ІНФОКОМУНІКАЦІЙНІ ТЕХНОЛОГІЇ

УДК 004.056 (083.94)
DOI https://doi.org/10.36994/2788-5518-2023-02-06-01

ОЦІНКА ЗАХИЩЕНОСТІ БЕЗДРОТОВИХ МЕРЕЖ У МІСЬКОМУ СЕРЕДОВИЩІ З УРАХУВАННЯМ ВИКОРИСТАННЯ ПРОТОКОЛІВ БЕЗПЕКИ

Гальчинський Л. Ю., *канд. техн. наук, доцент, Національний технічний університет України «Київський політехнічний інститут імені Ігора Сікорського», Київ, Україна*
https://orcid.org/0000-0002-3805-1474, hleonid@gmail.com

Корольова В. Р., *Національний технічний університет України «Київський політехнічний інститут імені Ігора Сікорського», Київ, Україна*
korolova.workspace@gmail.com

Анотація. *У цій роботі представлені результати дослідження оцінювання рівня захищеності бездротових мереж у міському середовищі на прикладі міста Києва. Здійснено аналіз чинників, що впливають на рівень безпеки, зокрема шифрування, автентифікації та цілісності, які впливають на рівень механізму захисту трафіку бездротових мереж, зокрема типів протоколів WEP, WPA, WPA2 та WPA3, залежно від моделей атак. Показані вразливості протоколів у контексті різновидів конфігурацій протоколів. Визначена перевага з точки зору безпеки одного типу протоколу стосовно іншого. На основі даних публічних БД визначено актуальну кількість бездротових мереж і відповідні частки протоколів безпеки у світовому масштабі. Було проведено автоматизоване дослідження безпеки бездротової мережі на основі методології Wardriving у міському середовищі Києва, за допомогою якої в пасивному режимі були отримані дані типів протоколів безпеки. Результати сканування показали відсутність використання як застарілого протоколу WEP, так і новітнього протоколу WPA3. За результатами обробки даних сканування були визначені частки різних типів протоколів безпеки. Причому методика сканування дала змогу отримати не тільки ширший спектр типів протоколів безпеки, ніж класичні значення WEP, WPA, WPA2 чи WPA3, а й варіанти використання стандартів, які забезпечують шифрування, автентифікацію та цілісність. На основі двоетапної процедури було побудовано інтервальну шкалу оцінювання рівня безпеки кожного з типів протоколів. На першому етапі протоколи були згруповані за певними рівнями захисту, а потім проранжовані в межах відведеного інтервалу за перевагами використаних стандартів, завдяки чому було отримано порядкову шкалу оцінки рівня безпеки типу протоколу. Далі експертно були визначені оцінки кожного типу протоколу, що дає змогу здійснювати перехід до інтервальної шкали оцінювання. На основі цієї шкали та визначених часток типів протоколу за цією вибіркою сканувань отримано оцінку рівня захищеності мереж у міському середовищі Києва.*

Ключові слова: *бездротові мережі; рівень безпеки; протоколи безпеки; типи протоколів безпеки; сканування мережі Wardriving; методика оцінювання.*

ASSESSMENT OF THE SECURITY OF WIRELESS NETWORKS IN AN URBAN ENVIRONMENT, TAKING INTO ACCOUNT THE USE OF SECURITY PROTOCOLS

Leonid Galchynsky, *Ph. D Assoc. National Technical University of Ukraine "Ihor Sikorsky Kyiv Polytechnic Institute", Kyiv, Ukraine*
https://orcid.org/0000-0002-3805-1474, hleonid@gmail.com

Valeriia Korolova, *National Technical University of Ukraine "Ihor Sikorsky Kyiv Polytechnic Institute", Kyiv, Ukraine*
korolova.workspace@gmail.com

Abstract. *This paper presents the results of a study of assessing the level of security of wireless networks in an urban environment on the example of Kyiv. An analysis of factors affecting the level of security, in particular encryption, authentication and integrity, which affect the level of the mechanism for protecting wireless network traffic, in particular the types of protocols WER, WPA, WPA2 and WPA3, depending on the attack models, is carried out. Protocol vulnerabilities are shown in the context of different protocol configurations. The security advantage of one type of protocol over another is determined. Based*

on the data from public databases, the current number of wireless networks and the corresponding shares of security protocols on a global scale are determined. An automated study of wireless network security based on the Wardriving methodology in the urban environment of Kyiv was conducted, which was used to obtain data on the types of security protocols in a passive mode. The scan results showed the absence of the use of both the outdated WEP protocol and the newest WPA3 protocol. As a result of scan data processing, the shares of different types of security protocols were determined. Moreover, the scanning methodology allowed us to obtain a wider range of security protocol types than the classic values of WEP, WPA, WPA2 or WPA3, and options for using standards that provide encryption, authentication and integrity. Based on a two-stage procedure, an interval scale for assessing the security level of each type of protocol was built. At the first stage, the protocols were grouped by certain levels of protection, and then ranked within the allocated interval according to the advantages of the standards used, which allowed us to obtain an ordinal scale for assessing the security level of a protocol type. Next, the expert assessment of each type of protocol was determined, which allows for the transition to an interval assessment scale. Based on this scale and the determined shares of protocol types in this sample of scans, an assessment of the level of security of networks in the urban environment of Kyiv was obtained.

Key words: *wireless networks; security level; security protocols; types of security protocols; Wardriving network scan; assessment methodology.*

Вступ

Бездротова мережа, яка зараз відома широкому загалу як Wi-Fi, – це скорочення від Wireless Fidelity. Стандарт, що дає змогу отримати доступ до мережі без використання будь-яких кабелів, тобто можливість передавати дані за допомогою невидимих радіохвиль. Він ґрунтується на стандарті IEEE 802.11, впровадженому в 1991 році, хоча практичну реалізацію цієї технології було здійснено лише в 1997 році. Впровадження стандартів IEEE 802.11 WLAN у 1997 році сприяло зростанню популярності WLAN, який став повсюдним рішенням щодо підключення для багатьох користувачів по всьому світу [1]. На рис. 1а та рис. 1б показані ключові елементи WLAN:

Рис. 1а. Інтерфейс бездротових мереж

Рис. 1б. Бездротова точка доступу

Започаткування ери бездротових мереж ініціювало перехід до нового формату використання мережі, що полягало в значних перевагах завдяки низькій затримці та високій швидкості під час передачі даних, зручному налаштуванню, мобільності, масштабованості, відсутності кабелів і можливому підключення з різних регіонів світу, що призвело до фантастичного зростання мереж Wi-Fi.

Розвиток мереж Wi-Fi забезпечують дві організації: IEEE та Wi-Fi Alliance®. IEEE розробляє стандарти, які описують процедури, обмеження, значення й алгоритми для встановлення з'єднання WLAN. Wi-Fi – це торговельна марка, що належить Wi-Fi Alliance, яка за допомогою ретельних тестів підтверджує взаємодію між усіма пристроями із цим знаком і надає сертифікати розробникам і виробникам обладнання.

Відповідно до дослідження, проведеного Wi-Fi Alliance®, глобальна економічна вартість Wi-Fi у 2023 році оцінюється в понад 3,5 трильйона доларів США. Очікується, що до 2025 року ця вартість зросте майже до 5 трильйонів доларів [2]. Дані в мережах Wi-Fi передаються за аналогічним протоколом TCP/IP, як і у разі передачі по кабелю. Проте середовище, яким передаються пакети в мережевій комунікації, суттєво відрізняється. Бездротові мережі для зв'язку між пристроями в домашніх і корпоративних мережах використовують радіодіапазони 2,4 та 5 ГГц. Рішення цього типу вважаються набагато менш безпечними, ніж стандартні кабельні або оптичні мережі. Неавторизовані користувачі можуть розмістити станції для несанкціонованого прихованого прослуховування. Таке середовище породжує ряд критичних вразливостей, які призводять до суттєво негативних наслідків. На перших етапах розвитку бездротових мереж питання про безпеку даних не було актуальним, бо цільова аудиторія була занадто вузькою, а вартість послуг – занадто високою, тому шифрування даних та автентифікація сутностей, які здійснювали підключення до мереж, практично не передбачались. Хоча деякі механізми безпеки Wi-Fi, створені для захисту бездротової локальної мережі, передбачалися стандартом IEEE 802.11. Зокрема, це ідентифікатор набору послуг (SSID), який використовується для контролю доступу до точки доступу (AP), список контролю доступу (ACL) для запобігання неавторизованому доступу, а також алгоритм протоколу Wired Equivalent Privacy (WEP). Проте WEP був визначений стандартом як необов'язковий, тому ні точки доступу, ні бездротові пристрої не зобов'язані його використовувати [3].

