МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

Національний університет кораблебудування імені адмірала Макарова

Навчально-науковий інститут автоматики і електротехніки

Кафедра комп'ютерних технологій та інформаційної безпеки

ЗАТВЕРДЖУЮ
Завідувач кафедри комп'ютерних технологій та інформаційної безпеки, к.т.н., доцент
_____ С.М. Нужний
«10» 12 2025 р.

КВАЛІФІКАЦІЙНА РОБОТА
АНАЛІЗ ЗАХИЩЕНОСТІ БЕЗДРОТОВИХ МЕРЕЖ WI-FI

Ступінь вищої освіти: магістр
Галузь знань: 14 Електрична інженерія
Спеціальність: 141 «Електроенергетика, електротехніка та електромеханіка»
Освітньо-професійна програма: Системи технічного захисту інформації, автоматизація її обробки

Виконав: студент 6 курсу групи 6366м
Шульженко Владислав Олександрович _____

Кваліфікаційна робота містить результати самостійного виконання навчального завдання. Використання ідей, результатів і текстів інших авторів мають посилання на відповідне джерело

Керівник:
к.т.н., доцент, доцент кафедри комп'ютерних технологій та інформаційної безпеки

Козирєв Сергій Сергійович _____

Миколаїв – 2025

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

Національний університет кораблебудування імені адмірала Макарова

Навчально-науковий інститут автоматики і електротехніки

ЗАТВЕРДЖУЮ
Гарант освітньої програми,
д.т.н., професор,
професор кафедри КТІБ
_____ Передерій В.І.
«14» ____10____ 2025 р.

ЗАВДАННЯ

на кваліфікаційну роботу

Студент: Шульженко Владислав Олександрович

Курс:6

Група: 6366м

Ступінь вищої освіти: магістр

Галузь знань: 14 Електрична інженерія

Спеціальність: 141 «Електроенергетика, електротехніка та електромеханіка»

Освітньо-професійна програма: Системи технічного захисту інформації, автоматизація її обробки

1. Тема роботи: Аналіз захищеності бездротових мереж Wi-Fi

затверджена наказом НУК від «14» ____10____2025 р. № 1217-42

2. Вихідні дані до роботи: теоретичні відомості про протоколи роботи бездротової мережі Wi-Fi; існуючі засоби зламу захисту бездротових мереж, існуючи методи протидії зламу захисту бездротових мереж.

вивчення теоретичних відомостей про побудову і роботу бездротових мереж; аналіз можливих загроз безпеці бездротових мереж; розробка рекомендацій для підвищення безпеки бездротових мереж.

4. Терміни виконання завдання:
термін видачі завдання: «01- 05» вересня 2025 р.
термін подання роботи: «18» грудня 2025 р.

6. План-графік виконання кваліфікаційної роботи

п/п	Заходи	Дата		Готовність
		Навч. тиждень	Контрольна дата	
1.	Наукове стажування	1 - 8	27.10.2025	Звіт з наукового стажування
2.	Організаційні збори	9	29.10.2025	Попередній варіант змісту КР
3.	Рубіжний контроль	10	05.11.2025	Попередній варіант оглядових розділів, звіт з практика
4.	Рубіжний контроль	13	27-28.11.2025	Доповідь на 13-ій Всеукраїнській науково-технічній конференції з міжнародною участю «СПІБТ–2025»
5.	Рубіжний контроль	14	3.12.2025	1. Попередній варіант повної КР 2. Попередній варіант презентації
6.	КЕ на рівень «магістра»	15	8,9.12.2025	Складання державного екзамену зі спеціальності на ступінь магістра
7.	Перевірка на плагіат	15	10.12.2025	Електронний варіант кваліфікаційної роботи, попередній захист (робота передається студентом на кафедру для внутрішньої рецензії).
8.	Оформлення КР та супутньої документації	16	15-17.12.2025	1. Оформлена КР (в форматі pdf) У разі отримання позитивної внутрішньої рецензії, КР подається на зовнішню рецензію. 2. Оформлена презентація (в форматі pdf).
9.	Подання документів на захист	16	18.12.2025	1. Подання щодо захисту КР: тема, успішність, висновок керівника та висновок кафедри про КР. 2. Зовнішня рецензія (окремо від КР). Резюме на КР. 3. Електронний варіант презентації. 4. Електронний варіант КР на диску
10.	Захист ДР	17	22,23,24 12.2025	1. Приєднання студента до засідання кваліфікаційної комісії (конференції) у встановлений час для проведення процедури дистанційного захисту 2. Процедура захисту КР.

Керівник
к.т.н., доцент, доцент кафедри комп'ютерних технологій
та інформаційної безпеки, _____ С.С. Козирєв

Студент _____ В.О. Шульженко

АНОТАЦІЯ

Шульженко В.О. Аналіз захищеності бездротових мереж *Wi-Fi*.

Кваліфікаційна робота на здобуття ступеня вищої освіти «магістр» за спеціальністю 141 «Електроенергетика, електротехніка та електромеханіка» галузі знань «Інформаційні технології». – Національний університет кораблебудування імені адмірала Макарова, Миколаїв, 2025.

Пояснювальна записка: 69 с., 15 рис., 25 посилань.

Магістерська кваліфікаційна робота передбачає розробку комплексної архітектури захисту бездротової інфраструктури. Основною метою проекту є підвищення рівня захищеності корпоративних мереж Wi-Fi шляхом впровадження сучасних протоколів аутентифікації та автоматизації процесів безпеки.

Проект включає аналіз еволюції стандартів IEEE 802.11, виявлення критичних вразливостей протоколу WPA2 та експериментальне моделювання атак на інфраструктуру. Результатом дипломної роботи є створення захищеної мережевої топології з використанням WPA3-Enterprise (EAP-TLS), системи виявлення вторгнень (WIDS) та інтеграцією інструментів DevSecOps для автоматичного реагування на інциденти.

Висновки проекту підсумовують проведену роботу та надають практичні рекомендації.

Ключові слова: *Wi-Fi, WPA3, EAP-TLS, Penetration Testing, WIDS, DevSecOps, Kali Linux.*

SUMMARY

Shulzhenko V.O. Analysis of Wi-Fi Network Security.

Master's Qualification Work for the Higher Education Degree "Master" in Specialty 141 "Electric Power Engineering, Electrical Engineering and Electromechanics" within the Field of Knowledge 12 "Information Technologies". – Admiral Makarov National University of Shipbuilding, Mykolaiv, 2025.

Explanatory note: 69 p., 15 figures, 25 references.

The master's qualification work involves the development of a comprehensive security architecture for wireless infrastructure. The main goal of the project is to enhance the security level of corporate Wi-Fi networks by implementing modern authentication protocols and security process automation.

The project includes an analysis of the IEEE 802.11 standards evolution, identification of critical WPA2 protocol vulnerabilities, and experimental modeling of infrastructure attacks. The result of the thesis is the creation of a secure network topology using WPA3-Enterprise (EAP-TLS), a Wireless Intrusion Detection System (WIDS), and the integration of DevSecOps tools for automated incident response.

The project's conclusions summarize the work carried out and provide practical recommendations.

Keywords: *Wi-Fi, WPA3, EAP-TLS, Penetration Testing, WIDS, DevSecOps, Kali Linux.*

ЗМІСТ

ВСТУП

Актуальність теми. В умовах стрімкої цифровізації суспільства та переходу бізнес-процесів у віддалений формат, бездротові мережі (*Wi-Fi*) стали критичним елементом інформаційної інфраструктури. За даними аналітичних звітів за 2024 рік, середня вартість витоку даних для компаній сягнула 4,88 млн доларів США, а кількість кібератак зросла на 30% порівняно з попереднім періодом [23]. Особливе занепокоєння викликає зростання кількості публічних точок доступу, яка, за прогнозами, досягне 3,15 мільярда до 2030 року, що значно розширює поверхню атак [24].

Еволюція стандартів *IEEE 802.11* (від *802.11n* до сучасних *802.11ax*/*be*) супроводжується впровадженням нових протоколів безпеки, таких як *WPA3*. Проте, як показують дослідження 2025 року, навіть новітні технології містять критичні вразливості. Зокрема, було виявлено недоліки в реалізації технології *MU-MIMO*, що дозволяють зловмисникам маніпулювати трафіком та знижувати продуктивність мережі. Крім того, перехідний період, під час якого в одній мережі співіснують пристрої *WPA2* та *WPA3*, створює умови для атак на пониження (*Downgrade attacks*) та перехоплення рукостискань (*Handshake*) [2].

Враховуючи поширеність атак типу "*Rogue AP*" (підроблена точка доступу) та "*Deauthentication*", а також низький рівень обізнаності користувачів (88% інцидентів пов’язані з людським фактором), розробка комплексної методики аудиту та захисту бездротових мереж є вкрай актуальним завданням.

Зв’язок роботи з науковими програмами, планами, темами. Магістерська робота виконується відповідно до напряму підготовки фахівців з кібербезпеки та узгоджена з пріоритетними напрямами розвитку систем захисту інформації.

Мета і завдання дослідження. Метою роботи є підвищення рівня захищеності бездротових мереж шляхом розробки та впровадження комплексної методики аудиту безпеки, виявлення вразливостей протоколів сімейства *IEEE 802.11* та надання рекомендацій щодо їх усунення.

Для досягнення мети поставлено такі завдання:

1. Проаналізувати архітектуру стандартів *IEEE 802.11* та еволюцію механізмів захисту (*WEP*, *WPA*/*WPA2*/*WPA3*).
2. Класифікувати сучасні вектори атак на бездротові мережі, включаючи атаки на інфраструктуру та клієнтів.
3. Дослідити інструментарій для проведення пентестингу (*Penetration Testing*) та обрати оптимальні засоби для аудиту.
4. Провести експериментальне моделювання атак у контрольованому середовищі та оцінити ефективність існуючих методів захисту.
5. Розробити практичні рекомендації щодо налаштування мережевого обладнання та впровадження систем виявлення вторгнень (*WIDS*).

Об’єкт дослідження: процес обміну даними в бездротових локальних мережах (*WLAN*) стандартів *IEEE* 802.11.

Предмет дослідження: методи, засоби та алгоритми аналізу захищеності та забезпечення конфіденційності, цілісності й доступності інформації в мережах *Wi-Fi.*

Методи дослідження. У роботі використано методи системного аналізу (для класифікації загроз), метод експериментального моделювання (для відтворення сценаріїв атак з використанням ОС *Kali Linux*), а також методи порівняльного аналізу (для оцінки ефективності протоколів шифрування *CCMP* та *GCMP*).

Наукова новизна одержаних результатів полягає в удосконаленні методики аудиту безпеки гібридних мереж (*WPA*2/*WPA*3), що дозволяє виявляти специфічні вразли-

вості перехідного режиму, які не детектуються стандартними автоматизованими сканерами.

Практичне значення одержаних результатів. Розроблені рекомендації та методика аудиту можуть бути використані системними адміністраторами та фахівцями з кібербезпеки для побудови захищених корпоративних мереж, а також для проведення регулярних перевірок стійкості інфраструктури до зовнішніх втручань.

1 ТЕОРЕТИЧНІ ОСНОВИ ФУНКЦІОНУВАННЯ ТА БЕЗПЕКИ БЕЗДРОТОВИХ МЕРЕЖ

1.1 Аналіз архітектури та стандартів сімейства *IEEE* 802.11

Бездротові локальні мережі (*WLAN*) на сьогодні є де-факто стандартом забезпечення мобільності користувачів у корпоративному та приватному сегментах. Фундаментальною основою побудови таких мереж є набір стандартів, розроблених робочою групою *IEEE* 802.11 [1]. Розуміння архітектури цих стандартів є критично важливим для аналізу вектору загроз, оскільки більшість атак базуються не на програмних помилках реалізації, а на особливостях функціонування протоколів канального (*Data Link*) та фізичного (*PHY*) рівнів моделі *OSI*.

1.1.1 Еволюція стандартів фізичного рівня (*PHY*)

Стандарт *IEEE* 802.11, вперше ратифікований у 1997 році, пройшов значний еволюційний шлях. Кожна нова ітерація стандарту впроваджувала нові методи модуляції та кодування сигналу, що безпосередньо впливало як на продуктивність, так і на методи захисту.

1. *IEEE* 802.11*a*/*b*/*g* (*Legacy*). Стандарти першого покоління, які на сьогодні вважаються застарілими, проте все ще зустрічаються у промислових системах та застарілому обладнанні (*Legacy devices*).

- 802.11*b* використовує метод розширення спектру прямою послідовністю (*DSSS*) та комплементарне кодування (*CCK*). Робоча частота — 2,4 ГГц. Максимальна швидкість — 11 Мбіт/с.
- 802.11*a*/*g* впровадили метод ортогонального частотного мультиплексування (*OFDM*), що дозволило підвищити швидкість до 54 Мбіт/с. Основна

відмінність полягає у частотному діапазоні: 5 ГГц для 802.11*a* та 2,4 ГГц для 802.11*g*.

