Міністерство освіти і науки України
Тернопільський національний технічний університет імені Івана Пулюя
(повне найменування вищого навчального закладу)
Факультет комп'ютерно-інформаційних систем і програмної інженерії
(назва факультету)
Кафедра кібербезпеки
(повна назва кафедри)

КВАЛІФІКАЦІЙНА РОБОТА

на здобуття освітнього ступеня

магістр
(освітній рівень)

на тему: "Розробка портативного пристрою для тестування безпеки бездротових мереж у межах етичного хакінгу"

Виконав: студент VI курсу, групи СБм-61

Спеціальності:
125 «Кібербезпека та захист інформації»
(шифр і назва напряму підготовки, спеціальності)
Матюк Данило Сергійович
підпис (прізвище та ініціали)

Керівник Деркач М.В.
підпис (прізвище та ініціали)

Нормоконтроль Стадник М.А.
підпис (прізвище та ініціали)

Завідувач кафедри Загородна Н.В.
підпис (прізвище та ініціали)

Рецензент Яцишин В.В.
підпис (прізвище та ініціали)

м. Тернопіль – 2025

Міністерство освіти і науки України
Тернопільський національний технічний університет імені Івана Пулюя

Факультет комп'ютерно-інформаційних систем і програмної інженерії
(повна назва факультету)
Кафедра кібербезпеки
(повна назва кафедри)

ЗАТВЕРДЖУЮ
Завідувач кафедри
_____ Загородна Н.В.
(підпис) (прізвище та ініціали)
«__» _____ 2025 р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ

на здобуття освітнього ступеня Магістр
(назва освітнього ступеня)
за спеціальністю 125 Кібербезпека та захист інформації
(шифр і назва спеціальності)
Студенту Матюк Данилу Сергійовичу
(прізвище, ім'я, по батькові)
1. Тема роботи Розробка портативного пристрою для тестування безпеки бездротових мереж у межах етичного хакінгу

Керівник роботи Деркач Марина Володимирівна, к.т.н., доц.
доцент кафедри КБ
(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)
Затверджені наказом ректора від « 24 » 11 2025 року № 4/7-1024
2. Термін подання студентом завершеної роботи 16.12.2025
3. Вихідні дані до роботи портативний пристрій для тестування безпеки бездротових мереж

4. Зміст роботи (перелік питань, які потрібно розробити)
Аналіз сучасного стану захисту бездротових мереж
Стандарти безпеки бездротових мереж та атаки на них
Розробка та експлуатація портативного пристрою для тестування безпеки бездротових мереж
Охорона праці та безпека в надзвичайних ситуаціях

5. Перелік графічного матеріалу (з точним зазначенням обов'язкових креслень, слайдів)
Актуальність дослідження. Мета, об'єкт, предмет дослідження. Завдання дослідження.
Наукова новизна та практичне значення. Стандарти бездротового зв'язку.
Програмні й апаратні інструменти тестування безпеки бездротового з'єднання.
Стандарти безпеки бездротових мереж та атаки на них.
Портативний пристрій для тестування безпеки бездротових мереж.
Тестування розробленого пристрою з використанням реальних сценаріїв атак.
Висновки.

6. Консультанти розділів роботи

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв
Охорона праці	Осухівська Г.М., к.т.н., зав. каф. КС		
Безпека в надзвичайних ситуаціях	Теслюк В.М., проректор з адміністративно-господарської роботи та будівництва		

7. Дата видачі завдання 19.09.2025 р.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів роботи	Термін виконання етапів роботи	Примітка
1.	Ознайомлення з завданням до кваліфікаційної роботи	19.09 – 20.09	Виконано
2.	Підбір джерел для аналізу в галузі дослідження	21.09 – 28.09	Виконано
3.	Опрацювання джерел в галузі дослідження	29.09 – 03.10	Виконано
4.	Розробка портативного пристрою для тестування безпеки бездротових мереж	04.10 – 18.10	Виконано
5.	Тестування розробленого пристрою з використанням реальних сценаріїв атак	19.10 – 29.10	Виконано
6.	Оформлення розділу «Аналіз сучасного стану захисту бездротових мереж»	30.10 – 09.11	Виконано
7.	Оформлення розділу «Стандарти безпеки бездротових мереж та атаки на них»	10.11 – 18.11	Виконано
8.	Оформлення розділу «Розробка та експлуатація портативного пристрою для тестування безпеки бездротових мереж»	19.11 – 29.11	Виконано
9.	Виконання завдання до підрозділу «Охорона праці та безпека в надзвичайних ситуаціях»	30.11 – 02.12	Виконано
10.	Оформлення кваліфікаційної роботи	03.12 – 07.12	Виконано
11.	Нормоконтроль	08.12 – 11.12	Виконано
12.	Перевірка на плагіат	12.12 – 14.12	Виконано
13.	Попередній захист кваліфікаційної роботи	15.12 – 16.12	Виконано
14.	Захист кваліфікаційної роботи	23.12.2025	

Студент _____ Матюк Д.С.
(підпис) (прізвище та ініціали)

Керівник роботи _____ Деркач М.В.
(підпис) (прізвище та ініціали)

АНОТАЦІЯ

Розробка портативного пристрою для тестування безпеки бездротових мереж у межах етичного хакінгу // Кваліфікаційна робота ОР «Магістр» // Матюк Данило Сергійович // Тернопільський національний технічний університет імені Івана Пулюя, факультет комп'ютерно-інформаційних систем і програмної інженерії, кафедра кібербезпеки, група СБм-61 // Тернопіль, 2025 // С. 74, рис. – 16, табл. – 4, кресл. – 17, додат. – 1.

Ключові слова: автентифікація, атака, безпека, тестування, WiFi.

У кваліфікаційній роботі магістра розроблено портативний пристрій для тестування безпеки бездротових мереж, що дає змогу проводити польові випробування, швидко розгортати точки атаки та мінімізувати час налаштування.

У першому розділі роботи представлені результати аналізу стандартів бездротового зв'язку, зокрема IEEE 802.11, IEEE 802.15.1, IEEE 802.15.4, стільникового зв'язку; та функціональних можливостей апаратних інструментів для тестування безпеки, таких як WiFi Pineapple, Flipper Zero; також описані інструменти тестування безпеки бездротового з'єднання, а саме Kali Linux, Aircrack-ng, Wifite, Reaver, PixieWPS, Kismet.

У другому розділі проведено дослідження стандартів безпеки бездротових мереж, зокрема WEP, WPA, WPA2, WPA3, на предмет відмінності алгоритмів шифрування та процедури автентифікації з захищеним доступом до бездротової мережі, оскільки саме ці механізми перешкоджають проведенню більшості атак.

У третьому розділі представлено розробку портативного пристрою, його функціональні можливості та тестування у межах етичного хакінгу з використанням реальних сценаріїв атак. Результати роботи підтверджують, що розроблений пристрій здатний автоматично виявляти бездротові мережі та підключені пристрої, проводити атаки, включаючи атаки деавтентифікації, спам-маяки, перевіряти стійкість до MitM-сценаріїв, а також клонувати мережі.

ABSTRACT

Development of a portable device for wireless network security testing within ethical hacking // Thesis of educational level "Master"// Danylo Matiuk // Ternopil Ivan Puluj National Technical University, Faculty of Computer Information Systems and Software Engineering, Department of Cybersecurity, group СБм-61 // Ternopil, 2025 // P. 74, figs. 16, tbls 4, drws 17, apps. – 1.

Keywords: authentication, attack, security, testing, WiFi.

In the master's qualification work, a portable device for wireless networks security testing was developed, which allows for field testing, rapid deployment of attack points, and minimizing setup time.

In first chapter, studies present the analysis results of wireless communication standards, including IEEE 802.11, IEEE 802.15.1, IEEE 802.15.4, cellular communication; and functionality of hardware tools for security testing, such as WiFi Pineapple, Flipper Zero; wireless connection security testing tools are also described, namely Kali Linux, Aircrack-ng, Wifite, Reaver, PixieWPS, Kismet.

In second chapter, studies examine wireless network security standards, specifically WEP, WPA, WPA2, and WPA3, focusing on differences in encryption algorithms and authentication mechanisms that ensure secure access to wireless networks, as these mechanisms prevent many common attacks.

In third chapter, studies present the development of a portable device, its functionality, and testing within ethical hacking using real attack scenarios.

The work results confirm that the developed device is capable of automatically detecting wireless networks and connected devices, conducting attacks, including deauthentication attacks, spam beacons, testing resistance to MitM scenarios, and cloning networks.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СИМВОЛІВ, ОДИНИЦЬ, СКОРОЧЕНЬ І ТЕРМІНІВ

AES	—	Advanced Encryption Standard
AES-CMAC	—	AES Cipher-based message authentication code
ANonce	—	Authenticator Nonce
AP	—	Access Point
BSSID	—	Basic Service Set Identifier
CBC	—	Cipher Block Chaining
CCMP	—	Counter Mode with CBC Message Authentication Code Protocol
DoS	—	Denial of Service
DSSS	—	Direct Sequence Spread Spectrum
EAP	—	Extensible Authentication Protocol
EAP-PSK	—	Pre-Shared Key
EAP-TLS	—	Transport Layer Security
EAP-TTLS	—	Tunnelled Transport Layer Security
ECDSA	—	Elliptic Curve Digital Signature Algorithm
IoT	—	Internet of Things
ISM	—	Industrial, Scientific, Medical
GCMP	—	Galois/Counter Mode Protocol
GSM	—	Global System for Mobile Communications
HMAC	—	Hash-based message authentication code
KRACK	—	Key Reinstallation Attack
LEAP	—	Lightweight Extensible Authentication Protocol
LTE	—	Long-Term Evolution
MAC	—	Message Authentication Code
MIC	—	Message Integrity Check
PMF	—	Protected Management Frames
PMK	—	Pairwise Master Key
PMKID	—	Pairwise Master Key Identifier Dump
PSK	—	Pre-Shared Key

PTK	—	Pairwise Transient Key
RADIUS	—	Remote Authentication Dial-In User Service
RSSI	—	Received Signal Strength Indicator
SAE	—	Simultaneous Authentication of Equals
SNonce	—	Supplicant Nonce
SSID	—	Service Set Identifier
STA	—	Station Mode
TKIP	—	Temporal Key Integrity Protocol
UART	—	Universal Asynchronous Receiver-Transmitter
WEP	—	Wired Equivalent Privacy
Wi-Fi	—	Wireless Fidelity
WLAN	—	Wireless Local Area Network
WPA	—	Wi-Fi Protected Access
WPAN	—	Wireless Personal Area Network
WPS	—	Wifi Protected Setup

ВСТУП

Актуальність теми. Сучасні бездротові мережі є ключовими каналами обміну даними, але водночас залишаються одними з найвразливіших елементів корпоративних і побутових систем безпеки. Загрози безпеці у бездротових мережах, згідно з міжнародними дослідженнями в галузі кібербезпеки, поступово входять до найпоширеніших векторів атак, оскільки тільки за останній рік кількість зареєстрованих інцидентів збільшилась на 45%. Тому тестування безпеки необхідно для виявлення можливості доступу до мережі чи системи, що призводить до порушення конфіденційності та цілісності даних. До того ж все більше організації використовують бездротове з’єднання для критично важливих операцій, тому значення пристроїв у практиці етичного хакінгу для ретельної оцінки безпеки пропорційно зростає. Отже розробка портативних пристроїв для тестування безпеки бездротових мереж актуальна для використання в різних галузях, оскільки це доступне та портативне рішення для швидкої оцінки безпеки у бездротових мережах у реальних умовах, особливо корисне для навчальних закладів, державних підприємств, малих фірм, які не мають власних фахівців або ресурсів для регулярного тестування мережевих з’єднань на проникнення.

Метою кваліфікаційної роботи магістра є розробка портативного пристрою для тестування безпеки бездротових мереж, який надає змогу проводити польові випробування, швидко розгортати точки атаки та мінімізувати час налаштування.

Для досягнення визначеної мети поставлені наступні **задачі**:

– проаналізувати стандарти бездротового зв’язку, зокрема IEEE 802.11, IEEE 802.15.1, IEEE 802.15.4 та стільниковий зв'язок;

– провести огляд інструментів тестування безпеки бездротового з'єднання, а саме Kali Linux, Aircrack-ng, Wifite, Reaver, PixieWPS, Kismet;

– проаналізувати функціональні можливості апаратних інструментів для тестування безпеки, таких як WiFi Pineapple, Flipper Zero;

– дослідити стандарти безпеки бездротових мереж, зокрема WEP, WPA, WPA2, WPA3, та атаки на них;

– розробити портативний пристрій для тестування безпеки бездротових мереж у межах етичного хакінгу;

– провести тестування розробленого пристрою з використанням реальних сценаріїв атак.

Об’єкт дослідження – пристрій для тестування безпеки бездротової мережі.

Предмет дослідження – стандарти, протоколи та інструменти тестування безпеки бездротового з'єднання.

Наукова новизна отриманих результатів полягає у впровадженні повного комплексу пентест-інструментів від сканування до етичного хакінгу на енергоефективній мікропроцесорній платформі, що мінімізує апаратні ресурси та фінансові витрати.

Практичне значення отриманих результатів полягає у розробленні зручного у використанні пристрою, що вирішує актуальну проблему – тестування безпеки, зокрема він дозволяє оперативно перевірити безпеку бездротових мереж у будь-якому місці; забезпечує зниження ризиків витоку даних шляхом швидкої діагностики вразливостей та може бути використаний як: навчальний інструмент для курсів з кібербезпеки, польовий пристрій для аудитів безпеки, інтегрований компонент систем моніторингу підприємств або смарт-будівель.

Апробація результатів кваліфікаційної роботи. Основні результати проведених досліджень представлені на: XIV Міжнародній науково-практичній конференції молодих учених та студентів «Актуальні задачі сучасних технологій» (м. Тернопіль, Україна), XI Міжнародному Форуму «ІТ-Ідея 2025» (м. Київ, Україна), а також отримано 1 місце у ІІІ-му конкурсі стартапів ТНТУ «International Global Innovation Research» – 2025.

Публікації. За темою кваліфікаційної роботи магістра з викладенням її основних результатів опубліковано 2 тез в збірниках матеріалів науково-практичних конференцій (Додаток А).

РОЗДІЛ 1 АНАЛІЗ СУЧАСНОГО СТАНУ ЗАХИСТУ БЕЗДРОТОВИХ МЕРЕЖ

1.1 Стандарти бездротового зв’язку

Бездротові мережі можуть бути розгорнуті та працювати у різних середовищах: комерційних, урядових, освітніх, а також у звичайних житлових будинках. До того ж технології бездротової передачі сигналу особливо сприяють концепції Інтернету речей (IoT), на яку переходять все більше пристроїв, що підвищують наш комфорт перебування в Інтернеті [1-3].

В результаті кількість бездротових мереж, як і кількість об'єктів для атак, буде тільки збільшуватися [4,5]. Клієнти та організації повинні розуміти всі ризики використання бездротових мереж та знати, як зловмисники атакують ці системи. Пентестери повинні гарантувати, що ці мережі мають необхідну кількість елементів керування безпекою та у їхній конфігурації відсутні помилки.

Стандарти та технології бездротового зв'язку, такі як Wi-Fi, ZigBee, Bluetooth, WiMAX, LoRaWAN та радіочастотний спектр, керуються протоколами та конфігураціями так само, як і провідна мережа, а для передачі даних між точкою доступу та підключеними мережами/пристроями використовують загально узгоджені протоколи, найпопулярніші з них IEEE 802.11, IEEE 802.15.1, IEEE 802.15.4 та стільникового зв'язку (GSM, 4G LTE, 5G) [6].

Основна увага фахівців зосереджена на ідентифікації цільової мережі та отриманні доступу, проте мобільність, вартість, простота встановлення викликають швидкозростаючий інтерес розробників радіоелектронної апаратури, оскільки це є суттєвими перевагами перед дротовим зв’язком. Ще одним критерієм, що впливає на вибір технології, є радіус дії, який варіюється від кількох метрів до кількох тисяч кілометрів, в разі використання супутникового зв’язку, в залежності від розташування передавача і приймача бездротового сигналу. Існує велика різноманітність приймально-передавальних

радіотехнічних пристроїв, тобто модулів для кожної бездротової технології передачі даних.

1.1.1 Стандарт IEEE 802.11

Базовий стандарт IEEE 802.11, що регулює бездротову мережу, представляє собою набір протоколів, який був вперше розроблений Інститутом інженерів з електротехніки та електроніки (IEEE) для зручності використання та можливості швидкого підключення пристроїв. У початкових стандартах, опублікованих 1997 року, питання безпеки не розглядалися.

Стандарт IEEE 802.11 визначає протоколи, що необхідні для організації WLAN. Основні з цих протоколів: управління доступом MAC (Medium Accsess Control) до середовища на нижньому підрівні канального рівня і специфікації фізичного шару PHY. В якості останнього допускається використання інфрачервоного випромінювання та радіохвиль.

З того часу до стандарту було внесено поправки, перша з яких вплинула на бездротову мережу стандарту 802.11b, знаний також як Wi-Fi. Це найпоширеніший стандарт, запроваджений у 1999 році, завдяки своїй до 11 Мбіт/с високій швидкості передачі даних, що практично еквівалентна пропускній спроможності Ethernet - звичайних провідних локальних мереж, а також завдяки орієнтації на опанований радіочастотний діапазон 2,4 ГГц. В якості базової радіотехнології в ньому застосовується метод DSSS з 8-розрядними послідовностями Уолша. Так як обладнання працює на 11 Мбіт/с (максимальна швидкість) та має менший радіус дії, ніж на нижчих швидкостях, стандартом 802.11b при погіршенні якості сигналу передбачено автоматичне зниження швидкості.

Основні стандарти, які позначаються як Wi-Fi 4, 5, 6 і 6E, і відрізняються поколіннями, є Wi-Fi 4 (802.11n), Wi-Fi 5 (802.11ac), Wi-Fi 6 (802.11ax) та найновіший стандарт, що використовує діапазон 6 ГГц, — Wi-Fi 6E (табл. 1.1). У зв’язку з тим, що стандарт 802.11 використовує радіосигнали, у певних регіонах передбачені різні закони та правила щодо роботи бездротових мереж.