У такому стані система Wi-Fi не забезпечувала захист конфіденційності, цілісності та надійності даних, що передавались мережею. Зловмисники могли збирати, аналізувати, модифіковувати вміст перехоплених пакетів, у яких могли міститися критичні дані користувачів. З поширенням попиту й удосконаленням інфраструктури бездротових мереж постали питання про захист даних.

Реальне використання WEP почалося тільки через два роки, після впровадження стандарту IEEE 802.11 [4]. Як наслідок цих викликів, організацією Wi-Fi Alliance у 1999 році був доопрацьований до практичного використання перший протокол безпеки WEP (Wired Equivalent Privacy). Цей протокол мав 64/128-бітне шифрування з використанням алгоритму RC4. Проте із часом виявилися слабкі сторони WEP, а саме вразливість у побудові протоколу безпеки стосовно статичних ключів шифрування, вектора ініціалізації, що призвело до реалізації численних кібератак. Для вирішення проблеми безпечного використання мереж 2003 року було представлено нове покоління протоколів – WPA, яке ґрунтувалось на подальшій підтримці у використанні алгоритму RC4, зі 128-бітним шифруванням і новим протоколом цілісності тимчасового ключа в протоколі захищеного доступу TKIP. WPA вважався програмною обгорткою WEP, яка вирішувала проблеми та вразливості, виявлені в попередньому протоколі безпеки. Згодом з'ясувалося, що протокол WPA теж ненадійний через існування автентифікації PSK, технології WPS, тому 2004 року з'явилась оновлена версія протоколів безпеки – WPA2, з наявним алгоритмом AES і режимом лічильника CCMP (Cipher Block Chaining Message Authentication Protocol). WPA2 став гарантом безпеки бездротових мереж, пропагував надійність і постійну підтримку через оновлення, які регулярно впроваджувалися для покращення захисту. Протокол WPA2 вирішував недоліки попередніх протоколів, інтегрував функції захисту та досяг покращення режимів безпеки Personal та Enterprise. У 2006 році організація Wi-Fi Alliance оголосила, що технологія безпеки шифрування WPA2 має бути обов'язковою функцією для всіх нових Wi-Fi CERTIFIED-продуктів, оскільки відсутність цієї сертифікації сповільнюватиме пристрої, мінімізуватиме широкий спектр додаткового функціонала та технічної підтримки.

На поточний момент протокол WPA2 продовжує залишатися популярним у середовищі користувачів, незважаючи на вразливості автентифікації 4-way handshaking, що призвели до імплементації однієї з основних атак – KRACK (2017 рік), за допомогою якої зловмисники можуть перехоплювати мережеві пакети, зчитувати й модифіковувати дані. Розробники випускали патчі, щоб боротись з такими атаками, проте остаточно цю проблему не вирішили.

Із метою подолання вразливості KRACK та ряду інших вразливостей у 2018 році Wi-Fi Alliance було прийнято рішення про впровадження наступного покоління протоколів безпеки – WPA3. У цьому протоколі використовується 128/192-бітне шифрування, протокол автентифікації SAE, вдосконалені режими WPA3-Personal, WPA3-Enterprise. Створено нові технології підключення до бездротових мереж, як-от Enhanced Open та Easy Connect.

Незважаючи на очевидні переваги, з 2018 року і дотепер реалізації WPA3 не довелося стати повноцінним стандартом сертифікованого апаратного забезпечення. Причиною цього стали як приховані нові вразливості цього протоколу, так і складнощі його впровадження в реальних мережах Wi-Fi, у яких використовуються різнотипні протоколи захисту даних. Отже, сучасні мережі Wi-Fi функціонують у стані використання різнотипних протоколів безпеки. Найбільш масштабні Wi-Fi мережі сконцентровані в міських агломераціях. Тож виникають питання про рівень захищеності таких мереж як загалом, так і для окремо взятого користувача.

Виконання досліджень

Спочатку проаналізуємо характеристики протоколів безпеки, які використовують користувачі бездротових мереж.

Механізм Wired Equivalent Privacy (WEP). Назва протоколу Wireless Equivalent Privacy – WEP вказує на наміри розробників [5] зробити безпеку бездротових мереж, еквівалентну рівню безпеки, яку забезпечують дротові локальні мережі. Незабаром практика показала, що рівень безпеки, який пропонує WEP, не став цільовим, хоча це також був значний еволюційний крок порівняно з відкритим доступом. Проте, незважаючи на виявлені пізніше недоліки протоколу, WEP забезпечує певний рівень безпеки, наприклад може стримувати випадкове стеження. Деякі користувачі вважають цей рівень безпеки достатнім, навіть протягом чверть століття після появи цього протоколу.

Коли WEP активний, кожен пакет 802.11 шифрується окремо, як потік шифру RC4, згенерований 64-бітним ключем RC4. RC4 – це симетричне кодування, яке складається з двох частин: алгоритму планування ключів (KSA), який отримує початкову перестановку з ключа випадкового розміру (типовий розмір становить 40–256 біт) і алгоритму псевдовипадкової генерації (PRGA), який використовує початкову перестановку для генерації псевдовипадкової вихідної послідовності (ключ RC4). Цей ключ складається з 24-бітного вектора ініціалізації (IV) і 40-бітного ключа WEP. Зашифрований пакет генерується за допомогою побітового виключного АБО (XOR) вихідного пакета та потоку RC4. IV вибирається відправником і може періодично змінюватися, щоб кожен пакет не шифрувався повторним потоком шифру. Вектор ініціалізації надсилається у відкритому вигляді з кожним пакетом. Додаткове 4-байтове значення перевірки цілісності (ICV) обчислюється на вихідному пакеті та додається. ICV також шифрується за допомогою потоку шифрів RC4.

Проте цього виявилося недостатньо. Однією з найслабших частин WEP є 24-бітний вектор ініціалізації, який може призвести до повторного використання потоку ключів. Повторне використання потоку ключів, зі свого боку, забезпечує успішні атаки криптоаналізу на зашифрований текст. Отже, WEP було визнано нездатним у досягненні цілей безпеки та таким, який містить серйозні недоліки безпеки [6]. Іншою вразливістю було використання алгоритму CRC-32 для перевірки цілісності. CRC не є криптографічно надійним і поступається для використання більш надійним засобам, таким як хеш-функції. Слабкість також була виявлена в механізмі планування ключів RC4. Шляхом ідентифікації великої кількості слабких ключів, а також через те, що перший байт, згенерований RC4, містить інформацію про окремі ключові байти, можна проаналізувати достатню кількість пакетів, зашифрованих WEP, тобто відновити секретний ключ у WEP [7]. Крім того, були виявлені ще деякі слабкості, зокрема використання одного ключа WEP, який спільно використовується для кожного вузла в мережі. Оскільки зміна ключів є виснажливим процесом, системні адміністратори рідко змінюють їх.

За декілька років як користувачам, так і експертам стало зрозуміло, що WEP – далеко не ідеальне рішення безпеки. Проте його використовували і продовжують надалі використовувати. Частина користувачів Wi-Fi не надто переймається проблемами захисту, хоч і вважає, що краще мати якийсь механізм безпеки стримування, ніж не мати жодного. Так, зловмисник може зламати ключі WEP за наявності часу та достатньо слабких ключів, але це не є приводом уникати можливого захисту.