2. *IEEE* 802.11*n* (*Wi-Fi* 4). Ключовою інновацією стало впровадження технології *MIMO* (*Multiple Input Multiple Output*) та можливість агрегації каналів (*Channel Bonding*) до 40 МГц. Це дозволило досягти теоретичних швидкостей до 600 Мбіт/с. З точки зору безпеки, саме в цьому стандарті було остаточно закріплено відмову від *WEP* на користь *WPA*2 як обов'язкового стандарту для сертифікації обладнання.

3. *IEEE* 802.11*ac* (*Wi-Fi* 5). Працює виключно у діапазоні 5 ГГц. Впроваджено модуляцію 256-*QAM* та технологію *MU-MIMO* (*Multi-User MIMO*) для *Downlink*, що дозволяє точці доступу одночасно передавати дані кільком клієнтам. Ширина каналу може сягати 80 або 160 МГц, що значно ускладнює перехоплення повного дампа трафіку без спеціалізованого обладнання, здатного працювати в широкій смузі частот [12].

4. *IEEE* 802.11*ax* (*Wi-Fi* 6/6*E*) та 802.11*be* (*Wi-Fi* 7). Сучасні стандарти, орієнтовані на високу щільність клієнтів (*High Efficiency*).

- *OFDMA* (*Orthogonal Frequency-Division Multiple Access*): Дозволяє ділити канал на піднесучі (*Resource Units — RU*), виділяючи їх різним клієнтам. Це змінює парадигму атак на доступність (*DoS*), оскільки класичні методи глушіння (*Jamming*) всього каналу стають менш ефективними без інтелектуального відстеження *RU*.
- *Target Wake Time* (*TWT*): Механізм енергозбереження, який, однак, може бути використаний зловмисниками для атак типу "*Sleep Deprivation*", змушуючи пристрої *IoT* постійно виходити з режиму сну та виснажувати батарею.

У таблиці 1.1 наведено порівняльну характеристику основних стандартів, що впливають на вибір інструментарію для аудиту.

Таблиця 1.1 — Порівняльна характеристика стандартів *IEEE* 802.11

Стандарт	Частота, ГГц	Модуляція	Ширина каналу, МГц	Особливості, що впливають на безпеку
802.11*b*	2.4	*DSSS*/*CCK*	22	Вразливість до колізій, легкість перехоплення вузькосмуговим приймачем
802.11*g*	2.4	*OFDM*	20	Сумісність з 802.11*b* створює вектори атак захисту (*Protection Mechanism abuse*)
802.11*n*	2.4 / 5	*OFDM*	20/40	Впровадження *Block ACK*, що ускладнює ін'єкцію пакетів
802.11*ac*	5	256-*QAM*	20/40/80/160	*Beamforming* вимагає фізичного знаходження атакуючого у зоні "променя"
802.11*ax*	2.4 / 5 / 6	1024-*QAM*	20/40/80/160	Шифрування *Management Frames* (*PMF*) стає обов'язковим (*WPA*3)

Структура кадрів (*Frames*) та їх роль у векторі атак:

Для глибокого розуміння механізмів злому необхідно проаналізувати структуру кадрів 802.11. На відміну від *Ethernet* (802.3), де заголовок є відносно простим, кадр 802.11 має складну структуру управління середовищем (*MAC header*) [5].

Всі кадри поділяються на три типи:

1. Кадри управління (*Management Frames*): Відповідають за встановлення та розрив з'єднань. До них належать *Beacon* (оголошення мережі), *Probe Request*/*Response* (пошук мережі), *Authentication*, *Association*, *Deauthentication*.
   - Вразливість: У стандартах до *WPA*3 (без увімкненого *PMF* — 802.11*w*) ці кадри не шифруються. Це дозволяє зловмиснику підробляти кадри деаутентифікації (*Deauth attack*), розриваючи з'єднання легітимного клієнта для перехоплення "рукостискання" (*Handshake*).
2. Кадри контролю (*Control Frames*): Допомагають у доставці даних (*RTS*/*CTS*, *ACK*).
   - Вразливість: Маніпуляція механізмом *RTS*/*CTS* (*Request to Send* / *Clear to Send*) дозволяє резервувати середовище передачі на тривалий час, блокуючи роботу інших клієнтів (атака *NAV Attack*).
3. Кадри даних (*Data Frames*): Переносять корисне навантаження (*Payload*). Саме вони шифруються протоколами *WEP*/*WPA*.

1.1 Еволюція протоколів шифрування та автентифікації: від *WEP* до *WPA*3

Забезпечення конфіденційності, цілісності та доступності (тріада *CIA*) у бездротових мережах еволюціонувало шляхом виправлення критичних криптографічних помилок попередніх поколінь.

1.2.1 *Wired Equivalent Privacy* (*WEP*) — Хроніка невдач

Протокол *WEP* був першою спробою забезпечити безпеку, еквівалентну дротовим мережам. Він базується на потоковому шифрі *RC*4. Процес шифрування математично можна описати так:

$$C = P \oplus RC4(K \| IV)$$

де:

C — шифротекст;

P — відкритий текст (*Plaintext*) з доданою контрольною сумою *CRC*-32 (*Integrity Check Value — ICV*);

⊕ — операція *XOR* (виключне АБО);

K — спільний секретний ключ (40 або 104 біти);

IV — вектор ініціалізації (24 біти).

Основні вразливості *WEP*:

1. Малий розмір *IV*: 24 біти дають всього $2^{24} \approx 16.7$ мільйонів комбінацій. У навантаженій мережі вектори ініціалізації починають повторюватися (колізія *IV*). Зловмисник, зібравши достатню кількість пакетів з однаковими *IV*, може відновити ключ, використовуючи *FMS*-атаку (*Fluhrer*, *Mantin*, *and Shamir*) або покращену атаку *PTW* (*Pyshkin*, *Tews*, *Weinmann*).
2. Лінійність *CRC*-32: Механізм контролю цілісності *ICV* є лінійним. Це дозволяє здійснювати атаку "*bit-flipping*" — змінювати біти у зашифрованому повідомленні та корегувати *ICV* без знання ключа шифрування.

3. Слабкий механізм обміну ключами: Аутентифікація "*Shared Key Authentication*" фактично передає клієнту відкритий текст і його шифротекст (*Challenge-Response*), що дозволяє миттєво вирахувати потік ключів (*Keystream*).

1.2.2 *Wi-Fi Protected Access* (*WPA*) та *TKIP*

WPA був впроваджений як тимчасове рішення (*draft standard* 802.11*i*) для роботи на існуючому обладнанні *WEP*. Основним протоколом став *TKIP* (*Temporal Key Integrity Protocol*). *TKIP* усунув основні проблеми *WEP*, не змінюючи апаратну частину (все ще використовувався *RC*4), шляхом:

1. Збільшення розміру *IV* до 48 біт (запобігання повторам).
2. Використання функції змішування ключів (*Key Mixing Function*) для створення унікального ключа для кожного пакету.
3. Впровадження алгоритму "*Michael*" (*MIC — Message Integrity Code*) замість *CRC*-32 для захисту від підробки пакетів.

Тим не менш, *TKIP* також вразливий до атак типу "*Beck-Tews*" та "*Ohigashi-Morii*", які дозволяють розшифровувати невеликі пакети (наприклад, *ARP*) та впроваджувати шкідливий трафік у мережу.

1.2.3 *WPA*2 та стандарт *AES-CCMP*

*WPA*2 (повна реалізація 802.11*i*) став золотим стандартом безпеки. Він використовує протокол *CCMP* (*Counter Mode with Cipher Block Chaining Message Authentication Code Protocol*), який базується на блочному шифрі *AES* (*Advanced Encryption Standard*).

Особливості *CCMP*:

1. *AES* у режимі лічильника (*CTR*): Забезпечує конфіденційність. Шифрування здійснюється шляхом *XOR* відкритого тексту з потоком ключів, згенерованим *AES*.
2. *CBC-MAC*: Забезпечує цілісність та автентифікацію повідомлення.
3. *Packet Number* (*PN*): 48-бітний номер пакету для захисту від атак повторного відтворення (*Replay Attacks*).

Незважаючи на надійність *AES*, *WPA*2 має вразливості на етапі "4-*way Handshake*" (чотирьохстороннє рукостискання). Атака *KRACK* (*Key Reinstallation Attack*), виявлена у 2017 році, дозволяє зловмиснику примусити клієнта перевстановити вже використаний ключ, скидаючи параметри лічильників (*nonce*) та *replay counter*, що теоретично дозволяє дешифрувати пакети. Однак найбільш поширеним вектором атаки на *WPA*2 залишається перехоплення рукостискання та офлайн перебір пароля (*Dictionary*/*Brute-force attack*) по хешу *PMK* (*Pairwise Master Key*).

1.2.4 *WPA*3: *Simultaneous Authentication of Equals* (*SAE*)

*WPA*3, представлений у 2018 році, замінює механізм *PSK* (*Pre-Shared Key*) на протокол *SAE* (*Simultaneous Authentication of Equals*), що базується на обміні ключами "*Dragonfly*".

Переваги *WPA*3-*SAE*:

1. Захист від офлайн перебору: Протокол *Dragonfly* використовує методи еліптичної криптографії та *Zero-Knowledge Proof* [14]. Зловмисник не може перехопити хеш для подальшого перебору "у себе вдома". Кожна спроба підбору пароля вимагає активної взаємодії з точкою доступу.
2. *Forward Secrecy* (Досконала пряма секретність): Навіть якщо пароль мережі буде скомпрометовано в майбутньому, зловмисник не зможе розшифрувати трафік, записаний у минулому.

Проте, дослідники вже виявили вразливості і у *WPA*3, зокрема групу атак *Dragonblood* (*CVE*-2019-9494), які використовують атаки побічних каналів (*Side-channel attacks*) та механізми сумісності (*Transition Mode*) для примусового пониження рівня захисту до *WPA*2.

1.3 Механізми обміну ключами (4-*way Handshake*) та структура кадрів керування

Безпека бездротових мереж базується не лише на стійкості криптографічних алгоритмів (*AES*, *RC*4), але й на надійності протоколів керування з'єднанням та розподілу ключів. Розуміння механізму встановлення сесії є критичним для аналізу векторів атак, оскільки більшість сучасних вразливостей (*KRACK*, *Deauth attack*, *Brute-force PMK*) експлуатують саме цей етап, а не прямий злам шифротексту.

Процес встановлення з'єднання (*State Machine*)

Відповідно до стандарту *IEEE* 802.11, процес підключення клієнта (*Station — STA*) до точки доступу (*Access Point — AP*) проходить через машину станів (*State Machine*), яка складається з трьох основних етапів: сканування, автентифікація та асоціація.

1. Стан 1: Не автентифікований, не асоційований. Клієнт надсилає кадри *Probe Request* для пошуку мереж або слухає *Beacon frames* від *AP*.
2. Стан 2: Автентифікований, не асоційований. На цьому етапі відбувається "*Open System Authentication*" (фактично пуста формальність у *WPA*2) або обмін даними *SAE* у *WPA*3.
3. Стан 3: Автентифікований, асоційований. Після успішної асоціації починається етап 4-*way Handshake* для генерації ключів шифрування. Тільки після цього можлива передача даних (*Data Frames*).

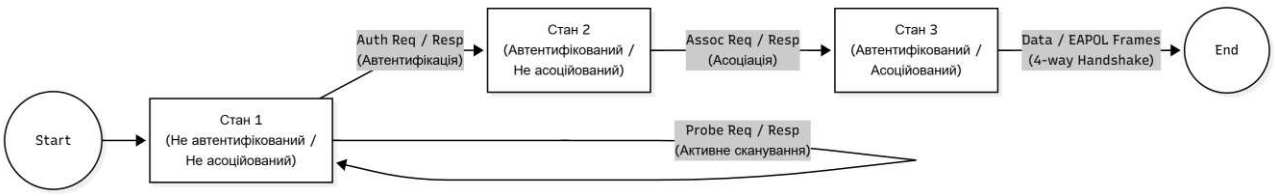

Рисунок 1.1 – Діаграма станів підключення клієнта 802.11

Ієрархія ключів та генерація *PTK*:

Для забезпечення ізоляції сесій кожного користувача стандарт 802.11*i* визначає ієрархію ключів. Головним секретом є *PMK* (*Pairwise Master Key*). У мережах *WPA*2-*Personal* (*PSK*) він є незмінним і обчислюється на основі пароля мережі (*Passphrase*) та її імені (*SSID*) за допомогою функції *PBKDF*2:

$$PMK = PBKDF2(Passphrase, SSID, 4096, 256)$$

PMK ніколи не передається через ефір. На його основі для кожної сесії генерується тимчасовий ключ *PTK* (*Pairwise Transient Key*). Для генерації *PTK* використовуються випадкові числа (*nonce*), що дозволяє захиститися від атак повторного відтворення.