Таблиця 1.1 – Популярні стандарти Wi-Fi

Стандарт	Назва покоління	Частотні діапазони	Максимальна швидкість (Мбіт/с)
802.11b	—	2,4 ГГц	до 11
802.11a	—	5 ГГц	до 54
802.11g	—	2,4 ГГц	до 54
802.11n	Wi-Fi 4	2,4 ГГц, 5 ГГц	до 600
802.11ac	Wi-Fi 5	5 ГГц	до 6933
802.11ax	Wi-Fi 6	2,4 ГГц, 5 ГГц	до 9608
802.11ax	Wi-Fi 6E	2,4 ГГц, 5 ГГц, 6 ГГц	до 9608
802.11be	Wi-Fi 7	2,4 ГГц, 5 ГГц, 6 ГГц	до 30000

Загалом, є лише кілька типів елементів керування безпекою, вбудованих у стандарт 802.11, та пов'язані з ним поправки.

1.1.2 Стандарт IEEE 802.15.1

Стандарт IEEE 802.15.1, відомий як технологія Bluetooth, базується на наборі специфікацій Bluetooth v1.x, які активно просуваються консорціумом Bluetooth SIG. Він призначений для побудови WPAN.

Фактично технологія Bluetooth визначає функціонування компактних систем зв'язку на відносно невеликих відстанях між мобільними ПК, телефонами та різними портативними пристроями.

Цей недорогий радіоінтерфейс з низьким енергоспоживанням, потужність передавача якого близько 1 мВт, використовується для організації персональних мереж, які забезпечують в реальному часі передачу як звукових сигналів, так і цифрових даних. Спершу дальність дії радіоінтерфейсу закладалася приблизно на рівні 10 метрів, а саме в межах однієї кімнати, однак тепер специфікаціями Bluetooth визначено вже і іншу зону приблизно 100 м, тобто для покриття стандартного будинку або поза ним. При цьому немає необхідності для того, щоб пристрої перебували в прямій видимості один одного, їх можуть розділяти "радіопрозорі" перешкоди (стіни, меблі та т.п.), і до того ж прилади можуть знаходитися в русі. Для роботи Bluetooth застосовується діапазон ISM на нижній

частоті 2,45 ГГц, яка призначена для роботи медичних, промислових та наукових приладів.

Технологія Bluetooth працює в якості багатоточкового радіоканалу, керованого, так само як стільниковий зв'язок GSM, який теж є багаторівневим протоколом. Як заходи захисту в Bluetooth передбачено кодування даних, що передаються, та виконання процедур авторизації пристроїв. При цьому можливі три рівні захисту:

– мінімальний - дані приймаються різними пристроями без обмежень і кодуються загальним ключем;

– на рівні пристроїв - безпосередньо у чіпі прописується рівень доступу, відповідно до якого пристрій може отримувати деякі дані від різних пристроїв;

– лише на рівні сеансу зв'язку - дані кодуються 128-бітними випадковими числами, що зберігаються для кожної пари пристроїв, які у певному сеансі зв'язку приймають участь.

1.1.3 Стандарт IEEE 802.15.4

IEEE 802.15.4, відомий як технологія ZigBee, орієнтований безпосередньо на застосування, як засіб зв'язку між автономним обладнанням та приладами. В межах корпоративного сектору це, наприклад, складські системи, системи автоматизації виробництва, сенсори, електронні мітки, різні датчики, сервоприводи, а серед домашніх умов – системи безпеки, кондиціювання, освітлення, ПК, радіофіковані іграшки, ігрові приставки, в тому числі пульти віддаленого керування [7,8].

IEEE 802.15.4 окреслює PHY та MAC, що пропонують підтримку різних топологій мереж. Схеми мережної маршрутизації покликані забезпечити збереження енергії та найкоротші затримки, що укладаються в гарантований часовий інтервал, а за рахунок наявності кількох маршрутів до кожного вузла в мережах ZigBee передбачено запобігання можливості "збою в одній точці".

Ключові функції PHY включають контроль за якістю ланок та енергією, а ще для успішного існування з іншими мережами бездротових операторів оцінку

каналів. Підтвердження отримання пакетів визначається автоматично протоколом MAC, що забезпечує можливість передачі даних у конкретні часові інтервали та підтримує 128-бітові функції-безпеки AES. Якщо в межах досяжності пристроїв ZigBee виявиться обладнання Wi-Fi або Bluetooth, в якості тунеля для трафіку ZigBee будуть використані їх канали.

IEEE 802.15.4 працює на невеликій дальності дії (близько 10 метрів) та пропускній спроможності каналу - до 250 кбіт/с в діапазоні 2,4 ГГц. Невелика потужність і швидкість обумовлені малими енергоресурсами пристроїв, що зв'язуються. Також передача швидкості може вестись в діапазонах 858 МГц (20 кбіт/с) та 902-928 МГц (40 кбіт/с).

Даний стандарт, що активно просувається організацією Альянсом ZigBee, заповнить вакуум у спектрі бездротових мережевих технологій, оскільки він пропонує розробникам можливість створювати недорогі продукти з дуже низьким споживанням потужності та надзвичайно гнучкими функціями підтримки бездротових мереж.

1.1.4 Стандарти стільникового зв’язку

Еволюція бездротового стільникового зв'язку представлена на рисунку 1.1 [9].

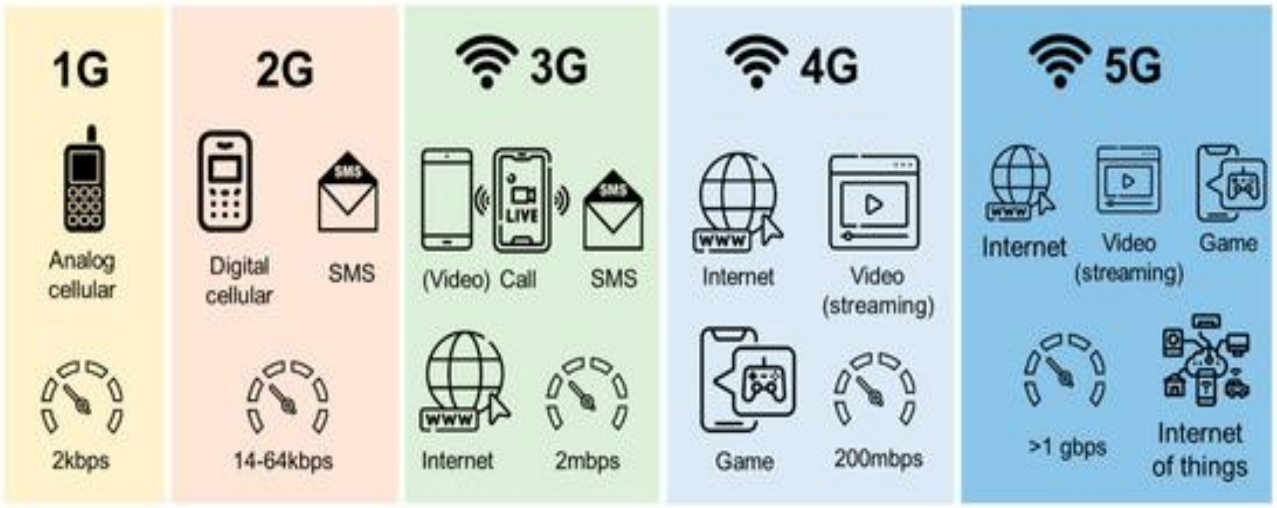


Рисунок 1.1 – Еволюція мережі мобільного зв'язку

1G або перше покоління – аналогова система бездротового доступу – в першу чергу було для голосового трафіку.

Незабаром 1G була замінена технологіями 2G або другого покоління, що представляли перехід з аналогової радіомережі на цифрову. Цифрова технологія, яка спрощує калібрування та обслуговування, побудована на повторному відтворенні бінарних сигналів у порівнянні з безперервними аналоговими сигналами, а отже, вона дешевше за аналогові пристрої. Стандарт GSM повністю цифровий, хоча розроблений у 80-х роках минулого сторіччя, та належить до мереж другого покоління. Активно стандарт GSM почали впроваджувати з 1991 року у багатьох країнах світу. Він підтримує 4 діапазони роботи GSM: 850, 900, 1800 для країн Європи та Азії, 1900 для таких країн, як США, Канада, окремих країн Латинської Америки та Африки. В Україні більшість мобільних телефонів, що продаються, працюють у трьох стандартах зв'язку (900, 1800 та 1900 МГц.). Насьогодні оператори понад 200 країн та територій застосовують стандарт GSM. За даними асоціації GSM (GSMA) ці мережі покривають близько 82 % світового ринку мобільного зв'язку.

Кращої спектральної ефективності по широкосмугових стільникових мережах досягають технології 3G, які не лише мають вищу швидкість передачі даних, а й надають розширені послуги.

LTE належить до стандарту бездротового широкосмугового зв'язку 4 покоління або технології 4G. Цей стандарт зв'язку для мобільних пристроїв, терміналів даних й смартфонів. Стандарт бездротової високошвидкісної передачі даних LTE має високий рівень безпеки для мобільних телефонів та будь-яких терміналів, які працюють з даними, що засновані на мережевих технологіях UMTS/HSPA та GSM/EDGE, що збільшують швидкість та пропускну здатність внаслідок застосування іншого радіоінтерфейсу спільно з покращенням ядра мережі. Бездротовий інтерфейс LTE за сигналами та протоколами є несумісним з 2G/3G. Стандарт LTE надає швидкість завантаження до 3 Гбіт/сек, а затримка може бути знижена до 2 мілісекунд.

5G або п'яте покоління мобільного зв'язку, яке засноване на стандартах телекомунікацій (5G/IMT-2020), є новим поколінням. Технології 5G в порівнянні

з технологіями 4G забезпечують більш високу пропускну здатність, що дає можливість використовувати режими прямого з'єднання між абонентами (device-to-device), швидкість інтернету приблизно 1-2 Гбіт/сек, менший час затримки, більшу доступність широкосмугового мобільного зв'язку, менші витрати енергії батареї, ніж 4G-обладнання, а також є наднадійними масштабними системами комунікації між пристроями.

1.2 Аналіз інструментів тестування безпеки бездротового з'єднання

Оскільки кількість кібератак зростає, організаціям необхідно приділяти велику увагу тестуванню на проникнення і моніторити свою бездротову мережу, щоб запобігти можливій серйозній шкоді.

Для забезпечення безпеки фахівці з безпеки, зокрема етичні хакери, повинні покладатися на інструменти безпеки і злому, які допомагають мінімізувати час тестування, ефективно контролювати і виконувати пентестінг в бездротовій мережі задля її захисту.

1.2.1 Aircrack-ng

Kali Linux – це спеціалізований дистрибутив на базі Debian, створений для фахівців з інформаційної безпеки. Він поставляється з сотнями інструментів для аналізу мереж, тестування програм, пошуку вразливостей та проведення аудитів безпеки. Головна відмінність Kali у тому, що він є робочим середовищем для етичного хакінгу. Тобто, для легального тестування на замовлення компаній, щоб захистити їх від реальних атак. До складу інструментів Kali Linux входить кілька інструментів, що працюють як з командного рядка, так і базового графічного інтерфейсу. Ці інструменти можна використовувати для перетворення мережного інтерфейсу на мережевий монітор, захоплення трафіку та зворотного пароля автентифікації (рис. 1.2).

Перший із цих інструментів є Aircrack-ng. Це набір інструментів, що дають змогу пентестерам перевірити рівень безпеки бездротових мереж [10].

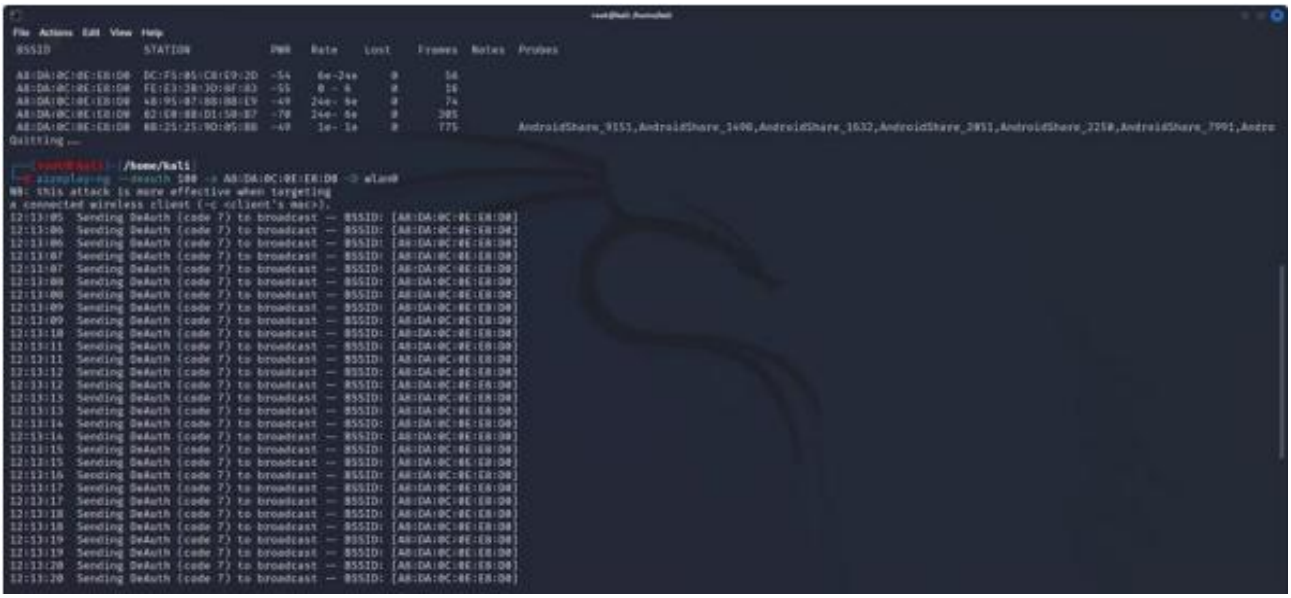


Рисунок 1.2 – Приклад використання атаки деавтентифікації на Kali Linux

Пакет містить інструменти для наступних завдань.

– Моніторинг. Це інструменти, що розроблені спеціально для сніфінгу з метою аналізу в подальшому, для цього використовуючи інше програмне забезпечення, наприклад Wireshark.

– Атаки. Інструменти експлуатації атаки для цільових мереж. До них належать такі засоби, які дозволяють проводити атаку в процесі автентифікації. Aircrack-ng на момент експлуатації атаки проводить ін'єкції пакетів, що були відправлені в потік даних як точці доступу, так і клієнтам.

– Тестування. Такі інструменти надають можливість проводити тестування бездротових карт.

– Злом. Також Aircrack-ng вміє зламувати бездротові ключі, що знайдені напередодні у протоколах WEP/WPA/WPA2.

Крім інструментів, які працюють у командному рядку, він також застосовується серед інструментів із графічним інтерфейсом.

1.2.2 Wifite

Wifite – автоматизований інструмент тестування бездротових мереж на проникнення, що використовує засоби з набору Aircrack-ng та інструменти командного рядка Reaver та PixieWPS.

Reaver призначений для вибірки піна WPS шляхом перебору. Кінцевою метою є розшифрування пароля WPA/WPA2. Reaver був розроблений як надійний та практичний засіб для боротьби з WPS, і був протестований на широкому спектрі точок доступу та реалізацій WPS. У середньому Reaver відновлює текстову парольну фразу WPA/WPA2 цільової точки доступу за 4-10 годин, залежно від точки доступу. На практиці, як правило, знадобиться вдвічі менше часу, щоб підібрати правильний PIN-код WPS та відновити парольну фразу.

PixieWPS – це автономний інструмент грубої сили, який використовується для зворотного виведення бездротової точки доступу WPS. Назва PixieWPS походить від атаки Pixie-Dust, яка була виявлена Домініком Бонгардом (Dominique Bongard). Ця вразливість дозволяє застосувати грубу силу WPS PIN. Щоб PixieWPS працював правильно, необхідно мати таку інформацію: відкритий ключ реєстрації, відкритий ключ користувача, отриманий хеш-1, отриманий хеш-2, ключ сеансу автентифікації, спеціальне слово. Оскільки потрібно стільки компонентів, PixieWPS часто запускається як частина іншого інструменту, наприклад Wifite.

Wifite може захопити трафік, розірвати зв'язок, простежити за новим підключенням та здійснити перевірку справжності логіна та пароля для бездротових мереж типу WEP, WPA та WPS.

1.2.3 Kismet

Kismet — це консольний детектор і є комбінацією сканера, системи виявлення вторгнень IDS/IPS і пакетного аналізатора трафіку бездротових мереж 802.Q1 рівня 2 [11]. Він ідентифікує мережі шляхом пасивного сніфінгу та може розкривати приховані (немаякові) мережі, якщо вони використовуються (рис. 1.3). Він може автоматично виявляти блокування IP-адрес мережі шляхом сніфінгу пакетів TCP, UDP, ARP та DHCP, реєструвати трафік у форматі, сумісному з Wireshark/tcpdump, і навіть відображати виявлені мережі та приблизні діапазони на завантажених картах.

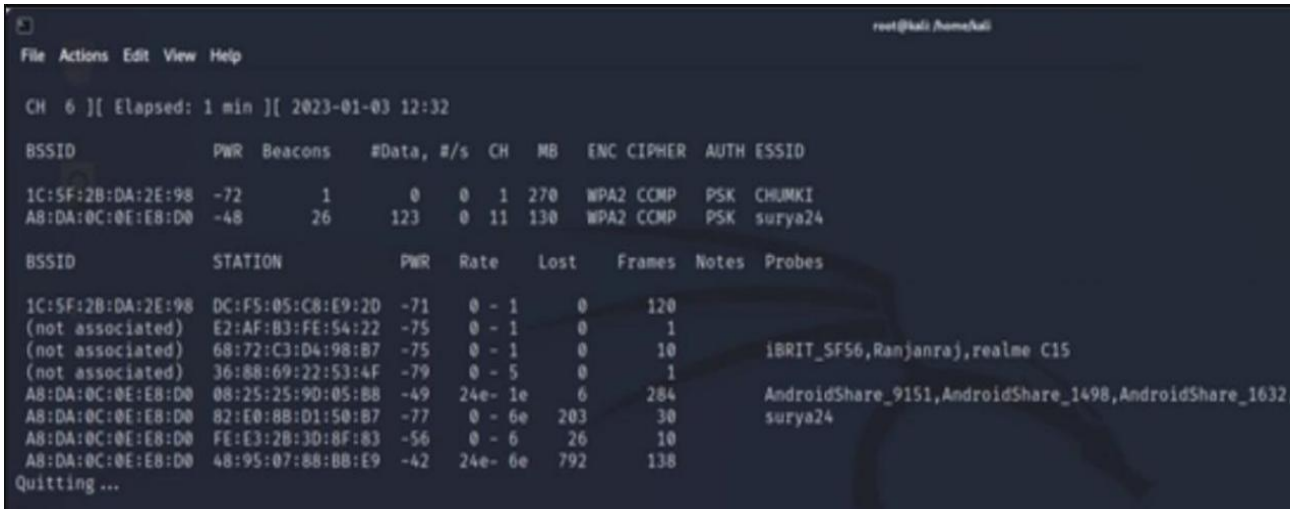


Рисунок 1.3 – Приклад використання Kali Linux для аналізу підключених пристроїв до точки Wi-Fi

Kismet також встановлений в Kali Linux 2 за замовчуванням, написаний на C++, пропонує додаткові функції, які зазвичай не зустрічаються в інструментах, що запускаються з командного рядка.