Однак значна частина користувачів була надто стурбована, і це спонукало шукати більш надійне рішення. Зважаючи на вразливі місця та недоліки WEP, Wi-Fi Alliance створив стандарт Wi-Fi Protected Access (WPA), який є підмножиною 802.11i (2003).

Протокол WPA був задуманий не як принципово інше рішення, а як покращення недоліків функції безпеки WEP. Так, ідея мала сенс, бо покращена технологія була придатна для роботи з існуючими продуктами Wi-Fi, у яких увімкнено WEP. Технологія WPA переважно має три вдосконалення порівняно з WEP:

- посилення шифрування даних через використання протоколу цілісності тимчасового ключа (TKIP) за допомогою алгоритму хешування та додавання функції перевірки цілісності. TKIP – це функція хешування тимчасового ключа, яка є альтернативою WEP і не потребує нового обладнання. Як і WEP, TKIP використовує потоковий шифр RC4, як для шифрування, так і для дешифрування, і всі залучені сторони мають використовувати один секретний ключ;
- автентифікація користувача, яка відсутня у WEP, через розширений протокол автентифікації (EAP). Для WEP доступ до бездротової мережі був на основі спеціальної апаратної MAC-адреси комп'ютера, яку порівняно легко виявити та викрасти. EAP побудовано на більш безпечній системі шифрування з відкритим ключем, щоб забезпечити доступ до мережі лише авторизованим користувачам мережі [8];
- новий спосіб цілісності повідомлення (MIC) для TKIP. Для усунення слабкості алгоритм планування ключа було запропоновано замінити на хеш-алгоритм альтернативного тимчасового ключа (ATKH), який був названий Michael [9].

Протокол WPA2. Покращення безпеки Wi-Fi здавалось очевидним, однак через короткий час, у 2004 році було випущено протокол WPA2, який справді підвищив рівень захищеності мереж Wi-Fi. З 2006 року WPA офіційно замінено на WPA2. Однією з найбільш значних змін між WPA та WPA2 є обов'язкове використання алгоритмів AES і введення CCMP (Counter Cipher Mode with Block Chaining Message Authentication Code Protocol) як заміна TKIP. Проте TKIP досі зберігся в WPA2 як резервна система, а також для взаємодії з WPA. Ця оновлена версія WPA ґрунтується на механізмі мережі високої безпеки (RSN) і працює у двох режимах:

- персональний режим, або спільний ключ Pre-Shared Key (WPA2-PSK), використовує спільний пароль доступу та зазвичай застосовується в домашніх мережах;
- корпоративний режим (WPA2-EAP) орієнтується на мережі організацій і комерційне використання.

В обох режимах використовується протокол CCMP, що ґрунтується на алгоритмі розширеного стандарту шифрування (AES), який забезпечує автентифікацію та цілісність повідомлення. Протокол CCMP є більш надійним, ніж протокол TKIP, що використовується в WPA, тому його використання ускладнює атаки зловмисників.

Відповідно до режиму Personal, автентифікація досягається за допомогою Pre-Shared Key та в режимі Enterprise завдяки стандарту IEEE 802.1X/EAP.

Характерною рисою протоколу WPA2 є також технологія WPS (Wi-Fi Protected Setup), яка спрощує підключення WPA2 у житлових мережах, тобто для підключення в домашньому середовищі можливо використовувати звичайні PIN-коди або шляхом натискання кнопок на роутері. Такий функціонал сильно сприяв поширенню WPA2, але водночас став джерелом вразливостей, адже призводить до можливості здійснення атак на стандарт WPS, тому для кращої безпеки рекомендовано вимкнути опцію WPS і, якщо можливо, прошивку. Цей протокол підтримується всіма можливими сертифікованими пристроями Wi-Fi. Наразі переважна більшість локальних бездротових мереж тривалий час працює в режимі захисту протоколу WPA2.

При цьому вразливості вказаного протоколу вже добре відомі [10, 11]. За час використання WPA2 було виявлено немалий список вразливостей:

Технологія «рукостискання» Four-way handshaking (FWH), переустановлення ключів парного шифрування PTK-TK, ключ групи GTK, ключ цілісності IGTK; переустановлення ключа STK. використання шифрування TKIP, механізм Fast Transition (FT), тунельне підключення TDLS та його одноразовий ключ TPK, технологія керування фреймами, відкриті контрольовані фрейми, дисоціація відносно точок доступу, повторна автентифікація.

Перелічені вразливості визначаються певними рівнями, які залежать від режимів і налаштувань мережі та можуть призводити до значного набору атак, щодо мережі Wi-Fi [12]:

- атаки за словником;
- офлайн-атаки підбору паролю за перехопленим рукостисканням;
- KRACK (Key Reinstallation Attacks), основою якого є 4-етапне рукостискання;
- зламування WPS;
- Advanced Stealth Man-in-the-middle (Hole 196);
- атака на PSK;
- Brute force;
- Evil Twin.

Тривалий досвід використання WPA2 призвів у 2018 року альянс Wi-Fi до представлення якісно нового протоколу WPA3, який мав би знівелювати перелічені вразливості та сильно знизити ефективність атак.

Протокол безпеки WPA3, який на сьогодні є найсучаснішим щодо надання покращеного захисту бездротових мереж, визначається новими опціями шифрування й автентифікації. Головною особливістю WPA3 є те, що забороняється використовувати застарілі протоколи безпеки, можлива інтеграція лише з протоколом WPA2, але за визначених умов використання.

Провідні характеристики WPA3:

1) строге використання стійкості мережі з використанням захищених кадрів керування PMF;

2) підтримка й оновлення тенденції режимів безпеки Enterprise та Personal;

3) ініціювання автентифікації SAE;

4) сприяння перехідного режиму безпеки, яке визначається підтримкою взаємодії з пристроями, які послуговуються протоколом WPA2;

5) обмін ключами Dragonfly за криптографічним експоненціальним методом SPEKE;

6) технологія Opportunistic Wireless Encryption (OWE), яка дає змогу шифрувати з'єднання між пристроєм користувача та точками доступу мережі за механізмом Діффі – Хеллмана, що, зі свого боку, сприяє генеруванню різних ключів дешифрування для кожного з користувачів. Примітка: технологія OWE також шифрує відкриті мережі;

7) додаткова опція DPP дає змогу здійснювати автентифікацію клієнтів за допомогою тегів NFC та QR-коду.

Покращені нововведення в протоколі WPA3 порівняно з протоколом WPA2:

1) алгоритм SAE замінює WPA-PSK;

2) шифрування OWE замінює відкриту автентифікацію 802.11;

3) протокол DPP замінює технологію WPS.

Таблиця 1

Порівняльні показники протоколів безпеки

Складові механізму протоколу	**WEP**	**WPA**	**WPA2**	**WPA3**
Механізм шифруванння	RC4 (Використання – IV вектора)	RC4/TKIP	AES/CCMP CCMP/TKIP	GCMP-256 Simultaneous Authentication of Equals (SAE)
Розмір ключа шифрування	40 біт	128 біт	128 біт	256 біт
Шифрування ключа пакета	Конкатенація	Змішаний	Немає потреби	Немає потреби
Шифрування ключа управління	Жодного	802.1x	802.1x	WLAN 802.11i OWE
Шифрування зміни ключа	Жодного	Для кожного пакета	Немає потреби	Немає потреби

