DOI: 10.25140/2411-5363-2022-1(27)-123-135
УДК 004.77.056(045)

Наталія Фролова[1], Інна Михальчук[2], Олександр Тищенко[3]

[1]асистент кафедри комп'ютеризованих систем захисту інформації
Національний авіаційний університет (Київ, Україна)
E-mail: talaf@ukr.net. **ORCID:** https://orcid.org/0000-0001-7935-6496

[2]кандидат технічних наук, асистент кафедри кібербезпеки та захисту інформації
Київський національний університет імені Тараса Шевченка (Київ, Україна)
E-mail: mykhalchuk.inna.kbzi@gmail.com. **ORCID:** https://orcid.org/0000-0002-1802-7653
ResearcherID: ABF-8615-2020. **SCOPUS Author ID:** 57188710011

[3]студент освітнього ступеня магістр
Національний авіаційний університет (Київ, Україна)
E-mail: stischenk0@icloud.com

ЗАХИСТ ПУБЛІЧНИХ ТОЧОК ДОСТУПУ WI-FI

Розглянуто технології та засоби розгортання публічних мереж на базі сімейства стандартів IEEE 802.11, проаналізовано типи хакерських атак у загальнодоступній Wi-Fi мережі, на основі проведеного аналізу найпоширеніших вразливостей та загроз публічних точок доступу Wi-Fi запропоновано рекомендації щодо впровадження WEP, WPA, WPA2, WPA3 та OWE технологій залежно від роду діяльності й обсягів конфіденційної інформації, підтримки технології захисту кінцевими пристроями користувачів та актуальності протоколів безпеки, які надає та чи інша технологія безпеки.

Ключові слова: *публічні точки доступу Wi-Fi; стандарт; вразливості; методи захисту; зловмисник; безпека мережі; інформаційна безпека.*

Табл.: 2. Рис.: 1. Бібл.: 11.

Актуальність теми дослідження. Стрімкий розвиток методів побудови бездротових локальних мереж зумовив підвищення їх доступності та попиту на ринку інформаційних технологій. Сучасні підприємства та організації зацікавлені в розгортанні публічних точок доступу Wi-Fi, щоб приваблювати більшу кількість клієнтів, ніж конкуренти. Забезпечення зручного бездротового доступу безлічі користувачів до мережі Інтернет шляхом підключення їх до публічних точок доступу Wi-Fi зумовлює передачу великих об'ємів конфіденційних даних у мережі.

Для того щоб задовольнити потреби окремих користувачів мобільних пристроїв, публічні точки доступу Wi-Fi стали повсюдними в кав'ярнях, аеропортах та інших комерційних закладах. Користувачі використовують такі точки доступу для підключення до Інтернету своїх ноутбуків, смартфонів та планшетів.

Трафік у загальнодоступних мережах значною мірою незашифрований, але більшість користувачів загальнодоступного Wi-Fi не знають про пов'язані з цим ризики та продовжують входити в облікові записи електронної пошти, банківських установ або будь-які інші домени, що містять конфіденційну особисту інформацію.

Актуальність проблеми захисту публічних мереж посилюється ще й тим, що більшість провайдерів загальнодоступних точок доступу Wi-Fi приділяють увагу лише зручності та простоті доступу користувачів до мережі, ігноруючи при цьому питання забезпечення захисту даних користувачів.

Постановка проблеми. Більшість мережевих провайдерів, розгортаючи публічні точки доступу Wi-Fi, надають перевагу зручності їх використання користувачами, приділяючи при цьому незначну увагу заходам безпеки, що ставить під загрозу цілісність та конфіденційність даних користувачів та сприяє реалізації хакерських атак на мережу. Кіберзлочинці ефективно використовують наявні вразливості безпеки публічних точок доступу Wi-Fi з метою перехоплення трафіку мережі та викрадення конфіденційних даних. Саме тому важливим завданням є впровадження методів виявлення та протидії подібним кіберзлочинним атакам, які засновані на аналізі хакерської діяльності, що дає змогу оцінити доцільність та ефективність використання тих чи інших технологій забезпечення конфіденційності даних та значною мірою може покращити захист даних користувачів, а отже, і загальну репутацію компанії-надавача мережевих послуг.

Аналіз останніх досліджень та публікацій. У більшості сучасних досліджень цієї проблеми описується розвиток та причини поширення технологій розгортання бездротової локальної мережі, відповідно до сімейства стандартів IEEE 802.11, де передусім акцентується увага на тому, що бездротові локальні мережі мають певний радіус дії, зумовлений загасанням сигналу у просторі, у межах якого користувачі можуть мати доступ до мережі. Зважаючи на цей фактор, не тільки правомірні, але й неправомірні користувачі мають доступ до бездротової мережі. Як варіанти вирішення цієї проблеми, здебільшого пропонується фізичне обмеження доступу, відповідно до меж розповсюдження сигналу мережі, примусове обмеження поширення бездротового сигналу за допомогою його екранування та застосування надійних криптостійких паролів [1].

Більш ефективними сучасними підходами до захисту бездротових мереж є використання відкритої автентифікації, автентифікації зі спільним ключем WEP (Wired Equivalent Privacy), WPA (Wi-Fi Protected Access) та автентифікації за допомогою RADIUS-сервера WPA2 [2]. Проте більшість досліджень, спрямованих на вирішення проблеми захисту публічних точок доступу Wi-Fi, розглядають питання захисту інформації в загальнодоступних бездротових мережах Wi-Fi, не аналізуючи при цьому наявні вразливості та пов'язані з ними загрози, які наявні для цих мереж [3; 4].

Виділення недосліджених частин загальної проблеми. У дослідженнях та публікаціях, які розглядались, не наведено обґрунтування доцільності та ефективності використання того чи іншого методу захисту точок доступу Wi-Fi мереж залежно від виду загроз, для запобігання яких розгортається ця технологія захисту. Також відсутність наочного порівняння запропонованих методів захисту мережі ускладнює розуміння відмінностей, переваг та недоліків кожного з методів.

Метою статті є оцінка ефективності сучасних методів захисту загальнодоступних Wi-Fi мереж на основі аналізу актуальних загроз і вразливостей таких мереж та розробка рекомендацій щодо їх застосування для забезпечення безпеки даних під час розгортання та підтримки різних типів загальнодоступних Wi-Fi мереж, у тому числі й на пристроях користувачів.