1.3 Пристрої для проведення етичного хакінгу

Різноманітність мережевих протоколів для ефективного захисту вимагають багаторівневих контрзаходів, які охоплюють як пасивні, так і активні вектори атак.

Таким чином необхідно комбінування програмних й апаратних інструментів, що здатні перевіряти рівень захищеності точок доступу, клієнтських пристроїв, контролерів, виявити вразливості бездротових мереж. Для цієї мети використовують сканери вразливостей, фреймворки пентестінгу та аналізу трафіку, які виявляють конфігураційні похибки й відомі CVE.

Крім програмних сканерів і фреймворків, у практиці етичного хакінгу активно застосовуються готові апаратні платформи. Вони дають змогу проводити польові випробування, швидко розгортати точки атаки та мінімізувати час налаштування.

Найбільш поширені з таких рішень – WiFi Pineapple та Flipper Zero.

1.3.1 WiFi Pineapple

WiFi Pineapple - пристрій, розроблений компанією Hak5, для авторизованих та комплексних аудитів бездротових мереж IEEE 802.11, включаючи тести на проникнення.

Хоча на ринку є безліч інструментів кібербезпеки, які можуть працювати так само добре, WiFi Pineapple є однією з найпотужніших платформ завдяки можливостям пристрою та простоті використання, що спеціально розроблена для оцінки безпеки Wi-Fi. Він дозволяє користувачам шукати та знаходити вразливості в бездротових мережах, аналізувати та ідентифікувати потенційні цілі, а також оперативно вживати коригувальних заходів до того, як мережа буде скомпрометована.

Пристрій також надає у своєму вебінтерфейсі набір модулів, які можна налаштувати та використовувати для розвідки, проникнення в мережу, відстеження, реєстрації та звітності про активність цих мереж, а також для експлуатації більшості атак і оцінки безпеки Wi-Fi.

Пристрій набирає популярності завдяки доступній ціні та всім програмам та модулям, які можна безкоштовно завантажити з вебінтерфейсу WiFi Pineapple. Його унікальний дизайн та розмір дозволяють користувачам виконувати будь-які його функції будь-де та непомітно носити пристрій. Має складну технічну архітектуру, оскільки він поєднує цільовий програмний стек зі спеціалізованим обладнанням.

Апаратне забезпечення: чотирьохядерний процесор, двохдіапазонні радіомодулі (2,4 ГГц та 5 ГГц), зовнішні, високопідсилювальні, змінні антени, достатній обсяг RAM та флеш-пам'яті, порти Ethernet та USB, акумуляторні блоки.

Програмне забезпечення: програмна платформа PineAP Suite, вебінтерфейс у вигляді панелі керування, додаткові модулі, API тощо.

Ця платформа (рис. 1.4) спеціально оптимізована для оцінки бездротової безпеки, що і відрізняє її від комп'ютерів, перепрофільованих для тестування безпеки.

Рисунок 1.4 - Зовнішній вигляд пристрою WiFi Pineapple

Незважаючи на те, що пристрій призначений для проведення легітимного пентестінгу професіоналами, які на підставі оцінки зміцнюють безпеку Wi-Fi, він постійно використовується хакерами завдяки всім своїм функціям та можливостям [12]. Кілька його програм та модулів використовуються для створення фальшивих точок доступу, підробки серверів доменних імен (DNS), перехоплення файлів cookie та перехоплення повідомлень у загальнодоступних точках доступу.

Проблема з бездротовими точками доступу часто полягає у відсутності безпеки, саме тому, що це ефективним рішенням для побудови масштабованих, гнучких мобільних мереж. Користувачі регулярно підключаються до бездротових точок доступу, не замислюючись про те, чи є вони справжніми чи зловмисними. Більше того, користувачі не знають про типи атак, що можуть виходити з «шахрайських» точок доступу, встановлених зловмисниками, на кшталт атаки Evil Twin та атаки MitM («людина посередині») [13]. Зловмисники використовують цю перевагу, реплікуючи легітимні мережеві ідентифікатори (SSID), щоб примусити пристрої автоматично підключатися до них, отримуючи доступ до конфіденційних потоків даних, включаючи облікові дані для входу та приватні повідомлення користувачів [14]. Компрометація бездротових мереж не залишається ізольованою проблемою, а часто слугує плацдармом для глибших вторгнень у IT-середовище. Тому Wifi Pineapple підходить лише для ретельно

контрольованого використання в межах етичного хакінгу, враховуючи правові наслідки, вплив та пошкодження, які цей високоризиковий інструмент може завдати пристроям, що знаходяться поруч, навіть внаслідок випадкового прийому сигналу [15].

1.3.2 Flipper Zero

Flipper Zero – багатофункціональний портативний пристрій для дослідження бездротових протоколів ближньої дії та IoT-пристроїв. Спочатку задуманий як універсальний пристрій для злому в межах етичного хакінгу, цей пристрій привернув прицільну увагу за рахунок своїх широких можливостей та зручному дизайну. Потужність пристрою визначається його універсальною апаратною конфігурацією, розробленою для взаємодії з кількома цифровими комунікаційними технологіями, може функціонувати як програмований USB HID-пристрій. Пристрій відрізняється від традиційних інструментів для злому поєднанням широкого спектру різних функцій, включаючи радіочастотний (RF) зв'язок, інфрачервоне (IR) керування та універсальний асинхронний приймач-передавач (UART) [16]. Ці функції дозволяють користувачам взаємодіяти з широким спектром електронних пристроїв, від міток радіочастотної ідентифікації (RFID) до систем розумного дому, що підкреслює потенціал інструменту як для легітимного тестування безпеки, так і для потенційного неправильного використання.

Апаратне забезпечення: мікроконтролер STM32WB55 ARM Cortex-M4, монохромний РК-дисплей 1,4”, 5-позиційний джойстик, порт USB Type-C, слот для картки MicroSD, літієво-полімерний акумулятор, 12 налаштовуваних GPIO-пінів, FreeRTOS з прошивкою.

Комунікаційні можливості: трансивер Sub-1 GHz на чіпі CC1101, зчитувач NFC та RFID-карт, Bluetooth 5.0, інфрачервоний трансивер, iButton/1-Wire тощо.

Flipper Zero може взаємодіяти з багатьма системами: від автомобільних ключів та від гаражних воріт до карт доступу та бездротових датчиків, це робить його потужним інструментом для дослідження безпеки у різних галузях.

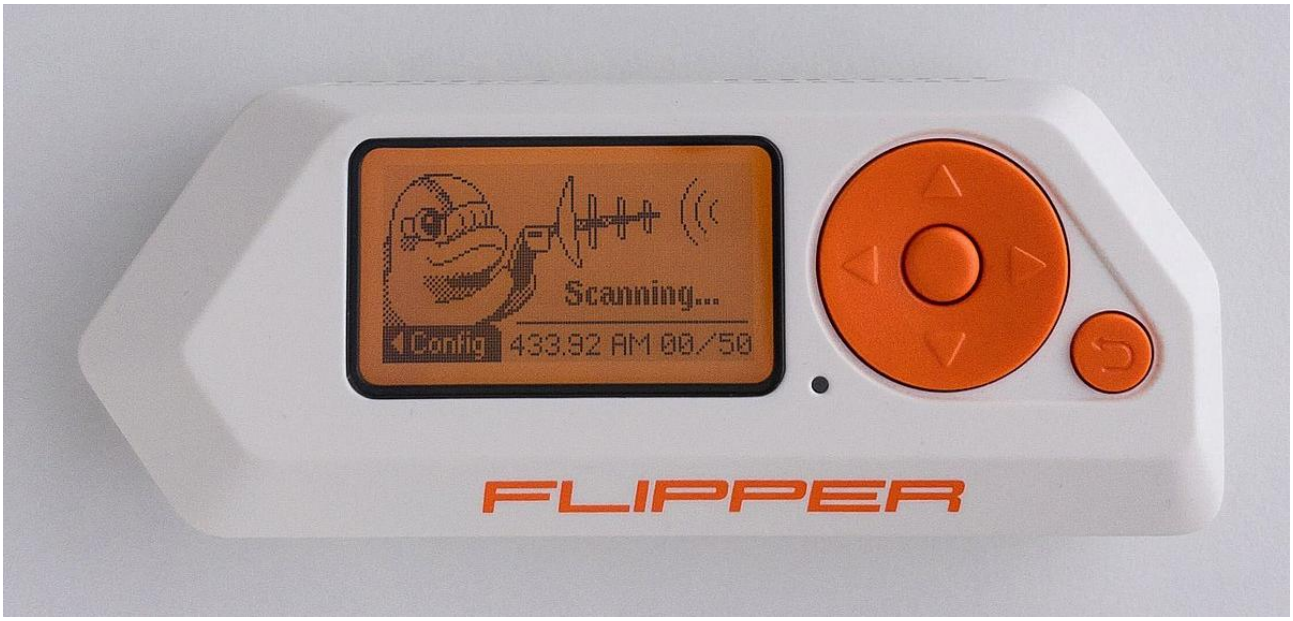


Рисунок 1.5 - Зовнішній вигляд пристрою Flipper Zero

До переваг пристрою можна віднести його кишеньковий розмір, автономність (Li-Ion батарея), відкритий код і архітектуру на основі плагінів (community firmwares), широкий спектр підтримуваних протоколів ближньої дії.

В якості недоліків можна виділити обмежену радіопотужність, що визначається законодавчими нормами, а також відсутність штатного Wi-Fi чіпу для пакетного аналізу стандарту IEEE 802.11 та невеликий обсяг пам’яті для довготривалого зберігання дампів.

Тестування на проникнення є важливим засобом контролю безпеки, який гарантує, що небажане шкідливе програмне забезпечення або вектори загроз не отримають доступу до приватної мережі. Пристрій Flipper Zero як інструмент для тестування на проникнення у фізичних та мережевих сферах безпеки може моделювати реальні сценарії атак. Однак, саме за це пристрій Flipper Zero, завдяки своїй універсальності слід серйозно розглядати як потенційну загрозу безпеці, в разі його використання поза межами етичного хакінгу [17]. Цей інструмент має використовуватися для легітимних досліджень безпеки та в особистих проєктах, але потенційно може бути використаний незаконним шляхом для несанкціонованих спроб доступу. В різних країнах правовий статус Flipper Zero відрізняється. Саме володіння пристроєм в більшості міст є законним, але деякі його методи можуть порушувати закони, що пов'язані з

конфіденційністю чи правилами радіопередачі, а також несанкціонованим доступом.

Отже, портативні апаратні засоби відіграють суттєву роль у розширенні доступу до інструментів дослідження апаратної безпеки та сприяють популяризації практичних аспектів кіберзахисту. Завдяки таким пристроям складні поняття безпеки бездротових мереж стають більш наочними та зрозумілими, що дозволяє ефективніше поєднувати теоретичні знання з їх практичним застосуванням. Для організацій ознайомлення з подібними інструментами є важливим чинником формування адекватних моделей загроз і впровадження дієвих механізмів контролю безпеки. Водночас для окремих дослідників і фахівців ці рішення відкривають можливості вивчення апаратної безпеки без необхідності володіння глибокими спеціалізованими знаннями або доступу до дорогого обладнання.

З огляду на те, що зростає залежність сучасного суспільства від бездротових технологій та пристроїв Інтернету речей, здатність аналізувати, оцінювати та підвищувати рівень захищеності таких систем набуває особливої актуальності. Порушення безпеки бездротових мереж часто не є локальною загрозою, а може бути відправною точкою для подальших атак на інформаційні ресурси організації. Саме тому під час проведення легітимного аудиту безпеки фахівці все частіше використовують апаратні інструменти для виявлення вразливостей і підвищення стійкості мережевої інфраструктури. Платформи на кшталт WiFi Pineapple та Flipper Zero, за умови відповідального й етичного застосування, роблять вагомий внесок у формування практичних навичок і підготовку у сфері інформаційної безпеки нового покоління спеціалістів.

Водночас ключовим залишається дотримання балансу між відкритістю таких інструментів і відповідальністю їх використання. Орієнтація на етичні принципи, освітні цілі, авторизоване тестування та підвищення рівня захищеності дозволяє спільноті з інформаційної безпеки повною мірою реалізувати потенціал апаратних засобів, мінімізуючи ризики їх неналежного або зловмисного застосування.

РОЗДІЛ 2 СТАНДАРТИ БЕЗПЕКИ БЕЗДРОТОВИХ МЕРЕЖ ТА АТАКИ НА НИХ

2.1 Стандарти безпеки бездротових мереж

Існує чотири поширені стандарти забезпечення безпеки Wi-Fi мереж:

– WEP надає базовий захист даних шляхом шифрування завдяки алгоритму RC4, але вважається вразливим та застарілим.

– WPA – популярна родина протоколів, розроблених для заміни WEP (WPA, WPA2, WPA3). Протокол включає методи WPA-Personal і WPA-Enterprise, основні особливості яких подано у таблиці 2.1.

Таблиця 2.1 – Методи стандарту безпеки WPA

Метод	WPA-Personal	WPA-Enterprise
Спосіб автентифікації	Метод призначений для захисту бездротових мереж за допомогою попередньо узгодженого пароля або загального ключа PSK, який повинні знати всі пристрої та користувачі, щоб отримати доступ до мережі.	Замість PSK використовується автентифікація на сервері RADIUS. Сервер перевіряє облікові дані користувачів та керує всіма процесами централізовано. Зниження ризиків компрометації облікових даних відбувається завдяки тому, що кожен користувач має власний ідентифікаційний ключ для доступу до мережі.
Застосування	Часто використовується для безпеки Wi-Fi для домашніх мереж та невеликих офісів.	В основному використовується для захисту корпоративних мереж.

WPA забезпечує більш надійне шифрування та автентифікацію, оскільки кожен пристрій, підключений до мережі, має власний унікальний ключ для шифрування та дешифрування даних.

2.1.1 Протокол безпеки бездротових локальних мереж

Протокол безпеки бездротових локальних мереж (WEP) був першим стандартом безпеки, розробленим у поєднанні зі стандартами 802.11. Вперше впроваджений у 1999 році поряд з першою широко прийнятою ітерацією 802.11, WEP був розроблений для забезпечення рівня безпеки, характерного для провідних мереж. Це було зроблено за допомогою комбінації шифрів RC4 для забезпечення конфіденційності та шифрів CRC32 для забезпечення цілісності.

Автентифікація в мережі WEP виконується за допомогою 64- або 128-бітного ключа. 64-розрядний ключ являє собою чотири послідовності з десяти шістнадцяткових символів. Потім ці початкові 40 біт поєднуються з 24-бітовим вектором ініціалізації (IV), який формує ключ шифрування RC4. Для 128-бітного ключа 104-бітний ключ або 26 шістнадцяткових символів об'єднуються з 24-бітним IV для створення ключа RC4.

Автентифікація у бездротовій мережі WEP проводиться у чотири етапи.

– Клієнт надсилає запит точці доступу WEP для автентифікації.

– Точка доступу WEP надсилає клієнтові текстове повідомлення.

– Клієнт бере введений ключ WEP, шифрує передане точкою доступу текстове повідомлення, після чого відправляє його на точку доступу.

– Точка доступу розшифровує надіслане їй повідомлення, зашифроване клієнтом за допомогою власного ключа WEP. Якщо повідомлення розшифровано правильно, клієнту можна підключитися.

При розробці WEP завдання конфіденційності та цілісності повідомлень не було основним. В результаті WEP отримав дві ключові вразливості. По-перше, головна мета алгоритму CRC32 – контрольна сума, що дозволяє уникнути помилок, а не шифрування як таке. По-друге, RC4 сприйнятливий до того, що називають векторною атакою ініціалізації. Атака IV можлива через те, що шифр RC4 призначений для шифрування потоку і як слідство, той самий ключ не можна використовувати двічі; 24-бітний ключ занадто короткий для завантаженої бездротової мережі. Приблизно в 50% випадків той же IV

використовуватиметься у бездротовому каналі зв'язку в межах 5000 варіацій. Це призведе до колізії, в результаті якої IV та весь ключ WEP можуть бути скасовані.

Через уразливість безпеки WEP у 2003 році почав поступово згортатися на користь безпечніших бездротових реалізацій. В результаті, на сьогодні майже не можливо зіткнутися з точками доступу, що працюють на основі протоколу WEP, але можна виявити застарілу мережу, де ще використовується цей неактуальний протокол.

2.1.2 Захищений доступ до Wi-Fi

Для процедури автентифікації з захищеним доступом до бездротової мережі існують такі відомі протоколи, як WPA, WPA2, WPA3. Всі протоколи відрізняються один від одного набором даних, які потрібні для успішної автентифікації (табл. 2.2).

Таблиця 2.2 – Родина протоколів WPA

Основні характеристики	WPA	WPA2	WPA3
Випущено	2003	2006	2018
Режими автентифікації	WPA-PSK WPA-Enterprise	WPA2-PSK WPA2-Enterprise	WPA3-Personal WPA3-Enterprise
Алгоритм шифрування	TKIP	AES-CCMP	AES-CCMP AES-GCMP
Розмір ключа	128	128	192/256
Протоколи автентифікації та обміну ключами	4-way handshake	4-way handshake	ECDH ECDSA
Вважається застарілим	С 2012	Актуальний	Актуальний

Тобто кожен із протоколів використовує свій метод шифрування та валідації даних. По таблиці 2.2 видно, що протокол WPA вважається застарілим і більше не використовується для сучасних пристроїв, але в реальному житті це не так, пристрої, які вимогливі до живлення, можуть все ще використовувати старі алгоритми.

