом прогресс не всегда связан с созданием новых протоколов – иногда достаточно грамотной комбинации существующих решений. Успешные кейсы, будь то умный город или распределённая корпоративная сеть, объединяет одно: многоуровневая защита, где аутентификация, авторизация и шифрование работают как части единого механизма.

Однако даже самые совершенные технологии бессильны перед двумя вызовами: человеческим фактором и инерцией внедрения. Пользователи, использующие одинаковые пароли для рабочей и домашней сети, или компании, откладывающие переход на WPA3 из-за стоимости обновления, создают риски, которые не устранить на уровне протоколов. Это подчеркивает необходимость не только технологических, но и организационных изменений – от обучения сотрудников до пересмотра регуляторных требований.

Перспективы развития протоколов видятся в двух направлениях. Первое – упрощение без потери безопасности. Примеры вроде WPA3 Easy Connect или интеграции OAuth с биометрией показывают, что удобство и защита не всегда взаимоисключающи. Второе – адаптивность. Машинное обучение и анализ поведения уже начинают использоваться для динамического изменения политик доступа, и в будущем это может стать стандартом. Например, сеть, которая автоматически ужесточает аутентификацию при обнаружении подозрительной активности, или IoT–устройство, временно блокирующееся при отклонении от типичного сценария использования.

В конечном итоге, безопасность беспроводных сетей – это не конечная цель, а непрерывный процесс. Технологии будут меняться, угрозы – эволюционировать, но принцип останется неизменным: защита должна быть не сложнее, чем сама атака. Только тогда у злоумышленников не останется шансов.

MODERN AUTHENTICATION AND AUTHORIZATION PROTOCOLS IN WIRELESS NETWORKS

E.V. BEGLIAK, U.A. MARTSINKEVICH

Abstract. The article analyzes modern authentication and authorization protocols in wireless networks, focusing on their security, efficiency, and applicability in various scenarios. Key standards such as WPA3, EAP, OAuth 2.0, OpenID Connect, as well as access control methods (RBAC, ABAC, SAML), are examined. A comparative analysis of protocols is conducted based on their resilience to cyberattacks, performance, and ease of implementation. The study identifies critical challenges, including vulnerabilities in legacy systems and integration complexity in heterogeneous networks. Recommendations are provided for selecting protocols for corporate networks, public Wi–Fi, and IoT devices. The review highlights the need to adapt existing security protocols and develop new solutions to effectively counter modern cyber threats.

Keywords: authentication, authorization, wireless networks, WPA3, EAP, OAuth 2.0, cybersecurity, access control, RBAC, ABAC, SAML, IoT.

Список литературы

1. Global Threat Landscape Report. A Semiannual Report by FortiGuard Labs [Электронный ресурс]. – Режим доступа: https://www.fortinet.com/content/dam/fortinet/assets/threat-reports/threat-report-1h-2023.pdf. – Дата доступа: 22.03.2025.
2. Security. Wi-Fi Alliance. [Электронный ресурс]. – Режим доступа: https://www.wi-fi.org/discover-wi-fi/security. – Дата доступа: 25.03.2025.
3. Hu Vincent C., Ferraiolo D. // Guide to Attribute Based Access Control (ABAC). NIST. Computer security. 2014. P. 5-6.
4. Avast Q4/2023 Threat Report - Avast Threat Labs [Электронный ресурс]. – Режим доступа: https://decoded.avast.io/threatresearch/avast-q4-2023-threat-report/. – Дата доступа: 24.03.2025.
5. Chinese Standard GB/T; GBT; GB; YY/T; QC/T [Электронный ресурс]. – Режим доступа: https://www.chinesestandard.net/. – Дата доступа: 20.03.2025.
6. 8 Scary Statistics about the Password Reuse Problem [Электронный ресурс]. – Режим доступа: https://www.enzoic.com/blog/8-stats-on-password-reuse/. – Дата доступа: 20.03.2025.