Виклад основного матеріалу. Організація бездротових Wi-Fi мереж базується на сімействі стандартів IEEE 802.11 Інституту інженерів електротехніки та електроніки (IEEE - Institute of Electrical and Electronics Engineers), які забезпечують високу швидкість передачі й гарантують стабільність та надійність мережі. Бездротова локальна мережа WLAN (Wireless Local Area Network) розглядається як технологія, яка забезпечує найбільш зручний зв'язок між наявними дротовими мережами та портативним обчислювальним та комунікаційним обладнанням, таким як портативні комп'ютери та цифрові помічники персоналу, на рівні офісу, готелю, компанії чи університету.

Рис. 1. Набір послуг передачі даних
Джерело: [9].

Архітектура IEEE 802.11 визначає дев'ять служб, які можна поділити на дві групи: служби станцій і служби розповсюдження. Служби станцій забезпечують аутентифікацію, деаутентифікацію, конфіденційність та доставку даних, тоді як служби розповсюдження – асоціацію, повторну асоціацію, роз'єднання, розповсюдження та інтеграцію (рис. 1).

Станції – це пристрої, які містять специфікацію IEEE 802.11 з інтерфейсом MAC (Media access control) та PHY (Physical layer) для бездротової мережі. Функції 802.11 реалізовані на станціях програмним або апаратним забезпеченням мережевого адаптера або картки мережевого інтерфейсу (NIC- Network interface controller).

Точка доступу – це пристрій, який забезпечує з'єднання бездротової станції з дротовою або бездротовою мережею. Найважливішою функцією точок доступу є функція мостування [5]. Бездротове середовище використовується для транспортування кадру з однієї станції на іншу.

У табл. 1 наведено різновиди сімейства стандарту 802.11 та їхні основні характеристики.

Типова Wi-Fi мережа включає три складові частини: дротове з'єднання з широкосмуговим провайдером, точку доступу і, зазвичай, комп'ютер, з'єднаний за допомогою дротового та/або бездротового з'єднань. Wi-Fi пропонує різну швидкість широкосмугового доступу та працює в промисловому, науковому та медичному діапазоні частот (діапазон ISM) [6]. Зв'язок між вузлами або комп'ютерами здійснюється через точки доступу. Точка доступу також виконує функцію бездротового адаптера Ethernet. Мережі Wi-Fi легко розгортаються на ринках, в офісах, аеропортах та інших місцях, забезпечуючи такі переваги, як гнучкість, мобільність, простота використання та низька вартість [7].

Таблиця 1

Основні специфікацій стандарту 802.11

Стандарт	Дата прийняття	Робоча частота, ГГц	Швидкість передачі	Робоча відстань, м	Вид модуляції	Застосування
802.11a	1999	5	54 Мбіт/с	120	DSSS, FHSS	WLAN
802.11b	1999	2.4	11 Мбіт/с	140	OFDM	WLAN
802.11g	2003	2.4	54 Мбіт/с	140	DSSS	WLAN
802.11n	2009	2,4/5	600 Мбіт/с	250	DSSS, OFDM	WLAN
802.11ac	2014	5	1 Гбіт/с	305	QAM	WLAN

Доступ до мереж Wi-Fi можна здійснити різними способами. Якщо мережа WLAN має бути спільною для декількох користувачів, ключ мережі зазвичай потрібно вводити вручну. Тому Android і Apple iOS розробили метод спільного використання мережі WLAN у смартфонах Android та iPhone. Пристрій Android генерує QR-код, який можна відсканувати іншими смартфонами Android для автоматичного приєднання до мережі. Функція Apple для спільного використання мережі WLAN базується на Bluetooth. Це працює лише в тому випадку, якщо Bluetooth увімкнено на обох пристроях і хоча б один інший iPhone поблизу підключений до відповідної мережі.

NFC (Near-Field Communication – технологія бездротового високочастотного зв'язку малого радіуса дії «в один дотик») може значно спростити цей процес, поділившись даними доступу через тег NFC. Щоб зберігати бездротову мережу під тегом NFC, необхідно мати ідентифікатор бездротової мережі SSID (Service Set Identifier) та пароль бездротової мережі. За замовчуванням ці дані зберігаються безпосередньо на маршрутизаторі. Сканування доступу до мережі WLAN за допомогою тегу NFC на пристроях з ОС Android здійснюється за вбудованими функціями читання міток NFC. Для iPhone потрібен сторонній додаток.

Аналіз методів атак на публічні WLAN.

Точка доступу керує технологією Wi-Fi через маршрутизатор, який забезпечує доступ до Інтернету кінцевих пристроїв користувачів. Безкоштовні точки доступу, як правило, працюють у загальнодоступній мережі, у якій функції автентифікації вимкнені, саме тому виникають такі стратегії захисту як, наприклад, «модель справедливості користувачів» - це модель платежів, яка може бути реалізована за допомогою розширеної функції розподіленої координації EDCF (Enhanced Distributed Coordination Function), що робить ревізію рівня MAC поточного стандарту IEEE 802.11, щоб розширити підтримку додатків локальної мережі, які мають вимоги QoS (Quality of Service) [4].

Кіберзагрози для мобільних пристроїв у громадському середовищі Wi-Fi включають: фінансові втрати, витік даних, крадіжку пароля чи особистої інформації тощо. При цьому в багатьох випадках виявити наявність нападу дуже важко, а то й неможливо. Це пояснюється відкритим характером підключення до точки доступу загальнодоступного Wi-Fi.

Незашифрований характер загальнодоступних Wi-Fi мереж та відсутність фізичного бар'єру для прийому всіх пакетів у мережі дають змогу зловмисникам анонімно приєднатися до мережі, перехоплювати пакети, перенаправляти трафік на свій тощо, а отже, забезпечувати відносно легкий доступ до даних інших користувачів.

Сніфінг (sniffing – нюхання) пакетів на сьогодні є найпростішим і прихованим методом перехоплення даних користувачів. У відкритій, незахищеній мережі пакети даних, призначені для конкретного користувача, фактично надсилаються незашифрованими всім іншим користувачам, підключеним до мережі. Існує кілька популярних інструментів, які дозволяють здійснювати пошук пакетів, наприклад: Wireshark, tcpdump. За допомогою вивчення HTTP-трафіку, пакети можна аналізувати та визначати пари логін/пароль, файли, миттєві повідомлення або будь-які інші незашифровані дані, надіслані через мережу. У відкритій мережі захист від сніфінгу пакетів майже відсутній, оскільки це абсолютно пасивна атака. Звичайному одержувачу ніяк не потрібно активно змінювати мережевий потік, а досить просто «слухати» трафік. Це також унеможливлює ідентифікацію «сніфера» технологічними засобами.