2.1.2.1 WPA

При реалізації бездротової мережі WEP стандарти безпеки 802.11 були оновлені з урахуванням нових вразливостей. Таке оновлення забезпечило більший ступінь конфіденційності та цілісності бездротових мереж. Це було зроблено відповідно до стандарту WPA, який був вперше реалізований у 2003 році у стандарті 802.11i. Фактично WPA є комбінацією технологій: 802.1X, EAP, TKIP, MIC.

EAP – протокол автентифікації, що застосовується не лише для визначення методу передачі ключів, а й для автентифікації та обробки даних ключів модулями, що підключаються. Методи автентифікації в межах фреймворку EAP, які забезпечують безпечний доступ до мережі:

– LEAP завдяки динамічним ключам WEP;
– EAP-TLS завдяки сертифікатам з обох сторін;
– EAP-TTLS завдяки тунелю TLS для інших методів (паролі/сертифікати);
– EAP-PSK завдяки спільному секретному ключу.

Вони відрізняються вимогами до сертифікатів та механізмами захисту даних, але всі слугують для перевірки ідентичності користувача перед доступом до мережі Wi-Fi або дротової мережі.

Протокол TKIP передбачає збільшення довжини криптографічного ключа до 128 біт і замінює використання одного статичного ключа WEP системою динамічно змінюваних ключів. У межах TKIP реалізовано механізм зниження передбачуваності ключового матеріалу, що ґрунтується на ієрархічній схемі керування ключами. Загальний двосторонній ключ використовується як основа для генерації унікальних ключів шифрування, що застосовуються окремо для

кожного переданого пакета даних. Таким чином, замість одного фіксованого ключа формується велика кількість можливих комбінацій ключів, що суттєво ускладнює криптоаналіз зашифрованого трафіку.

Для забезпечення цілісності переданих даних у TKIP використовується механізм перевірки повідомлень MIC. Його призначення полягає у виявленні несанкціонованих змін вмісту пакетів під час передавання мережею та запобіганні їх повторній або підробленій трансляції. MIC базується на застосуванні математичної функції, результати якої обчислюються на обох сторонах, як відправника, так і одержувача. У разі невідповідності отриманих значень пакет вважається скомпрометованим і відхиляється як помилковий.

Розраховується MIC завдяки алгоритму автентифікації на основі CMAC зі 128-бітним розширеним стандартом шифрування AES [18].

AES-CMAC – це модифікована версія CBC-MAC, що використовує симетричні ключі AES для створення коду автентифікації повідомлення MAC для заданого повідомлення [19]. Він використовує режим ланцюжка блоків шифрування CBC блочного шифру AES для генерації MAC. Для цього алгоритм приймає секретний ключ, повідомлення змінної довжини та довжину повідомлення в октетах як вхідні дані та повертає рядок з фіксованим бітами MAC.

Секретний ключ, що позначається K, є ключем для AES-128. Повідомлення та його довжина в октетах позначаються відповідно M та len. MIC обчислюється за всіма полями повідомлення, включаючи MHDR (MAC Header) – загальні дані, FHDR (Frame Header) – службові дані, FPort – номер порту (0 для команд, 1-223 для додатків), а FRMPayload – зашифровані дані (команди або дані додатку).

Повідомлення M позначається послідовністю M_i, де M_i — i-й блок повідомлення. Тобто, якщо M складається з n блоків, то M записується як:

$$M = M\_1 \,||\, M\_2 \,||\, \ldots \,||\, M\_\{n\text{-}1\} \,||\, M\_n \qquad (2.1)$$

Довжина M_i становить 128 бітів для i = 1,...,n-1, а довжина останнього блоку M_n менша або дорівнює 128 бітам. Виходом алгоритму генерації MAC є

128-бітний рядок, який використовується для перевірки вхідного повідомлення. MAC позначається як T, тоді:

$$T := AES\text{-}CMAC(K,M,len) \tag{2.2}$$

Перевірка MAC забезпечує гарантію цілісності та автентичності повідомлення від джерела. Можна скоротити MAC, але принаймні 64-бітний MAC слід використовувати як захист від brute-force атак. Результат скорочення слід брати в найстарших значущих бітах першого порядку. Довжина блоку AES-128 становить 128 бітів (16 октетів). Існує спеціальна обробка, якщо довжина повідомлення не є додатним кратним довжині блоку. Спеціальна обробка полягає в доповненні M бітовим рядком 10^i, щоб скоригувати довжину останнього блоку до довжини блоку.

Для вхідного рядка x з r октетів, де 0 <= r < 16, функція доповнення, padding(x), визначається наступним чином:

$$padding(x) = x \,||\, 10^i \tag{2.3}$$

де i дорівнює 128-8*r-1. Тобто, padding(x) — це об'єднання x та однієї «1», за якою йде мінімальна кількість «0», щоб загальна довжина дорівнювала 128 бітам.

Тобто, існує два випадки роботи AES-CMAC. На рисунку 2.1 показано роботу CBC-MAC в обох випадках [20]. Якщо розмір вхідного блоку повідомлення дорівнює позитивному кратному розміру блоку (а саме 128 бітам), останній блок повинен бути об'єднаний операцією XOR з K1 перед обробкою. В іншому випадку, останній блок повинен бути доповнений 10^i та об'єднаний операцією XOR з K2. Результатом попереднього процесу будуть вхідні дані останнього шифрування. Вихідні дані AES-CMAC забезпечують цілісність даних усього вхідного повідомлення. AES_K — це AES-128 з ключем K. K1 — це підключ для випадку (а), та K2 — це підключ для випадку (б).

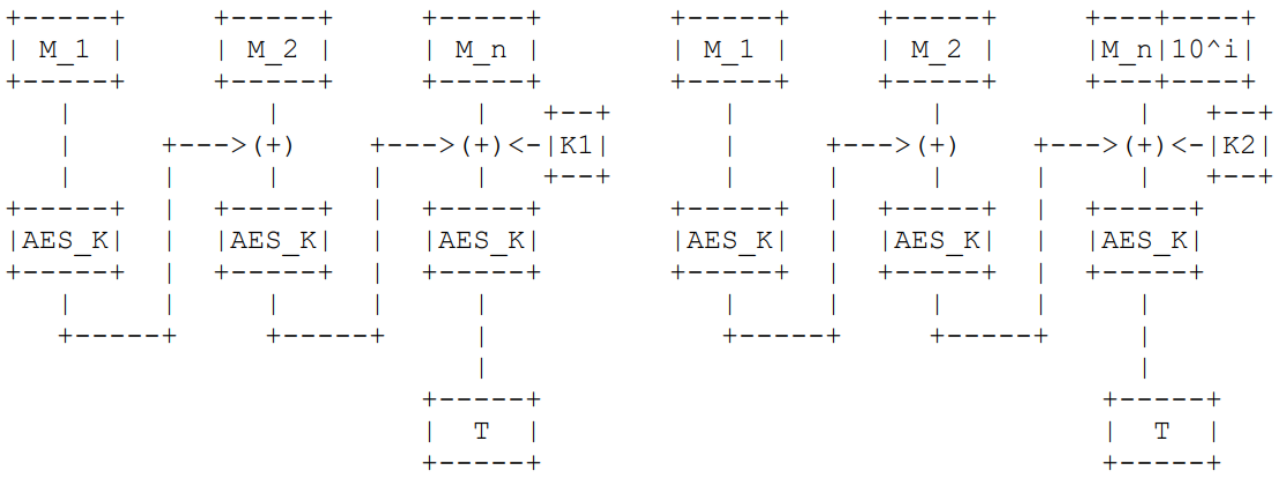


Рисунок 2.1 - Два випадки роботи AES-CMAC: а) позитивна кратна довжина блоку, б) в іншому випадку

Алгоритм генерації підключів Generate_Subkey() приймає секретний ключ K. Виходами алгоритму генерації підключів є два підключі, K1 та K2:

$$(K1,K2) := Generate\_Subkey(K) \tag{2.4}$$

Підключі K1 та K2 використовуються як в алгоритмах генерації MAC, так і в алгоритмах перевірки MAC. K1 використовується у випадку, коли довжина останнього блоку дорівнює довжині блоку. K2 використовується у випадку, коли довжина останнього блоку менша за довжину блоку.

2.1.2.2 WPA2

WPA було додатково оновлено до WPA2 у 2006 році, тим самим ставши стандартом для мереж захищеного доступу Wi-Fi. WPA2 має вже шифрування CCMP (прийшло заміну TKIP), і шифрування AES.

Насьогодні шифрування AES є одним з найбезпечніших алгоритмів шифрування і ґрунтується на досить продуктивному і гнучкому алгоритмі, що складається з кількох підстановок, перестановок та лінійних перетворень. Кожна операція виконується на блоках даних по 16 байтів (розмір блоку завжди

дорівнює 128 біт) і повторюється по кілька разів, які називаються "раундами". У кожному раунді із ключа шифрування розраховується унікальний ключ раунду. Оскільки структура AES блокова, зміна в блоці відкритого тексту або окремого біта в ключі призводить до абсолютно іншого блоку шифрованого тексту. Ключі AES бувають 128, 192 та 256-бітними.

CCMP – протокол шифрування, що має у своїй основі алгоритм AES зі 128-бітним блоком і 128-бітовим ключем. Алгоритм шифрування, що використовується в протоколі безпеки 802.11i, використовує блочний шифр AES, але обмежує довжину ключа 128 бітами. AES-CCMP включає два складні криптографічні методи (режим лічильника та CBC-MAC) та адаптує їх до кадрів Ethernet, щоб забезпечити надійний протокол безпеки між мобільним клієнтом і точкою доступу. Сам по собі AES є дуже надійним шифром, але режим лічильника ускладнює для підслуховувача виявлення шаблонів, а метод цілісності повідомлень CBC-MAC гарантує, що повідомлення не були підроблені.

WPA2 розроблено у трьох різних версіях, кожна з яких передбачає свої власні механізми автентифікації.

– WPA-Personal. Підключення до бездротової мережі WPA2 часто зустрічається в житлових приміщеннях або невеликих офісах. WPA2 використовує попередній загальний ключ, який є похідним від комбінації коду доступу та ідентифікатора (SSID) бездротової мережі. Цей код налаштовується користувачем, і довжина його може становити від 8 до 63 символів. Потім цей код доступу разом із 4096 взаємозв'язками алгоритму хешування SHA1 додається до SSID.

– WPA-Enterprise. У корпоративній версії WPA/WPA2 використовується сервер автентифікації RADIUS. Це дозволяє автентифікувати користувача та пристрій, що значно зменшує можливість попереднього підбору ключів за допомогою грубої сили.

– Wi-Fi Protected Setup (WPS). Захищене встановлення Wi-Fi – це зручний для кінцевих користувачів спосіб підключення пристроїв до бездротової мережі, при якому для підключення застосовується PIN-код замість пароля або секретної

фрази. Спочатку цей варіант розроблявся як найпростіший спосіб підключення пристроїв до бездротових мереж. Таку технологію часто використовують у принтерах чи ігрових пристроях. Користувач повинен лише натиснути кнопку на точці доступу з підтримкою WPS, а потім на пристрої, що підтримує WPS, і з'єднання буде встановлено.

При використанні WPA-Personal автентифікація та шифрування обробляються за допомогою чотиристороннього рукостискання – 4-way handshake (рис. 2.2).

Крок 1. Точка доступу передає клієнту випадкове число, що називається ANonce.

Крок 2. Клієнт створює інше випадкове число, що називається SNonce. SNonce, ANonce та введений користувачем код доступу поєднуються для створення так званої перевірки цілісності повідомлень (MIC). MIC та SNonce відправляються назад точці доступу.

Крок 3. Точка доступу хешує ключ ANonce, SNonce та попередній загальнодоступний ключ і, якщо вони збігаються, автентифікує клієнта. Потім вона надсилає ключ шифрування клієнту.

Крок 4. Клієнт підтверджує ключ шифрування.

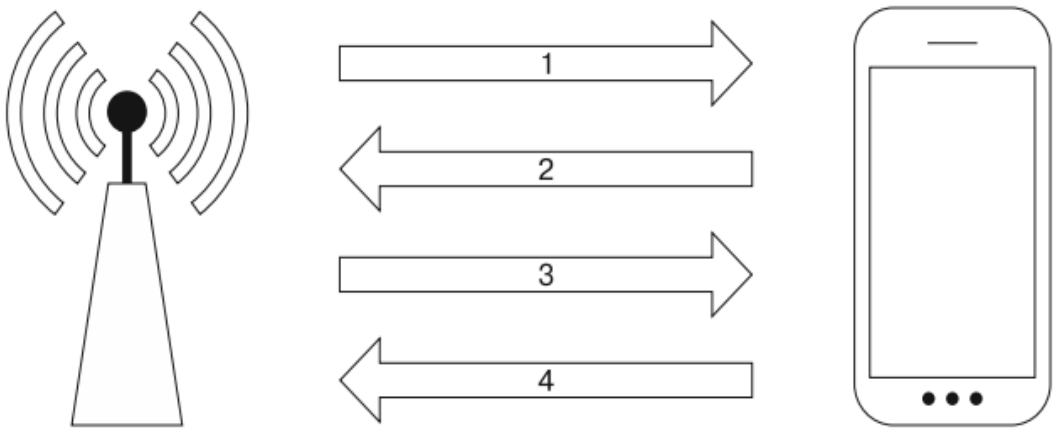


Рисунок 2.2 – Чотиристоронє рукостискання

У підключенні типу WPA-Personal є дві ключові вразливості:

– Слабкий загальний ключ. При підключенні WPA-Personal користувач має налаштувати параметри точки доступу. Часто користувачі для цього

використовують короткий, простий пароль, що добре запам'ятовується. Якщо перехопити чотиристоронніє рукостискання, буде доступна вся інформація, необхідна для перехоплення пароля та автентифікації в мережі.

– WPS. В процесі експлуатації стало ясно, що захист методу підключення, де автентифікація виконується за допомогою PIN-коду, ненадійний. Зловмисник при атаці може отримати як PIN-код, так і код доступу, що використовується пристроєм для підключення до бездротової мережі.

2.1.2.3 WPA3

Зі зростанням поширеності пристроїв "Інтернету речей" та систем "робота з дому" люди прагнуть захистити свої мережі Wi-Fi та запобігти будь-яким можливостям для проникнення в них зловмисників. Кіберзлочинці часто швидко використовують слабкі місця у старих стандартах безпеки, що робить необхідним використання більш надійної автентифікації та шифрування. WPA3 вирішує ці проблеми, впроваджуючи складніші криптографічні методи, які ускладнюють зловмисникам перехоплення даних.

WPA3 – це найновіший та найдосконаліший протокол безпеки Wi-Fi, покликаний замінити протокол WPA2 та посилити захист бездротових мереж. Розроблений Wi-Fi Alliance, WPA3 покращує шифрування та захищає від атак із зломом пароля. Він також був розроблений для підвищення безпеки як громадських мереж, так і мереж "розумного дому", які в іншому випадку можуть зробити людей вразливими.

У WPA3 з'явилися такі функції, як Wi-Fi Easy Connect, які спрощують процес налаштування та одночасно підвищують рівень безпеки. Замість того, щоб вводити довгі паролі вручну, користувачі можуть відсканувати QR-код або використовувати пару NFC для безпечного підключення своїх IoT-пристроїв [21]. Це не тільки підвищує зручність, а й усуває поширені вразливості, пов'язані зі слабкими паролями.

Багато компаній працюють з великими обсягами конфіденційних даних, на кшталт інформації про клієнтів та навіть банківські реквізити. WPA3-Enterprise

посилює безпеку мережі завдяки 192-бітному шифруванню та новим протоколам автентифікації, що робить корпоративні мережі набагато менш сприйнятливими до кібератак. Великі підприємства, державні установи та медичні організації все частіше використовують WPA3 для забезпечення відповідності нормам безпеки та захисту конфіденційних даних.

WPA3-Enterprise – це режим роботи, який вимагає обладнання, здатного обробляти підвищені вимоги до шифрування. Оскільки дані захищені 256-бітним шифром Galois/Counter Mode Protocol (GCMP-256) з використанням 384-бітної еліптичної кривої ECDH або ECDSA для обміну ключами з хеш-автентифікацією HMAC SHA384. Захищені кадри керування PMF захищені за допомогою 256-бітного коду автентифікації повідомлень Galois протоколу Broadcast/Multicast Integrity Protocol (BIP-GMAC-256).

WPA3 замінює вразливий для атак методом грубої сили метод автентифікації за попереднім ключем (PSK), при якому зловмисники могли перехоплювати пакети Wi-Fi і за допомогою програмного забезпечення багаторазово вгадувати паролі, поки не отримували доступ, на сучасний безпечний протокол обміну ключами на основі паролів SAE, що є набагато безпечніше:

– Навіть якщо зловмисник перехопить дані рукостискання Wi-Fi, він не зможе використовувати їх для вгадування паролів в автономному режимі.

– Кількість спроб підбору пароля обмежена, а значить, хакери не зможуть зламати мережу спробами входу в систему.

– Зламати мережу стає значно складніше, навіть якщо користувачі вибирають слабші паролі (це, звичайно, не рекомендується).

Робота алгоритму AES-GCMP складається з двох основних компонентів: шифрування за допомогою AES у режимі лічильника (CTR) і обчислення тегу автентичності за допомогою хеш-функції GHASH. Процес починається з генерації ключа довжиною 256 біт та 96-бітного вектору ініціалізації (IV), які використовуються для формування спеціального лічильника. Після шифрування алгоритм обчислює тег автентичності, який перевіряє, чи не були змінені дані під час передачі.

