DOI https://doi.org/10.32782/2220-8674-2025-15-1-29
УДК 004.738.5:004.056

Р. О. Яровий, канд. техн. наук ORCID: 0000-0001-8978-8137
А. В. Подвиженко, ст. викладач ORCID: 0000-0003-1826-7566
А. М. Переверзєв, ст. викладач ORCID: 0000-0003-0778-9203
С. В. Левченко, ст. викладач ORCID: 0009-0006-8497-0515
Приватний вищий навчальний заклад «Європейський університет»

ПУБЛІЧНІ WI-FI МЕРЕЖІ: ЗАХИСТ ОСОБИСТОЇ ІНФОРМАЦІЇ

Анотація. Сучасний світ характеризується невпинним зростанням мобільності та потребою в постійному доступі до інформації, що робить публічні Wi-Fi-мережі невід'ємною частиною повсякденного життя мільйонів людей. Кафе, аеропорти, готелі, громадський транспорт та міські площі пропонують зручний доступ до інтернету, сприяючи продуктивності, комунікації та розвагам. Однак ця цифрова зручність несе в собі значні ризики для безпеки особистої інформації. Публічні мережі, часто недостатньо захищені або взагалі відкриті, стають привабливим полем діяльності для кіберзлочинців. У статті детально проаналізовано основні загрози, з якими стикаються користувачі публічних Wi-Fi: перехоплення незашифрованих даних (сніфінг), атаки типу «людина посередині» (Man-in-the-Middle), створення фальшивих точок доступу (Evil Twin), розповсюдження шкідливого програмного забезпечення та фішинг. Розглядаються потенційні наслідки таких атак, включаючи крадіжку облікових даних (логінів, паролів), фінансової інформації (номерів банківських карток, даних онлайн-банкінгу), особистого листування, компрометацію корпоративних даних та репутаційні втрати. Наголошується на недостатній обізнаності багатьох користувачів щодо цих ризиків та їх схильності нехтувати базовими правилами безпеки заради зручності. У статті запропоновано комплексний огляд як традиційних, так і новітніх методів захисту персональних даних під час використання публічних Wi-Fi. До класичних рекомендацій відносяться: обов'язкове використання віртуальних приватних мереж (VPN) для шифрування всього трафіку; перевірка автентичності мережі перед підключенням; надання переваги вебсайтам, що використовують протокол HTTPS; вимкнення функції автоматичного підключення до Wi-Fi; своєчасне оновлення операційної системи та програмного забезпечення; використання надійного антивірусного ПЗ та фаєрволу; вимкнення загального доступу до файлів та принтерів. Особливу увагу приділено новітнім технологіям та підходам, що підвищують рівень безпеки: стандарт WPA3, який пропонує індивідуальне шифрування даних навіть у відкритих мережах (через OWE – Opportunistic Wireless Encryption) та покращений захист від атак підбору паролів; технології шифрування DNS-запитів (DNS over HTTPS – DoH, DNS over TLS – DoT), що унеможливлюють перехоплення інформації про відвідувані сайти; сучасні рішення Endpoint Security, що включають проактивний захист та аналіз поведінки; застосування принципів «нульової довіри» (Zero Trust), які вимагають постійної автентифікації та перевірки навіть у межах знайомих мереж. Підкреслено важливість комбінованого підходу, що поєднує технологічні засоби захисту і свідому поведінку користувача. Статтю призначено для широкого кола читачів: від пересічних користувачів, які прагнуть убезпечити свої дані, до фахівців із кібербезпеки та адміністраторів мереж, відповідальних за налаштування і підтримку публічних точок доступу.

*Ключові слова***:** публічний Wi-Fi, кібербезпека, захист персональних даних, VPN, HTTPS, WPA3, DNS over HTTPS, DoH, DNS over TLS, DoT, Man-in-the-Middle, Evil Twin, сніфінг, інформаційна безпека, цифрова гігієна.