Спуфінгу (*spoofing – підробка*). Однією з ключових властивостей відкритих мереж стандартів 802.11 є те, що вони побудовані навколо середовища передачі даних, де будь-яка бездротова станція може передавати кадри й може прослуховувати всі інші кадри, що передаються в мережі. Ця властивість робить WLAN мережі сприйнятливими до спуфінгу та ін'єкційних атак. Основна ідея полягає в тому, що зловмисник може контролювати зв'язок між хостами в бездротовій мережі. Якщо комунікація не зашифрована належним чином, зловмисник може виявити стан сеансу шляхом прослуховування, а якщо зв'язок не автентифікований, він може потім ввести кадри в одну кінцеву точку сеансу, видаючи себе за іншу кінцеву точку сеансу.

Більшість протоколів, таких як DNS (Domain Name System), DHCP (Dynamic Host Configuration Protocol) і TCP (Transmission Control Protocol), сприйнятливі до цієї атаки. У разі DNS зловмисник може стежити за вихідними запитами DNS та вводити відповіді, що вказують на підконтрольний йому хост. Для TCP зловмиснику потрібно знати лише поточний стан з'єднання з точки зору порядкових номерів. Під час налаштування з'єднання він може навіть повністю взяти на себе з'єднання, ввівши відповідний SYN-ACK, у результаті чого законна кінцева точка буде не синхронізована. Ін'єкція також можлива в будь-який момент з'єднання, поки зловмисник може вчасно ввести спроби ін'єкції, щоб належним чином доставити сегменти TCP до мережевого стека жертви. Протокол DHCP може бути підробленим, щоб жертва використовувала IP-адресу та шлюз за замовчуванням, що дає зловмиснику повний контроль над усім його трафіком.

Підробка DNS дуже приваблива для такого виду атак, як фішинг, оскільки, наприклад, зловмисник може створити імітаційний банківський вебсайт, який би передавав маніпульовані запити на реальний сайт у режимі «людина посередині». У цьому випадку навіть двофакторна автентифікація не може допомогти. Подібним чином ін'єкція TCP може бути використана для вставлення інструкцій щодо переспрямування, реклами чи спаму на легальні в іншому випадку вебсторінки.

Сканування. Атака на зразок «*сканування*» використовується для визначення інших хостів у мережі. Таку атаку, зазвичай, важко виявити, і більшість загальнодоступних точок доступу не мають ресурсів для моніторингу такої діяльності. Існує кілька різних типів методів сканування, хоча кожен дотримується основного принципу надсилання певних типів пакетів на всі можливі IP-адреси в мережі та перевірки відповідей. За цими відповідями зловмисник може виявити конкретну інформацію про кінцеві пристрої користувачів, такі як операційна система або відкриті порти. Озброївшись цими знаннями, зловмисник може мати можливість розповсюджувати шкідливе програмне забезпечення, використовувати інший хост у атаці відмови в обслуговуванні (DoS) або виконувати іншу форму незаконної поведінки.

Атака MITM (*man-in-the-middle – людина посередині*) є складнішою за попередні та може спричинити більш серйозні наслідки. Ця атака ґрунтується на здатності хакера маніпулювати протоколом розрішення адрес (ARP – Address Resolution Protocol), який пов'язує IP-адреси з адресами Ethernet. Усі хости в мережі спілкуються через ARP і зберігають таблицю з адресами всіх інших хостів. Вразливість виникає через те, що будь-який хост може оголосити, що він пов'язаний із будь-якою IP-адресою, що дає змогу хосту видавати себе за іншого. Ця стратегія відома як підробка ARP, і є інструменти, які її реалізують.

Більш серйозна атака MITM може навіть обійти заходи, спрямовані на збереження конфіденційності даних, наприклад, надсилання даних за протоколом Secure Socket Layer (SSL). Діючи як тунель від початкової до кінцевої точки, SSL забезпечує рівень шифрування HTTP-трафіку. Однак зловмисник може зірвати цю систему, переконавши іншого хоста, що він є орієнтованим одержувачем вихідних даних. У наведеному вище прикладі зловмисник також запустив підробку системи доменних імен (DNS – Domain Name Service). Коли користувач робить перший запит, він запитує у DNS-сервера IP-адресу потрібного домена. Оскільки хакер бачить цей трафік першим, він відповідає користувачу своєю власною IP. Користувач ініціює безпечне з'єднання з хакером, який може розшифрувати його дані. Потім він повторно шифрує дані та надсилає на справжній вебсайт, імітуючи безпечне з'єднання.

За атаки на зразок *«шахрайські точки доступу» (RAP – Rogue access points)* зловмисник видає себе за допустиму точку доступу. Користувач може підключитися до цієї точки доступу, що надає зловмиснику повний доступ до всіх мережевих підключень цього користувача [8]. RAP виникають із нещодавно винайденої атаки «заперечення зручності»: користувачі очікують підключення до Інтернету, де б вони не були, і безкоштовно. Через цю вимогу забезпечення автентичності точки доступу є складним, оскільки це може перешкоджати можливості користувача швидко та прозоро підключатися до точки доступу в будь-яких умовах. У цьому випадку користувач підключиться до шахрайської точки доступу, але запити на передачу даних не пройдуть. Оскільки більшість смартфонів відключать широкосмугове з'єднання на користь Wi-Fi, це робить телефон нездатним приймати дані [10].

Відмова в обслуговуванні (DoS, Denial of Service). Як і атака «заперечення зручності» така має на меті перервати обслуговування кінцевих пристроїв. Атака DoS може або використовувати підробку, тактику MITM, або перевантаження мережі.

Використовуючи підробку, зловмисник змушує інших користувачів у мережі надсилати запити зловмиснику. Щоб виконати відмову в наданні послуги, зловмиснику не потрібно передавати пакети запиту цільовому одержувачу. У загальнодоступній точці доступу Wi-Fi користувач більше не матиме доступу до маршрутизатора, і як наслідок, весь мережевий трафік припиниться.