Для цього використовується спеціальна хеш-функція GHASH, що виконує математичні операції в полі Галуа GF(2^{128}):

$$GHASH(H, AAD, Ciphertext) = X_{m+n+1} \quad (2.5)$$

де H = $E_k(0^{128})$ – ключ хешування, що є результатом шифрування 128 нульових бітів на ключі K, зашифрований за допомогою блокового шифру; m – кількість 128-бітових блоків в AAD (округлена в більшу сторону), n – кількість 128-бітових блоків у Ciphertext (округлена в більшу сторону). X_i визначається як:

$$X_i = \sum_{j=1}^{i} S_j \cdot H^{i-j+1} = \begin{cases} 0, \text{для i} = 0 \\ (X_{i-1} \oplus S_i) \cdot H, \text{для } i = 1, \dots, m+n+1 \end{cases}, \quad (2.6)$$

Кожен блок відкритого тексту X_i послідовно поєднується з попереднім результатом шифрування лічильника за допомогою XOR, а потім множиться на ключ H. Це дозволяє виконувати шифрування паралельно та швидко, оскільки шифрування блоків незалежне. Результат останньої ітерації використовується як хеш-значення. Автентифікований і зашифрований текст окремо доповнюються нулями до значень, кратних 128 бітам, і об'єднуються в одне повідомлення S_i:

$$S_i = \begin{cases} AAD_i, \text{для } i = 1, \dots, m-1 \\ AAD_m^* \,||0^{128-v}, \text{для } i = m \\ Ciphertext_{i-m}, \text{для } i = m+1, \dots, m+n-1 \\ Ciphertext_n^* \,||0^{128-u}, \text{для } i = m+n \\ len(AAD)||len(Ciphertext), \text{для } i = m+n+1 \end{cases}, \quad (2.7)$$

де len(AAD) та len(Ciphertext) – це 64-бітові представлення бітових довжин AAD та Ciphertext відповідно, v = len(AAD) mod 128 – це бітова довжина останнього блоку AAD, u = len(Ciphertext) mod 128 – це бітова довжина останнього блоку Ciphertext, та || позначає об'єднання бітових рядків.

І тепер одержувач, знаючи K, після отримання AAD, Ciphertext та тегу автентичності, може розшифрувати шифротекст, щоб відновити відкритий текст

Plaintext, та може перевірити тег Tag, щоб переконатися, що ні шифротекст, ні пов'язані з ним дані не були підроблені. У разі зміни навіть одного біта даних — тег автентифікації не пройде перевірку.

2.2 Атаки на протоколи безпеки бездротових мереж

Більшість атак, які відомі на бездротові мережі, це атаки на механізми автентифікації для доступу до бездротової мережі. Вибираються ці механізми невипадково, оскільки вони перешкоджають безконтрольному підключенню до точки доступу.

2.2.1 Атаки на протокол WPA2-PSK

Атаки на протокол WPA2-PSK становлять серйозну загрозу безпеці бездротових мереж. В рамках цієї групи атак проводиться аналіз на вразливості та слабкі місця у механізмах автентифікації та шифрування, що використовуються у мережах WPA2-PSK. Це такі атаки, як:

– Cracking the 4-way handshake;
– WPS PIN Bruteforce;
– PMKID Dump

Атака Cracking the 4-way handshake спрямована на пошук слабких місць у процесі встановлення безпечного з'єднання між пристроєм та бездротовим маршрутизатором. Під час атаки зловмисники намагаються зламати 4-бічне рукостискання, яке використовується для автентифікації та встановлення ключа для шифрування даних. Основною метою процесу 4-way handshake є створення унікального ключа для кожної сесії, який називається PTK. Для створення цього ключа попередньо застосовується узгоджений ключ PSK та такі параметри: SSID мережі, ANonce - випадкове число, що генерується точкою доступу, SNonce - випадкове число, що генерується клієнтським пристроєм, MAC-адреса точки доступу, MAC-адреса клієнтського пристрою Wi-Fi. PTK створюється за допомогою всіх цих параметрів і використовується для шифрування даних між

точкою доступу та клієнтським пристроєм. Це дозволяє забезпечити безпеку передачі даних у бездротовій мережі, оскільки кожна сесія використовує свій унікальний ключ. У разі успішного злому пароля зі словника, PTK може бути використаний для дешифрування даних у зашифрованих Wi-Fi мережах. Тому від таких атак для захисту важливо використовувати складні та унікальні паролі.

WPS PIN Bruteforce – ще одна потенційна вразливість у протоколі WPA2-PSK – можливість атак на систему захисту WPS. Такі атаки спрямовані на виявлення проблем у процесі встановлення безпечного з'єднання між пристроєм та бездротовим маршрутизатором з використанням WPS. Процес налаштування WPS включає використання 8-значного PIN, який може складатись лише цифр від 0 до 9. На перший погляд, 8-значний PIN може являти собою 100 000 000 різних комбінацій. Проте фактична кількість унікальних комбінацій скорочується через особливості валідації цього PIN у реальній реалізації WPS. Зокрема, останній символ PIN-коду обчислюється як контрольна сума попередніх семи символів. Таким чином, передостанній символ залишається єдиним невідомим значенням, інші символи можна підібрати перебором. Крім того, перші чотири символи та наступні три символи перевіряються незалежно один від одного. Через цю особливість загальна кількість дійсних комбінацій, які можуть бути перевірені при брутфорс-атаці на WPS PIN, скорочується всього до 11 000 можливих комбінацій, що робить цю атаку досить простою.

Pairwise Master Key Identifier Dump (PMKID) – це процес отримання та збереження PMKID з бездротової мережі, що працює за протоколом WPA/WPA2. PMKID – це частина ключової інформації, яка використовується для встановлення безпечного з'єднання між клієнтським пристроєм та точкою доступу. Цей процес нагадує перемикання між осередками в стільникових мережах. Іноді він позначається на стабільності з'єднання, оскільки кожного разу, коли клієнт виходить з діапазону однієї точки доступу та переходить до іншої, відбувається нове 4-стороннє потискання рук. Для зниження затримок таких переходів існує функція кешування Pairwise Master Key (PMK). Багато маршрутизаторів кешують PMKID, щоб наступного разу клієнт міг повторно автентифікуватися без виконання рукостискання. Маршрутизатори з цією

функцією включають PMKID кадру EAPOL. Тут вже можливі варіанти: наприклад, можна спробувати перехопити PMKID і запустити атаку методом підбору пароля для вгадування PMK, необхідного для аутентифікації в мережі. Сама атака на PMKID вимагає доступу до бездротової мережі, а її здійснення потрібен певний інструментарій.

2.2.2 Атаки на WPA2-Enterprise

Атаки на системи WPA2-Enterprise націлені на аналіз рівня безпеки, що надається серверами автентифікації та механізмами керування ключами у складних корпоративних мережах. Серед цілей можуть бути і фізичні атаки на мережеве обладнання. WPA-Enterprise також відомий як стандарт WPA-EAP або WPA-802.1X. Він використовує протокол EAP для делегування автентифікації клієнтів бездротової мережі на сервер RADIUS. EAP надає набір стандартизованих функцій та правил для реалізації конкретних методів автентифікації, відомих як методи EAP. Серед таких методів можуть бути як автентифікація на основі сертифікатів, так і на основі облікових даних. Ось кілька прикладів EAP-методів:

– EAP-TLS — метод є оригінальним стандартом EAP автентифікації, що широко підтримується, він дозволяє автентифікацію лише на основі сертифікатів.

– PEAP був розроблений компаніями Microsoft, Cisco та RSA Security і використовує тунельне шифрування TLS для передачі даних EAP.

– EAP-TTLS є розширенням TLS для забезпечення EAP через TLS-тунель і також широко підтримується в корпоративному середовищі, за винятком Microsoft.

– LEAP був розроблений Cisco до встановлення стандарту і не має нативної підтримки в продуктах Microsoft, що в даний час вважається застарілим.

– EAP-FAST був розроблений Cisco як заміна LEAP.

Найпоширенішими реалізаціями протоколу EAP є EAP-PEAP та EAP-TTLS. PEAP використовує сертифікати на стороні сервера для перевірки автентичності

сервера RADIUS. Майже всі атаки на PEAP пов'язані з неправильним настроюванням перевірки сертифікатів.

Основні види атак на системи WPA2-Enterprise: Evil Twin (Stealing Credentials) та Online Bruteforce.

Атака Evil Twin включає створення підробленої точки доступу, яка імітує цільовий SSID, щоб залучити клієнтів і змусити їх виконати автентифікацію в другій фазі з підробленим RADIUS-сервером. Слід зазначити, що ця атака не спрацює проти клієнтів, які: використовують автентифікацію на основі сертифікатів (наприклад, EAP-TLS або PEAP з EAP-TLS), тому що тут відсутні облікові дані, які можна вкрасти; перевіряють сертифікат сервера під час першої фази автентифікації.

Незважаючи на те, що мережі WPA-Enterprise вважаються безпечнішими, ніж мережі WPA-PSK, вони нерідко піддаються атакам онлайн-перебору паролів (Online Bruteforce). Оскільки облікові дані WPA-Enterprise часто є обліковими даними користувача домену, можна використовувати виявлені облікові дані, щоб отримати доступ до додаткових систем корпоративної мережі.

2.2.3 Атаки на WPA3

У січні 2018 року Wi-Fi Alliance оголосила про створення WPA3, який мав стати заміною WPA2, який вважався вразливим для Key Reinstallation Attack (KRACK-атак). Новий стандарт використовує 128-бітове шифрування в режимі WPA3-Personal або 192-бітове шифрування в режимі WPA3-Enterprise. Атакувати його складніше через наявність сучасного протоколу встановлення ключів (SAE) та безпечного рукостискання Dragonfly Key Exchange. Інші важливі функції безпеки WPA3 включають:

– захист клієнтських кадрів MFP, що запобігає несанкціонованій взаємодії із зовнішніми джерелами;

– безперервну генерацію нових сесійних ключів при кожній новій комунікації, що запобігає розшифровці попередніх повідомлень - Perfect Forward Secrecy;

– протокол для налаштування пристроїв, що дозволяє новим пристроям підключатися до мережі за допомогою QR-кодів — DPP.

У 2019 році дослідники з безпеки Mathy Vanhoef та Eyal Ronen виявили недоліки в WPA3, що діляться на два типи: downgrade-атаки та слабкі моменти у Dragonfly handshake, що використовується у WPA3:

– Downgrade & Dictionary Attack проти WPA3-Transition - атаки через зловживання зворотною сумісністю WPA3, коли клієнта змушують підключитися до підробленої точки доступу WPA2 для захоплення рукостискання.

– Security Group Downgrade — коли клієнта змушують вибирати слабкі групи безпеки шляхом відхилення його коміт-фреймів через rogue AP.

– Timing-Based Side-Channel Attack - зловживання часом відповіді точки доступу на коміт-фрейми при використанні груп безпеки MODP.

– Cache-Based Side-Channel Attack — коли memory access patterns розкривають інформацію про паролі, якщо сторона, що атакує, контролює додаток на пристрої жертви.

– DoS – зловживання коміт-фреймами, що викликає велике навантаження на процесор або призводить до відключення клієнта.

РОЗДІЛ 3 РОЗРОБКА ТА ЕКСПЛУАТАЦІЯ ПОРТАТИВНОГО ПРИСТРОЮ ДЛЯ ТЕСТУВАННЯ БЕЗПЕКИ БЕЗДРОТОВИХ МЕРЕЖ

3.1 Розробка портативного пристрою для тестування безпеки бездротових мереж

Результати проведеного дослідження демонструють потребу в пристрої для тестування безпеки бездротових мереж як зручного у використанні рішення, завдяки реалізації повного комплексу пентест-інструментів від сканування до етичного хакінгу на енергоефективній мікропроцесорній платформі, що мінімізує апаратні ресурси та фінансові витрати.

Саме тому, у межах кваліфікаційної роботи розроблено портативний пристрій, що названо NetScope, який перейняв переваги багатофункціонального Flipper Zero, при цьому має відносно малу собівартість навіть порівняно з WiFi Pineapple (табл. 3.1).

Таблиця 3.1 – Аналіз пристроїв для тестування бездротових мереж

Критерій	Wi-Fi Pineapple	Flipper Zero	NetScope
Ціна	до 250 USD	до 400 USD	до 70 USD
Розмір / портативність	Середній, потребує додаткових модулів	Компактний, кишеньковий формат	Компактний, кишеньковий формат
Простота використання	Потребує знань Linux / CLI	Інтуїтивно зрозумілий інтерфейс	Інтуїтивно зрозумілий інтерфейс
Функціональність	Обмежена Wi-Fi	Підтримка Wi-Fi, BLE, RFID/NFC, Radio 300-928 MHz	Підтримка Wi-Fi, Radio 2.4 GHz
Призначення	Для фахівців	Для фахівців	Для фахівців і освітніх установ

Розроблений пристрій являє собою вбудовану апаратно-програмну систему для тестування бездротових мереж стандарту IEEE 802.11 та збору телеметричних даних з зовнішніх модулів через послідовний інтерфейс у

реальному часі. NetScope поєднує функції моніторингу бездротового середовища, візуалізації результатів тестування та забезпечення зручного інтерфейсу доступу до даних як локально, так і віддалено через вебінтерфейс.

Система побудована на базі мікроконтролера ESP32, який обрано з огляду на його обчислювальні можливості, наявність апаратної підтримки Wi-Fi, достатній обсяг оперативної пам’яті та розвинену екосистему програмних бібліотек. Пристрій функціонує як автономний вузол, що не потребує постійного підключення до ПК завдяки живленню від літій-іонного акумулятора.

Апаратна частина NetScope складається з кількох функціональних модулів (рис. 3.1):

– центральний обчислювальний модуль;

– модуль візуалізації;

– зовнішній аналізатор.

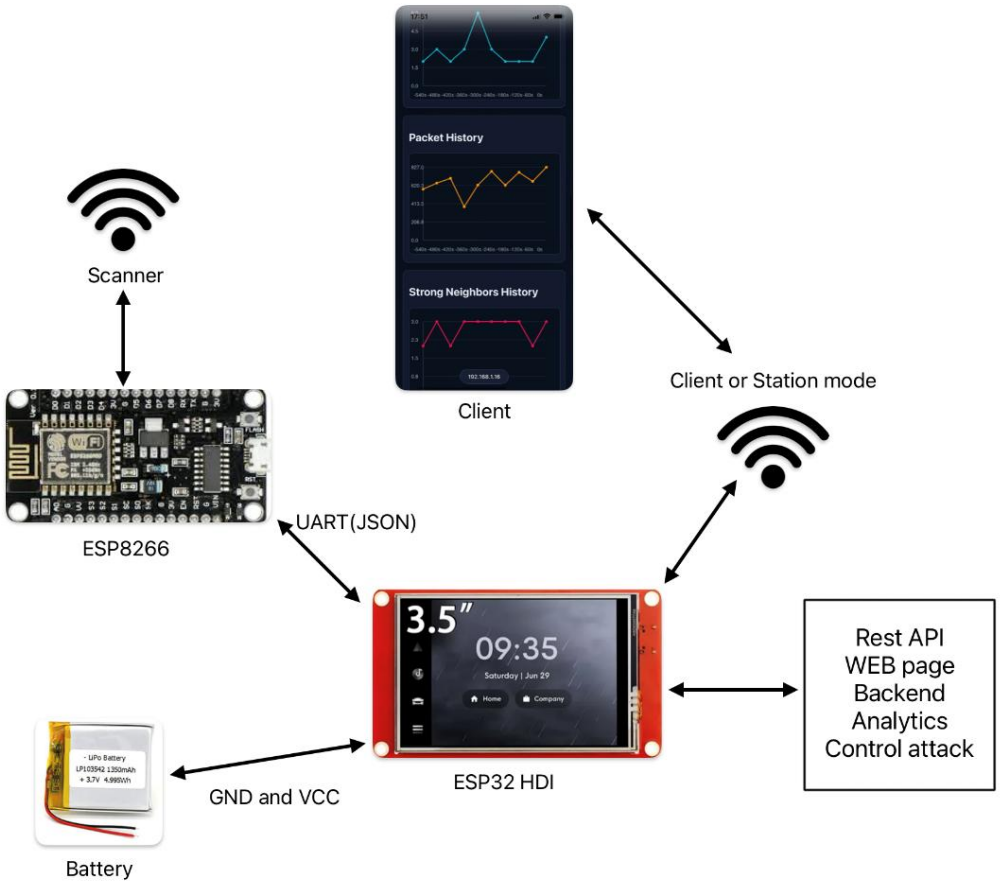


Рисунок 3.1 – Схема взаємодії модулів пристрою

Мікроконтролер ESP32 виступає в якості центрального обчислювального модуля розробленого пристрою, що відповідає за прийом і обробку даних через UART, мережеву взаємодію через Wi-Fi, формування вебінтерфейсу, обробку сенсорного введення, графічне виведення на дисплей. Завдяки двоядерній архітектурі ESP32 можливе паралельне виконання задач, зокрема одночасна обробка даних, оновлення інтерфейсу та обслуговування HTTP-запитів.

У модулі візуалізації використовується кольоровий TFT-екран на базі контролера ILI9488 з роздільною здатністю 320×480 пікселів. Дисплей підключений до ESP32 за допомогою SPI-інтерфейсу та підтримує апаратне прискорення передачі даних. Поверх дисплея встановлена резистивна сенсорна панель XPT2046, яка забезпечує взаємодію користувача з графічним інтерфейсом. Такий підхід дозволяє реалізувати повноцінне меню, навігацію між екранами та отримання детальної інформації без використання додаткових фізичних кнопок.

Зовнішній аналізатор на основі компактного Wi-Fi мікроконтролера ESP8266 підключається до ESP32 через послідовний інтерфейс UART. ESP8266 дає змогу швидко побудувати простий сервер, зчитувач сенсорів або інструмент для тестування радіочастотного середовища, завдяки вмінню одночасно бути «точкою доступу» (AP) — тобто роздавати Wi-Fi, або «станцією» (STA), підключеною до існуючої мережі. Обмін даними здійснюється у вигляді текстових команд та структурованих відповідей у форматі JSON.

Такий підхід дозволяє розмежувати функції збору сирих даних та їх подальшої обробки та візуалізації. ESP32 у цьому випадку виступає в ролі шлюзу (bridge), який забезпечує агрегацію, збереження та інтерпретацію отриманої інформації. Отримані дані одночасно використовуються для оновлення інформації на вбудованому дисплеї, збереження у буфері історії, передачі у вебінтерфейс, що дозволяє уникнути дублювання та забезпечує цілісність даних у всіх режимах роботи пристрою.

Центральний контролер координує роботу дисплея, сенсорної панелі, мережевого інтерфейсу та UART-каналу.

Для підвищення надійності передбачено механізми повторної ініціалізації дисплея, контроль переповнення буферів та обмеження обсягу збережених даних.