Постановка проблеми. В епоху тотальної цифровізації та мобільності доступ до інтернету став базовою потребою для роботи, навчання, спілкування та доступу до послуг. Публічні Wi-Fi-мережі, що розгорнуті в численних громадських місцях, надають зручну можливість

залишатися онлайн поза домом чи офісом. Ця зручність, однак, має зворотний бік – значні ризики для безпеки даних [1]. На відміну від приватних домашніх або корпоративних мереж, публічні точки доступу часто мають мінімальний рівень захисту, а іноді є повністю відкритими, що робить їх легкою мішенню для зловмисників [2]. Зростання кіберзагроз, зокрема тих, що спрямовані на пересічних користувачів, ставить питання захисту особистої інформації під час використання публічних мереж на одне з перших місць у сфері інформаційної безпеки. Крадіжка облікових даних, фінансової інформації, шпигунство, розповсюдження шкідливого ПЗ – це лише деякі з потенційних наслідків необережного використання незахищених Wi-Fi-з'єднань [2; 3]. Актуальність проблеми посилюється недостатньою обізнаністю значної частини користувачів про реальні загрози та методи протидії їм [4]. Багато хто нехтує елементарними правилами безпеки, підключаючись до будь-якої доступної мережі без належної перевірки та захисту. Таким чином, існує нагальна потреба в систематизації знань про ризики публічних Wi-Fi та ефективні методи захисту, включаючи новітні технологічні рішення, що дозволить підвищити рівень кіберграмотності та безпеки користувачів.

Аналіз останніх досліджень. Проблема безпеки публічних Wi-Fi-мереж активно досліджується науковою спільнотою та фахівцями з кібербезпеки [1; 2]. Дослідження зосереджені на кількох ключових напрямах. Проводиться детальний аналіз векторів атак, характерних для публічних Wi-Fi, як-от Man-in-the-Middle (MitM), створення «злих двійників» (Evil Twin) [5], сесійний хайджекінг (Session Hijacking) та пакетний сніфінг [1], при цьому аналізується ефективність цих атак залежно від конфігурації мережі та поведінки користувача. Значна увага також приділяється оцінюванню ефективності різних засобів захисту, зокрема дослідженню надійності VPN-сервісів, їх впливу на швидкість з'єднання та здатності протистояти різним типам перехоплення даних [6], а також аналізу ролі й обмежень HTTPS у захисті вебтрафіку.

Крім того, дослідження супроводжують розроблення та впровадження нових стандартів бездротової безпеки, наприклад WPA3 [7]. Аналізуються його переваги над попередніми версіями, включаючи покращене шифрування (SAE – Simultaneous Authentication of Equals), захист від офлайн-атак підбору пароля та підвищену безпеку відкритих мереж за допомогою Opportunistic Wireless Encryption (OWE) [8], а також досліджуються його потенційні вразливості [9]. Розробляються також методи та інструменти для автоматичного виявлення фальшивих точок доступу (Evil Twins) та інших аномалій у бездротовому середовищі, що використовують аналіз сигнатур мережі, геолокаційні дані та поведінкові патерни [5], поряд із дослідженням методів аналізу мережевого трафіку для виявлення аномалій [10].

Важливим аспектом є вивчення поведінки користувачів та соціальної інженерії, зокрема рівня обізнаності користувачів про ризики, їхньої поведінки під час підключення до публічних мереж і вразливості до методів соціальної інженерії, як-от фішингові сторінки авторизації [4]. Нарешті, аналізується проблема приватності DNS, зокрема витік інформації через незашифровані DNS-запити, розроблення стандартів для їх шифрування (DoH [11], DoT [12]) та дослідження стану їх впровадження [13].

Аналіз публікацій свідчить про постійний розвиток як методів атак [2], так і засобів захисту. Однак залишається актуальною проблема розриву між технологічними можливостями захисту та рівнем їх застосування та обізнаності серед кінцевих користувачів [4].

Формулювання мети статті. Метою статті є комплексний аналіз проблеми забезпечення безпеки особистої інформації під час використання публічних Wi-Fi-мереж і надання практичних рекомендацій для користувачів.

У статті поставлено завдання детально описати основні типи загроз та вразливостей, характерних для публічних Wi-Fi-мереж, а також проаналізувати потенційні наслідки компрометації даних через незахищені з'єднання [2]. Крім того, в роботі систематизовано та пояснено

ефективні методи захисту, починаючи від базових правил цифрової гігієни до використання сучасних технологій [6]. Особливу увагу приділено новітнім методам захисту, як-от стандарт WPA3, технології шифрування DNS (DoH/DoT), сучасні рішення Endpoint Security та принципи «нульової довіри» [14]. Загалом, статтю спрямовано на підвищення рівня обізнаності користувачів щодо ризиків та способів їх мінімізації, сприяючи формуванню відповідального ставлення до власної кібербезпеки в публічному бездротовому просторі [4].