Недоліком загальнодоступного Wi-Fi є обмежена пропускна спроможність, яку він накладає на користувачів, особливо під час завантаженості [10]. У цьому випадку зловмисник може заповнити мережу фальшивими пакетами, по суті, зменшуючи корисну пропускну здатність. Користувачі помічають або дуже повільний, або взагалі відсутній мережевий трафік, що надходить і виходить із їхніх пристроїв. Може здатися, що зловмисника в цьому випадку було б легко ідентифікувати, однак зловмисник може підробити адресу відправника зловмисних пакетів. Зловмисник також може реалізувати атаку, коли термінал іншого користувача виступає як винний у здійсненні атаки.

Дослідження методів та технологій захисту публічних точок доступу Wi-Fi.

Переважно технології безпеки мобільних пристроїв у мережі Wi-Fi орієнтовані на забезпечення конфіденційності, цілісності та автентифікації. При цьому загрози для мобільних пристроїв при використанні мережі Wi-Fi, пов'язані переважно з ненадійними третіми

сторонами, що стоять за атакою, копіюванням, крадіжкою або зміною інформації. Кіберзлочинці завжди намагаються знайти шляхи доступу до мобільного пристрою. Бездротовий зв'язок є більш вразливим порівняно з дротовим. Тому дані, що передаються у відкритій мережі Wi-Fi, легко прослуховуються або викрадаються невідомою третьою стороною.

Метою технологій забезпечення конфіденційності є недопущення читання та збереження переданих даних мережею неправомірними особами. Контроль цілісності дає змогу виявляти будь-які навмисні або ненавмисні зміни даних, які відбуваються під час передавання, а автентифікація надає доступ до мережі лише правомірним особам.

Конфіденційність дротового еквівалента WEP (Wired Equivalent Privacy). У 1999 році Альянсом Wi-Fi для захисту конфіденційності даних у бездротовій мережі була сертифікована технологія WEP як частина оригінального стандарту 802.11. WEP використовує RC4 для шифрування та CRC-32 для перевірки цілісності даних. RC4 вимагає парольної фрази, яка складається з двох частин. Перша частина – статична, це загальнодоступний ключ PSK **(**Pre-Shared Key)**,** який потрібно ввести в налаштування конфігурації (зазвичай завдовжки 5 або 10 символів) кожного вузла перед підключенням до бездротової мережі. Друга частина – динамічна, це вектор ініціалізації IV (Initialization vector), який використовується для генерації ключа шифрування кожного пакета і змінюється в процесі функціонування мережі. Це значення надсилається заздалегідь до пакета даних у вигляді відкритого тексту, який одержувач використовує в процесі дешифрування. Однак IV не були унікальними і повторювались через деякі проміжки часу, після того, як вони були створені з використанням парольної фрази як однієї зі змінних. Зловмисники можуть витягувати ці повтори шляхом пасивного сніфінгу зашифрованих пакетів [3]. І, оскільки, керування ключами не передбачено і вектор ініціалізації повторюється, то декілька користувачів використовують однакові вектори і зловмисник перехопивши їх, отримує доступ до даних усіх користувачів.

WEP – найслабший метод шифрування порівняно з іншими технологіями конфіденційності. Однак він широко використовується протягом тривалого часу, оскільки доступний для всіх бездротових продуктів стандарту IEEE 802.11.

Захищений доступ Wi-Fi (WPA - Wi-Fi Protected Access) успадкував основний принцип WEP та усунув його недоліки. WPA використовує протокол цілісності тимчасового ключа (TKIP - Temporal Key Integrity Protocol) для створення ключа шифрування, який є динамічним та не підтримується WEP і використовує вектор ініціалізації довжиною 48 біт для постійної генерації нового ключа довжиною 128 біт для шифрування кожного окремого пакету. Тому навіть якщо зловмисник збирає багато пакетів, обчислити загальний ключ практично неможливо. WPA також створює контрольні суми за методом MIC (Message Integrity Code), коли в кожний кадр записується код цілісності повідомлення довжиною 8 байт для запобігання фальсифікації даних та автентифікації.

Захищений доступ Wi-Fi WPA2 (Wi-Fi Protected Access 2). У 2004 році був розроблений повний стандарт IEEE 802.11i під назвою WPA2, що усуває певні недоліки методу WPA.

WPA2 включає обов’язкову підтримку CCMP (Counter Mode with Cipher Block Chaining Message Authentication Code Protocol) на основі криптосистеми AES (Advanced Encryption Standard). Сертифікація WPA2 є обов’язковою для всіх нових пристроїв, що мають торговельну марку Wi-Fi. WPA2 забезпечує аутентифікацію, шифрування та перевірку цілісності даних, що є повноцінною програмою безпеки. Залежно від версії WPA, кінцевого користувача та використовуваного протоколу шифрування можна виділити різні режими WPA:

• режим WPA-Personal (WPA-PSK загальнодоступний ключ). Призначений для домашніх та невеликих офісних мереж і не потребує сервера аутентифікації. Кожен пристрій бездротової мережі аутентифікується точкою доступу з використанням 256-розрядного ключа, створеного за допомогою пароля або парольної фрази;

• режим шифрування WPA-Enterprise, призначений для корпоративних мереж Wi-Fi. Для забезпечення додаткової безпеки WPA-Enterprise потрібен сервер автентифікації RADIUS (Remote Authentication Dial In User Service - віддалений ідентифікаційний набір у службі користувача), що являє собою транспортний протокол, який використовується для захищеного віддаленого доступу користувачів до мережі із забезпеченням моделі AAA (авторизація, автентифікація та аудит (облік)). Фактично сервер RADIUS виконує функції із первинної аутентифікації користувачів, надання їм відповідних привілеїв та може бути налаштований для ведення журналу обліку (запису дій користувачів).

Захищений доступ Wi-Fi WPA3 (Wi-Fi Protected Access 3). WPA3 - це остання, оновлена реалізація WPA2. Сертифікація продуктів WPA3 триває з 2018 року. WPA3 надає функції для особистого та корпоративного використання такі, як 256-розрядний протокол Галуа/Режим лічильника GCMP-256 (Galois/Counter Mode Protocol), 384-розрядний режим автентифікації хешованих повідомлень HMAC (Hash-based Message Authentication Code) та 256-розрядний протокол цілісності багатоадресної розсилки BIP-GMAC-256 (Broadcast/Multicast Integrity Protocol Galois Message Authentication Code).

Хоча WPA3 є більш безпечним і всеосяжним, ніж WPA2, проте протокол WPA2 все ще буде підтримуватися та оновлюватися Альянсом Wi-Fi у найближчому майбутньому.