Продовження таблиці 1

Складові механізму протоколу	WEP	WPA	WPA2	WPA3
Апаратна сумісність	Можливе розгортання на поточній апаратній інфраструктурі	Можливе розгортання як на поточному, так і на старішому обладнанні	Старіші карти мережевого інтерфейсу не підтримуються	Можливе розгортання на обладнанні WPA2 з оновленнями ПЗ
Управління ключами	Жодного	4-стороннє рукостискання	4-стороннє рукостискання	384-розрядна еліптична крива Діффі – Хеллмена (ECDH)
Автентифікація	Слабка	802.1x – EAP	802.1x – EAP	Одночасна автентифікація (SAE)
Цілісність даних	CRC-32	MIC (Michael)	CCM	256-bit Broadcast/ Multicast Integrity Protocol
Атака з найбільшою загрозою	Вразливий до зламу ключа методом проб і помилок фрагментації Bittu та DoS-атак на відмову в обслуговуванні, включно з різноманітними DoS-атаками	Вразливий до зламу ключа методом проб і помилок, Ohigashi-Morii, WPA-PSK і Dos-атаки	Вразливий до DoS-атак через незахищені контрольні кадри та підробку MAC-адрес	Вразливий до видалення SSL, Evil Twin Attack і DNS Spoofing

WEP відрізняється від WPA і WPA2 як необхідністю специфічного обладнання, так і використовуваним програмним забезпеченням. У таблиці 1 наведено відмінності між WEP, WPA, WPA2 і WAP3 з точки зору підходів до шифрування й автентифікації. У WPA2 атака «грубою силою», імовірно, використовувалася для виявлення пароля Wi-Fi. Це пояснюється процедурою передбачення пароля, яка може відбуватися в автономному режимі. У WPA3 атак грубої сили успішно уникають, оскільки нові стандартні дозволи не дають можливості хакерам передбачати пароль в автономному режимі. Це і є перевагою у використанні WPA3-SAE порівняно з WPA2-PSK. Відмінності в процесі шифрування досліджуваних стандартів безпеки Wi-Fi залежать від використовуваних алгоритмів шифрування, які певним чином впливають на рівень захищеності мережі.

На рис. 2 показано як приклад вибір політики безпеки мережі Wi-Fi з доступних на маршрутизаторах, а саме на застарілому обладнанні, після 2006 року:

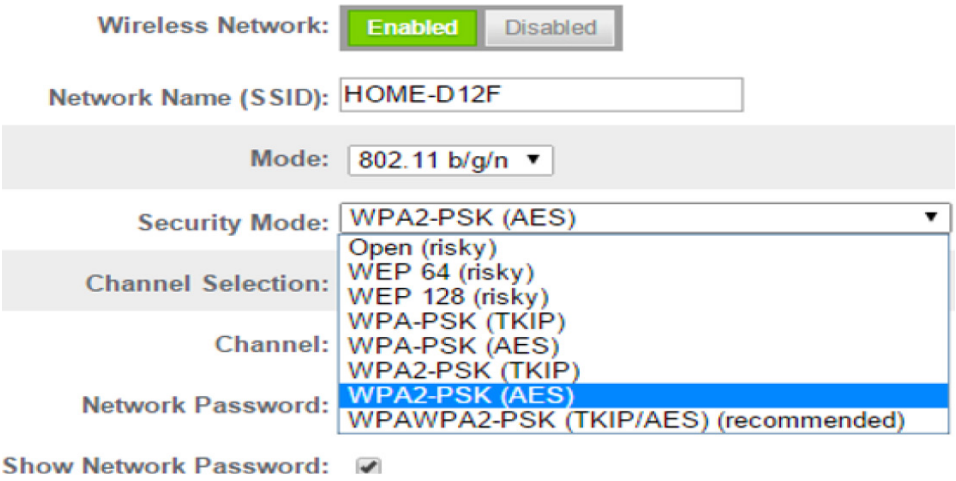

Рис. 2. Налаштування захисту локальної бездротової мережі

У наведеному прикладі налаштування режиму безпеки обладнання не містить можливості використання WPA3. З точки зору стандарту WPA3, поточне обладнання є застарілим. Однак це не означає, що воно встановлено до 2018 року. Виробники продовжують випускати наведене обладнання, тобто воно має попит, хоча поряд із ним саме на ринку маршрутизаторів достатньо номенклатури, яка забез-

печує функціонування WPA3, але підтримує також WPA2. Це свідчить, що протокол WPA3 за ці всі роки з моменту появи у 2018 році не став домінуючим. До того ж цей протокол як засіб захисту до цього часу займає малу частку мереж Wi-Fi. Так, за даними публічної бази даних вебсайту **WiGLE** [13], онлайн-ресурсу, який збирає інформацію про різні бездротові точки доступу Wi-Fi по всьому світу, кількість мереж Wi-Fi перевищувала 1 мільярд екземплярів уже у 2021 році і продовжувала зростати. У таблиці 2 наведено дані WiGLE про частки протоколів безпеки в мережах Wi-Fi за останні три роки.

Таблиця 2

Частки протоколів безпеки в мережах Wi-Fi

Протокол безпеки Wi-Fi (шифрування)	**Період часу**		
	01.01.2021 – 31.12.2021	**01.01.2022 – 31.12.2022**	**01.01.2023 – 03.05.2023**
WPA3	0,003%	0,05%	0,195%
WPA2	69,98%	71,93%	72,86%
WPA	4,45%	3,9%	3,58%
WEP	4,6%	4,0%	3,7%
Незашифровані мережі	2,9%	2,5%	2,4%
Невідомі мережі	18,1%	17,6%	17,4%

Як ми бачимо, існує тенденція до зростання частки WPA3 та зниження часток застарілих протоколів. Але привертає увагу дивовижно низький рівень частки WPA3. Причини цього явища ще достеменно не досліджені, проте існує ряд факторів, які стримують темпи поширення цього протоколу. Цей протокол практично усунув проблеми атаки KRACK (Key Reinstallation Attacks), які найбільше загрожують протоколу WPA2. Справа в тому, що ці атаки небезпечні тим, що використовують вразливості в самому стандарті Wi-Fi, а не в окремих продуктах чи рішеннях. Тобто проблема полягає в тому, що цей протокол теж має свої вразливості. У таблиці 1 вони відображені в загальному вигляді. Ряд дослідників ґрунтовно дослідили вразливості WPA3 [14–17]. Далі розглянемо одну з найбільш загрозливих. Ряд провідних експертів, незважаючи на значну кількість проведених покращень для зниження вразливостей, які притаманні протоколу WPA2, не визначають принципово нового протоколу WPA3. Натомість це сертифікація, що визначає, які ж існуючі протоколи має підтримувати пристрій. Дещо спрощено WPA3 вимагає підтримки рукостискання Dragonfly і його єдиною новою функцією є перехідний режим, де WPA2 і WPA3 одночасно підтримуються для зворотної сумісності. І сама безпека протоколу WPA3 та його рукостискання Dragonfly – під сумнівом. На рис. 3 показано схему обміну, між клієнтом і точкою доступу відома під назвою Dragonfly.

Варіант рукостискання Dragonfly, який використовується в WPA3, також відомий як одночасна автентифікація рівних (SAE). У 2020 році М. Вангоф і Е. Ронен показали, що має місце витік, пов'язаний із паролем, що дає можливість здійснити словникову атаку в автономному режимі.