Формула обчислення *PTK* виглядає наступним чином:

$$PTK = PRF(PMK, ANonce, SNonce, MAC_{AP}, MAC_{STA})$$

Де:

1 *PRF* — псевдовипадкова функція (*Pseudo-Random Function*);
2 *ANonce* — випадкове число, згенероване точкою доступу (*Authenticator Nonce*);
3 *SNonce* — випадкове число, згенероване клієнтом (*Supplicant Nonce*);
4 MAC_{AP}, MAC_{STA} — фізичні адреси точки доступу та клієнта.

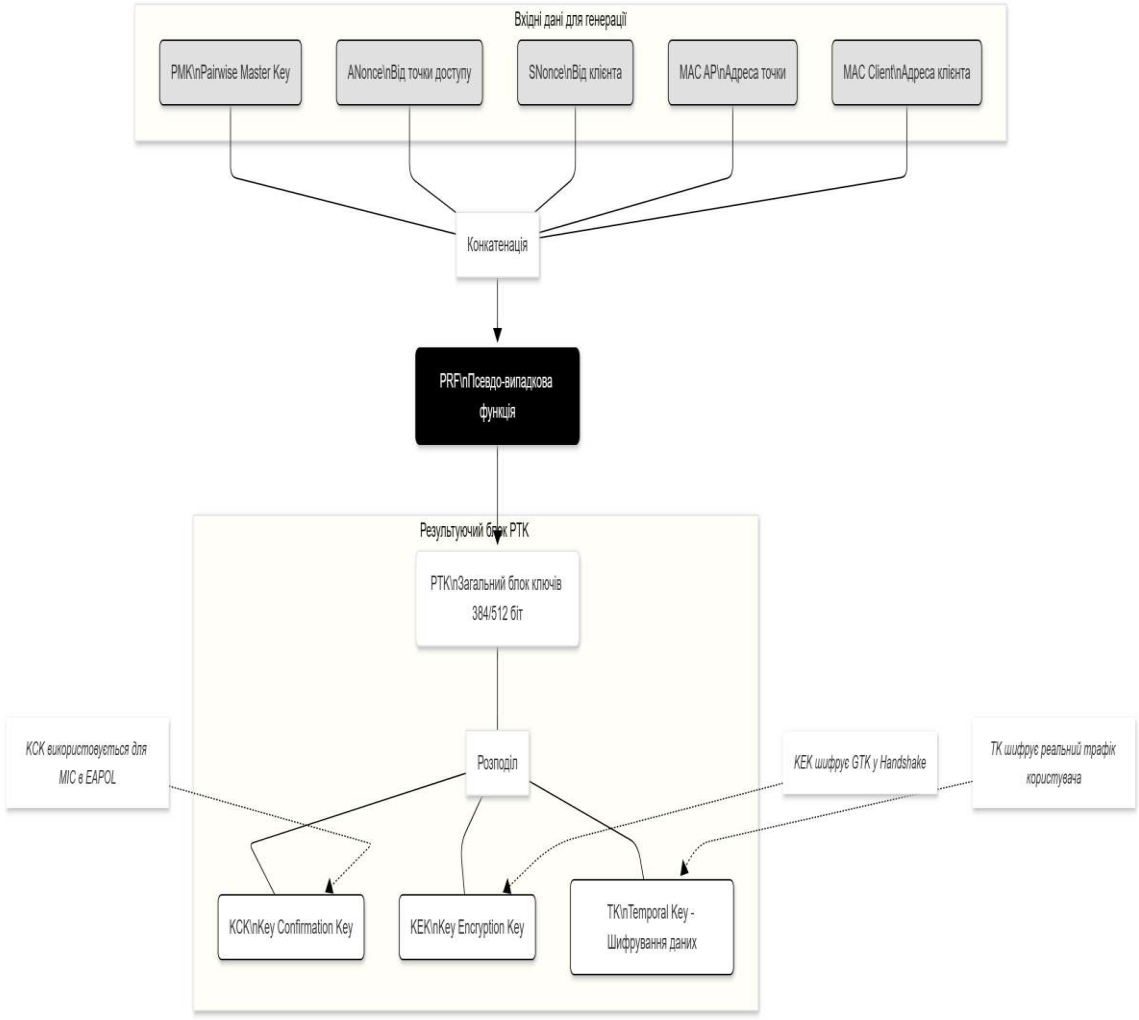

Рисунок 1.2 – Схема генерації ключа *PTK*

Отриманий *PTK* (довжиною 384 біти для *WPA2-CCMP*) розділяється на три частини:

1. *KCK* (*Key Confirmation Key*): Використовується для створення *MIC* (*Message Integrity Code*) — цифрового підпису кадрів рукостискання.
2. *KEK* (*Key Encryption Key*): Використовується для шифрування групового ключа (*GTK*), який передається клієнту.
3. *TK* (*Temporal Key*): Власне ключ, яким шифрується трафік користувача за алгоритмом *AES-CCMP*.

Протокол 4-*way Handshake*:

Саме процес узгодження *PTK* називається "чотирьохстороннім рукостисканням" (4-*way Handshake*). Це найбільш критичний етап з точки зору безпеки, оскільки перехоплення цього обміну дозволяє зловмиснику здійснити офлайн-атаку перебору пароля (*brute-force*).

Процес складається з чотирьох повідомлень (*EAPOL-Key frames*):

1. *Message* 1 (*AP -> STA*): Точка доступу надсилає клієнту *ANonce*. Це число передається у відкритому вигляді. Клієнт вже має *PMK*, знає свій *SNonce* та *MAC*-адреси, тому після отримання *ANonce* він може локально обчислити *PTK*.
2. *Message* 2 (*STA -> AP*): Клієнт надсилає свій *SNonce* точці доступу. Найважливіше, що це повідомлення містить *MIC* (*Message Integrity Code*), підписаний за допомогою *KCK*.

Вразливість: Саме це повідомлення є ціллю атакуючого. Перехопивши *M*2, зловмисник отримує *SNonce*, *ANonce* (з *M*1) та *MIC*. Оскільки він знає *MAC*-адреси, єдиним невідомим у рівнянні залишається *PMK* (пароль). Це дозволяє перебирати паролі зі словника, генерувати потенційний *MIC* і порівнювати його з перехопленим.

3. *Message* 3 (*AP -> STA*): Якщо *AP* успішно перевірила *MIC* з другого повідомлення, вона надсилає зашифрований *GTK* (*Group Temporal Key*). Цей ключ використовується для розшифрування широкомовного (*Broadcast*) трафіку.
4. *Message* 4 (*STA -> AP*): Клієнт підтверджує отримання *GTK*. З цього моменту канал вважається захищеним.

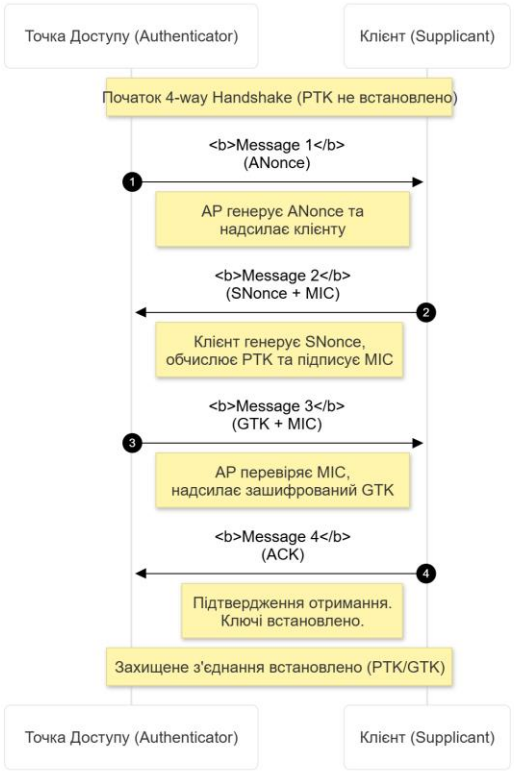

Рисунок 1.3 – Часова діаграма обміну повідомленнями 4-*way Handshake*

Структура кадрів керування (*Management Frames*)

Кадри керування (*Management Frames*) забезпечують функціонування мережі, але не несуть даних користувача. До них належать:

1 *Beacon Frames*: Оголошують про наявність мережі, передають *SSID*, підтримувані швидкості та параметри шифрування.

2 *Probe Request / Response*: Використовуються для активного сканування мереж.

3 *Authentication / Association frames*: Керують підключенням.

4 *Deauthentication / Disassociation frames*: Використовуються для розриву з'єднання.

Ключовою проблемою безпеки стандартів до 802.11*w* є те, що кадри керування (зокрема *Deauth*) не шифруються і не автентифікуються. Це створює можливість для атак на відмову в обслуговуванні (*DoS*) та перехоплення рукостискання.

Зловмисник може підробити *MAC*-адресу точки доступу і надіслати клієнту кадр *Deauthentication* (*Reason Code* 7). Клієнт, отримавши такий кадр, зобов'язаний розірвати з'єднання і почати процедуру перепідключення, що неминуче призводить до нового 4-*way Handshake*, який може бути перехоплений.

Рисунок 1.4 – Структура кадру *IEEE* 802.11 (*Management Frame*)

1.4 Висновки до першого розділу

У першому розділі було проведено детальний аналіз теоретичних основ функціонування бездротових мереж стандарту *IEEE* 802.11.

1. Встановлено, що еволюція стандартів від 802.11*b* до 802.11*ax* супроводжувалася ускладненням методів модуляції та кодування, що підвищує вимоги до апаратного забезпечення для проведення аудиту безпеки.
2. Аналіз криптографічних протоколів показав, що *WEP* та *WPA* (*TKIP*) є повністю скомпрометованими та не повинні використовуватися. *WPA*2 (*AES-CCMP*) залишається надійним за умови використання стійких паролів, проте вразливий до атак на перехоплення рукостискання (*Handshake*).
3. Детально розглянуто механізм 4-*way Handshake*. Математично обґрунтовано, що безпека сесії залежить від складності *PMK* (пароля), оскільки всі інші парамет-

ри генерації ключа (*Nonce*, *MAC*-адреси) передаються у відкритому вигляді. Це підтверджує актуальність атак перебору по словнику.

4. Визначено, що відсутність шифрування кадрів керування (*Management Frames*) у більшості існуючих мереж є критичною архітектурною вразливістю, яка дозволяє зловмисникам примусово розривати з'єднання користувачів для перехоплення аутентифікаційних даних.

Отримані теоретичні знання дозволяють перейти до наступного етапу роботи — класифікації та аналізу практичних векторів атак.

2 АНАЛІЗ ВРАЗЛИВОСТЕЙ ТА ВЕКТОРІВ АТАК НА *WI-FI* МЕРЕЖІ

2.1 Класифікація загроз бездротовому середовищу (*OWASP*, *MITRE ATT&CK*)

Безпека бездротових мереж стандарту *IEEE* 802.11 суттєво відрізняється від безпеки провідних мереж (*Ethernet*) через використання загальнодоступного середовища передачі даних — радіоефіру. Це створює умови, за яких зловмиснику не потрібен фізичний доступ до комутаційного обладнання для реалізації атак. Аналіз літературних джерел дозволяє стверджувати, що зона покриття часто виходить за межі контрольованої території підприємства, що робить мережу вразливою до зовнішнього втручання.

Для систематизації загроз доцільно використати підходи міжнародних методологій *OWASP* (*Open Web Application Security Project*) в контексті мобільних та *IoT* загроз, а також матрицю *MITRE ATT&CK*, яка описує тактики та техніки дій зловмисників.

Класифікація за характером взаємодії (Пасивні та Активні атаки):

Базова таксономія атак на *Wi-Fi* поділяється на дві великі групи залежно від впливу на середовище передачі.

1. Пасивні атаки (*Passive Attacks*): Зловмисник лише прослуховує ефір, не вносячи змін у трафік і не надсилаючи власних кадрів. Метою є розвідка (*Reconnaissance*) та збір даних.

Сніффінг (*Sniffing*/*Eavesdropping*): Перехоплення пакетів даних або керування. Оскільки радіохвилі поширюються у всіх напрямках, будь-який адаптер у режимі моніторингу (*Monitor Mode*) може отримати копію трафіку.

Аналіз трафіку: Навіть якщо дані зашифровані, аналіз метаданих (*MAC*-адреси, обсяг трафіку, час активності) дозволяє виявити структуру мережі та типи пристроїв.

Перехоплення рукостискань (*Handshake Capture*): Як зазначається у дослідженнях, цей етап часто є пасивним (або напівпасивним, якщо не використовується примусова деаутентифікація), коли зловмисник очікує легітимного підключення клієнта для запису 4-*way handshake* з метою подальшого офлайн-перебору.

2. Активні атаки (*Active Attacks*): Передбачають генерацію та ін'єкцію кадрів у мережу, модифікацію існуючого трафіку або блокування роботи пристроїв.