WPA3, у порівнянні зі стандартом WPA2, додатково забезпечує такі важливі функції:

• одночасну автентифікацію протоколу Equals. Ця функція дає змогу утворити безпечне з'єднання. Так, коли мережевий пристрій підключатиметься до точки доступу, то обидва пристрої спілкуватимуться для перевірки автентифікації та з'єднання. Навіть якщо пароль користувача слабкий, WPA3 забезпечує більш безпечне з'єднання за допомогою протоколу надання пристроїв Wi-Fi DPP (Device Provisioning Protocol);

• індивідуальне шифрування даних. Під час входу до загальнодоступної мережі WPA3 реєструє новий пристрій за допомогою системи DPP, яка дає змогу користувачам використовувати NFC-теги або QR-коди для доступу пристроїв у мережу. Захист WPA3 використовує шифрування GCMP-256 замість раніше використовуваного шифрування 128-біт;

• більш потужний захист від атак повним перебором. WPA3 захищає від автономного вгадування пароля, дозволяє користувачеві лише одну здогадку та змушує йог безпосередньо взаємодіяти з пристроєм Wi-Fi;

• підтримку великих розмірів ключів сеансів, зокрема до 192-розрядних ключів у випадках використання WPA3 ENT;

• наявність розширеного відкритого режиму Wi-Fi, що підвищує конфіденційність у відкритих мережах, запобігає пасивному снiфінгу, шифруючи трафік, навіть якщо пароль не використовується. Однак це не посилює безпеку, оскільки будь-хто може підключитися до мережі.

Особливості WPA3:

- наділений функцією шифрування фреймів управління одноадресної передачі. Це є запобіжником, наприклад неправомірної деавторизації клієнтів за наявності атаки «людина посередині» або для виведення клієнтів у системах IDS/IPS. Системи WIDS/WIPS характеризуються менш жорсткими способами запровадження політики для клієнтів і більше залежать від сповіщення системного адміністратора про точки доступу або несанкціоновані програми.

- наявність механізму автентифікації SAE, який забезпечує більш безпечну аутентифікацію на основі пароля та механізму узгодження ключів, навіть якщо паролі не відповідають вимогам складності, захищає від атак грубої сили та значно ускладнює небажане розшифрування сеансів під час або після сеансу (одного знання парольної фрази недостатньо для розшифрування сеансу);

- забезпечує перехід від особистого, підприємницького або розширеного режимів WPA3 до WPA2 для підключення клієнтів, які не підтримують WPA3.

Щоб мінімізувати незручності з боку користувачів та забезпечити поступовий шлях міграції до WPA3-Personal зі збереженням сумісності із пристроями, що підтримують лише WPA2-PSK, Wi-Fi Альянсом був визначений перехідний режим WPA3-Personal (WPA3-Personal Transition Mode). Оскільки SAE – це новий протокол аутентифікації Wi-Fi і не сумісний із PSK, встановлення WPA3-Personal вимагає, щоб кожен клієнтський пристрій підтримував WPA3-Personal, що порушує роботу пристроїв, які підтримують лише WPA2-Personal. Як тільки доступність WPA3-Personal досягне достатнього рівня серед клієнтських пристроїв, власники мереж повинні вимкнути режим переходу WPA3-Personal для досягнення всіх переваг WPA3-Personal.

Режим переходу WPA3-Personal підтримує аутентифікацію як WPA3-Personal, так і WPA2-Personal з тим самим ідентифікатором бездротової мережі SSID та паролем. Компроміс полягає в тому, що загальний пароль мережі WPA3-Personal можна визначити шляхом атаки на пристрій WPA2-Personal за допомогою простої атаки офлайн-словника. Атака WPA2-Personal може бути виконана пасивно на застарілому клієнтському пристрої, який підтримує лише WPA2-Personal, або більш складну активну атаку на пониження можна здійснити на клієнті, який підтримує WPA3-Personal.

Пасивна атака на застарілі клієнтські пристрої WPA2-Personal є такою ж, як і у застарілих мережах WPA2-Personal. Активна атака на клієнтський пристрій WPA3-Personal є складною і приносить зловмиснику порівняно небагато, якщо враховувати можливість простішої пасивної атаки на застарілих клієнтів. Зловмисник, який визначає пароль, може отримати доступ до мережі просто за допомогою вразливостей WPA2-Personal, незалежно від WPA3-Personal. Крім того, навіть після того, як ця атака буде успішною і зловмисник визначить пароль, клієнти, які підключаються до WPA3-Personal, однаково матимуть переваги від секретності пересилання, яку надає SAE, оскільки в цьому разі ключі шифрування трафіку залишатимуться невідомими, навіть якщо пароль відомий.

Узагальнені дані порівняння за певними ознаками технологій WEP, WPA, WPA2 та WPA3 наведені в табл. 2.

Таблиця 2

Порівняння протоколів безпеки WEP, WPA, WPA2 та WPA3

	WEP	**WPA**	**WPA2**	**WPA3**
Рік випуску	1999	2003	2004	2018
Криптосистема	RC4	TKIP із RC4	AES-CCMP	AES-CCMP(Personal) AES-GCMP(Enterprise)
Розмір сесійного ключа	40 біт	128 біт	128 біт	128 біт(Personal) 256 біт(Enterprise)
Тип шифру	потоковий	потоковий	блочний	блочний
Цілісність	CRC-32	MIC	CBC-MAC	CCMP-HMAC (Personal) GCMP-HMAC(Enterprise)
Автентифікація	WEP-Open WEP-Shared	WPA-PSK WPA-Enterprise	WPA2-Personal WPA2-Enterprise	SAE EAP
Управління ключами	-	чотиристоронє рукостискання	чотиристоронє рукостискання	ECDH, ECDSA, SAE

Бездротове шифрування OWE (Opportunistic Wireless Encryption). OWE – це технологія, яка дає змогу бездротовим пристроям встановлювати зашифровані з'єднання із загальнодоступними точками доступу Wi-Fi навіть без інформації про доступ до Wi-Fi. За допомогою OWE бездротовий пристрій та точка доступу автоматично шифрують з'єднання із загальнодоступними точками доступу Wi-Fi. У цьому випадку пристрої узгоджують унікальний ключ сеансу (PMK – Pairwise Master Key), який можна використовувати лише один раз. Цей ключ сеансу використовується замість мережевого ключа для

шифрування з'єднання Wi-Fi за допомогою протоколу блочного шифрування з кодом автентичності повідомлення WPA2 CCMP (Counter Mode with Cipher Block Chaining Message Authentication Code Protocol).