Апаратна частина пристрою NetScope тісно інтегрована з програмною частина, яка реалізує повний цикл обробки, аналізу та візуалізації даних. Програмне забезпечення не лише є окремим елементом, а розглядається в якості функціонального продовження апаратної платформи, що дозволяє максимально ефективно використати її ресурси.

Архітектура програмної частини теж побудована за модульним принципом. Кожен програмний модуль відповідає окремому апаратному або логічному блоку: робота з UART, керування дисплеєм, обробка сенсорного введення, мережеві сервіси тестування безпеки та оцінка отриманих даних. Такий підхід спрощує масштабування системи та її супровід.

Задля реалізації програмної частини системи пристрою NetScope використані наступні інструменти:

– ESP-IDF.

– Arduino IDE.

– Visual Studio Code.

IoT Development Framework (ESP-IDF) є офіційним фреймворком для розробки програмного забезпечення під мікроконтролери Espressif і надає доступ до внутрішніх механізмів керування бездротовим модулем. У межах кваліфікаційної роботи ESP-IDF використовується як базовий інструмент для роботи з низькорівневими компонентами Wi-Fi-підсистеми, зокрема керуванням MAC-рівнем, радіоканалами та параметрами фізичного інтерфейсу. Фреймворк забезпечує реалізацію стандарту IEEE 802.11 та дозволяє працювати з кадрами керування без залучення повного мережевого стеку.

Для прикладу наведено фрагмент коду, який реалізує абстрактну модель формування та передавання кадру керування стандарту IEEE 802.11, що використовується для демонстрації принципів низькорівневого керування бездротовим інтерфейсом (див. лістинг 3.1). Основною метою функції є

демонстрація структури кадрів керування та механізмів їх передавання на рівні канального та фізичного рівнів моделі OSI.

Лістинг 3.1 – Абстрактна модель формування та передавання кадру керування стандарту IEEE 802.11

```
/**
 * Demonstration of management frame construction
 * and forced disconnection logic
 */
bool performDeauthSimulation(
    uint8_t* accessPointAddr,
    uint8_t* clientAddr,
    uint8_t  radioChannel,
    uint8_t  disconnectReason
) { uint8_t mgmtFrame[26] = {0};
    // 1. Set frame type (management: deauthentication)
    mgmtFrame[0] = 0xC0;
    // 2. Fill MAC address fields
    copyMac(&mgmtFrame[4],  clientAddr); // destination (STA)
    copyMac(&mgmtFrame[10], accessPointAddr);  // source (AP)
    copyMac(&mgmtFrame[16], accessPointAddr);  // BSSID
    // 3. Specify reason code
    mgmtFrame[24] = disconnectReason;
    // 4. Switch physical radio channel
    setRadioFrequency(radioChannel);
    // 5. Transmit raw management frame
    bool transmitted = sendManagementFrame(
        mgmtFrame,
        sizeof(mgmtFrame)
    );
    // 6. Optional logging for monitoring
    if (transmitted) {
        registerStatistic(EVENT_FRAME_SENT);
    }
    return transmitted;
}
```

У процесі виконання функції формується кадр типу deauthentication, який належить до підкласу кадрів керування IEEE 802.11. Такі кадри використовуються стандартом для керування станами асоціації клієнтських пристроїв у бездротовій мережі та не містять корисних даних прикладного рівня. Формування кадру здійснюється шляхом прямого заповнення байтового буфера відповідно до формату заголовка IEEE 802.11 Management Frame.

Перший байт кадру визначає тип і підтип кадру та відповідає значенню, яке ідентифікує deauthentication-повідомлення. Наступні поля кадру містять MAC-адреси отримувача (Receiver Address), передавача (Transmitter Address) та ідентифікатора мережі (BSSID). Явне задання цих адрес дозволяє змоделювати процес адресації на канальному рівні без використання стеку мережевих протоколів. Окреме поле кадру відводиться під код причини деавтентифікації, який визначається стандартом IEEE 802.11 та використовується для формалізованого опису події розірвання з'єднання. Наявність цього поля дозволяє аналізувати логіку обробки повідомлень керування приймаючою стороною та оцінювати вплив різних сценаріїв керування з'єднанням. Перед передаванням кадру здійснюється вибір радіочастотного каналу, що відповідає фізичному рівню моделі OSI. Такий підхід демонструє зв'язок між логічною структурою кадру та параметрами фізичного середовища передавання, зокрема частотним каналом та радіоінтерфейсом. Передавання кадру виконується через абстрактний низькорівневий інтерфейс, який імітує безпосередню взаємодію з MAC-рівнем без використання протоколів IP, TCP або UDP.

Arduino IDE застосовується як середовище швидкого прототипування та тестування окремих функціональних блоків. Завдяки спрощеній моделі розробки та великій кількості готових бібліотек середовище дозволяє зосередитися на алгоритмічній частині роботи, одночасно забезпечуючи доступ до апаратних ресурсів мікроконтролера. У контексті кваліфікаційної роботи Arduino IDE використовується для первинної валідації логіки роботи з бездротовим інтерфейсом.

Visual Studio Code використовується як основне середовище розробки та аналізу програмного коду. Завдяки підтримці розширень для ESP-IDF і Arduino,

середовище забезпечує інтегровану роботу з системою збору, підсвічування синтаксису, статичний аналіз коду та зручну навігацію великих проєктів. Використання Visual Studio Code сприяє підвищенню якості програмної реалізації та полегшує супровід коду.

3.2 Тестування розробленого пристрою з використанням реальних сценаріїв атак

Під час оцінки безпеки бездротових мереж потрібно дотримуватися певної методології та стандартів — такий підхід допомагає систематизувати інформацію про потенційні вразливості, якими потенційними точками доступу може скористатися зловмисник, які дані можуть ризикувати витоком.

Підхід тестування безпеки в межах етичного хакінгу включає основні етапи: планування, розвідка, атака.

На етапі планування пентестер повинен дотриматися двох особливостей - продумати план і не забути отримати узгодження клієнта. Угода про нерозголошення (NDA) здатна убезпечити від негативних наслідків у майбутньому. Завдяки цьому, приступивши до розвідки, пентестер розумітиме, яка частина мережі має оцінюватися, яка інформація буде зібрана, які методи роботи він буде використовувати.

На етапі розвідки, пентестер вже повинен володіти інформацією про всі бездротові мережі та пристрої, щоб розробити стратегію проведення атаки. Цей процес включає виявлення та документування всіх бездротових мереж, включаючи приховані (неконфігуровані SSID/BSSID), каналів, рівнів сигналу та режимів шифрування, шляхом пасивної операції.

Розроблений пристрій на етапі розвідки забезпечує сканування для зчитування та відображення завдяки вебінтерфейсу інформації про бездротові мережі, що транслюються в ефірі, зокрема:

- ідентифікатор мережі (SSID);
- MAC-адреса точки доступу (BSSID);
- рівень сигналу (RSSI);

– номер каналу;

– тип захисту;

– виробник обладнання.

На основі зібраних даних формується узагальнена статистика, яка дозволяє оцінити стан ефіру в радіочастотному діапазоні заданого середовища для вибору оптимального каналу, виявлення сусідніх мереж і базового аналізу навантаження (рис. 3.2).

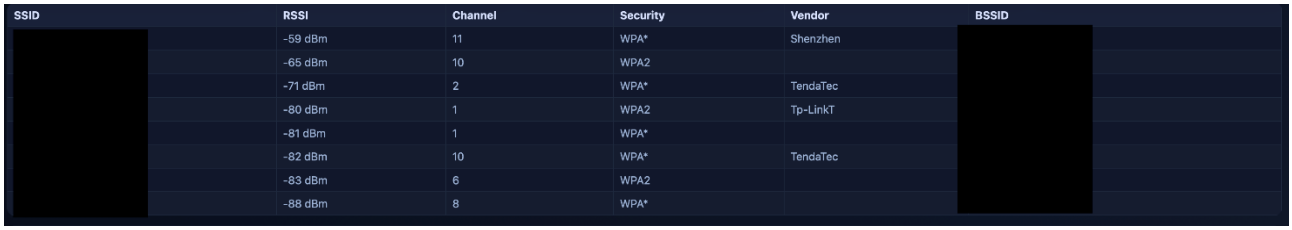


Рисунок 3.2 – Узагальнена статистика бездротових мереж

Важливою частиною цієї фази є надання для кожної мережі рекомендацій/висновків про ступінь захисту та визначення чи існують місця, з яких зловмисник може здійснити атаку. Окрім точок доступу, система підтримує ідентифікацію клієнтських пристроїв, тобто визначення списку MAC-адрес пристроїв, які асоційовані з конкретною точкою доступу (рис. 3.3).

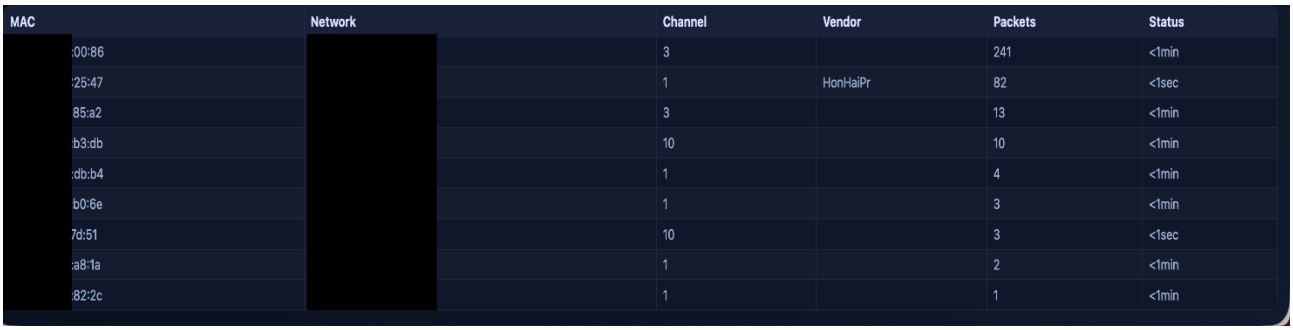


Рисунок 3.3 – Ідентифікація клієнтських пристроїв

Для кожного клієнта фіксується (рис. 3.4):

– MAC-адреса;

– асоційована точка доступу;

– канал зв’язку;

– виробник обладнання;

– кількість переданих пакетів;

– статус активності.

Рисунок 3.4 – Інформація по кожному клієнту

Цей функціонал може бути використаний для базової ідентифікації активних вузлів у мережі та дає змогу оцінити навантаження на AP та виявити невідомі підключення.

Також NetScope підтримує збереження історії сканувань та побудову графіків, які відображають динаміку змін параметрів мережі у часі.

Зокрема візуалізуються такі параметри, як (рис. 3.5):

– рівні сигналу;
– розподіл каналів;
– клієнтські пакети;
– теплова карта каналу;
– навантаження мережі;
– середній рівень RSSI;
– завантаженість каналів;
– загальна кількість пакетів;
– кількість активних клієнтів.
– історія клієнта.

Рисунок 3.5 – Візуалізація статистики та історія сканувань

Історичні дані дозволяють проводити аналіз та виявляти патерни у роботі бездротового середовища.

До додаткових функціональних можливостей розробленого пристрою належать:

– віддалений доступ через вебінтерфейс;
– керування зовнішніми лініями введення-виведення;

– оновлення прошивки по Wi-Fi (OTA);

– автоматичне періодичне сканування.

Завдяки модульній архітектурі NetScope може бути розширений шляхом підключення додаткових сенсорів або модулів без істотних змін базової апаратної частини.

Фаза атаки передбачає, що пентестер може використовувати виявлені вразливості та слабкі місця у бездротовій мережі для злому чи доступу до мережі. Важливо виконати експлуатацію вразливості таким чином, щоб вона була якнайменш помітною.

Після сканування розроблений пристрій має на екрані перелік доступних в радіусі дії мережеві з'єднання з вказаною потужністю сигналу, використаним номером каналу та протоколом безпеки для захисту бездротових мереж; далі NetScope проводить активні методи мережевої розвідки для обраної мережі.

Для прикладу в межах етичного хакінгу для проведення пентесту розроблений пристрій спрямовує деавтентифікаційні пакети проти завчасно підготовленої тестової точки доступу. Приклад логів атаки на вразливу точку доступу представлено на рис. 3.6.

Рисунок 3.6 – Приклад атаки деавтентифікації

Зв'язок на вразливій точці доступу різко стає нестабільним (рис. 3.7). Це свідчить про можливість проведення атаки, оскільки поки мережа слабшає,

зловмисник може розгорнути підроблену точку з тією ж назвою (SSID). Якщо зловмисник ще й знатиме спільний пароль для доступу до мережі (PSK), може реалізувати атаку «Evil twin», тобто розгорнути фальшиву точку доступу, і в приватній мережі весь трафік жертви проходитиме через атакуючий вузол, що дозволяє проводити MITM-сценарії: перехоплення логінів, паролів і зміни контенту.

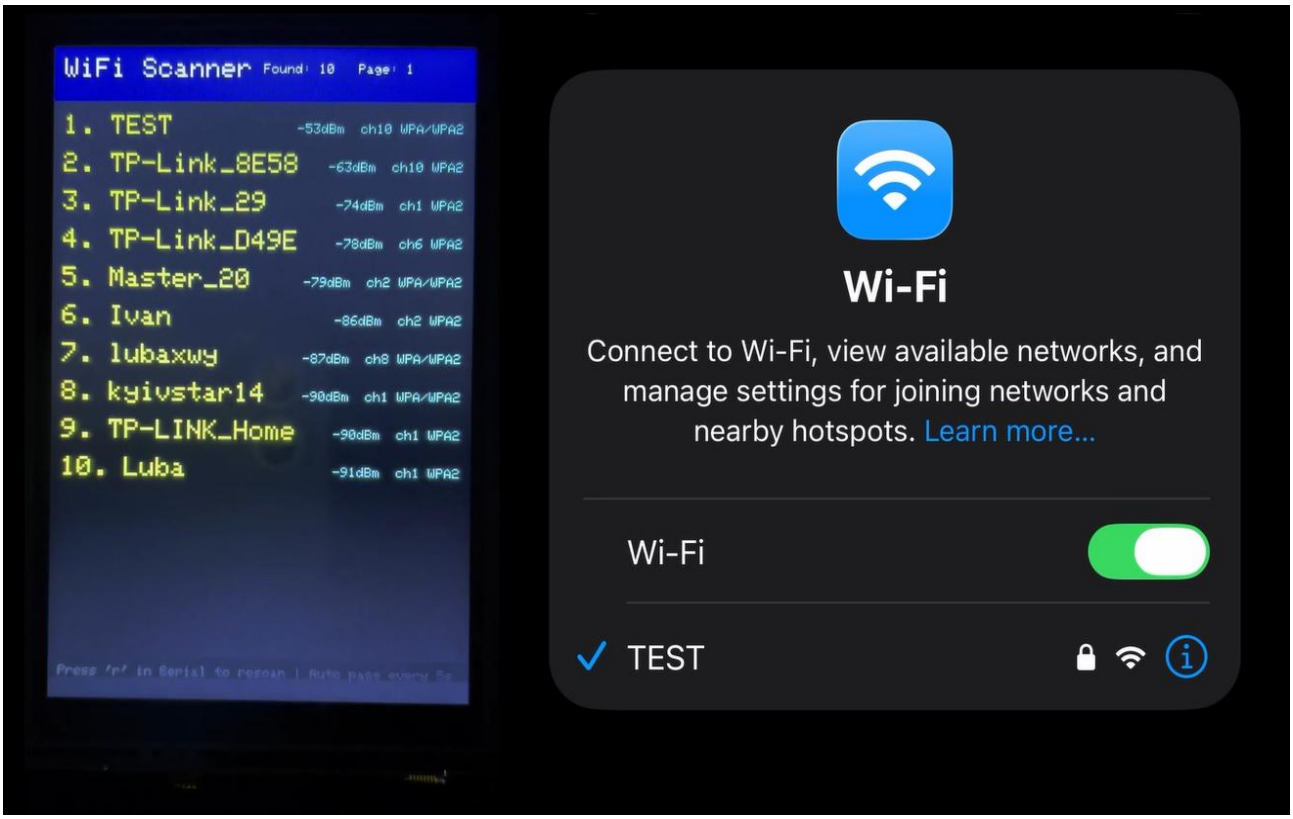
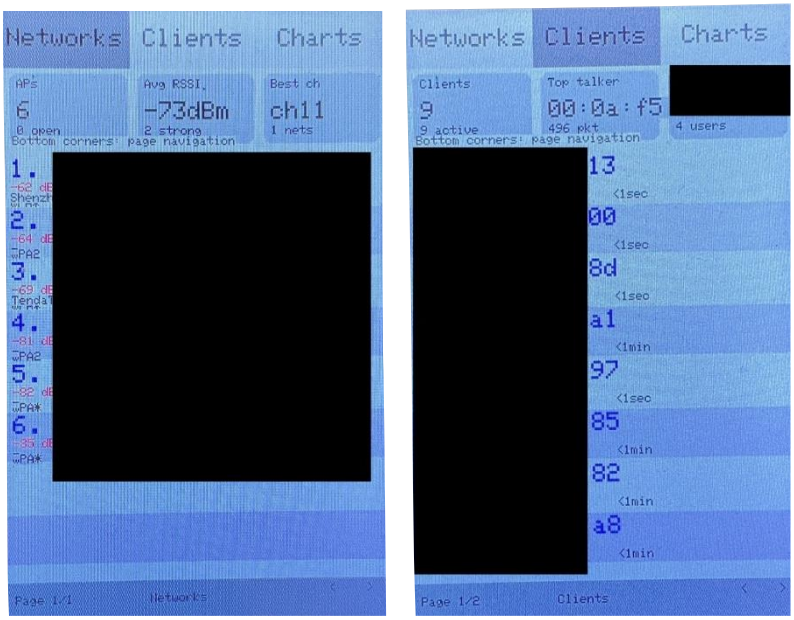


Рисунок 3.7 – Приклад атаки «Evil twin»

Однією з ключових особливостей розробленого пристрою є можливість повноцінної автономної роботи без підключення зовнішніх пристроїв відображення та необов’язкового використання вебінтерфейсу для формування звіту про оцінку безпеки бездротової мережі. Вбудований дисплей забезпечує користувачу доступ до всієї ключової інформації у зручному графічному вигляді.