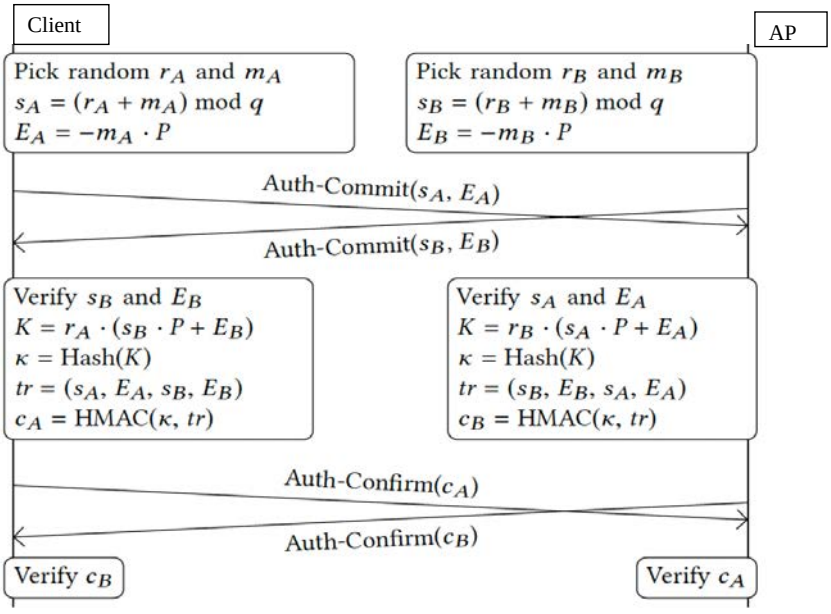

Рис. 3. Рукостискання Dragonfly WPA3 [15]

Ця атака отримала образну назву Dragonblood унаслідок метафори графічного зображення 4-етапного рукостискання. Відкриття атаки Dragonblood стало неприємною несподіванкою для Wi-Fi Alliance, який щойно отримав найбільше оновлення за 14 років. Однак постачальники обладнання продовжують впровадження WPA3, керуючись тим, що KRACK WPA2 є більш серйозною загрозою, оскільки стосується самого стандарту, тоді як Dragonblood переважно використовує недоліки реалізації, пов'язані з витоками побічних каналів. Альянс Wi-Fi опублікував деякі вказівки щодо реалізації, яких мають дотримуватися виробники, щоб забезпечити безпечну зворотну сумісність реалізацій WPA3. Незважаючи на це, впровадження WPA3 йде дуже повільно. Наразі швидка глобальна заміна протоколу WPA2 сучасною технологією WPA3 практично неможлива, і такий стан ще порівняно довгий час зберігатиметься.

Проведений аналіз відтворює, що сучасні бездротові мережі, зокрема в міському середовищі, являють собою конгломерат підмереж, кожна з яких підтримується різними протоколами й технологіями інформаційного захисту. При цьому жоден протокол не гарантує стовідсоткового захисту, хоча експерти оцінюють їх можливості по-різному – від відкритого доступу до найвищого, у ролі якого виступає WPA3. Постають питання: як оцінити рівень захищеності мереж Wi-Fi загалом? як конкретному споживачу вибрати прийнятний варіант захисту своєї мережі?

Ці питання виникають у користувачів Wi-Fi скрізь, але особливо вони актуальні в міському середовищі, де спостерігається щільна забудова. У міському середовищі Wi-Fi мереж багато, а щільність забудови дає змогу легко організувати «підслуховування». Проте спочатку треба встановити реальний стан оснащення протоколами захисту мереж Wi-Fi для середовища певного населеного пункту. У ролі об'єкта в цьому дослідженні було вибрано середовище міста Києва.

Методологія дослідження

Для визначення оснащення протоколами захисту мереж Wi-Fi у міському середовищі треба мати відповідні методології. Такими є методології Wardriving або Access Point mapping. У нашому дослідженні ми використали Wardriving. Термін Wardriving описує техніку, що використовується для пошуку й відображення сигналів WLAN у певному місті чи районі. Wardriving зазвичай визначається як переміщення транспортним засобом, зазвичай автомобілем, у визначеній географічній зоні й сканування для перерахування точок бездротового доступу та їх робочий стан у режимі реального часу. Використання Wardriving дає змогу отримати реальні дані про оснащення протоколами безпеки цих типів мереж. Було проведено пасивне дослідження зі збору лише загальнодоступних даних, які передаються з кожної бездротової точки. Будь-які спроби проникнення в будь-яку мережу не допускались. За допомогою використаної техніки Wardriving [18], яка базується на застосуванні мережевої карти, GPS-приймачів, відбувається процес «непомітного» сканування безпровідних мереж на виявлення розташувань і налаштування найближчих мереж із використанням авто як засобу пересування. Вибрана техніка дає змогу проводити легальне сканування бездротових мереж, оскільки законами не заборонено збирати дані з бездротових мереж, як і жодні закони не забороняють переписувати номери будинків у місті. Wardriving не є хакерською, незаконною або шкідливою діяльністю для перевірених бездротових мережевих пристроїв або їхніх власників. Назва цієї методології походить від кінофільму Wargames і не має нічого спільного з будь-якими військовими застосуваннями. Як методологія дослідження міських мереж Wi-Fi, технологія Wardriving використовується досить давно. Перше автоматизоване дослідження безпеки бездротової мережі було проведено Шиплі наприкінці 1999 року в Каліфорнії та вперше оприлюднене у 2001 році [18]. З того часу дослідники з різних країн, застосовуючи Wardriving, провели численні дослідження стану захищеності міських мереж, причому на цьому матеріалі можна дослідити як еволюцію бездротових в містах [19–24] різних країн і континентів, так і еволюцію їх захисту. В Україні було досить давно проведено одне таке дослідження, а саме у 2008 році [25], результати якого мають дуже суттєву різницю із сучасними даними.

Проведення сканування мереж

Для збору даних було вибрано стільниковий пристрій із параметрами: display=SP1A.210812.016.G780GXXU3CVI4, model=SM-G780G, release=12, device=r8q, board=kona, brand=samsung, Було встановлено програмне забезпечення для сканування мережі застосунок WiGLE в середовищі ОС Android.

З врахуванням величезних масштабів мегаполіса Києва повне дослідження міста вимагало надто багато часу й ресурсів, тому були проведені вибіркові заміри на території м. Києва для сканування бездротової мережі на правому та лівому берегах річки Дніпро, загальною площею близько 9 км^2, у травні 2023 року. Дослідженням вибірково охоплені спальні райони, промислові зони та певна частка центру міста. З огляду на стан безпеки, тобто травень 2023 року, конкретна локація сканувань не вказується. За результатами сканування у вибраних ділянках всього було виявлено 331 мережу типу Wi-Fi. З них 61 було з невизначеним (невідомим) SSID.

Сканування відбувалось автоматично під час пересування та використання застосунку WiGLE у визначених місцях із налаштуванням параметрів для сканування та фільтрування.

Параметри для сканування охоплювали: основні налаштування щодо часу сканування Wi-Fi (50 мс), коли швидкість близько 8 км/год (без зупинки), перевірка призупинення Wi-Fi (1,5 хв); GPS-на-

лаштування щодо тайм-ауту мережевого місцезнаходження (1 хв), час між GPS-оновленнями (1 с) та таймаутом (15 с). Параметри для фільтрування такі: відображення відкритих мереж, WEP та WPA-типізованих мереж.

Дані, зібрані унаслідок сканування мереж у визначених місцевостях міста Києва з використанням застосунку WiGLE, були експортовані у формат .csv для утворення датасету. Дані не завантажувалися на ресурс сайту WiGLE, а зберігалися локально для подальшого аналізу даних.

Дані у форматі csv були завантажені в локальне сховище Jupyter Notebook для подальшої обробки датасету.

Результат обробки даних на основі датафрейму, який відображає поточну ситуацію розподілу використання протоколів безпеки у досліджених ділянках міста Києва мереж Wi-Fi, наведено на рис. 4.