Незашифровані з'єднання Wi-Fi та з'єднання Wi-Fi, зашифровані за допомогою OWE, можна одночасно встановити на загальнодоступну точку доступу Wi-Fi. Це означає, що бездротові пристрої, які не підтримують OWE, можуть встановлювати незашифровані з'єднання з точкою доступу Wi-Fi без використання інформації про доступ до Wi-Fi.

Розширена відкрита аутентифікація Wi-Fi (EOA – Enhanced Open Authentication). Wi-Fi EOA – це протокол для шифрування сеансів Wi-Fi, які відбуваються в загальнодоступних мережах. Забезпечує захист у сценаріях, коли автентифікація користувача не потрібна, захист від пасивного прослуховування, не вимагаючи пароля або додаткових кроків для приєднання до мережі.

На основі OWE відкрита аутентифікація наділяє кожного користувача унікальним індивідуальним шифруванням, яке захищає обмін даними між пристроєм користувача та мережею Wi-Fi. EOA вимагає обміну ключами шифрування за схемою Діффі-Хеллмана. Після успішного обміну ключами, мережі виконують чотиристоронне рукостискання перед завершенням та увімкненням зашифрованого з'єднання.

Оскільки EOA базується на OWE, для неї характерні ті ж самі недоліки. Хоча OWE шифрує сеанси між користувачем та мережею Wi-Fi, вона не запускає процес автентифікації для жодної зі сторін. Це робить мережеве з'єднання сприйнятливим до атаки «злого близнюка», під час якого неправочинна сторона перейменовує свій пристрій, маскуючись під мережу Wi-Fi. Хоча EOA шифрує відкрите мережеве з'єднання Wi-Fi і краще, ніж повністю незашифрована мережа, Wi-Fi Alliance визнає, що ні користувач, ні мережа не перевірені. Навіть із EOA відкритої загальнодоступної мережі Wi-Fi несе ризик.

Підтримка WPA3, OWE та Enhanced Open.

Що стосується термінів, то широке впровадження WPA3 відбудеться не за один день, оскільки наразі підтримка WPA3 все ще є необов'язковою функцією для сертифікації Wi-Fi Alliance. Навіть якщо користувач купує пристрій з підтримкою WPA3, варто зважати на те, що мережа повинна підтримувати WPA3, щоб отримати будь-яке покращення безпеки, хоча пристрій WPA3 все одно зможе підключатися до мереж WPA2. Вдома користувач має контроль над мережею і може вибрати оновлення маршрутизатора та пристроїв до WPA3. Однак витрати на великі мережі можуть означати дуже довгий період впровадження WPA3 підприємствами. Це також може мати місце навіть для невеликих загальнодоступних точок доступу Wi-Fi, оскільки бездротовий Інтернет, зазвичай, не є доволі витратним, то провайдери не будуть витрачати додаткові кошти на поліпшення заходів безпеки.

Перше покоління підтримки WPA3 на клієнтських пристроях тільки розгортається. Android 10 має підтримку, але вона все ще знаходиться в бета-версії. Те саме стосується Apple, яка випустила підтримку WPA3 в iOS 13. В останніх версіях Windows 10 є підтримка WPA3-SAE, але його також повинен підтримувати драйвер пристрою мережного обладнання.

З урахуванням зазначених застережень можна стверджувати, що неповна підтримка WPA3 набагато цінніша, ніж універсальна та зріла підтримка WPA2.

Що стосується бездротового пристрою, наприклад, смартфона або ноутбука, то операційна система та драйвер пристрою Wi-Fi повинні підтримувати WPA3. Нижче наведені найбільш популярні користувацькі ОС та їх версії, з яких вводиться підтримка WPA3 та OWE:

– Windows 10: версія 1903 або пізніша підтримує WPA3, підтримка драйверів пристрою різна;

– macOS підтримує WPA3, починаючи з версії 10.15 (Catalina);

– iOS та iPadOS: підтримка WPA3 з версії 13 або пізнішої;

– Android: WPA3 був представлений з Android 10. Фактична підтримка може відрізнятися залежно від смартфона або планшета.

WPA3-Personal забезпечує режим переходу, що дозволяє поступово переходити до мережі WPA3-Personal, одночасно дозволяючи підключення пристроїв WPA2-Personal. Однак усі переваги WPA3-Personal реалізуються лише тоді, коли мережа знаходиться в лише в режимі WPA3.

Щодо Enhanced Open, то пристрої повинні мати розширену версію операційної системи для підтримки цієї технології. Наприклад, Android потребує мови дизайну інтерфейсу HAL 1.2 для запуску цієї функції, а також потрібна версія Android 10 та новіші версії.

Wi-Fi Enhanced Open можна розгортати в режимі переходу, що дозволяє поступово переходити з відкритої мережі до в Wi-Fi Enhanced Open без перешкод для користувачів Wi-Fi або операторів мережі. При цьому немає потреби в додатковій конфігурації з боку користувача.

Аналіз способів автентифікація IEEE 802.1X.

У сучасних бездротових локальних мережах існують такі основні способи автентифікації: автентифікація з відкритою системою та спільним ключем WPA; WPA2 із автентифікацією за допомогою загальнодоступних ключів; WPA та WPA2 із автентифікацією підприємства.

Ідентифікація відкритої системи - це найпростіший метод, який дозволяє будь-якому користувачеві аутентифікувати їх у точці доступу, доки пристрій знає ідентифікатор набору послуг (SSID) цієї мережі. Хоча SSID зазвичай надсилається як трансляція, його можна легко зрозуміти за допомогою пасивних методів перехоплення даних. Автентифікація за спільним ключем, який надано обом сторонам з'єднання, зазвичай використовується в бездротових мережах невеликого офісу. Як тільки ключі збігаються з ключами бездротової мережі, пристрій буде допущений до мережі. Аутентифікація за допомогою спільного ключа може використовуватися лише з шифруванням WEP, і тому не вважається безпечним методом надання доступу до мережі.

Для автентифікації відповідно до методів WPA (PSK) та WPA2 (Personal) Wi-Fi із захищеним доступом використовується попередньо розподілений ключ захисту. Аутентифікація WPA та WPA2 PSK є більш безпечною, ніж автентифікація за спільним ключем WEP. Ці методи дозволяють користувачам, які знають цей ключ, мати доступ до мережі.