Основна частина. Публічні Wi-Fi-мережі за своєю природою є менш безпечними, ніж приватні. Основні ризики включають:

1. Незашифровані мережі: багато публічних мереж не використовують шифрування. Це означає, що дані передаються у відкритому вигляді й можуть бути легко перехоплені зловмисником у тій же мережі (сніфінг) [1];

2. Атаки «людина посередині» (Man-in-the-Middle, MitM): зловмисник розміщує себе між користувачем і точкою доступу, перехоплюючи або змінюючи трафік. Такі атаки є поширеною загрозою в публічних мережах [2];

3. Фальшиві точки доступу (Evil Twin): зловмисник створює Wi-Fi-мережу з ім'ям, схожим до легітимної, щоб обманом змусити користувачів підключитися та перехопити їхні дані [5];

4. Пакетний сніфінг (Packet Sniffing): навіть у зашифрованих мережах зі старими протоколами існують вразливості, що дозволяють перехоплювати пакети. У відкритих мережах це зробити ще простіше [1];

5. Розповсюдження шкідливого програмного забезпечення (ПЗ): зловмисники можуть використовувати скомпрометовані мережі для розповсюдження вірусів, троянів та іншого шкідливого ПЗ [3], наприклад, через фальшиві оновлення або перенаправлення на шкідливі сайти [2];

6. Сесійний хайджекінг (Session Hijacking): Перехоплення сесійних файлів cookie в незахищеній мережі може дозволити зловмиснику отримати доступ до облікових записів користувача без пароля.

Стандартні методи захисту

Щоб зменшити потенційні загрози під час підключення до загальнодоступних мереж Wi-Fi, варто вжити певних запобіжних заходів. Насамперед рекомендовано використовувати VPN (віртуальну приватну мережу). VPN створює захищений, зашифрований канал для вашого інтернет-трафіку, що унеможливлює його перехоплення в межах локальної мережі; ефективність цього методу для запобігання витокам даних підтверджена дослідженнями [6].

Не менш важливо переконуватися в автентичності мережі, до якої ви підключаєтесь. Завжди уточнюйте офіційну назву (SSID) мережі в закладі та остерігайтеся підключень до мереж із підозрілими назвами, які можуть маскуватися під легітимні точки доступу [5]. Під час перегляду вебсторінок віддавайте перевагу сайтам, що використовують протокол HTTPS, оскільки він забезпечує шифрування даних між вашим браузером та сервером сайту.

Також доцільно відключити функцію автоматичного підключення до Wi-Fi-мереж на вашому пристрої, щоб уникнути ненавмисного з'єднання з невідомими або небезпечними мережами. Регулярне оновлення операційної системи та всіх установлених програм є критично важливим, адже оновлення часто містять виправлення вразливостей, якими можуть скористатися зловмисники [2].

Для базового рівня захисту переконайтеся, що на вашому пристрої активований фаєрвол і встановлено надійне антивірусне програмне забезпечення. Крім того, перебуваючи в публічній мережі, обов'язково вимикайте функцію спільного доступу до файлів та принтерів у налаштуваннях мережі вашого пристрою. Нарешті, намагайтеся обмежувати дії, пов'язані з передачею чутливої інформації (наприклад, онлайн-банкінг, здійснення покупок), коли ви підключені до публічного Wi-Fi, якщо є така можливість.

Найновіші методи захисту інформації в публічних мережах

Крім стандартних рекомендацій щодо захисту інформації в публічних мережах, активно розвиваються та впроваджуються нові технології та підходи. Серед них виділяється стандарт безпеки WPA3, який у версії WPA3-Personal використовує протокол SAE, що підвищує стійкість до офлайн-атак підбору пароля, попри виявлені на ранніх етапах вразливості. Для корпоративних потреб існує WPA3-Enterprise з вищим рівнем безпеки, а технологія Opportunistic Wireless Encryption (OWE) забезпечує індивідуальне шифрування даних навіть у відкритих мережах, захищаючи від пасивного прослуховування [8].

Також набирають популярності протоколи DNS over HTTPS (DoH) та DNS over TLS (DoT), які шифрують DNS-запити, унеможливлюючи їх перехоплення зловмисниками. Важливу роль відіграють і сучасні рішення Endpoint Security, що включають проактивний захист, системи виявлення та реагування на загрози на кінцевих точках (EDR), а також захист від фішингу, що є критичним в умовах кіберзагроз, що постійно зростають [13].

