УДК 621.396.946:004.056.523

МЕТОДИ АВТЕНТИФІКАЦІЇ У Wi-Fi МЕРЕЖАХ: СУЧАСНИЙ СТАН ТА ПЕРСПЕКТИВНІ ДОСЛІДЖЕННЯ

Сливар У. М.
e-mail: uliana.slyvar@nure.ua
Науковий керівник – к.т.н., доц. Ликов Ю.В.
Харківський національний університет радіоелектроніки, каф. КРіСТЗІ
м. Харків, Україна

This paper reviews Wi-Fi authentication methods, covering deployed standards (WPA3, EAP-TLS, 2FA) and experimental approaches such as post-quantum cryptography, blockchain authentication, and AI-based device fingerprinting. The study highlights the shift toward multi-layered wireless network security.

Бездротові мережі Wi-Fi є невід'ємною частиною сучасної цифрової інфраструктури – від домашніх мереж до корпоративних середовищ і критично важливих об'єктів. Попри постійне вдосконалення стандартів безпеки, зловмисники застосовують нові методи атак: брутфорс паролів WPA/WPA2, WPS Pixie Dust Attack, атаки типу KRACK, що експлуатують уразливості рукостискання, та Evil Twin – підроблені точки доступу. Методи захисту поділяються на дві категорії: впроваджені у серійне обладнання та експериментальні, що перебувають на стадії досліджень [1].

Впроваджені методи автентифікації. Стандарт WPA3, обов'язковий для Wi-Fi CERTIFIED™ пристроїв з липня 2020 р., замінив чотиристороннє рукостискання WPA2 на протокол SAE («Dragonfly»). Він потребує інтерактивного обміну під час кожної спроби автентифікації, що ускладнює перебір паролів і дозволяє блокувати серії невдалих спроб [4]. У корпоративному сегменті використовується WPA3-Enterprise з 802.1X і RADIUS-сервером; режим 192-bit Security Suite (AES-256-GCM, HMAC-SHA-384) рекомендований для установ з підвищеними вимогами безпеки. Protected Management Frames (PMF) є обов'язковими та захищають службові кадри від підробки.

Протокол EAP-TLS забезпечує взаємну автентифікацію на основі X.509-сертифікатів, що ефективно запобігає атакам Man-in-the-Middle та підробленим точкам доступу. Прив'язка сертифікатів до пристроїв забезпечує точний контроль доступу. Серед альтернатив: EAP-PEAP (TLS-тунель із парольною автентифікацією) та EAP-TTLS (автентифікація клієнта без власного сертифіката).

Двофакторна автентифікація (2FA) з одноразовими паролями (OTP) підвищує безпеку незалежно від стандарту WPA. Реалізація з використанням Google Authenticator і бібліотеки pyotp перевіряє TOTP-код (RFC 6238). Після підключення трафік блокується до підтвердження OTP, а IP-адреса додається до білого списку лише після успішної перевірки [2].

Експериментальні та перспективні методи. Одним із ключових напрямів є постквантова криптографія (PQC). Квантові комп'ютери теоретично здатні зламати RSA та алгоритми на еліптичних кривих. У 2024 р. NIST стандартизував FIPS 203 (CRYSTALS-Kyber), FIPS 204 (Dilithium) та FIPS 205 (SPHINCS+) [3]. Тривають дослідження інтеграції цих алгоритмів у TLS 1.3 для IoT-пристроїв; зокрема, Kyber-512 демонструє високу ефективність і придатність для ресурсообмежених систем.

Децентралізована автентифікація на основі блокчейну розглядається як альтернатива RADIUS-серверу – розподілений реєстр зі смартконтрактами (Ethereum тощо). Її перевагами є відмовостійкість і незмінність записів. Кастомні прошивки на базі OpenWrt дозволяють реалізовувати додаткові механізми безпеки: VLAN-сегментацію, IDS/IPS (Snort), шифрування DNS та власні схеми 2FA без зовнішніх сервісів.

Ще одним перспективним напрямом є ШІ-орієнтований device fingerprinting. Запропонований підхід ідентифікує IoT-пристрої за характеристиками радіосигналу та поведінковими ознаками з використанням моделей машинного навчання, досягаючи високої точності без застосування традиційних облікових даних [5]. У майбутньому це може забезпечити безперервну та прозору автентифікацію.

Аналіз показує три ключові тенденції: WPA3 та EAP-TLS забезпечують найвищий рівень захисту серед впроваджених рішень; 2FA з OTP суттєво знижує ризики навіть у разі компрометації пароля; постквантова криптографія та блокчейн-автентифікація наближаються до практичного застосування. Синергія криптографічно стійких стандартів, багатофакторної автентифікації та поведінкового моніторингу є оптимальною стратегією захисту сучасних бездротових мереж.

Список використаних джерел

1. Fortinet. What is a Brute Force Attack? URL: https://www.fortinet.com/resources/cyberglossary/brute-force-attack (дата звернення: 15.03.2026).

2. Google. Google Authenticator. URL: https://support.google.com/accounts/answer/1066447?hl=uk (дата звернення: 13.03.2026).

3. NIST. Post-Quantum Cryptography: Selected Algorithms 2024. URL: https://csrc.nist.gov/projects/post-quantum-cryptography/selected-algorithms (дата звернення: 15.03.2026).

4. Wi-Fi Alliance. Wi-Fi CERTIFIED WPA3 Security. URL: https://www.wi-fi.org/discover-wi-fi/security (дата звернення: 15.03.2026).

5. Zhang S. et al. Wi-Fi device identification based on multi-domain physical layer fingerprint. Computer Communications. 2023. URL: https://www.sciencedirect.com/science/article/abs/pii/S0140366423001032 (дата звернення: 15.03.2026).