У корпоративних методах автентифікації WPA та WPA2 використовується стандарт IEEE 802.1X, який є більш безпечним, ніж WPA та WPA2 з автентифікацією за допомогою загальнодоступних ключів. Вони реалізують фреймворк EAP (Extensible Authentication Protocol – розширений протокол аутентифікації), щоб дозволити аутентифікацію користувача на зовнішньому сервері автентифікації RADIUS. У цьому разі автентифікація користувачів здійснюється за допомогою власних облікових даних замість спільного ключа. Простіше кажучи, автентифікація 802.1X включає три сторони: користувача (мобільний пристрій), автентифікатор (мережа Wi-Fi підприємства) та сервер автентифікації (хост із програмним забезпеченням, що підтримує протоколи RADIUS та EAP). Перед тим як користувач звернеться до корпоративної мережі, автентифікатор буде працювати для перевірки облікового запису користувача або цифрового сертифіката користувача. Якщо облікові дані дійсні, користувач має доступ до мережі.

Погляд на безпеку кінцевих пристроїв з погляду користувачів.

Користувачі можуть вжити декількох кроків для забезпечення належного захисту своїх даних під час доступу до публічних точок доступу Wi-Fi. Звичайно, найкращий захід безпеки – це не надсилати конфіденційні дані через незахищену публічну мережу. Однак це не означає, що користувач повинен поступатися певною зручністю, наприклад, оплатою рахунку в кав'ярні, заради безпеки. Якщо конфіденційні дані необхідно надсилати за протоколом HTTP із загальнодоступної мережі, користувач повинен переконатися, що весь трафік зашифрований за допомогою захищеного рівня сокету SSL (Secure Sockets Layer) або забезпечується безпека транспортного рівня TLS (Transport Layer Security) протягом усього віддаленого з'єднання.

Наступний варіант для користувачів – надсилати дані через віртуальну приватну мережу VPN (Virtual Private Network). VPN дозволяє користувачеві спілкуватися через зашифрований канал із будь-якою іншою точкою Інтернету. Одним із недоліків використання VPN є додаткова вартість, оскільки більшість постачальників VPN стягують постійну плату за свої послуги. Крім того, користувачі повинні заздалегідь знати про особливості використання технологій VPN, а потім вжити заходів щодо встановлення програмного забезпечення та налаштування відповідної служби VPN. Щоб вирішити цю проблему, пропонується розгортання виділених маршрутизаторів до домашніх точок доступу, які б прозоро обробляли VPN-з'єднання.

Висновки. Проведені дослідження дають змогу зробити такі висновки:

1. Такі методи захисту загальнодоступних Wi-Fi мереж, як WEP та WPA є застарілими. Саме тому для забезпечення достатнього захисту бездротової мережі пропонується використання WPA2 у режимі Personal або Enterprise залежно від типу та структури мережі.

2. Обмежене використання новітнього рішення безпеки WPA3 пояснюється необхідністю оновлення як програмного, так і апаратного забезпечення з боку провайдерів та користувачів. Тому повноцінне використання даної технології поки не підтримується на більшості пристроїв, а отже, не є ефективним.

3. Можливість роботи в режимі переходу від WPA2 до WPA3 дозволяє забезпечити поступовий перехід та розповсюдження технології WPA3. Перевагою цього режиму є те, що його підтримують усі пристрої, які підтримують WPA2, а також новітні пристрої, які підтримують WPA3. Ось чому, найкращим рішенням для забезпечення належного рівня безпеки є саме режим переходу від WPA2 до WPA3.

4. Технології OWE і Wi-Fi Enhanced Open не є надійними засобами захисту бездротової мережі, адже забезпечують лише шифрування сеансу з'єднання користувача із бездротовою точкою доступу і не забезпечують при цьому автентифікації. Тому вони мають використовуватись у поєднанні з іншими технологіями, наприклад, разом з WPA2.

Список використаних джерел

1. Паляниця В. А. Теоретичні та прикладні аспекти радіотехніки, приладобудування і комп'ютерних технологій / В. А. Паляниця // Матеріали IV Міжнародної науково-технічної конференції : збірник тез доповідей. – Тернопіль : ФОП Паляниця В. А., 2019. – 377 с.

2. Шувалова Л. А. Методи захисту даних у WI-FI мережах Методи захисту даних у WI-FI мережах [Електронний ресурс] / Л. А. Шувалова // Наука і техніка Повітряних Сил Збройних Сил України. – 2011. – № 2. - С. 133-135. – Режим доступу: http://nbuv.gov.ua/UJRN/ Nitps_2011_2_35.

3. An overview of the Wi-Fi WPA2 vulnerability. (2017, Octovber 19) [Electronic recourse]. – Accessed mode: https://www.enisa.europa.eu/publications/info-notes/an-overview-of-the-wi-fi-wpa2-vulnerability.

4. Hong Zimeng. Security of Mobile Devices and Wi-Fi Networks [Electronic recourse]. 2015. – Accessed mode: https://www.theseus.fi/bitstream/handle/10024/94480/Security%20of%20Mobile%20Devices%20and%20Wi-Fi%20Networks.pdf?sequence=1&isAllowed=y.

5. Gessner C., Roessler A. LTE technology and LTE test. 2009. [Electronic recourse]. – Accessed mode: http://www.scribd.com/doc/49762490/3/LTE-background-story-the-early-days.

6. Raman B., Chebrolu K. Experiences with WiFi for Rural Internet in India (2007) [Electronic recourse]. – Accessed mode: http://cse.iitk.ac.in/users/braman/papers/2007-exp-dgp.pdf.

7. Юдін О. К. Захист інформації в мережах передачі даних : підручник / О. К. Юдін, Г. Ф. Конахович, О. Г. Корченко. – К. :ТОВ НВП "ІНТЕРСЕРВІС, 2009. – 724 с.

8. Brody R. G. Wi-Fi hotspots: secure or ripe for fraud? / R. G. Brody, K. Gonzales, D. Oldham // Journal of Forensic Investigative Accounting. – 2013. – Vol. 5(2). – Pp. 27-47.

9. Dondyk E. Denial of Convenience Attack to Smartphones Using a Fake Wi-Fi Access Point / E. Dondyk, Zou Cliff C. // The 10th Annual IEEE CCNC – Mobile Device Platform Applications. 2013.