На екрані реалізовано багатовкладковий інтерфейс, який включає окремі режими перегляду мереж, клієнтів та статистичних графіків (рис. 3.8). Перемикання між режимами здійснюється за допомогою сенсорної панелі, що робить керування інтуїтивно зрозумілим.



а) б)

Рисунок 3.8 – Локальна візуалізація даних на вбудованому дисплею NetScope: а) режим мереж, б) режим клієнтів

На вкладці статистики відображаються узагальнені графіки, які формуються безпосередньо на мікроконтролері (рис. 3.9).

а) б) в)

Рисунок 3.9 – Графіки та статистика на дисплеї пристрою: а) графіки кількості клієнтів та обсягу переданих пакетів, б) стовпчикові діаграми рівнів RSSI для найсильніших точок доступу, в) діаграми завантаженості Wi-Fi каналів

Наявність графіків на вбудованому дисплеї NetScope дозволяє швидко оцінити стан мережі без необхідності використання браузера або ПК, що є особливо корисним у польових умовах.

Локальний дисплей та вебінтерфейс виконують взаємодоповнюючі функції. Локальна панель орієнтована на швидкий огляд і роботу у мобільному форматі, тоді як вебінтерфейс забезпечує функціональні можливості аналізу та зручність роботи з історичними даними. Поєднання локальної візуалізації на вбудованому дисплеї та розширеного вебінтерфейсу дозволяє реалізувати універсальний інструмент аналізу бездротових мереж, придатний для автономного використання та поглибленого дослідження мережевого середовища у стаціонарних умовах.

Фактично, це доступне та портативне рішення для швидкої оцінки безпеки бездротових мереж у реальних умовах, особливо корисне для навчальних закладів, державних підприємств, малих фірм, які не мають власних фахівців або ресурсів для регулярного тестування на проникнення мережевих з’єднань. Основною перевагою розробки є повна автономність пристрою. Він не потребує встановлення додаткового ПЗ чи підключення до живлення. Модульна структура дозволяє розширювати функціонал, наприклад, додавати підтримку нових протоколів чи типів тестів. Результати пентестінгу можуть бути доступні локально та через вебінтерфейс, що спрощує аналіз і створення звітів. Ще одна перевага — низька собівартість у порівнянні з аналогічними комерційними рішеннями.

РОЗДІЛ 4 ОХОРОНА ПРАЦІ ТА БЕЗПЕКА В НАДЗВИЧАЙНИХ СИТУАЦІЯХ

4.1 Охорона праці

Метою роботи є розробка портативного пристрою для тестування безпеки бездротових мереж у межах етичного хакінгу. Даний пристрій розгортаються на енергоефективній мікропроцесорній платформі.

При роботі з даним пристроєм потрібно забезпечити дотримання вимог з охорони праці, техніки безпеки та протипожежної безпеки. Основними регламентуючими нормативними документами є:

– Закон України «Про охорону праці»;

– НПАОП 0.00-7.15-18 «Вимоги щодо безпеки та захисту здоров'я працівників під час роботи з екранними пристроями»;

– ДСН 3.3.6.037-99 «Санітарні норми виробничого шуму, ультразвуку та інфразвуку» [24];

– НАПБ А.01.001-2014 «Правила пожежної безпеки в Україні».

Обов'язки роботодавця щодо забезпечення працівникам комфортних та безпечних умов для здійснення роботи, а також права працівників на такі умови передбачено частиною 2 ст. 2 та ч. 1 ст. 21 КЗпП, а також ст. 13 Закону України «Про охорону праці» [25]. Даний закон визначає основні положення щодо реалізації конституційного права працівників на охорону їх життя і здоров'я у процесі трудової діяльності, на належні, безпечні і здорові умови праці, регулює за участю відповідних органів державної влади відносини між роботодавцем і працівником з питань безпеки, гігієни праці та виробничого середовища і встановлює єдиний порядок організації охорони праці в Україні.

В середньому робочий день офісного працівника складає 7-8 годин (як передбачено нормами Кодексу законів про працю України) при п'яти – або шестиденному робочому тижні, можна зробити висновок, наскільки багато часу доводиться проводити за комп'ютером.

Під час проведення будь-яких робіт, де обробка отриманих даних здійснюється за допомогою комп'ютерів, потрібно дотримуватися гігієнічних норм, правил і вимог техніки безпеки при роботі з персональним комп'ютером (ПК).

Користувачі персональних комп'ютерів мають бути забезпечені відповідними робочими місцями, які відповідатимуть гігієнічним нормам. Конструкції всіх елементів робочого місця та їх взаємного розташування повинні відповідати ергономічним вимогам з урахуванням характеру і особливостей трудової діяльності. Конструкція робочого місця користувача персонального комп'ютера має забезпечити підтримання оптимальної робочої пози.

Робочі місця з персональними комп'ютерами слід так розташовувати відносно світлових прорізів, щоб природне світло падало збоку, переважно зліва.

При розміщенні робочих столів з персональними комп'ютерами слід дотримуватись таких відстаней між їх бічними поверхнями – 1,2 м, відстань від тильної поверхні однієї машини до екрана іншої – 2,5 м.

Конструкція робочого столу має відповідати вимогам ергономіки і забезпечувати оптимальне розміщення на робочій поверхні використовуваного обладнання (дисплея, клавіатури, принтера) і документів.

Екран ПК має розташовуватися на оптимальній відстані від очей користувача, яка становить 600-700 мм, але не ближче між за 700 мм з урахуванням розміру літерно-цифрових знаків і символів. Розташування екрана має забезпечувати зручність зорового споглядання у вертикальній площині під кутом 30° до нормалі.

Для забезпечення захисту і досягнення нормованих рівнів комп'ютерних випромінювань необхідне застосування приекранних фільтрів, локальних світлофільтрів (засобів індивідуального захисту очей) та інших засобів захисту, що пройшли випробування в акредитованих лабораторіях і мають щорічний гігієнічний сертифікат.

Таким чином, для того щоб особи, які працюють з комп'ютерною технікою, меншою мірою втомлювались і зберігали високий рівень працездатності, потрібно раціонально організовувати їхні робочі місця.

Згідно з НПАОП 0.00-7.15-18 «Вимоги щодо безпеки та захисту здоров'я працівників під час роботи з екранними пристроями» для забезпечення безпеки та захисту здоров'я працівників усе випромінювання від екранних пристроїв має бути зведене до гранично допустимого рівня (вплив на людину факторів довкілля - шуму, вібрації, забруднювачів, температури тощо, який не спричиняє соматичних або психічних розладів, а також змін стану здоров'я, працездатності, поведінки, що виходять за межі пристосувальних реакцій) з погляду безпеки та охорони здоров'я працівників [26]. Робочі місця працівників з екранними пристроями мають бути спроєктовані так і мати такі розміри, щоб працівники мали простір для зміни робочого положення та рухів. Цим документом регламентовані мінімальні вимоги безпеки до екранних пристроїв, що необхідно дотримуватись при розробці:

1. Екранні пристрої не мають бути джерелом ризику для працівників.

2. Усе випромінювання, за винятком видимої частини електромагнітного спектра, має бути зведене до незначного рівня з погляду безпеки і охорони здоров'я працівників.

3. Символи на екранних пристроях мають бути чіткими, відповідного розміру. Між символами і рядками символів має бути належна відстань.

4. Зображення на екрані має бути стабільним, без миготінь або інших видів нестабільності.

5. Під час розробки, вибору, замовлення та модифікації програмного забезпечення, а також під час розробки завдань, що передбачають використання устаткування з екранними пристроями, роботодавець має керуватися таким програмним забезпеченням, яке відповідає розв'язуваним завданням і є простим у використанні, а де необхідно - адаптованим до рівня знань і досвіду працівника.

Основні вимоги до пожежної безпеки вказані в НАПБ А.01.001-2014 «Правила пожежної безпеки в Україні», згідно яких у всіх незалежно від призначення приміщеннях, які після закінчення роботи замикаються і не контролюються черговим персоналом, з усіх електроустановок та електроприладів, а також з мереж їх живлення повинна бути відключена напруга (за винятком чергового освітлення, систем протипожежного захисту та

охоронної сигналізації, а також електроустановок, що за вимогами технології працюють цілодобово) [27]. Загальна потужність підключених електроприладів, які електрогенеруюче обладнання буде живити, не повинна перевищувати номінальне навантаження, визначене виробником зазначеного обладнання. Електричні машини, апарати, обладнання, електропроводи та кабелі за виконанням та ступенем захисту повинні відповідати класу зони згідно з ПУЕ, мати апаратуру захисту від струмів короткого замикання та інших аварійних режимів. До початку експлуатації об'єкти (будинки, споруди, приміщення, технологічні установки) повинні бути забезпечені первинними засобами пожежогасіння згідно з Правилами експлуатації та типовими нормами належності вогнегасників, затвердженими наказом Міністерства внутрішніх справ України від 15 січня 2018 року № 25, зареєстрованими в Міністерстві юстиції України 23 лютого 2018 року за № 225/31677.

Дослідження в роботі вимагали взаємодії людини з персональним комп'ютером та портативним пристроєм, тому важливим та актуальним було провести аналіз основних вимог до організації робочих місць з ПК, що дозволило забезпечити комфортні і безпечні умови праці пентестерів.

4.2 Фактори ризику і можливі порушення здоров'я користувачів комп'ютерної мережі

Велика кількість людей проводить багато часу за комп'ютером, що збільшує ризики та можливі негативні наслідки для здоров'я. Довге сидіння за комп'ютером призводить до різних проблем із здоров'ям.

Основні шкідливі чинники тривалої роботи за комп'ютером:

1. Працюючий за комп'ютером тривалий час повинен зберігати відносно нерухоме положення, що негативно позначається на хребті і циркуляції крові у всьому організмі (застій крові). Найпоширенішими причин погіршення стану здоров'я є порушення постави та біль у спині [28]. Неправильна постава, яка зумовлена внаслідок погано організованого робочого місця або неправильно підібраного комп'ютерного стільця, це може спричинити хронічні болі у спині,

шиї та плечах. При тривалих порушеннях циркуляції крові порушується живлення тканин, і пошкоджуються стінки судин, що в свою чергу призводить до їх необоротного розширення. Таке розширення судин спостерігається, наприклад, при геморої.

2. Ще одним серйозним ризиком, пов’язаним із тривалим використанням комп’ютера, є проблеми зі здоров’ям очей. Проведення надто тривалого часу перед екраном може призвести до таких симптомів, як погіршенням зору або напруження очей, яке характеризується сухістю, свербінням, подразненням і втомою очей. Читання інформації з монітора викликає напруження очей, під час читання з монітора відстань від тексту до людини постійно залишається одним і тим же, через це м’язи очей, що регулюють акомодацію, перебувають у постійній напрузі. З часом це може призвести до порушення акомодативної здатності очей і, отже, до порушень зору.

3. Тривала робота на клавіатурі призводить до перенапруження суглобів кисті і м’язів передпліччя. Це поширена проблема - із зап’ястям та кистями, наприклад синдром зап’ястного каналу, який виникає через повторюванні рухи, наприклад використання миші чи клавіатури [28].

4. Монітори – сильне джерело електромагнітних полів. Постійна дія на організм людини, прискореними електронами, приводить до різних розладів нервової системи та очей. Також важливо розглянути вплив на якість сну та загальне фізичне здоров'я. Багато користувачів комп'ютерів скаржаться на порушення сну, що може бути пов'язано з надмірним впливом на світлові екрани перед сном. Це світло пригнічує вироблення мелатоніну, гормону сну, заважаючи людям засинати та підтримувати здоровий цикл сну. Використання спеціальних програм або окулярів для блокування синього світла є важливим для тих, хто регулярно працює з комп'ютерами ввечері. Фізична неактивність, яка часто супроводжує довготривалу роботу за комп'ютером, також є фактором ризику для ряду хронічних захворювань, серцево-судинні захворювання та діабет другого типу. Недостатня фізична активність призводить до уповільнення метаболізму, що може спричинити набір ваги і зниження загальної фізичної форми. Це підвищує ризик розвитку серцевих захворювань.

5. Робота за комп’ютером передбачає переробку великого масиву інформації і постійну концентрацію уваги, тому при тривалій роботі за комп’ютером нерідко розвивається розумова втома і порушення уваги.

6. Людина, що працює за комп’ютером, змушена весь час приймати рішення, від яких залежить ефективність роботи. Тому тривала робота за комп’ютером часто є причиною хронічного стресу. Робота за комп'ютером часто пов'язана з високим рівнем стресу, особливо в умовах коли терміни стислі, а вимоги високі. Це може призвести до вигоряння, депресії та інших психологічних проблем. Крім того, ізоляція, яка часто супроводжує роботу вдома або в невеликих кабінетах, може вплинути на соціальне та емоційне самопочуття.

7. Залежність від Інтернету та соціальних медіа є ще однією проблемою, з якою стикаються користувачі комп'ютерних мереж. Ця залежність може призвести до зниження продуктивності, соціальної ізоляції та погіршення психічного здоров'я. Важливо встановлювати межі та регулярно проводити час без використання електронних пристроїв.

Працюючі починають акцентувати увагу на значну напругу зорового апарату з появою скарг на незадоволеність роботою, головні болі, дратівливість, порушення сну, втому і хворобливі відчуття в очах, в поясниці, в ділянці шиї і руках. Тому керівникам підприємств, де використовується комп’ютерна техніка, необхідно комплексно вирішувати проблеми ергономіки, гігієни і організації режимів праці та відпочинку.

Для зменшення цих ризиків існують різні стратегії.

По-перше, для збереження здоров’я працівників, необхідно дотримуватися всіх вимог до приміщень, де відбувається робота з комп’ютерами.

По-друге, необхідно подбати про правильне розміщення робочих місць як щодо безпосередньо кімнати, так і щодо всієї будівлі підприємства. Це важливо - правильно організувати робоче місце.

По-третє, слід забезпечити робітників сучасними комп’ютерними меблями, які були б зручними у використанні і не доставляли відчуття дискомфорту, були пристосовані до особливостей людського організму. Ергономічні крісла,

належно розташовані монітори та клавіатури, підставка для ніг, регулярні перерви для руху та розтяжки можуть значно знизити ризик мускул скелетних проблем.

Також не слід забувати і про самі комп’ютери. Необхідно забезпечити всіх працівників сучасною комп’ютерною технікою (рідкокристалічні дисплеї, які можна назвати майже «зеленими» пристроями, безпечними для здоров’я людей; використання різноманітних сучасних ергономічних клавіатур) або спеціальними захисними пристроями (наприклад, захисний фільтр). Використання спеціальних окулярів або застосування програм, що знижують синє світло від екранів, можуть допомогти зменшити втому очей [28].

Крім того, повинен бути встановлений правильний режим праці та відпочинку. Що стосується психологічного здоров'я, важливо забезпечити баланс між роботою та особистим життям, включаючи регулярні перерви, хобі, соціальну взаємодію та вправи на свіжому повітрі. Також корисною може бути практика медитації для зниження рівня стресу.

Дотримання вищевказаних заходів покращить роботу підприємства, що підвищить продуктивність праці. Працівники завжди будуть в гарному настрої і не скаржитимуся на погане самопочуття.

Адміністрація підприємства повинна періодично проводити з персоналом бесіди про можливі наслідки взаємодії з комп’ютером, інструктаж про правила роботи за комп’ютером (правильна поза, вправи, перерви і т.д.), щоб сформувати правильне, раціональне ставлення працівника до свого здоров’я, тому що всі перераховані вище заходи можуть виявитися марними, якщо працівники самі не оцінять ситуацію, що склалася і не змінять поведінку під час роботи на комп’ютері.

ВИСНОВКИ

В ході дослідження проведено детальний аналіз сучасного стану захисту бездротових мереж, в межах якого розглянуто стандарти бездротового зв’язку, такі як IEEE 802.11 - Wi-Fi, IEEE 802.15.1 - Bluetooth, IEEE 802.15.4 - ZigBee та стільникового зв'язку (GSM, 4G LTE, 5G); програмні та апаратні інструменти для тестування безпеки бездротових мереж, такі сканери вразливостей, фреймворки пентестінгу, аналізу трафіку, як Kali Linux, Aircrack-ng, Wifite, Reaver, PixieWPS, Kismet, а також пристрої WiFi Pineapple й Flipper Zero. Результати аналізу показують, що тестування безпеки бездротових мереж необхідно для виявлення можливостей доступу до мережі чи системи, яке дає підставу до порушення цілісності та конфіденційності даних. Ефективний захист неможливий без цілісного підходу, який поєднує криптографічні механізми, регулярний активний аудит, в тому числі етичний хакінг, лабораторні випробування з використанням апаратних платформ та постійну підготовку персоналу. Також проведено дослідження стандартів безпеки бездротових мереж, зокрема WEP, WPA, WPA2, WPA3, на предмет відмінності алгоритмів шифрування та процедури автентифікації з захищеним доступом до бездротової мережі, оскільки саме ці механізми перешкоджають проведенню більшості атак.

Як результат, розроблено пристрій для тестування безпеки бездротових мереж NetScope, що здатен автоматично виявляти бездротові мережі, підключені пристрої, вразливості, зокрема на WPA/WPA2, відкриті точки доступу, слабкі паролі, застарілі протоколи шифрування, WPS; проводити атаки, включаючи атаки деавтентифікації, спам-маяки, а також клонувати мережі.

Тобто, завдяки розробленому пристрою можна проводити тестування і оцінку безпеки бездротових мереж, в тому числі визначати чи піддається мережеве з’єднання атакам, які призводять до відмови або до різних типів MITM-атак, що несуть істотний ризик компрометації трафіку, особливо в корпоративному сегменті.

Розроблений доступний та портативний пристрій NetScope вирішує актуальну проблему, а саме дозволяє оперативно перевірити рівень захищеності точок доступу, контролерів, клієнтських пристроїв у будь-якому місці; забезпечує зниження ризиків витоку даних шляхом швидкої діагностики вразливостей в конфігурації бездротових мереж в реальних умовах та може бути використаний як: польовий пристрій для аудитів безпеки, інтегрований компонент систем моніторингу підприємств або смарт-будівель, навчальний інструмент для здобувачів ВО за спеціальністю «Кібербезпека та захист інформації».

Зокрема результати кваліфікаційної роботи магістра використано в навчальному процесі кафедри кібербезпеки при проведенні лабораторних робіт з дисципліни «Тестування та оцінка інформаційної безпеки».