Окрім технологічних рішень, поширюється концепція «Нульової Довіри» (Zero Trust), яка базується на принципі «ніколи не довіряй, завжди перевіряй». Цей підхід вимагає постійної автентифікації та ретельної перевірки прав доступу для будь-яких користувачів чи пристроїв, навіть якщо вони перебувають у знайомій мережі [14].

Варто також зазначити, що використання мобільного інтернету через точку доступу (хотспот) часто є безпечнішою альтернативою публічному Wi-Fi, оскільки мережі 4G/5G зазвичай використовують сильніші механізми шифрування та автентифікації.

Висновки. Публічні Wi-Fi мережі залишаються середовищем із підвищеними ризиками для безпеки даних [1; 2]. Перехоплення трафіку, атаки MitM та Evil Twin [5] є реальними загрозами.

Проведене дослідження підтверджує, що використання таких базових засобів захисту, як VPN [6], та дотримання правил цифрової гігієни значно знижує ризики. Нові технології, як-от WPA3 з OWE та шифрування DNS (DoH/DoT), пропонують суттєві покращення на технічному рівні.

Однак технології не є панацеєю. Людський фактор, зокрема недостатня обізнаність і необережна поведінка користувачів [4], залишається слабкою ланкою.

Перспективи подальших досліджень включають:

– аналіз практичного впровадження та ефективності WPA3/OWE та виявлення нових потенційних вразливостей;

– дослідження ефективності методів виявлення атак типу «Evil Twin» та MitM в умовах шифрованих протоколів;

– розроблення інтелектуальних систем оцінювання ризиків публічних мереж та аналізу аномалій трафіку;

– подальше вивчення поведінкових аспектів кібербезпеки користувачів та розроблення ефективних освітніх програм;

– адаптація та застосування принципів «нульової довіри» [14] для захисту персональних пристроїв.

Організація безпечного інтернету в публічних Wi-Fi-мережах вимагає комплексного підходу та спільних зусиль провайдерів, розробників і користувачів. Поєднання технологічних інновацій та підвищення цифрової грамотності є ключем до безпечного використання зручностей бездротового доступу.

Список використаних джерел

1. Cimpanu C. Most public WiFi networks are insecure, study finds. ZDNet. 2019. URL: https://www.zdnet.com/article/most-public-wifi-networks-are-insecure-study-finds/ (дата звернення: 15.04.2025).

2. European Union Agency for Cybersecurity (ENISA). ENISA Threat Landscape. 2023. URL: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2023 (дата звернення: 15.04.2025).

3. Shabtai A., Elovici Y., Shomron G. Android Malicious Code and Malware // *Information Security and Privacy Research. PRIME* 2012. Lecture Notes in Computer Science, vol. 7398. Springer, Berlin, Heidelberg. 2012. DOI: https://doi.org/10.1007/978-3-642-31513-8_1

4. Khan M. A., Siddiqui M. S., Ferens K. A Cognitive Study on Public Wi-Fi Security Risks and Users' Behavior // 2018 IEEE International Conference on Cognitive Computing (ICCC). 2018. pp. 57–60. DOI: https://doi.org/10.1109/ICCC.2018.00016

5. Apolonio K. F., Hernandez A. A. Detection and Prevention of Evil Twin Attack in a Public Wi-Fi Hotspot // 2017 International Conference on Information and Communications Technology (ICOIACT). 2017. pp. 1–6. DOI: https://doi.org/10.1109/ICOIACT.2017.8279046

6. Singh J., Pasquale J. Understanding the effectiveness of VPNs in mitigating web PII leakages // Proceedings of the 2015 ACM SIGCOMM Conference on Special Interest Group on Data Communication (SIGCOMM '15). 2015. pp. 591–592. DOI: https://doi.org/10.1145/2785956.2790023

7. Wi-Fi Alliance. Wi-Fi CERTIFIED WPA3™. 2024. URL: https://www.wi-fi.org/discover-wi-fi/security (дата звернення: 15.04.2025).