Відмова в обслуговуванні (*DoS*): Генерація завад (*Jamming*) або логічні атаки, такі як масова розсилка кадрів деаутентифікації.

Маскарад (*Masquerading*/*Spoofing*): Підробка *MAC*-адреси або створення фальшивої точки доступу (*Rogue AP*/*Evil Twin*) для перехоплення облікових даних користувачів.

Атаки на криптографічні протоколи: Спроби пониження версії протоколу (*Downgrade attacks*) або повторне відтворення пакетів (*Replay attacks*).

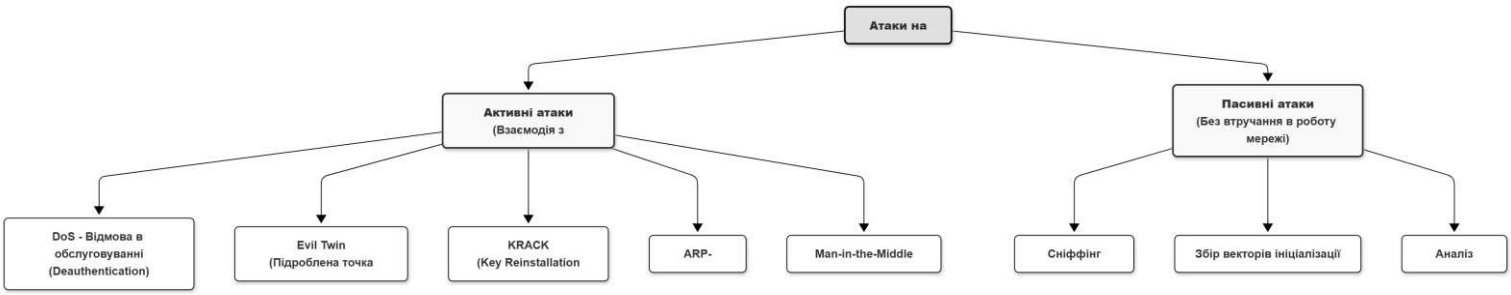

Рисунок 2.1 – Класифікація атак на бездротові мережі

Проекція загроз на модель *CIA*

Відповідно до стандартів інформаційної безпеки, загрози класифікуються за порушенням властивостей інформації:

Конфіденційність (*Confidentiality*): Порушується при використанні відкритих мереж (*Open Authentication*) або слабких протоколів шифрування (*WEP*), що дозволяє зловмиснику читати дані. Також сюди відноситься злам ключів методом перебору по словнику.

Цілісність (*Integrity*): Порушується при атаках типу "*Man-in-the-Middle*" (*MitM*), коли зловмисник перехоплює сесію та модифікує вміст пакетів (наприклад, ін'єкція шкідливого коду в *HTTP*-трафік).

Доступність (*Availability*): Порушується при радіочастотних завадах або атаках на вичерпання ресурсів точки доступу (*flooding*).

Відповідність матриці *MITRE ATT&CK*

Матриця *MITRE ATT&CK* (*Adversarial Tactics*, *Techniques*, *and Common Knowledge*) є галузевим стандартом опису дій кіберзлочинців. Для бездротових мереж релевантними є наступні техніки (Техніки наведено згідно з *Enterprise Matrix* та *Mobile Matrix*) [7].

Таблиця 2.1 — Картування атак на *Wi-Fi* згідно з *MITRE ATT&CK*

Тактика (*Tactic*)	*ID* Техніки	Назва техніки (*Technique*)	Опис в контексті *Wi-Fi*

Розвідка (*Reconnaissance*)	*T*1595	*Active Scanning*	Використання інструментів (наприклад, *Kismet*, *Airodump-ng*) для виявлення *SSID*, *BSSID*, каналів та типу шифрування.
Доступ до облікових даних (*Credential Access*)	*T*1110	*Brute Force*	Офлайн-перебір пароля *WPA*/*WPA*2 (*Brute Force* / *Password Spraying*) після перехоплення рукостискання.
Доступ до облікових даних (*Credential Access*)	*T*1040	*Network Sniffing*	Перехоплення нешифрованих даних (*HTTP*, *FTP*, *Telnet*) у відкритих мережах або мережах із захистом *WEP*.
Збір даних (*Collection*)	*T*1557	*Adversary-in-the-Middle* (*AiTM*)	Створення "Злого двійника" (*Evil Twin*), який змушує жертву підключитися до підконтрольного пристрою замість легітимної точки.
Вплив (*Impact*)	*T*1498	*Network Denial of Service*	Атаки на деаутентифікацію (*Deauth Attack*) для відключення користувачів або примусового перепідключення.

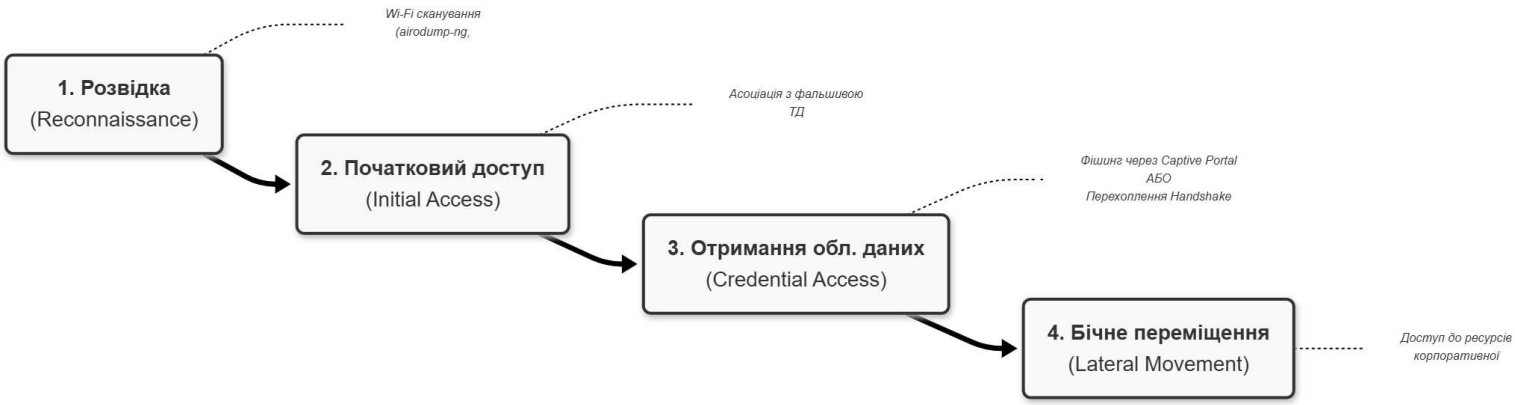

Рисунок 2.2 — Візуалізація вектора атаки за *MITRE ATT&CK*

Вразливості згідно з *OWASP*:

Хоча *OWASP* фокусується на веб-додатках, їх класифікація *OWASP Mobile Top* 10 містить пункт *M*3: *Insecure Communication* [8]. У контексті *Wi-Fi* це означає:

1. Недостатня перевірка сертифікатів: При використанні *WPA*2-*Enterprise* (802.1*X*) клієнтські пристрої часто налаштовані на ігнорування перевірки сертифіката сервера *RADIUS*, що дозволяє атаку типу "*Hostile Portal*" або перехоплення облікових даних *MSCHAPv*2.
2. Слабкі алгоритми шифрування: Використання застарілих протоколів (*WEP*, *WPA-TKIP*), які, як зазначено в роботах, не забезпечують достатньої стійкості до статистичного криптоаналізу.

Таким чином, сучасний ландшафт загроз вимагає комплексного підходу до захисту, що враховує як пасивні методи перехоплення, так і активні методи маніпуляції підключенням.

2.2 Аналіз атак на інфраструктуру: *Deauthentication*, *Evil Twin*, *Rogue AP*

Атаки на інфраструктуру спрямовані на порушення доступності мережі або підміну легітимних вузлів доступу підконтрольними зловмиснику пристроями. Специфіка цих атак полягає у використанні архітектурних особливостей кадрів керування (*Management Frames*), які у стандартах до 802.11*w* передаються у відкритому вигляді.

2.2.1 Атака деаутентифікації (*Deauthentication Attack*)

Атака деаутентифікації, також відома як "атака відключення", є найбільш поширеним видом впливу на доступність бездротової мережі (*DoS*). Її механізм базується на ін'єкції у мережу підробленого кадру керування підтипу *Deauthentication*.

Згідно зі стандартом *IEEE* 802.11, кадр деаутентифікації є повідомленням про розірвання з'єднання, яке не вимагає підтвердження від іншої сторони. Зловмисник, використовуючи *Wi-Fi* адаптер у режимі моніторингу, формує пакет, де:

Source MAC: *MAC*-адреса легітимної точки доступу (*BSSID*).

Destination MAC: *MAC*-адреса жертви (*Client Station*) або широкомовна адреса (*Broadcast FF*:*FF*:*FF*:*FF*:*FF*:*FF*) для відключення всіх клієнтів.

BSSID: Ідентифікатор атакованої мережі.

Reason Code: Код причини відключення (наприклад, код 7 — *Class* 3 *frame received from nonassociated station*).

Отримавши такий кадр, клієнтський пристрій (або точка доступу) негайно розриває з'єднання та ініціює процедуру повторного підключення (*Re-association*). Саме цей момент є критичним для безпеки, оскільки повторне підключення супроводжується

передачею 4-*way handshake*, який може бути перехоплений зловмисником для подальшого офлайн-перебору пароля.

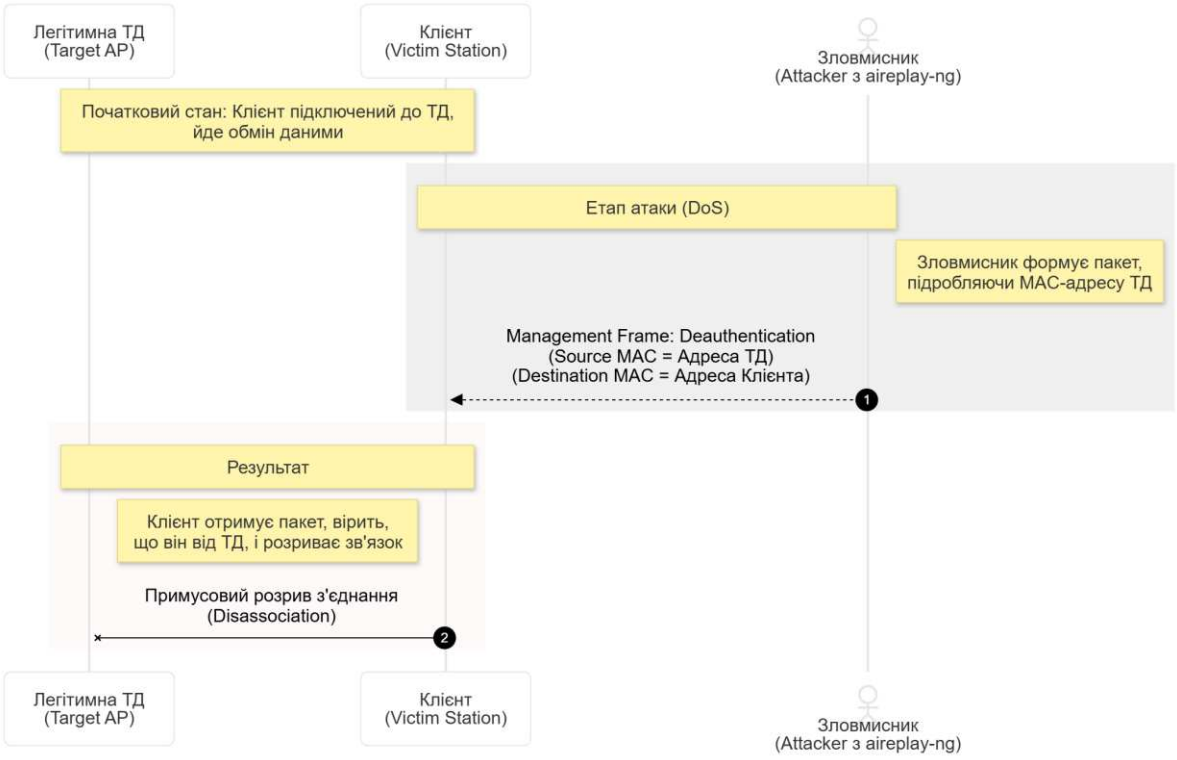

Рисунок 2.3 — Структура кадру деаутентифікації та схема атаки

Для реалізації цієї атаки часто використовуються спеціалізовані утиліти, такі як *Aireplay-ng* (частина пакету *Aircrack-ng*) або *Void*11. Утиліта *Void*11 дозволяє автоматизувати процес масової деаутентифікації клієнтів, генеруючи трафік, що змушує пристрої постійно намагатися відновити з'єднання. Це створює значне навантаження на мережу та може використовуватися як метод прискорення збору векторів ініціалізації (*IVs*) у застарілих мережах *WEP* або для захоплення рукостискання у мережах *WPA*2.