10. Noor M. M. Current threats of wireless networks / M. M. Noor, W. H. Hassan // The Third International Conference on Digital Information Processing and Communications. – 2013. -Pp. 704-713.

11. Підпалий Р. І. Аналіз вразливості бездротової мережі Wi-Fi з новим протоколом захищеності WPA3 [Електронний ресурс] / Р. І. Підпалий, О. І. Романов // Перспективи телекомунікацій: збірник матеріалів міжнародної науково-технічної конференції. – 2020. – Режим доступу: http://conferenc.its.kpi.ua/proc/article/view/200855.

References

1. Palianytsia, V. A. (2019). Teoretychni ta prykladni aspekty radiotekhniky, pryladobuduvannia i kompiuternykh tekhnolohii [Theoretical and applied aspects of radio engineering, instrumentation and computer technology]. *Materialy IV Mizhnarodnoi naukovo-tekhnichnoi konferentsii – Proceedings of the IV International scientific and technical conference: collection of abstracts.* Palianytsia V. A.

2. Shuvalova, L.A. (2016). Metody zakhystu danykh u WI-FI merezhakh [Methods of data protection in WI-FI networks Methods of data protection in WI-FI networks]. *Nauka i tekhnika Povitrianykh Syl Zbroinykh Syl Ukrainy – Science and Technology of the Air Force of the Armed Forces of Ukraine, 2,* 133-135. http://nbuv.gov.ua/UJRN/Nitps_2011_2_35.

3. An overview of the Wi-Fi WPA2 vulnerability. (2017, Octovber 19). https://www.enisa.europa.eu/publications/info-notes/an-overview-of-the-wi-fi-wpa2-vulnerability.

4. Hong Zimeng. (2015). *Security of Mobile Devices and Wi-Fi Networks.* https://www.theseus.fi/bitstream/handle/10024/94480/Security%20of%20Mobile%20Devices%20and%20Wi-Fi%20Networks.pdf?sequence=1&isAllowed=y.

5. Gessner, C., Roessler, A. (2009). *LTE technology and LTE test.* http://www.scribd.com/doc/49762490/3/LTE-background-story-the-early-days.

6. Raman, B., Chebrolu, K. (2007, January). *Experiences with WiFi for Rural Internet in India*. http://cse.iitk.ac.in/users/braman/papers/2007-exp-dgp.pdf .

7. Iudin, O. K., Konakhovych, H.F., Korchenko, O.H. (2009). Zakhyst informatsiї v merezhakh peredachi danykh [Protection of information in data transmission networks]. TOV NVP "INTERSERVIS.

8. Brody, R.G, Gonzales, K., & Oldham, D. (2013). Wi-Fi hotspots: secure or ripe for fraud? *Journal of Forensic Investigative Accounting*, 5(2), 27-47.

9. Dondyk, E., & Zou, C.C. (2013). Denial of Convenience Attack to Smartphones Using a Fake Wi-Fi Access Point. *The 10th Annual IEEE CCNC- Mobile Device Platform Applications.*

10. Noor, M.M., & Hassan, W.H. (2013). Current threats of wireless networks. *The Third International Conference on Digital Information Processing and Communications* (pp. 704-713).

11. Pidpalyi, R.I., Romanov, O.I. (2020). Analiz vrazlyvosti bezdrotovoi merezhi Wi-Fi z novym protokolom zakhyshchenosti WPA3 [Analysis of the vulnerability of the wireless Wi-Fi network with a new security protocol WPA3]. *Perspektyvy telekomunikatsii: zbirnyk materialiv mizhnarodnoi naukovo-tekhnichnoi konferentsii – Perspectives of telecommunications: a collection of materials of the international scientific and technical conference*. http://conferenc.its.kpi.ua/proc/article/view/200855.

Отримано 27.01.2022

TECHNICAL SCIENCES AND TECHNOLOGIES

UDC 004.77.056(045)

Nataliia Frolova[1], Inna Mykhalchuk[2], Oleksandr Tyshchenko[3]

[1]Assistant of Computerized Information Security Systems Department,
National Aviation University (Kyiv, Ukraine)
E-mail: talaf@ukr.net. **ORCID iD:** https://orcid.org/0000-0001-7935-6496

[2]PhD in Technical science, Assistant of Cybersecurity and Information Protection Department
Taras Shevchenko National University of Kyiv (Kyiv, Ukraine)
E-mail: mykhalchuk.inna.kbzi@gmail.com. **ORCID:** https://orcid.org/0000-0002-1802-7653
ResearcherID: ABF-8615-2020. **SCOPUS Author ID:** 57188710011

[3]Student of the Master`s degree
National Aviation University (Kyiv, Ukraine)
E-mail: stischenk0@icloud.com

PROTECTION OF PUBLIC WI-FI SPOTS

Traffic on public wireless networks is mostly unencrypted. Most users are usually unaware of the risks involved, and providers of public Wi-Fi hotspots do not pay attention to this, focusing only on convenience and ease of user to access the network, while ignoring the protection of user data.

Cybercriminals effectively use existing security vulnerabilities in public Wi-Fi spots to intercept network traffic and steal sensitive data. To ensure effective counteraction to hacking, an important task is to analyze methods and technologies for detecting and combating such cybercrime attacks.

The literature and research reviews of public Wi-Fi spots shows that the justification for the feasibility and effectiveness of using a method or technology of protecting Wi-Fi spots depending on the type of threat, network structure and type is not given enough attention.

The aim of this work is to evaluate the effectiveness of modern methods and technologies of protecting public Wi-Fi networks based on the analysis of current threats and vulnerabilities and develop recommendations for their use in deploying and supporting various types and features of public Wi-Fi networks including user devices.

Based on the analysis of the most common vulnerabilities and threats of public Wi-Fi spots, features, advantages and disadvantages of currently used technologies and methods to ensure adequate protection of wireless networks, it was recommended to implement WEP, WPA, WPA2, WPA3 and OWE technologies depending on the type of user activity and amount of confidential information, the availability of support for a particular end-user protection technology and the relevance of security protocols provided by a particular security technology.

Keywords: *public Wi-Fi access points; standard; vulnerabilities; security methods; attacker; network security; information security.*

Table: 2. Fig.: 1. References: 11.

Фролова Н., Михальчук І., Тищенко О. Захист публічних точок доступу Wi-Fi. *Технічні науки та технології.* 2022. № 1(27). С. 123-135.