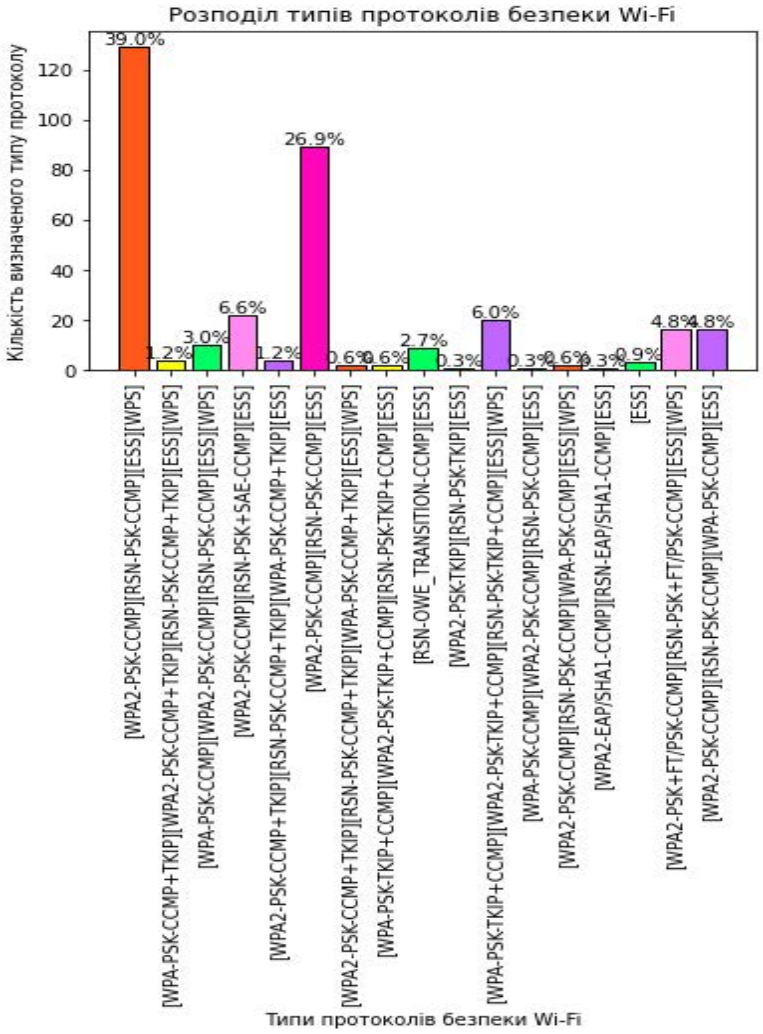

Рис. 4. Розподіл типів протоколів захисту мереж Wi-Fi у мережах м. Києва

Оцінювання рівня безпеки

Як можна бачити з представленої діаграми, розподіл систем кіберзахисту мереж Wi-Fi за даними вибірки для м. Києва дає досить строкату картину, яка, власне, дає можливість отримати тільки номінальну шкалу вимірювань. Перше, на що звертаємо увагу, – це відсутність застарілого протоколу WEP. Як ми бачили, за даними світової статистики, цей протокол продовжує залишатися в ужитку, хоча його частка вже досить мала, але в м. Києві (за результатами отриманої вибірки) він практично відсутній. Не виявлено також і використання новітнього протоколу WPA3. Переважає використання протоколу WPA2 різних версій, є певна частка протоколу WPA і невелика частка публічних мереж Wi-Fi як з певним захистом, так і повністю відкритих. Однак як оцінити загалом стан і цілісність захищеності мереж у мегаполісі на прикладі Києва? Для відповіді на це питання треба провести два вартісних і трудомістких дослідження:

- протестувати на зламування всі варіанти протоколів з усіма відомими для них атаками;
- просканувати всі мережі мегаполіса.

Малоймовірно, що коли-небудь ці завдання будуть виконані. Доводиться скористатися вибірковими даними, а рівень захищеності версій протоколу оцінювати альтернативним способом, опираючись на відносні оцінки рівня захищеності типу протоколу, яке надає обладнання мереж Wi-Fi.

Однак для оцінювання рівня захищеності цього недостатньо. У таблиці 3 наведено результати упорядкованого списку типів протоколів безпеки за рівнем захищеності разом з оцінкою захищеності за інтервальною шкалою. Слід зазначити, що йдеться не про абсолютну оцінку рівня захищеності, а про відносну. Тобто ту, яка відповідає поточному рівню можливостей технологій захисту бездротових мереж. Далі покажемо, як було отримано таблицю 3, у якій перша колонка позначає тип протоколу, друга – бренд Wi-Fi Alliance, третя – стандарт IEEE 802.11.

Побудуємо спочатку рангову шкалу вимірювань, тобто визначимо порядок, за якого певна політика безпеки, реалізована через компоненти технічної реалізації протоколів, буде краща чи гірша, ніж інша протиставлена їй політика. А потім побудуємо інтервальну шкалу.

Таблиця 3

Оцінка рівня захисту типів протоколу бездротових мереж

Сервіс захисту	**Протокол Wi-Fi alians**	**Відповідність протоколу IEEE 802.11i-2004 (RSN)**	**Технології зручності**	**Частка використання в міському середовищі, %**	**Рівень захисту***	**Індекс відносної безпеки**
P1	WPA2-EAP/SHA1-CCMP	EAP/SHA1-CCMP	–	0,3	вс	85
P2	WPA2-PSK-CCMP	PSK+SAE-CCMP	–	6,6	вс	82
P3	WPA2-PSK-CCMP	PSK-CCMP	–	26,9	вс	80
P4	WPA2-PSK-TKIP	PSK-CCMP	–	0,3	с	75
P5	WPA2-PSK-CCMP	PSK-CCMP	WPS	39	с	73
P6	WPA2-PSK-CCMP	PSK-CCMP	WPS, FT	4,8	с	70
P7	[WPA2-PSK-CCMP] [WPA-PSK-CCMP]	PSK-CCMP	–	4,8	нс	65
P8	[WPA2-PSK-CCMP] [WPA-PSK-CCMP]	PSK-CCMP	WPS	0,6	нс	60
P9	[WPA2-PSK-CCMP+TKIP] [WPA-PSK-CCMP+TKIP]	PSK-CCMP+TKIP	–	1,2	нс	58
P10	[WPA2-PSK-CCMP+TKIP] [WPA-PSK-CCMP+TKIP]	PSK-CCMP+TKIP	WPS	0,6	нс	56
P11	[WPA-PSK-CCMP] [WPA2-PSK-CCMP]	PSK-CCMP	–	0,3	нс	50
P12	[WPA-PSK-CCMP] [WPA2-PSK-CCMP]	PSK-CCMP	WPS	3	нс	46
P13	[WPA-PSK-CCMP+TKIP] [WPA2-PSK-CCMP+TKIP]	PSK-CCMP+TKIP	WPS	1,2	нс	46
P14	[WPA-PSK-CCMP+TKIP] [WPA2-PSK-CCMP+TKIP]	PSK-CCMP+TKIP	–	0,6	нс	43
P15	[WPA-PSK-CCMP+TKIP] [WPA2-PSK-CCMP+TKIP]	PSK-CCMP+TKIP	WPS	6	нс	43
P16	OWE_TRANSITION-CCMP	OWE_TRANSITIO-CCMP	–	2,7	нс	40
P17	OPEN AUTENTIFICATION	OPEN 802.11	–	0,9	нз	10

*Примітка: * вс – вище за середній, с – середній, нс – нижче за середній, нз – незадовільно*

З погляду інформаційного захисту вибір протоколу з комбінації технологій визначає вибір політики безпеки. Як показує практика, користувачі бездротових мереж не завжди ставлять інформаційну безпеку на перше місце. Значну роль також грають цінові фактори, зручність встановлення, налагодження й експлуатація. Для цього розробники обладнання надають широкий спектр рішень. Зо-

крема, це стосується технології спрощеного підключення або безшовного роумінгу Wi-Fi. У принципі, це правильно, бо сприяє розширенню використання бездротових мереж. Проте ці рішення ще більш ускладнюють проблему захищеності мереж Wi-Fi, бо самі вони додають власні вразливості в загальну проблему захищеності.

Дослідники інформаційної безпеки бездротових мереж виділили декілька категорій, які визначають рівень захищеності [26].

Автентичність: автентичність вказує на відмінність авторизованих користувачів від неавторизованих користувачів. Будь-які підключені вузли в бездротових мережах мають спочатку пройти ідентифікацію щодо один одного за вже існуючими та вказаними даними й авторизацію щодо отримання відповідних прав доступу.

Конфіденційність: конфіденційність передбачає обмеження доступу до бездротової мережі неавторизованим користувачам і блокування доступу таких користувачів до бездротової мережі та розголошення інформації.

Цілісність: цілісність означає збереження інформації, її точність і надійність під час передачі через бездротову мережу.