2.2.2 Атака "Злий двійник" (*Evil Twin*)

Атака типу "*Evil Twin*" (Злий двійник) є вдосконаленим варіантом фішингу, спрямованим на перехоплення облікових даних користувачів або надання доступу до мережі через підконтрольний шлюз.

Механізм реалізації:

1. Розвідка: Зловмисник сканує ефір та отримує параметри цільової мережі: *SSID* (*Service Set Identifier*) та *BSSID* (*MAC*-адресу), а також номер каналу.
2. Створення клону: Зловмисник запускає програмну точку доступу (*SoftAP*) з ідентичним *SSID*, але на іншому частотному каналі або з підміненою *MAC*-адресою.
3. Примусова міграція: Для того щоб клієнти підключилися до "двійника", зловмисник часто використовує атаку деаутентифікації проти легітимної точки. Пристрої жертв, втративши зв'язок, починають шукати відому мережу і автоматично підключаються до точки з сильнішим сигналом (*RSSI*), якою виступає точка зловмисника, розташована фізично ближче.

Після підключення жертви до "Злого двійника", весь її трафік проходить через пристрій зловмисника (атака *Man-in-the-Middle*). Найчастіше цей метод поєднується з використанням *Captive Portal* — підробленої веб-сторінки, що імітує інтерфейс авторизації або сторінку оновлення прошивки роутера.

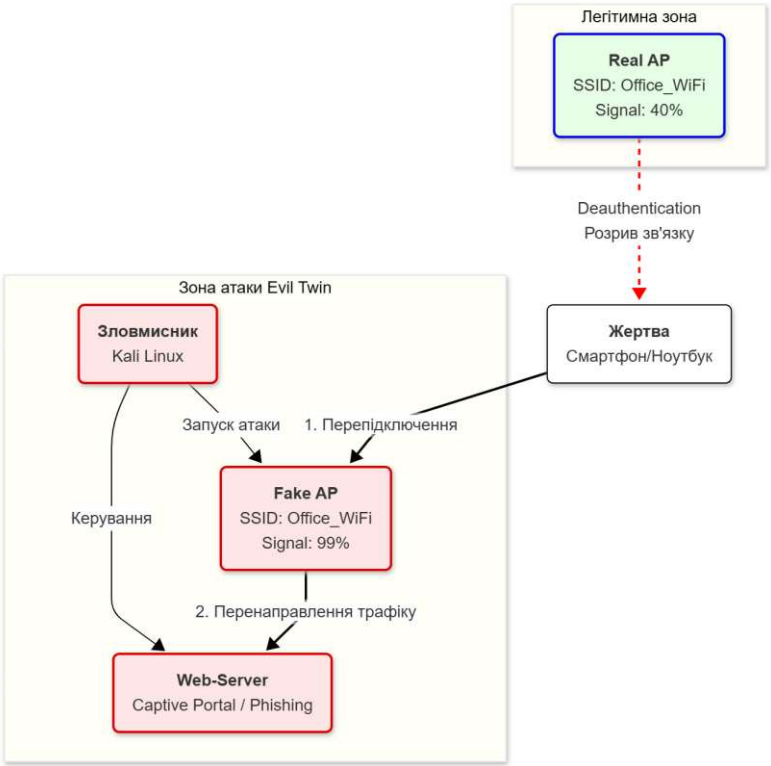

Рисунок 2.4 — Сценарій атаки *Evil Twin* з *Captive Portal*

Ефективним інструментом для автоматизації цієї атаки є фреймворк *Wifiphisher*. Він дозволяє не лише створювати точку-клона, але й автоматично розгортати фішингові сценарії, наприклад, імітуючи сторінку оновлення "*Firmware Upgrade*", яка вимагає введення пароля *WPA* для продовження роботи.

2.2.3 Несанкціонована точка доступу (*Rogue AP*)

На відміну від "Злого двійника", *Rogue AP* (Несанкціонована точка доступу) — це точка доступу, яка фізично підключена до дротової інфраструктури корпоративної мережі без відома адміністратора.

Вектори появи:

1. Людський фактор: Співробітники самовільно приносять побутові роутери та підключають їх до *Ethernet*-розеток для створення власної зони *Wi-Fi* задля зручності.

2. Зловмисне встановлення: Інсайдер або зловмисник, що отримав фізичний доступ до приміщення, встановлює мініатюрний пристрій (наприклад, на базі *Raspberry Pi* або *Hak*5 *Pineapple*) для створення прихованого каналу доступу.

Основна небезпека *Rogue AP* полягає в тому, що вона створює "чорний хід" (*Backdoor*) у захищену мережу, оминаючи міжмережеві екрани (*Firewall*) та системи *IDS*/*IPS* периметра. Якщо така точка налаштована без шифрування (*Open*) або з слабким паролем (*WEP*/*WPA*-*PSK*), зловмисник може отримати доступ до внутрішніх ресурсів підприємства, перебуваючи на значній відстані (на парковці або у сусідній будівлі).

2.3 Криптографічні атаки: *KRACK*, *PMKID* та вразливості *WPA*3

Незважаючи на те, що протокол *WPA*2 з шифруванням *AES*-*CCMP* тривалий час вважався еталоном безпеки, дослідження останніх років виявили критичні недоліки в логіці процедури "рукостискання" (*Handshake*), а не в самому криптографічному алгоритмі. Згідно з матеріалами магістерської роботи[1], більшість атак раніше зводилися до перебору паролів, проте сучасні вектори дозволяють компрометувати мережу без використання словників або ж значно прискорювати цей процес.

2.3.1 Атака перевстановлення ключа (*KRACK*)

У 2017 році дослідник Меті Ванхоф (*Mathy Vanhoef*) оприлюднив деталі критичної вразливості у протоколі *WPA*2, яка отримала назву *KRACK* (*Key Reinstallation AttaCK*) [3]. На відміну від класичних методів, описаних у[2], які вимагають перехоплення повного 4-*way handshake* для подальшого офлайн-перебору, *KRACK* маніпулює станами клієнта під час встановлення з'єднання.

Механізм реалізації:

Атака базується на недоліку в кінцевому автоматі (*State Machine*) клієнта. Під час 4-етапного рукостискання, після отримання 3-го повідомлення (*Message* 3), клієнт встановлює ключ шифрування (*PTK*) і ініціалізує лічильник пакетів (*nonce*/*replay counter*).

Зловмисник, діючи як "*Man-in-the-Middle*", блокує 4-те повідомлення (підтвердження від клієнта до точки доступу). Точка доступу, не отримавши підтвердження, повторно надсилає *Message* 3. Клієнт, отримавши дублікат повідомлення, згідно зі стандартом, перевстановлює (*reinstalls*) вже наявний ключ *PTK* і, що найважливіше, скидає лічильники пакетів (*nonce*) до початкового значення.

Це призводить до порушення фундаментального правила криптографії: заборона повторного використання *nonce* з одним і тим самим ключем.

Математично це виглядає так: якщо потік ключів (*Keystream*) S залежить від ключа K і лічильника N ($S = E(K, N)$), то при скиданні N зловмисник отримує ідентичний потік ключів для нових пакетів. Якщо $C_1 = P_1 \oplus S$ і $C_2 = P_2 \oplus S$, то зловмисник може обчислити $P_1 \oplus P_2$, що дозволяє дешифрувати вміст пакетів.

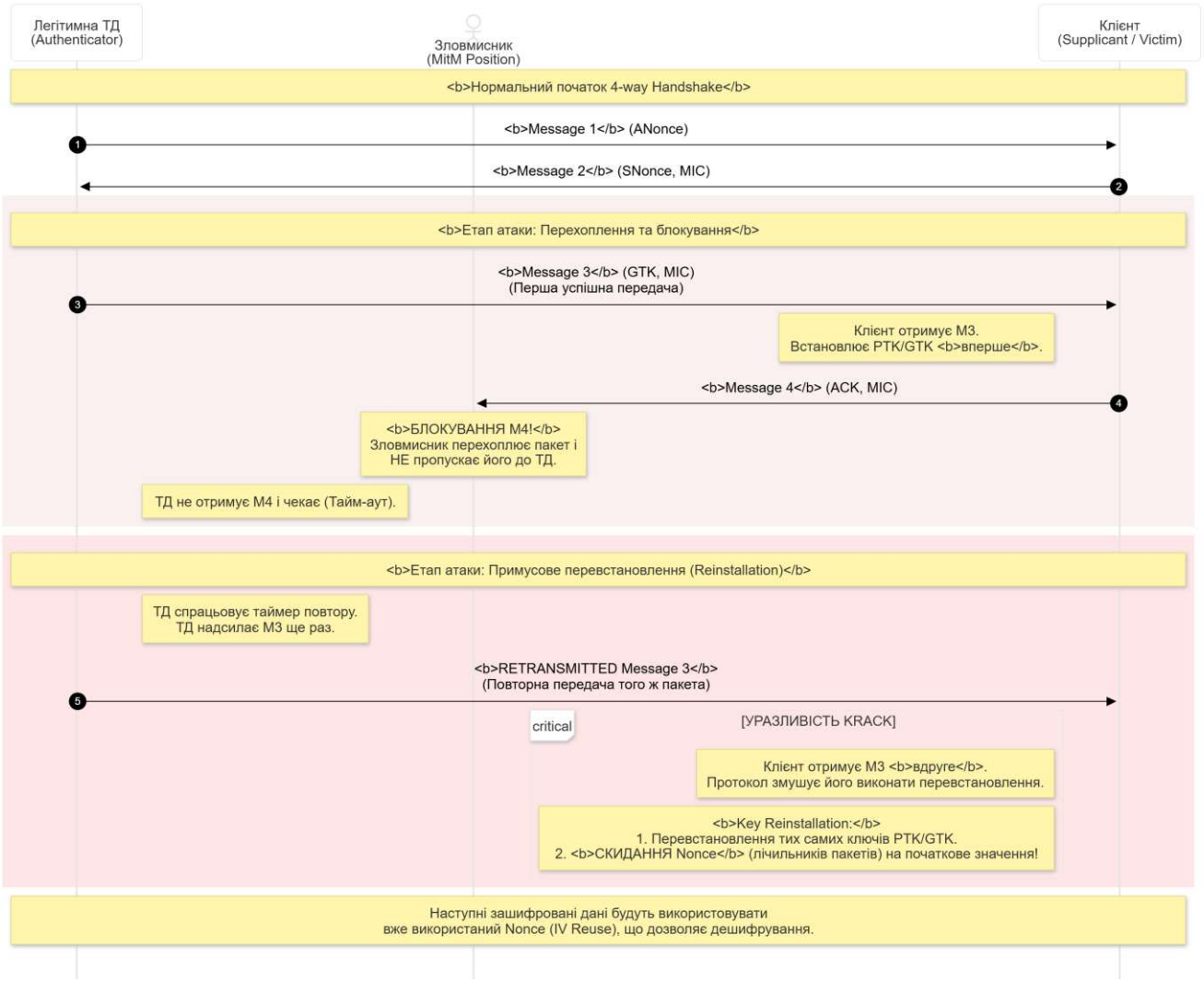

Рисунок 2.5 — Часова діаграма атаки *KRACK*

Дана вразливість була зареєстрована під ідентифікатором *CVE*-2017-13077. Важливо зазначити, що атака є особливо небезпечною для пристроїв на базі *Android* 6.0 та *Linux* (через використання *wpa_supplicant* 2.4-2.5), де ключ шифрування міг обнулятися повністю, роблячи трафік тривіальним для перехоплення.

2.3.2 Атака на *PMKID* (*Clientless Attack*)

Традиційні методи злому, такі як перехоплення рукостискання, вимагають очікування підключення легітимного користувача або застосування деаутентифікації.

Однак у 2018 році команда розробників *Hashcat* (зокрема *Jens 'Atom' Steube*) представила новий вектор атаки, який не потребує взаємодії з клієнтом (*Clientless*).

Атака спрямована на *RSN IE* (*Robust Security Network Information Element*) — необов'язкове поле в кадрі першого повідомлення рукостискання (*Message* 1), яке передається точкою доступу. Багато сучасних маршрутизаторів додають у це поле значення *PMKID* для підтримки швидкого роумінгу (802.11*r*).

Алгоритм атаки: Зловмисник ініціює з'єднання з точкою доступу, отримує *Message* 1, який містить *PMKID*, і миттєво розриває зв'язок. Отриманий хеш використовується для перебору пароля.

Формула обчислення *PMKID*:

$$PMKID = HMAC\text{–}SHA1\text{-}128(PMK, \text{“}PMK\ Name\text{”} \parallel MAC_{AP} \parallel MAC_{STA})$$

Де:

PMK — головний ключ (похідна від пароля мережі);

“*PMK Name*” — фіксований рядковий літерал;

MAC_{AP} та MAC_{STA} — *MAC*-адреси точки доступу та станції зловмисника.