8. Новітні протоколи бездротових мереж: переваги та недоліки / С. Левченко та ін. *Herald of Khmelnytskyi National University. Technical Sciences.* 2024. № 335(3(1)). С. 445–449. DOI: https://doi.org/10.31891/2307-5732-2024-335-3-61

9. Vanhoef M., Piessens F. Dragonblood: Analyzing the Dragonfly Handshake of WPA3 and EAP-pwd // Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security (CCS '19). 2019. pp. 1993–2007. DOI: https://doi.org/10.1145/3319535.3354217

10. Поночовний П., Пепа Ю. Реалізація системи захисту серверів з урахуванням аномалій в пакетах. *Вимірювальна та обчислювальна техніка в технологічних процесах.* 2025. № 1(81). С. 44–51. DOI: https://doi.org/10.31891/2219-9365-2025-81-6

11. Hoffman P., McManus P. RFC 8484: DNS Queries over HTTPS (DoH) Internet Engineering Task Force (IETF), 2018. URL: https://www.rfc-editor.org/info/rfc8484 (дата звернення: 15.04.2025).

12. Hu Z., Ma Z., Wang H., Zhang G. RFC 7858: Specification for DNS over Transport Layer Security (TLS). Internet Engineering Task Force (IETF), 2016. URL: https://www.rfc-editor.org/info/rfc7858 (дата звернення: 15.04.2025).

13. Hounsel A., Orme E., Johnson C. Measuring the deployment of DNSSEC, DANE, and DoT // Proceedings of the 22nd ACM Internet Measurement Conference (IMC '22). 2022. pp. 436–449. DOI: https://doi.org/10.1145/3517745.3561442

14. Rose S., Borchert O., Mitchell S., Connelly S. NIST Special Publication 800-207: Zero Trust Architecture. National Institute of Standards and Technology. 2020. URL: https://csrc.nist.gov/publications/detail/sp/800-207/final (дата звернення: 15.04.2025).

R. Yaroviy A. Podvyzhenko, A. Pereverziev, S. Levchenko
Higher Educational Institution "European University"

PUBLIC WI-FI NETWORKS: PROTECTING PERSONAL INFORMATION IN THE AGE OF DIGITAL CONVENIENCE

Summary

The modern world is characterized by relentless growth in mobility and the need for constant access to information, making public Wi-Fi networks an integral part of the daily lives of millions. Cafes, airports, hotels, public transport, and city squares offer convenient internet access, fostering productivity, communication, and entertainment. However, this digital convenience carries significant risks to personal information security. Public networks, often inadequately secured or entirely open, become an attractive field for cybercriminals. This article provides a detailed analysis of the main threats faced by users of public Wi-Fi: interception of unencrypted data (sniffing), Man-in-the-Middle (MitM) attacks, the creation of fake access points ("Evil Twin"), malware

distribution, and phishing. It examines the potential consequences of such attacks, including the theft of credentials (logins, passwords), financial information (bank card numbers, online banking data), personal correspondence, compromise of corporate data, and reputational damage. Emphasis is placed on the lack of awareness among many users regarding these risks and their tendency to neglect basic security rules for the sake of convenience. The article offers a comprehensive overview of both traditional and the latest methods for protecting personal data when using public Wi-Fi. Classic recommendations include: mandatory use of Virtual Private Networks (VPNs) to encrypt all traffic; verifying network authenticity before connecting; preferring websites that use the HTTPS protocol; disabling the automatic Wi-Fi connection feature; timely updating of operating systems and software; using reliable antivirus software and firewalls; disabling file and printer sharing. Special attention is paid to the latest technologies and approaches that enhance security levels: the WPA3 standard, which offers individualized data encryption even on open networks (via OWE – Opportunistic Wireless Encryption) and improved protection against password guessing attacks; DNS query encryption technologies (DNS over HTTPS – DoH, DNS over TLS – DoT), which prevent the interception of information about visited sites; modern Endpoint Security solutions that include proactive protection and behavioral analysis; application of Zero Trust principles, requiring constant authentication and verification even within familiar networks. The importance of a combined approach, integrating technological protection means and conscious user behavior, is underscored. The article is intended for a wide audience: from ordinary users seeking to secure their data to cybersecurity specialists and network administrators responsible for configuring and maintaining public access points.

Keywords: public Wi-Fi, cybersecurity, personal data protection, VPN, HTTPS, WPA3, DNS over HTTPS, DoH, DNS over TLS, DoT, Man-in-the-Middle, Evil Twin, sniffing, information security, digital hygiene.