Наявність: ця характеристика передбачає, що ця бездротова мережа дійсно доступна авторизованим користувачам для доступу за їхнім запитом.

Реалізація цих категорій залежить від показників безпеки, описаних у таблиці . Усі ці категорії технічного плану, які безпосередньо реалізують політику безпеки.

Крім того, ми вважаємо доцільним додати сюди категорію, яка безпосередньо не бере участі в реалізації варіанта технічного рішення, проте може вплинути на рівень захищеності бездротової мережі. Пропонуємо назвати цю категорію терміном «зручність».

Зручність: означає зручність встановлення, налаштування, використання. Наприклад, технологія WPS дає змогу зручно встановлювати обладнання в мережу, але разом із тим породжує нові вразливості.

Спочатку проведемо групове ранжування – виділимо групи типів протоколів за оцінками «добре», «посередньо», «нижче середнього», «незадовільно».

Оцінка «відмінно» тут відсутня, оскільки таку оцінку потенційно мав би протокол WPA3, але через виявлені вразливості його максимально можлива оцінка не 100, а 95.

Оцінки «добре» заслуговують протоколи P1–P3, оскільки до складу протоколу WPA2 входять сучасні засоби автентифікації, конфіденційності та цілісності.

Оцінки «посередньо» заслуговують протоколи P4–P6, оскільки до складу протоколу WPA2 входять дещо застарілі засоби автентифікації, конфіденційності та цілісності, або присутні засоби зручності.

Оцінки «нижче середнього» заслуговують протоколи P7–P15, оскільки до складу протоколу WPA2 входять різні варіанти переважно застарілих засобів автентифікації, конфіденційності та деякі типи протоколів, які мають засоби зручності. Але найважливіше, що впливає на таке оцінювання, – це гібридний характер цих типів протоколів, а саме можливість роботи в застарілому протоколі WPA. У цей інтервал потрапляє також і P16, хоча до класу гібридних не належить, а дає певні засоби захисту для користувачів відкритих мереж.

Нарешті оцінку «незадовільно» отримує протокол P17, призначений для обслуговування відкритих мереж без засобів захисту.

Щоб отримати інтервальні оцінки, потрібно провести ранжування типів протоколів у межах виділених класів і надати їм оцінку за певною шкалою. Ці результати представлені в таблиці 3. Причому типи протоколів ранжуються за критеріями більш надійних технологій захисту, наявності або відсутності технологій зручності.

Для визначення числової оцінки візьмемо 100-бальну шкалу. Для цієї вибірки максимальна можлива оцінка дорівнює 85, для оцінки «посередньо» максимальна можлива оцінка 75, для оцінки «нижче середнього» максимальна можлива оцінка 60, а мінімальна – 40. Те, що нижче за 40, оцінюється як «незадовільно». Числові значення оцінок типів протоколів у межах виділеної шкали отримані шляхом опитування групи спеціалістів з наступним усередненням.

Далі на підставі інтервальних оцінок захищеності типів протоколів і визначених їх часток в бездротових мережах міського середовища Києва, можемо вирахувати відносну оцінку захищеності мереж загалом.

$$RISN=\sum_1^n Pi * Fi, \tag{1}$$

де *RISN* – відносний індекс захищеності мереж міського середовища;
Pi – і-й протокол з таблиці 3;
Fi – частка і-го протоколу.

Підставляючи значення відповідних колонок Таблиці 3, у формулу отримаємо:

$$RISN = 70{,}113.$$

Тобто згідно з даними вибірки сканованих бездротових мереж у середовищі м. Києва загальна відносна оцінка їх захищеності лежить в діапазоні «посередньо».

Висновки

Дослідження оцінки рівня захищеності бездротових мереж у міському середовищі потребувало аналізу механізмів захисту протоколів, які мають забезпечувати надійне шифрування, автентифікацію та цілісність з'єднань. Для встановлення реального стану бездротових мереж проведено сканування бездротових мереж із використанням методології Wardrive у вибіркових локаціях міста Києва. Отримані дані після обробки були використані для оцінювання рівня захищеності мереж Wi-Fi для м. Києва на основі розробленої методики. Згідно з отриманою оцінкою рівень захищеності бездротових мереж міського середовища перебуває в задовільному стані.

Проте в перспективі отримане значення можна покращувати впровадженням нового протоколу безпеки WPA3, хоча це буде потребувати витрат. Однак існує можливість уже зараз як покращити загальний рівень захищеності мереж, так і підвищити індивідуальну безпеку, зокрема, завдяки кращому налаштуванню рівня безпеки обладнання.

Література

1. Kohlios C., Hayajneh T. A. Comprehensive Attack Flow Model and Security Analysis for Wi-Fi and WPA3. Electronics 7 (11), 284, 2018, pp. 1–28.

2. W-F Alliance, "Value of wi-fi" 2022, URL: https://www.wi-fi.org/ discover-wi-fi/value-of-wi-fi (дата звернення: 10.11.2023).

3. Wireless Security and the IEEE 802.11 Standards GIAC Security Essentials Certification (GSEC) Practical Assignment Version 1.4c. URL: https://www.giac.org/paper/gsec /4214/wireless-security-ieee-80211-standards/106760 (дата звернення: 10.11.2023).

4. Edney Jon, Arbaugh William A. Real 802.11 Security: Wi-Fi Protected Access and 802.11i. Publisher: Addison Wesley, Pub Date: July 15, 2003, ISBN: 0-321-13620-9, 451 p.

5. ANSI/IEEE Std 802.11, 1999 Edition (R2003), Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications, Section 8, Authentication and privacy, Sub section 8.2.1, p. 61.

6. Borisov N., Goldberg I., Wagner D. Intercepting Mobile Communications: The Insecurity of 802.11. URL: http://www.isaac.cs.berkeley.edu/isaac/ mobicom.pdf (дата звернення: 10.11.2023).

7. Fluhrer S., Mantin I., Shamir, A., Weaknesses in the Key Scheduling Algorithm of RC4. URL: http://www.drizzle.com/~aboba/IEEE/rc4_ksaproc.pdf (дата звернення: 05.11.2023).

8. Stuart J. Kerry et al. Response from the IEEE 802.11 Chair on WEP Security, IEEE 802.11 Working Group. URL: http://slashdot.org/articles/01/02/15/1745204.shtml (дата звернення: 01.11.2023).

9. Housley R., Whiting D. *Temporal Key Hash*. IEEE 802.11-01/550r3, Dec 2001.

10. Srikanth V., Reddy I. Wireless security protocols (WEP, WPA, WPA2 & WPA3) [Електронний ресурс] // JETIR. – 2019. – URL: https://www.jetir.org/ papers/ JETIRDA06001.pdf.

11. The State of Wi-Fi® Security Wi-Fi CERTIFIED™ WPA2 TM Delivers Advanced Security to Homes, Enterprises and Mobile Devices Wi-Fi Alliance® – URL: https://davidhoglund. typepad.com/files/20120229_state_of_wi-fi_security_09may2012_updated_cert.pdf.

12. Caneill M. Attacks against the WiFi protocols WEP and WPA [Електронний ресурс] / M. Caneill, J. Gilis. – 2010. – Режим доступу до ресурсу: https://matthieu.io/dl/papers/wifi-attacks-wep-wpa.pdf.

13. [Електронний ресурс] : [Вебсайт]. – Електронні дані. –2023. – URL: https://wigle.net/ (дата звернення: 12.09.2023). – Назва з екрана.

14. Опірський І., Максимів Н., Женчур М. Дослідження безпеки стандарту Wi-Fi Protected Access 3 (WPA3*). Безпека інформації* 2023. Том 29. С. 21–31.

15. Vanhoef M., Ronen E. Dragonblood: Analyzing the Dragonfly Handshake of WPA3 and EAP-pwd 2020 // IEEE Symposium on Security and Privacy (SP), San Francisco, CA, USA, 2020, pp. 517–533, doi: https://doi.org/10.1109/SP40000.2020.00031.