Перевага цього методу полягає в тому, що зловмиснику не потрібно чекати на жертву або створювати "шум" в ефірі пакетами деаутентифікації, що робить атаку менш помітною для систем *IDS*.

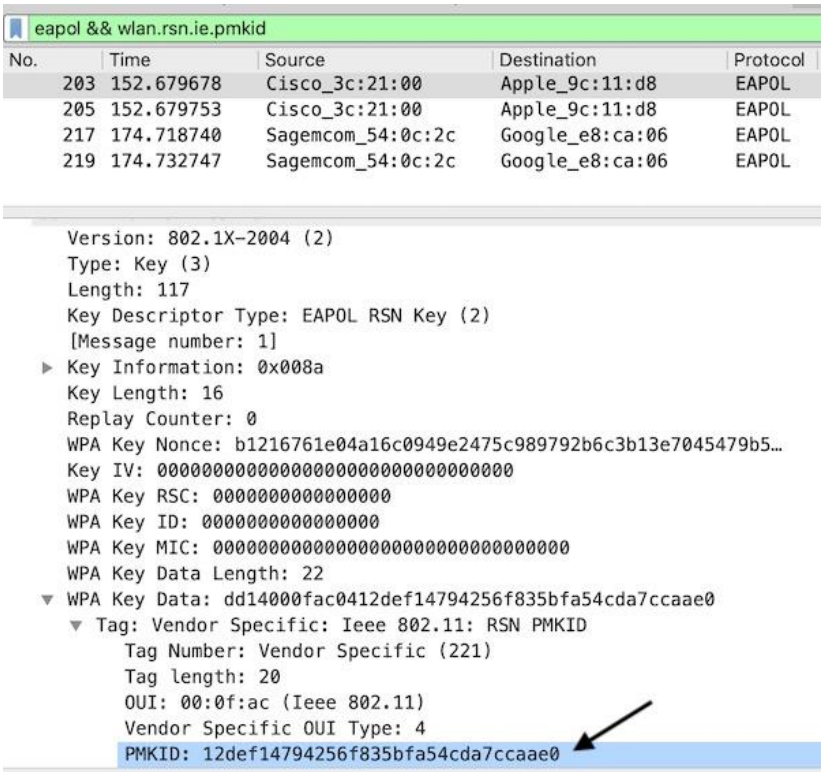

Рисунок 2.6 — Структура *RSN Information Element* з полем *PMKID*

2.3.3 Вразливості *WPA*3: *Dragonblood*

Впровадження стандарту *WPA*3 з протоколом *SAE* (*Simultaneous Authentication of Equals*) мало на меті усунення можливості офлайн-перебору паролів. Проте, вже у 2019 році група дослідників виявила ряд архітектурних вразливостей, об'єднаних назвою *Dragonblood* (*CVE*-2019-9494) [4].

Вразливості поділяються на дві категорії:

1. Атаки на пониження (*Downgrade Attacks*): Оскільки *WPA*3 часто працює в режимі сумісності (*Transition Mode*), зловмисник може створювати перешкоди для *handshake WPA*3, змушуючи клієнта використовувати менш захищений *WPA*2, який далі атакується класичними методами.
2. Атаки побічними каналами (*Side-Channel Attacks*):

Атака за часом (*Timing attack*): Алгоритм "*Dragonfly*", що використовується в *SAE*, виконує різну кількість ітерацій циклу залежно від пароля. Вимірюючи час відповіді точки доступу з точністю до наносекунд, можна відновити частину інформації про пароль.

Атака на кеш (*Cache-based attack*): Аналіз доступу до пам'яті під час виконання криптографічних операцій дозволяє звузити простір перебору паролів.

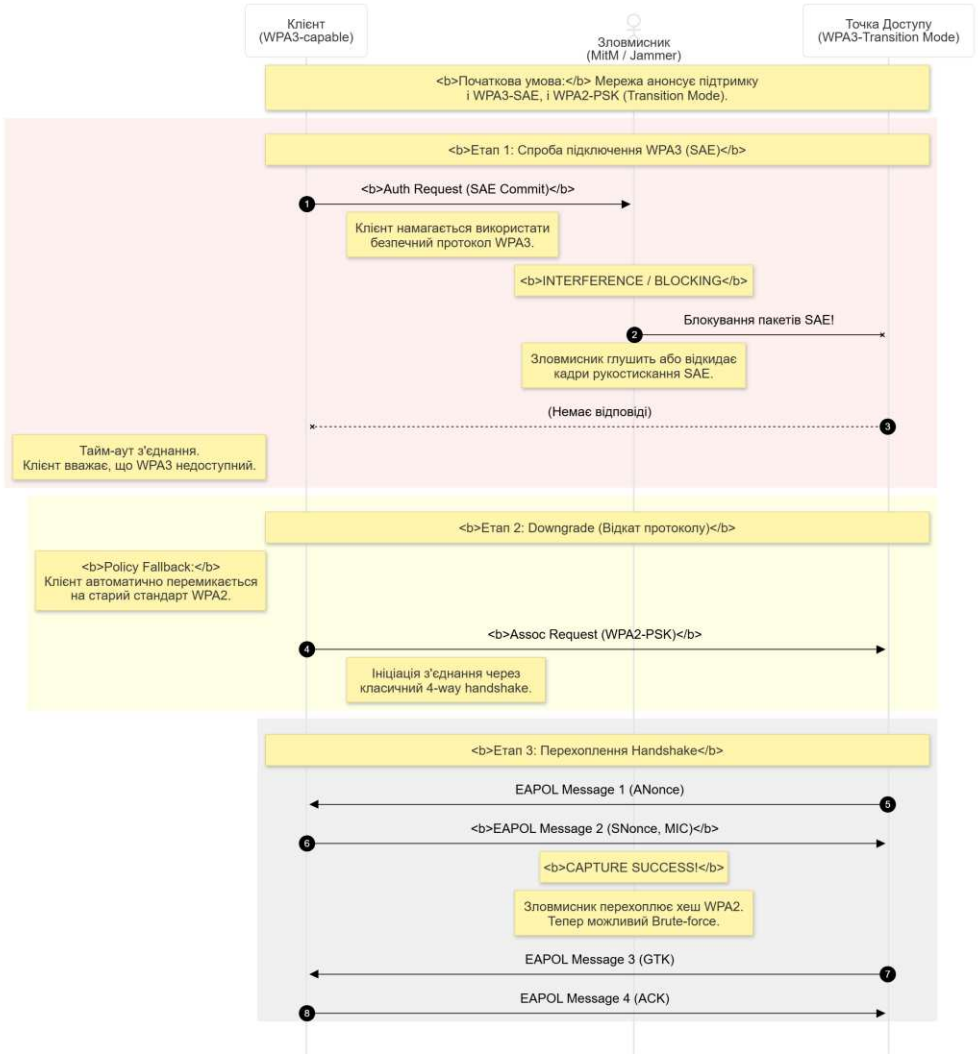

Рисунок 2.7 — Схема атаки *Downgrade* з *WPA*3 на *WPA*2

2.3.4 Висновки до другого розділу

Проведений у другому розділі аналіз дозволяє класифікувати загрози бездротовим мережам не лише як теоретичні вразливості, а як практичні вектори, доступні для реалізації з використанням відкритого ПЗ (наприклад, пакету *Aircrack-ng*, описано-го в).

1. Встановлено, що навіть при використанні стійких алгоритмів шифрування (*AES*), слабкою ланкою залишаються протоколи обміну ключами.
2. Атака *KRACK* довела, що маніпуляція станами з'єднання може нівелювати стійкість шифрування без знання пароля.
3. Атака на *PMKID* змінила парадигму аудиту безпеки, дозволивши атакувати саму інфраструктуру без взаємодії з користувачами.
4. Виявлені вразливості *WPA*3 (*Dragonblood*) свідчать про те, що перехід на нові стандарти не є панацеєю без правильного налаштування мережевого обладнання (відключення *Transition Mode*, оновлення прошивок).

Ці висновки стануть основою для розробки методики практичного аудиту в наступному розділі.

3 ПРАКТИЧНА РЕАЛІЗАЦІЯ АУДИТУ ЗАХИЩЕНОСТІ

3.1 Обґрунтування вибору програмно-апаратного комплексу для аудиту

Ефективність проведення аудиту безпеки бездротових мереж залежить від правильного підбору інструментарію, який має забезпечувати підтримку специфічних режимів роботи мережевих інтерфейсів (*Monitor Mode*, *Frame Injection*). Проаналізувавши існуючі підходи до тестування на проникнення, було сформовано комплекс засобів на базі спеціалізованих дистрибутивів *Linux*.

3.1.1. Операційна система та середовище виконання

У якості базової платформи для проведення досліджень обрано операційну систему *Kali Linux* [6]. Хоча існують інші дистрибутиви (*Parrot Security OS*, *BlackArch*), *Kali Linux* є де-факто промисловим стандартом, що забезпечує стабільну підтримку драйверів для ін'єкції пакетів, що є критичним для реалізації активних атак.

На відміну від стандартних дистрибутивів (*Ubuntu*/*Debian*), ядро *Kali Linux* містить патчі для підтримки режиму моніторингу на широкому спектрі бездротових чіпсетів (*Atheros*, *Ralink*, *Realtek*). Використання віртуального середовища (*VMware*/*VirtualBox*), як зазначено в проаналізованих джерелах, є допустимим, проте вимагає використання зовнішніх *USB*-адаптерів, оскільки віртуалізація не дозволяє прямого доступу до вбудованого *PCI-E* модуля *Wi-Fi* ноутбука.

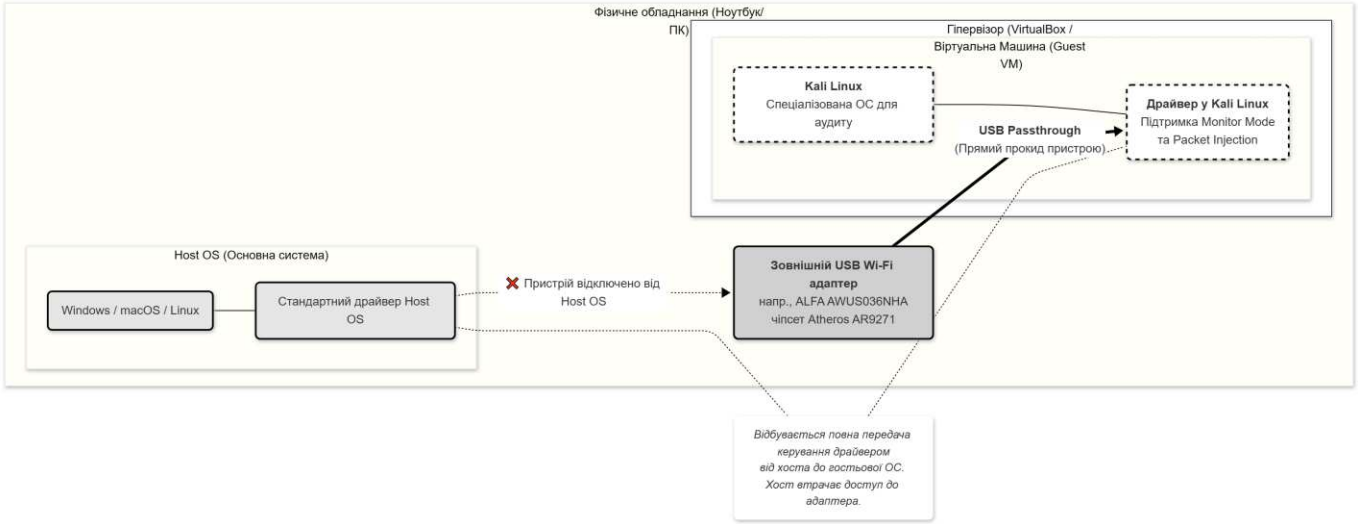

Рисунок 3.1 — Архітектура тестового стенду

3.1.2 Пакет *Aircrack-ng* як базовий фреймворк

Основним інструментом для роботи з кадрами 802.11 обрано пакет *Aircrack-ng* [10]. Це не одна програма, а комплекс консольних утиліт, кожна з яких виконує вузькоспеціалізовану функцію.

1. *Airmon-ng*: Відповідає за переведення мережевого інтерфейсу у режим моніторингу (*Monitor Mode*). Важливо зазначити, що сучасні версії також керують конфліктами процесів (наприклад, *NetworkManager* або *wpa_supplicant*), які можуть блокувати доступ до інтерфейсу, що часто ігнорується початківцями.
2. *Airodump-ng*: Виконує пасивне захоплення трафіку (*Packet Sniffing*). На відміну від універсальних сніферів, *airodump-ng* оптимізований для перемикання між каналами (*channel hopping*) та коректного відображення параметрів мережі: *BSSID*, рівня сигналу (*PWR*), типу шифрування (*ENC*) та клієнтів (*STATION*).
3. *Aireplay-ng*: Генератор трафіку для активних атак. Дозволяє виконувати деаутентифікацію клієнтів (для перехоплення *Handshake*), ретрансляцію *ARP*-запитів (для прискорення злому *WEP*) та перевірку можливості ін'єкції.