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Babakov, R. M., et al. "Internet of Things for Industry and Human Application. Vol. 3." (2019): 1-917.
2. Sachenko A.O., Kochan V.V., Bykovyy P.Ye., Zahorodnia D.I., Osolinskyy O.R., Skarga-Bandurova I.S., Derkach M.V., Orekhov O.O., Stadnik A.O., Kharchenko V.S., Fesenko H.V. Internet of Things for intelligent transport systems: Practicum / A.O. Sachenko (Eds.) – Ministry of Education and Science of Ukraine, Ternopil National Economic University, Volodymyr Dahl East Ukrainian National University, National Aerospace University "Kharkiv Aviation Institute", 2019. – 135 p. ISBN 978-617-7361-92-2. https://aliot.eu.org/wp-content/uploads/2019/10/ALIOT_ITM3_IoT-for-Int-TransSys_web.pdf
3. Palamar, A., Karpinski, M. P., Palamar, M., Osukhivska, H., & Mytnyk, M. (2022, November). Remote Air Pollution Monitoring System Based on Internet of Things. In ITTAP (pp. 194-204).
4. Karpinski, M., Korchenko, A., Vikulov, P., Kochan, R., Balyk, A., & Kozak, R. (2017, September). The etalon models of linguistic variables for sniffing-attack detection. In 2017 9th IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems : Technology and Applications (IDAACS) (Vol. 1, pp. 258-264). IEEE.
5. ZAGORODNA, N., STADNYK, M., LYPA, B., GAVRYLOV, M., & KOZAK, R. (2022). Network Attack Detection Using Machine Learning Methods. Challenges to national defence in contemporary geopolitical situation, 2022(1), 55-61.
6. Матюк Д.С. Бездротові технології системи управління квадрокоптером / Д.С. Матюк, М.В. Деркач // ІТ-Ідея – 2022: збірник науково-практичних праць. – Київ: вид-во Східноукр. ун-ту ім. В. Даля, 2022. – С.46-48.
7. Stanko, A., Wieczorek, W., Mykytyshyn, A., Holotenko, O., & Lechachenko, T. (2024). Realtime air quality management: Integrating IoT and Fog computing for effective urban monitoring. CITI, 2024, 2nd.

8. Malyuta Y., Derkach M., Lobur T. (2025) Modelling Fog Computing Network Architecture for Secure IoT Data Processing. Security of Infocommunication Systems and Internet of Things, vol 3, no 2.
9. Jang, Y., & Kim, S. (2024). Understanding Mobile OTT Service Users' Resistance to Participation in Wireless D2D Caching Networks. Behavioral Sciences, 14(3), 158.
10. Aircrack-ng. Available online: https://www.aircrack-ng.org/doku.php?id=aircrack-ng (accessed on 25 October 2025).
11. Kismet. Available online: https://www.kismetwireless.net/docs/readme/intro/kismet/ (accessed on 2 November 2025).
12. Witemyre, S.J.; Abegaz, T.T.; Payne, B.R.; Mady, A. Hijacking Wireless Communications Using WiFi Pineapple NANO as a Rogue Access Point. In Proceedings of the 2018 KSU Proceedings on Cybersecurity Education, Research and Practice (CCERP), Kennesaw,GA, USA, 29 October 2018 (PDF) Exploiting Maritime Wi-Fi: Practical Assessment of Onboard Network Vulnerabilities.
13. Banakh, R., Nyemkova, E., Justice, C., Piskozub, A., & Lakh, Y. (2024). Data Mining Approach for Evil Twin Attack Identification in Wi-Fi Networks. Data, 9(10), 119.
14. Vukšić, M., Ćelić, J., Panić, I., & Cuculić, A. (2025). Exploiting Maritime Wi-Fi: Practical Assessment of Onboard Network Vulnerabilities. Journal of Marine Science and Engineering, 13(8), 1576.
15. Hautzinger, D. The Wifi Pineapple-The Forbidden Fruit of Networking. In Proceedings of the Summer Interdisciplinary Research Symposium, Valparaiso, IN, USA, 7–12 July 2021.
16. ISCAP. (2024). Exploring Signals Hacking with Flipper Zero (teaching case/proceedings). ISCAP Conference Proceedings.
17. Pava, Robert & Martin, Reese & Mishra, Sushma. (2024). Unveiling exploitation potential: a comparative analysis of flipper zero and rubber ducky. Issues in Information Systems. 25. 84 - 95.

18. M. Derkach, et al., CrypticWave: A Zero-Persistence Ephemeral Messaging System with Client-Side Encryption, in: Cyber Security and Data Protection, vol. 4042, 2025, 316–323.
19. Деркач М. В., Мишко О. Є. Використання алгоритму шифрування AES-256-CBC для зберігання даних автентифікації автономного помічника. Наукові вісті Далівського університету. 2023. №24.
20. SONG, J. U. N. H. Y. U. K. (2008). Iwata T.: The Advanced Encryption Standard-Cipher-based Message Authentication Code Pseudo-Random Function-128 (AESCMAC-PRF-128) Algorithm for the Internet Key Exchange.
21. Mishko, O., Matiuk, D., & Derkach, M. (2024). Security of remote iot system management by integrating firewall configuration into tunneled traffic. Вісник Тернопільського національного технічного університету, 115(3), 122-129.
22. Матюк Д.С. Аналіз пристроїв для тестування бездротових мереж на проникнення / Д.С. Матюк, Б.В. Наконечний, С.І. Олійник, М.В. Деркач // ІТ-Ідея – 2025: збірник науково-практичних праць. – Київ: вид-во Східноукр. ун-ту ім. В. Даля, 2025.
23. Матюк Д.С. NetScope: ПЕНТЕСТІНГ БЕЗДРОТОВИХ МЕРЕЖ / Д.С. Матюк, М.В. Деркач // Актуальні задачі сучасних технологій : зб. тез доповідей XIV міжнар. наук.-техн. конф. молодих учених та студентів, (Тернопіль, 11-12 грудня 2025) / М-во освіти і науки України, Терн. націон. техн. ун-т ім. І. Пулюя [та ін.]. – Тернопіль: ФОП Паляниця В.А., 2025. – С. 302-304.
24. ДСН 3.3.6.037-99 «Санітарні норми виробничого шуму, ультразвуку та інфразвуку».
25. Закон України від 14.10.1992 № 2694-XII Про охорону праці.
26. НПАОП 0.00-7.15-18 «Вимоги щодо безпеки та захисту здоров’я працівників під час роботи з екранними пристроями».
27. НАПБ А.01.001-2014 «Правила пожежної безпеки в Україні».
28. Шкідливий вплив персонального комп’ютера на здоров’я людини. URL: https://ir.lib.vntu.edu.ua/bitstream/handle/123456789/21370/5363.pdf

Додаток А Публікації

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Тернопільський національний технічний університет імені Івана Пулюя
Маріборский університет (Словенія)
Технічний університет у Кошице (Словаччина)
Вільнюський технічний університет ім. Гедимінаса (Литва)
Краківський економічний університет (Польща)
Вроцлавський економічний університет (Польща)
Університет «Опольська Політехніка» (Польща)
Національний університет «Полтавська політехніка імені Юрія Кондратюка»
Вінницький національний аграрний університет
Львівський національний університет ім. І. Франка
Головне управління Пенсійного фонду в Тернопільській області
Наукове товариство ім. Шевченка
Тернопільський обласний комунальний інститут післядипломної педагогічної освіти
Сумський державний педагогічний університет
Запорізький національний університет

АКТУАЛЬНІ ЗАДАЧІ СУЧАСНИХ ТЕХНОЛОГІЙ

Збірник

тез доповідей

XIV Міжнародної науково-технічної конференції молодих учених та студентів

11-12 грудня 2025 року

УКРАЇНА
ТЕРНОПІЛЬ – 2025

Далеко не всі мед заклади можуть собі дозволити потрібне обладнання, тривалий процес дозрівання тканин - це з мінусів, плюсами ж є перспектива створення органів для: Трансплантації та лікування дефіциту донорських органів, можливість друкувати тканини з клітин пацієнта, створення хрящів, кісток, шкіри, судин для Реконструктивної медицини, а також зниження вартості лікування у майбутньому.

Біодрук має величезний потенціал кардинально змінити медицину та наукові дослідження. Очікується, що технологія дозволить створювати повноцінні живі органи для трансплантації, що допоможе вирішити проблему нестачі донорів і значно знизить ризик відторгнення, адже органи створюватимуться з клітин самого пацієнта. Також біодрук відкриє можливість персоналізованої медицини, коли тканини та імпланти точно відповідатимуть індивідуальним особливостям людини. Крім того, у перспективі лікарі зможуть друкувати тканини безпосередньо у тілі пацієнта під час операцій, що прискорить загоєння ран і відновлення пошкоджених ділянок. Загалом біодрук стане основою нової епохи регенеративної медицини, суттєво розширюючи можливості Лікування та підвищуючи якість життя людей.

Література

1. Michele Conti, Michele Marino. Bioprinting From Multidisciplinary Design to Emerging Opportunities, Academic Press, Elsevier, 2022.-P. 19-49.

2. Mitchell Maika G. Bioprinting: techniques and risks for regenerative medicine. London, San Diego, Cambridge, Oxford, 2017.-P. 123-140.

3. Yang Wu, Jerry Fuh and Ibrahim Tarik Ozbolat. 3D Bioprinting in Tissue and Organ Regeneration, 2023.-P. 247-264.

4. Що таке біодрук URL:
http://ua.insta3dm.com/info/what-is-3d-bioprinting-simply-explained-f-71989890.html

5. Перспективи біодруку URL:
https://easy3dprint.com.ua/uk/3d-druk-dlya-meditsini/

6. Принцип роботи біопринтингу URL:
https://www.imena.ua/blog/3d-bioprint-part-1/

УДК 004.7.056

Д.С. Матюк; М.В. Деркач, канд. техн. наук, доц.
(Тернопільський національний технічний університет імені Івана Пулюя, Україна)

NetScope: ПЕНТЕСТІНГ БЕЗДРОТОВИХ МЕРЕЖ

D.S. Matiuk, M.V. Derkach, Ph.D., Assoc. Prof.

NetScope: WIRELESS NETWORK PENTESTING

Бездротові мережі можуть бути розгорнуті та працювати у різних середовищах: комерційних, урядових, освітніх, а також у звичайних житлових будинках. До того ж технології бездротової передачі сигналу особливо сприяють концепції Інтернету речей (Internet of Things, IoT), на яку переходять все більше пристроїв, що підвищують наш комфорт перебування в Інтернеті [1].

В результаті кількість бездротових мереж, як і кількість об'єктів для атак, буде тільки збільшуватися. Клієнти та організації повинні розуміти всі ризики використання бездротових мереж та знати, як зловмисники атакують ці системи. Пентестери повинні гарантувати, що ці мережі мають необхідну кількість елементів керування безпекою та у їхній конфігурації відсутні помилки. Для цього використовують сканери

вразливостей, фреймворки пентестування та аналізу трафіку, що виявляють конфігураційні похибки й відомі CVE. Складність мереж і різноманітність протоколів (Wi-Fi, ZigBee, Bluetooth, радіочастотного діапозону 2.4 ГГц) для ефективного захисту вимагають багаторівневих контрзаходів, які охоплюють як активні, так і пасивні вектори атак, що призводить до комбінування програмних й апаратних інструментів, які здатні перевіряти рівень захищеності точок доступу, контролерів, клієнтських пристроїв, виявити вразливості бездротових мереж [2]. Розробка апаратної платформи надає змогу проводити польові випробування, швидко розгортати точки атаки та мінімізувати час налаштування.

Наразі, розроблено пристрій для тестування безпеки бездротових мереж NetScope, що здатен виявляти вразливості, зокрема WPA/WPA2, відкриті точки доступу, слабкі паролі, застарілі протоколи шифрування, WPS; здатний автоматично виявляти бездротові мережі та підключені пристрої; проводити атаки, включаючи атаки деавтентифікації, спам-маяки, а також клонувати мережі. Це доступне та портативне рішення для швидкої оцінки безпеки бездротових мереж у реальних умовах, особливо корисне для навчальних закладів, державних підприємств, малих фірм, які не мають власних фахівців або ресурсів для регулярного тестування на проникнення мережевих з'єднань. Основною перевагою розробки є повна автономність пристрою. Він не потребує встановлення додаткового програмного забезпечення чи підключення до живлення. Модульна структура дозволяє розширювати функціонал, наприклад, додавати підтримку нових протоколів чи типів тестів. Результати пентестінгу можуть бути доступні через вебінтерфейс, що спрощує аналіз і створення звітів. Ще одна перевага — низька собівартість у порівнянні з аналогічними комерційними рішеннями.

Фактично NetScope здатен виявляти вразливості до MITM-сценаріїв, підміни точок доступу та інших загроз у бездротових мережах. Принцип дії наступний: для початку пристрій проводить сканування, на екрані якого з'являється перелік доступних в радіусі дії мережевих з'єднань з вказаною потужністю сигналу, використаним номером каналу та протоколом безпеки для захисту бездротових мереж; далі розроблений пристрій проводить пентест для обраної мережі.

Для прикладу в межах етичного хакінгу для проведення пентесту розроблений пристрій NetScope спрямовує деаутентифікаційні пакети проти точки доступу TEST, зв'язок різко стає нестабільним (рис. 1). Це свідчить про можливість проведення атаки, оскільки поки мережа слабшає, зловмисник може розгорнути підроблену точку з тією ж назвою (SSID). Якщо зловмисник ще й знатиме спільний пароль для доступу до мережі (PSK), може реалізувати атаку «Evil twin», тобто розгорнути фальшиву точку доступу, і в приватній мережі весь трафік жертви проходитиме через атакуючий вузол, що дозволяє проводити MITM-сценарії: перехоплення логінів, паролів і зміни контенту.

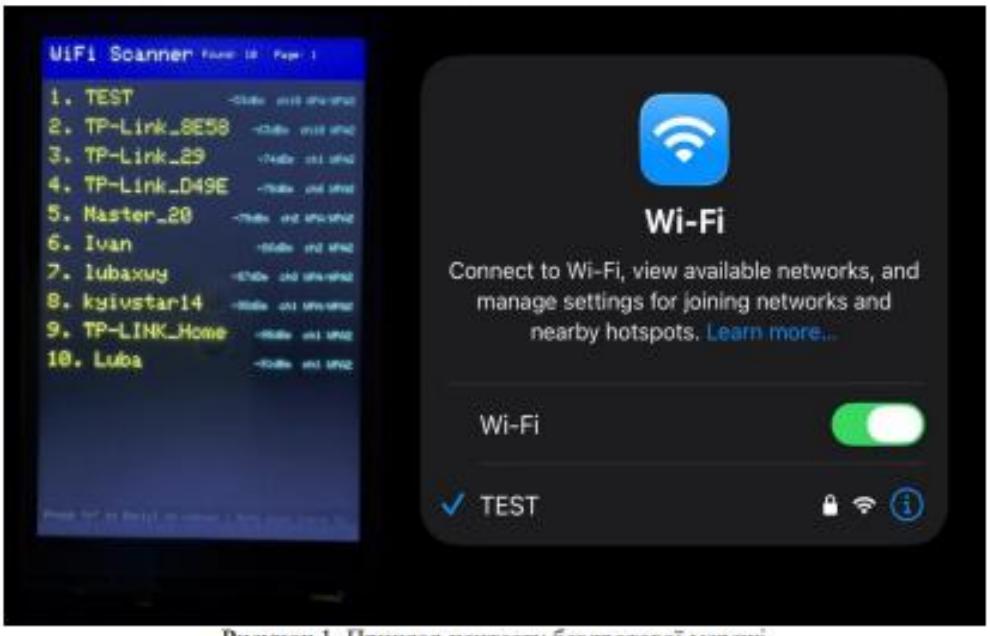


Рисунок 1. Приклад пентесту бездротової мережі

Тобто, завдяки розробленому пристрою можна проводити тестування і оцінку безпеки бездротових мереж, а саме визначати чи піддається мережеве з'єднання атакам, які призводять до відмови або до різних типів MITM-атак, що несуть істотний ризик компрометації трафіку, особливо в корпоративному сегменті.

В цілому пристрій NetScope вирішує актуальну проблему, зокрема дозволяє оперативно перевірити безпеку бездротових мереж у будь-якому місці; забезпечує зниження ризиків витоку даних шляхом швидкої діагностики вразливостей у реальних умовах та може бути використаний як: навчальний інструмент для здобувачів вищої освіти за спеціальністю «Кібербезпека та захист інформації», польовий пристрій для аудитів безпеки, інтегрований компонент систем моніторингу підприємств або смарт-будівель.

Література

1. Sachenko A.O., Kochan V.V., Bykovyy P.Ye., Zahorodnia D.I., Osolinskyy O.R., Skarga-Bandurova I.S., Derkach M.V., Orekhov O.O., Stadnik A.O., Kharchenko V.S., Fesenko H.V. Internet of Things for intelligent transport systems: Practicum. Ministry of Education and Science of Ukraine, Ternopil National Economic University, Volodymyr Dahl East Ukrainian National University, National Aerospace University "Kharkiv Aviation Institute", 2019. 135 p. ISBN 978-617-7361-92-2. URL: https://aliot.eu.org/wp-content/uploads/2019/10/ALIOT ITM3 IoT-for-Int-TransSys_web.pdf

2. Derkach, M., Matiuk, D., Skarga-Bandurova, I., & Zagorodna, N. CrypticWave: A zero-persistence ephemeral messaging system with client-side encryption, in: Cyber Security and Data Protection, vol. 4042, 2025, P.316–323.

СЕРТИФІКАТ

виданий

Матюк Данилу, Наконечному Богдану,

Олійнику Степану

за участь у XI Міжнародному Форумі "IT-Ідея 2025"

з проєктом

Аналіз пристроїв для тестування бездротових мереж

на проникнення

Проректор з наукової роботи СНУ ім. В.Даля
д.т.н., проф. **Целіщев О.Б.**

Завідувач кафедри КНІ СНУ ім. В.Даля
д.т.н., проф. **Рязанцев О.І.**

«12» грудня 2025р.

МП

СХІДНОУКРАЇНСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ ІМЕНІ ВОЛОДИМИРА ДАЛЯ

RESPONSE

CSE КАФЕДРА КОМП'ЮТЕРНИХ НАУК ТА ІНЖЕНЕРІЇ