16. Bednarczyk Mariusz, Piotrowski Zbigniew Will WPA3 really provide Wi-Fi security at a higher level? // Proc. SPIE 11055, XII Conference on Reconnaissance and Electronic Warfare Systems, 27 March 2019; doi: https://doi.org/10.1117/12.2525020.

17. Braga D. De Almeida, Fouque P, Sabt M. Dragonblood is still leaking: Practical cache-based side-channel in the wild // ACSAC. ACM, 2020, pp. 291–303.

18. Hurley C., Rogers R., Baker B., Thornton F. WarDriving & Wireless Penetration Testing. Canada: Syngress, 2007. 446 p.

19. Yek S. Wily attackers seek wireless networks in Perth, Western Australia foreasy targets // European Conference on Computer Network Defence, London,United Kingdom, 2006, pp. 125–136.

20. Sarkar I., Abdullah A. H.Exploring wireless network security in Auckland City through warwalking field trials // Proceedings of the 13th International Conference on Advanced Communication Technology (ICACT2011. January 2011.

21. Chih-Ta L., Hira S., Donald J. Wireless network security // Unitec New Zealand, 2004, pp. 337–339.

22. Mara´czi M. Wardriving in Eger // Proceedings of the IEEE 13th International Symposium on Applied Computational Intelligence and Informatics, IEEE, Timisoara, Romania, May 2019, pp. 127–130.

23. Valchanov H., Edikyan J., Aleksieva V. A study of wi-fi security in city environment//Proceedings of the IOP Conference Series: Materials Science and Engineering, IOP, October 2019.

24. Nasr E., Jalloul M., Bachalaany J., Maalouly R. Wi-fi network vulnerability analysis and risk assessment in Lebanon // Proceedings of the International Conference of Engineering Risk, Beirut, May 2019.

25. Дослідження захищеності Wi-Fi мереж в м. Києві [Електронний ресурс] : Електронні дані. – Київ, 2008. – URL: https://www.kaa.org.ua/22-articles/57-96.html (дата звернення: 12.11.2023). – Назва з екрана.

26. Yulong Jia Zhu, Xianbin Wang, Hanzo Lajos. A Survey on Wireless Security: *Technical Challenges. Recent Advances and Future Trends.* September 2016. Vol. 104. No. 9.

References

1. Kohlios, C., Hayajneh, T. (2018). A. Comprehensive Attack Flow Model and Security Analysis for Wi-Fi and WPA3. *Electronics 7* (11), 284, pp. 1–28.

2. W-F Alliance, "Value of wi-fi" (2022). [Online]. Available: https://www.wi-fi.org/ discover-wi-fi/value-of-wi-fi.

3. Wireless Security and the IEEE 802.11 Standards GIAC Security Essentials Certification (GSEC) Practical Assignment Version 1.4c [Online]. Available: https://www.giac.org/paper/gsec/ 4214/wireless-security-ieee-80211-standards/106760.

4. Jon Edney, William A. Arbaugh Real 802.11 Security: Wi-Fi Protected Access and 802.11i. Publisher: Addison Wesley, Pub Date: July 15, 2003, ISBN: 0-321-13620-9, 451 p.

5. ANSI/IEEE Std 802.11, 1999 Edition (R2003), Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications, Section 8, Authentication and privacy, Sub section 8.2.1, 61 p.

6. Borisov, N., Goldberg, I., Wagner, D. Intercepting Mobile Communications: The Insecurity of 802.11 [Online]. Available: http://www.isaac.cs.berkeley.edu/isaac/mobicom.pdf.

7. Fluhrer, S., Mantin, I., Shamir, A., Weaknesses in the Key Scheduling Algorithm of RC4 [Online]. Available: http://www.drizzle.com/~aboba/IEEE/rc4_ksaproc.pdf.

8. Stuart J. Kerry et al. Response from the IEEE 802.11 Chair on WEP Security, IEEE 802.11 Working Group [Online]. Available: http://slashdot.org/articles/01/02/15/1745204.shtml.

9. Housley, R., Whiting D. (2001). *Temporal Key Hash*. IEEE 802.11-01/550r3.

10. Srikanth, V., Reddy, I. (2019). *Wireless security protocols (WEP, WPA, WPA2 & WPA3)* / JETIR [Online]. Available: https://www.jetir.org/papers/JETIRDA06001.pdf.

11. The State of Wi-Fi® Security Wi-Fi CERTIFIED™ WPA2 TM Delivers Advanced Security o Homes, Enterprises and Mobile Devices Wi-Fi Alliance® January 2012.

12. Caneill, M., Gilis, J. (2010). Attacks against the WiFi protocols WEP and WPA [Electronic resource] / M. Caneill. Available: https://matthieu.io/dl/papers/wifi-attacks-wep-wpa.pdf.

13. [Electronic resource]: [Website] (2023). Electronic data [Online]. Available: https://wigle.net/ (Date: 12.09.2023).

14. Opirskyi, I., Maksymiv, N., Zhenchur, M. (2023). Doslidzhennia bezpeky standartu Wi-Fi Protected Access 3 ["Security research of Wi-Fi Protected Access 3 (WPA3) standard"]. *Bezpeka informatsii.* Vol. 29. № 1, pp. 21 [in Ukrainian].

15. Vanhoef, M., Ronen, E. (2020). Dragonblood: Analyzing the Dragonfly Handshake of WPA3 and EAP-pwd. IEEE Symposium on Security and Privacy (SP), San Francisco, CA, USA, pp. 517-533, doi: https://doi.org/ 10.1109/SP40000.2020.00031.

16. Mariusz Bednarczyk, Zbigniew Piotrowski (2019). Will WPA3 really provide Wi-Fi security at a higher level? // Proc. SPIE 11055, XII Conference on Reconnaissance and Electronic Warfare Systems, doi: https://doi.org/10.1117/12.2525020.

17. Braga, D. De Almeida, Fouque P, Sabt M. (2020). Dragonblood is still leaking: Practical cache-based side-channel in the wild in ACSAC. ACM, pp. 291–303.

18. Hurley, C., Rogers, R., Baker, B., Thornton, F. (2007). *WarDriving & Wireless Penetration Testing.* Canada: Syngress, 446 p.

19. Yek, S. (2006). Wily attackers seek wireless networks in Perth, Western Australia foreasy targets // European Conference on Computer Network Defence, London,United Kingdom, pp. 125–136.

20. Sarkar, I., Abdullah, A. (2011). Exploring wireless network security in Auckland City through warwalking field trials // Proceedings of the 13th International Conference on Advanced Communication Technology (ICACT2011), IEEE, Gangwon.

21. Chih-Ta, L., Hira, S., Donald, J. (2004). Wireless network security // Unitec New Zealand, pp. 337–339.

22. Mara´czi, M. (2019). Wardriving in Eger // Proceedings of the IEEE 13th International Symposium on Applied Computational Intelligence and Informatics, pp. 127–130, IEEE, Timisoara, Romania, May.

23. Valchanov, H., Edikyan, J., Aleksieva, V. (2019). A study of wi-fi security in city environment // Proceedings of the IOP Conference Series: Materials Science and Engineering, IOP.

24. Nasr, E., Jalloul, M., Bachalaany, J., Maalouly, R. (2019). Wi-fi network vulnerability analysis and risk assessment in Lebanon // Proceedings of the International Conference of Engineering Risk, Beirut.

25. Doslidzhennia zakhyshchenosti Wi-Fi merezh v m. Kyievi [Study of the security of Wi-Fi networks in Kyiv] (2008). [Online]: [Website]. Avaible: https://www.kaa.org.ua/22-articles/57-96 (date of application: 12.11.2023) [in Ukrainian]

26. Yulong Jia Zhu, Xianbin Wang, Hanzo Lajos (2016). A Survey on Wireless Security: *Technical Challenges. Recent Advances and Future Trends*. Vol. 104. No. 9.