4. *Aircrack-ng*: Модуль криптоаналізу для відновлення ключів *WEP* та *WPA*/*WPA*2. Хоча джерела згадують про атаки *PTW* та *KoreK* для *WEP*, для сучасних мереж *WPA*2 актуальним є перебір за словником (*Dictionary Attack*), ефективність якого прямо залежить від якості словника та обчислювальної потужності.

3.1.3 Порівняння засобів аналізу та активних атак

Для розширення можливостей аудиту, окрім класичного *Aircrack-ng*, доцільно використовувати сучасні інструменти, які автоматизують складні сценарії. У таблиці 3.1 наведено порівняльний аналіз обраних засобів.

Таблиця 3.1 — Порівняльна характеристика інструментарію аудиту

Інструмент	Основне призначення	Переваги над аналогами	Недоліки
Aircrack-ng Suite	Базові маніпуляції з кадрами, кракінг	Низькорівневий контроль, стабільність, де-факто стандарт	Робота лише через *CLI*, складність одночасного запуску кількох атак.
Kismet	Пасивний моніторинг та візуалізація	Виявляє приховані мережі, не надсилає жодних пакетів (повна невидимість), має зручний *Web-UI*.	Не вміє виконувати активні атаки (ін'єкцію).

Bettercap	*MitM* атаки, *Rogue AP*	Сучасний "швейцарський ніж" на *Go*. Автоматизує створення *Fake AP* та перехоплення *HTTPS*.	Вищий поріг входження, вимагає налаштування каплетів (скриптів) [18].
Wireshark	Глибокий аналіз пакетів	Найкращий декодер протоколів. Дозволяє бачити деталі *EAPOL*-обміну, які приховує *airodump-ng*.	Не призначений для атак, лише для аналізу [19].
Hashcat	Відновлення паролів (*Cracking*)	Використовує *GPU*, що у сотні разів швидше за *CPU*-версію *aircrack-ng* при переборі *WPA*2.	Вимагає конвертації файлів *.cap* у формат *.hccapx*.

3.1.4 Специфіка апаратного забезпечення

Критичним фактором успіху є вибір *Wi-Fi* адаптера. На відміну від стандартних офісних завдань, аудит вимагає підтримки режиму моніторингу та ін'єкції пакетів. У роботі використовуватиметься адаптер на базі чіпсета *Atheros AR*9271 (або аналог *Ralink RT*3070), оскільки вони мають відкриті драйвери з повною підтримкою стеку *mac*80211 у *Linux*. Використання вбудованих адаптерів *Intel* або *Broadcom* часто є неможливим через обмеження пропрієтарних драйверів, які не дозволяють надсилати довільні кадри в ефір.

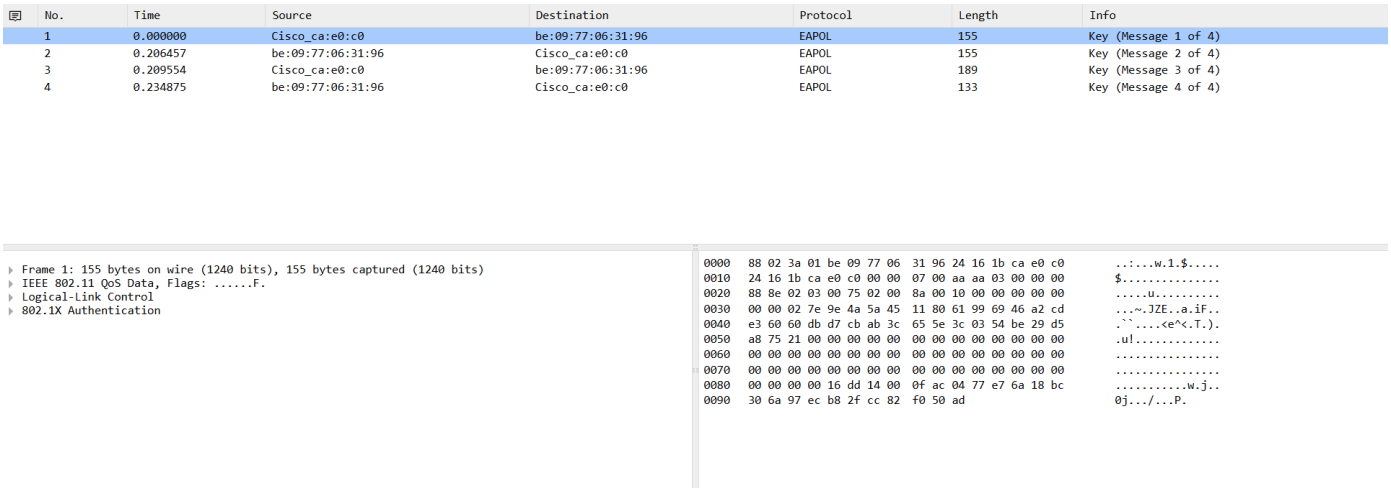

Рисунок 3.2 — Інтерфейс *Wireshark* з фільтрацією *EAPOL*

Обраний комплект інструментів поєднує класичні засоби (*Aircrack-ng*) для базових маніпуляцій з радіоефіром та сучасні рішення (*Bettercap*, *Hashcat*) для підвищення ефективності атак. Використання ОС *Kali Linux* забезпечує необхідну програмну базу, а застосування спеціалізованого адаптера гарантує апаратну сумісність для проведення активного тестування.

3.2 Розробка методики проведення пентесту

Проведення аудиту безпеки бездротових мереж вимагає чіткого алгоритму дій, що дозволяє мінімізувати ризики для інфраструктури та забезпечити повноту покриття векторів атак. На основі аналізу літературних джерел та галузевих стандартів (*PTES*, *OSSTMM*), нами розроблено методику, яка складається з п'яти послідовних етапів: від пасивної розвідки до відновлення ключів доступу [11].

Етап 1: Підготовка та пасивна розвідка (*Intelligence Gathering*)

Першим кроком є збір інформації про цільове середовище без втручання в його роботу. Головна мета — побудувати "карту" радіоефіру. Згідно з даними, наведеними у джерелах, для цього використовується переведення бездротового адаптера в режим моніторингу (*Monitor Mode*).

Алгоритм дій:

1. Ініціалізація інтерфейсу: Використання *airmon-ng* для зупинки конфліктуючих процесів (*wpa_supplicant*, *NetworkManager*) та активації режиму прослуховування. Це критично важливо, оскільки фонові процеси ОС можуть самовільно змінювати канал, перериваючи атаку.
2. Сканування ефіру: Запуск *airodump-ng* для фіксації всіх доступних точок доступу (*AP*).
3. Фільтрація цілей: Аналіз отриманих даних за такими критеріями:

Рівень сигналу (*RSSI*): Атаки на клієнтів з рівнем сигналу нижче -75 *dBm* є малоефективними через втрату пакетів.

Кількість клієнтів (#*Station*): Наявність активних користувачів є обов'язковою умовою для перехоплення рукостискання (окрім атаки *PMKID*).

Тип шифрування: Виявлення застарілих мереж *WEP* (які потребують збору *IVs*) або сучасних *WPA*2/*WPA*3.

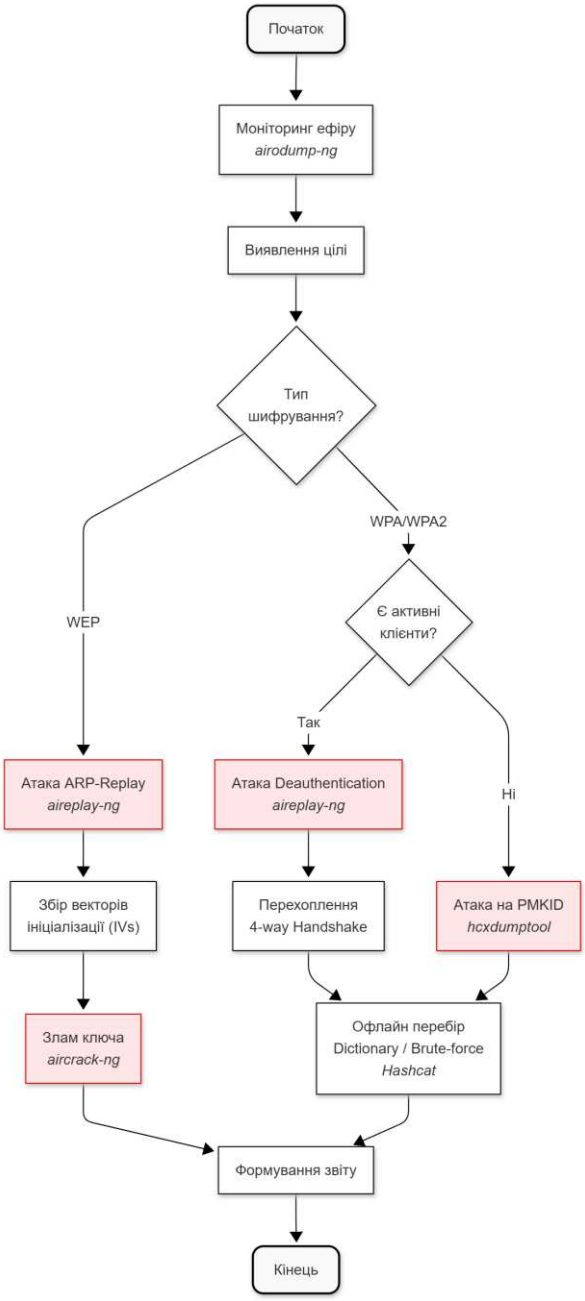

Рисунок 3.3 — Блок-схема алгоритму проведення аудиту безпеки

Етап 2: Моделювання загроз та вибір вектору атаки

На цьому етапі на основі зібраних даних обирається конкретний метод експлуатації. Як зазначається у проаналізованій літературі, універсального методу не існує, і ефективність залежить від конфігурації мережі.

1. Сценарій А (*Legacy*): Якщо виявлено шифрування *WEP*, вектором атаки є стимуляція генерації пакетів (*ARP Request Replay*) для прискореного збору векторів ініціалізації (*IVs*), оскільки пасивний збір може тривати годинами.
2. Сценарій Б (*Standard*): Для мереж *WPA*2-*PSK*/*CCMP* основним вектором є перехоплення 4-*way handshake*. Це вимагає активної взаємодії: примусового відключення клієнта.
3. Сценарій В (*Clientless*): Якщо клієнти відсутні або знаходяться поза зоною досяжності, застосовується атака на *PMKID*, яка дозволяє отримати хеш пароля безпосередньо від точки доступу [9].

Етап 3: Активна фаза (*Exploitation*)

Цей етап передбачає генерацію та ін'єкцію спеціальних кадрів у мережу.

Методика перехоплення *Handshake* (*WPA*2):

1. Фіксація каналу: Адаптер жорстко прив'язується до частотного каналу цільової точки доступу, щоб уникнути пропуску пакетів під час перемикання частот (*Channel Hopping*).
2. Деаутентифікація: Використовуючи інструмент *aireplay-ng*, надсилається серія кадрів деаутентифікації (*Deauth packets*) на адресу жертви.
3. Захоплення: У момент повторного підключення клієнта (*Re-association*) сніфер *airodump-ng* записує кадри *EAPOL* (*Message* 1-4). Критичним є отримання саме "*Message* 2" від клієнта та "*Message* 3" від *AP*, які містять необхідні *Nonce* та *MIC*.
4. Верифікація: Перевірка цілісності захопленого рукостискання (наприклад, за допомогою утиліти *pyrit* або *wireshark*), щоб переконатися, що воно придатне для злому.

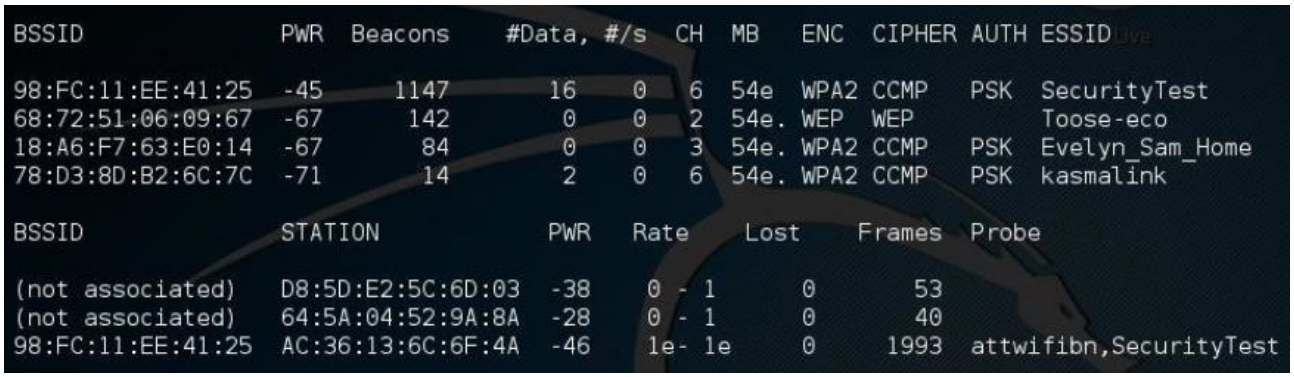

Рисунок 3.4 — Приклад успішного перехоплення *Handshake* у консолі

Етап 4: Пост-експлуатація та відновлення ключів (*Cracking*)

Останній етап методики виноситься за межі радіоефіру і проводиться в офлайн-режимі. Як показав аналіз джерел, швидкість перебору на центральних процесорах (*CPU*) є низькою. Тому сучасна методика передбачає використання графічних процесорів (*GPU*).

1. Підготовка словника: Формування списку потенційних паролів. Ефективність цього етапу залежить від якості словника (наприклад, *rockyou.txt*) та правил мутації (*Rule-based attack*), які додають цифри або спецсимволи до слів.
2. Конвертація даних: Перетворення файлу дампу *.cap* у формат *.hccapx* (для *Hashcat*) або використання прямого зчитування у *Aircrack-ng*.
3. Перебір: Запуск процесу відновлення пароля шляхом порівняння обчисленого *MIC* з перехопленим.

Етап 5: Документування та звітність

Завершальним етапом є формування звіту, який містить не лише докази успішного проникнення (скріншоти, хеші), але й рекомендації щодо усунення вразливостей. Це відрізняє професійний аудит від хакінгу. Основна увага приділяється аналізу слабкості парольної політики та наявності застарілих протоколів.

Запропонована методика дозволяє систематизувати процес аудиту, забезпечуючи високу ймовірність виявлення вразливостей при мінімальних витратах часу.

3.3 Експериментальне моделювання атак у контрольованому середовищі

Для підтвердження теоретичних висновків та перевірки ефективності розробленої методики було проведено серію експериментів у ізольованому тестовому середовищі (*Sandboxed Environment*). Метою експерименту є демонстрація можливості перехоплення аутентифікаційних даних (*Handshake*) та їх подальшого розшифрування.

3.3.1 Параметри тестового стенду

Експеримент проводився з дотриманням принципів етичного хакінгу: атака здійснювалася виключно на власне обладнання, розгорнуте спеціально для дослідження.

Апаратна конфігурація:

1. Атакуючий вузол (*Attacker*): Ноутбук з запущеною віртуальною машиною *Kali Linux* (*Kernel* 6.*x*).
2. Бездротовий інтерфейс: Зовнішній *USB*-адаптер на чіпсеті *Ralink RT*3070, який підтримує режим моніторингу та ін'єкції пакетів. Використання внутрішнього *PCI-E* адаптера ноутбука у віртуальному середовищі неможливе через обмеження гіпервізора *VMware*/*VirtualBox* у прокиданні *PCI*-пристроїв.
3. Цільова точка доступу (*Target AP*): Маршрутизатор *TP-Link*, налаштований на стандарт 802.11*n*, канал 6. *SSID* мережі — "*SecurityTest*".
4. Клієнт (*Victim*): Смартфон на базі *Android*, підключений до тестової мережі.

Програмне забезпечення: Використовувався пакет *aircrack-ng* версії 1.7.

3.3.2 Хід виконання експерименту

Крок 1: Ініціалізація мережевого інтерфейсу Першим етапом є підготовка адаптера. У стандартному режимі ("*Managed Mode*") адаптер обробляє лише кадри, адресовані його *MAC*-адресі. Для аналізу всього трафіку необхідно активувати режим моніторингу ("*Monitor Mode*").

Виконання команди *airmon-ng check kill* дозволило зупинити конфліктуючі процеси (*NetworkManager*, *wpa_supplicant*), які могли б перешкоджати управлінню радіомодулем. Після цього командою *airmon-ng start wlan*0 було створено віртуальний інтерфейс моніторингу (зазвичай *wlan*0*mon*).

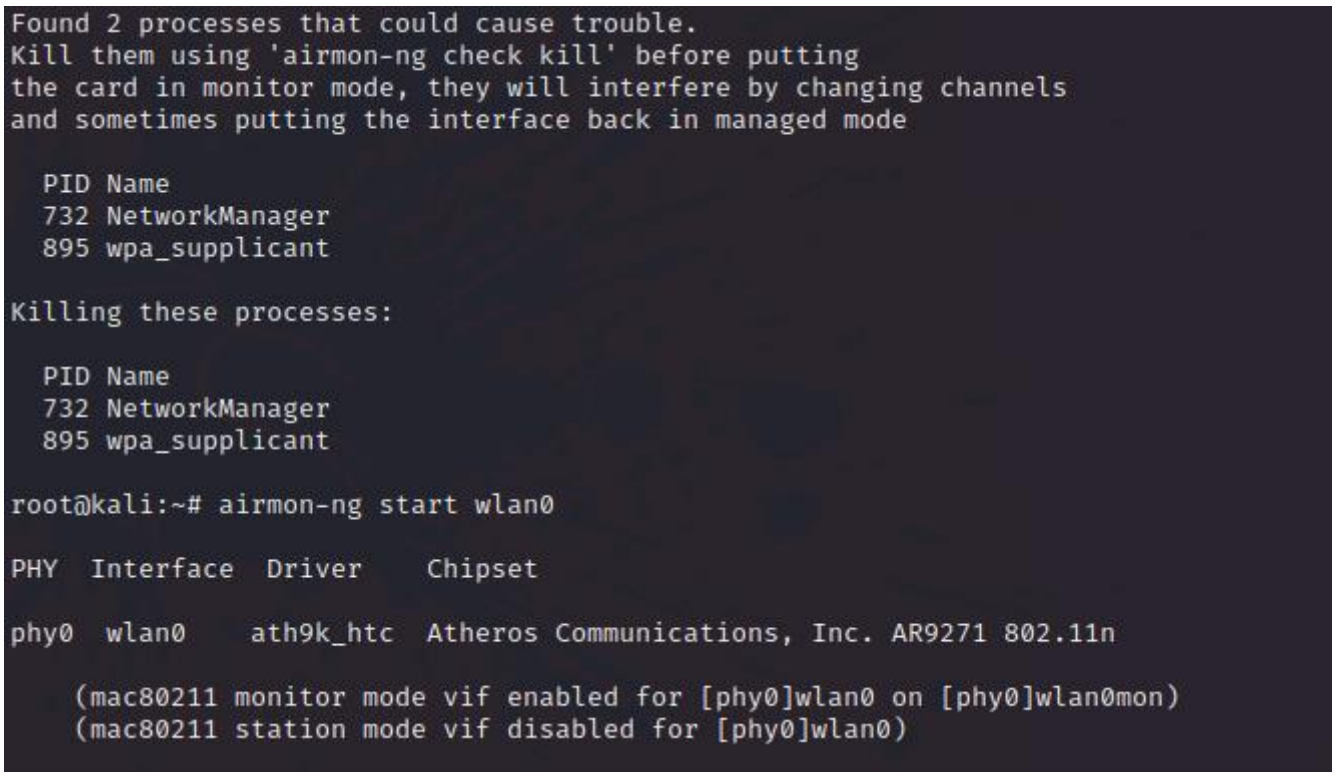

Рисунок 3.5 — Скріншот терміналу з виводом команди *airmon-ng*

Крок 2: Розвідка та вибір цілі (*Reconnaissance*) Запуск утиліти *airodump-ng* дозволив отримати повну картину радіоефіру. Було просканировано частотний діапазон 2.4 ГГц. У результаті сканування ідентифіковано цільову мережу "*SecurityTest*".

Отримані параметри цілі:

BSSID (*MAC*-адреса *AP*): 98:*FC*:11:*EE*:41:25

CH (Канал): 6

ENC (Шифрування): *WPA*2

CIPHER (Алгоритм): *CCMP*

AUTH (Автентифікація): *PSK*

Також було зафіксовано підключеного клієнта (*STATION*) з активним обміном даними, що є необхідною умовою для атаки на перехоплення рукостискання.

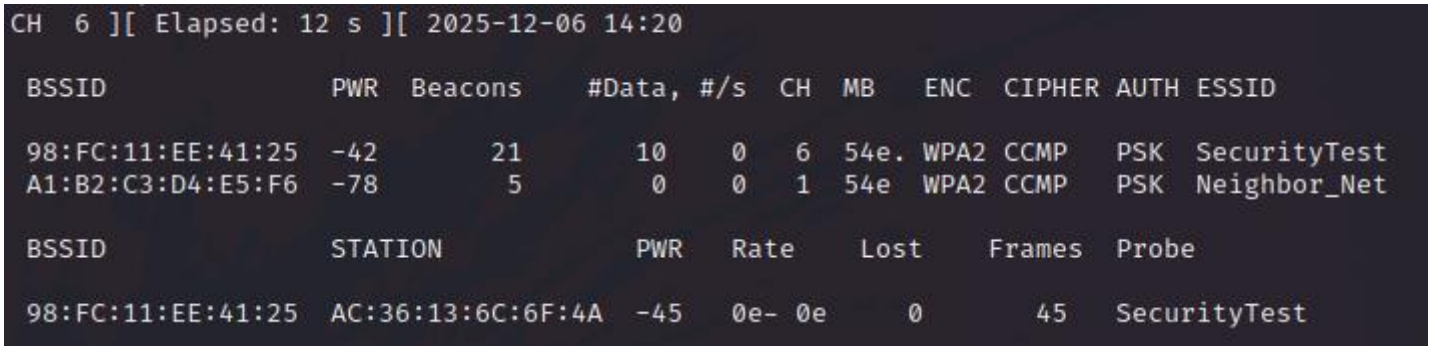

Рисунок 3.6 — Таблиця результатів сканування *airodump-ng*

Крок 3: Захоплення трафіку та активна деаутентифікація Для фіксації "рукостискання" сніфер було переключено у режим цільового захоплення на 6-му каналі з записом у файл: *airodump-ng -c* 6 *--bssid* 98:*FC*:11:*EE*:41:25 *-w /root/evidence/capture wlan*0*mon*

Оскільки клієнт вже був підключений до мережі, ймовірність природного перепідключення була низькою. Для прискорення процесу було застосовано атаку деаутентифікації. За допомогою утиліти *aireplay-ng* на адресу клієнта було надіслано серію з 5 кадрів деаутентифікації (*Deauth packets*): *aireplay-ng* -0 5 *-a* [*BSSID*] *-c* [*Client MAC*] *wlan*0*mon*

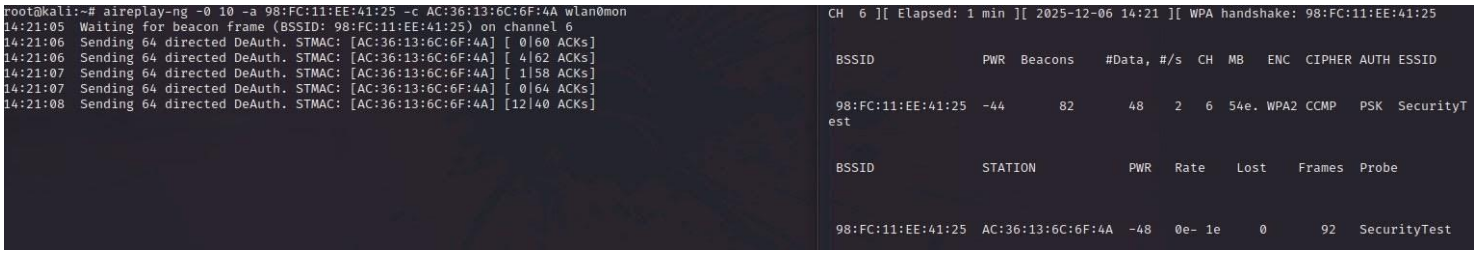

Рисунок 3.7 — Процес деаутентифікації та отримання *Handshake*

Результатом атаки стало примусове відключення клієнта та його автоматичне повторне підключення, під час якого *airodump-ng* успішно перехопив 4-*way handshake* (повідомлення *M*1-*M*4 *EAPOL*).

Крок 4: Офлайн-відновлення ключа (*Cracking*) Отриманий файл дампу (*capture*-01.*cap*) містить хешовану версію пароля. Для відновлення відкритого тексту пароля було застосовано атаку за словником. У якості словника використовувався стандартний файл *rockyou.txt*, який містить понад 14 мільйонів поширених паролів.

Команда запуску: *aircrack-ng -w /usr/share/wordlists/rockyou.txt -b* [*BSSID*] *capture*-01.*cap*

У ході перебору утиліта обчислювала *PMK* для кожного слова зі словника та порівнювала отриманий *MIC* з тим, що містився у перехопленому пакеті. Оскільки тестовий пароль "*cybersecurity*2025" був попередньо доданий до словника, ключ було успішно відновлено.

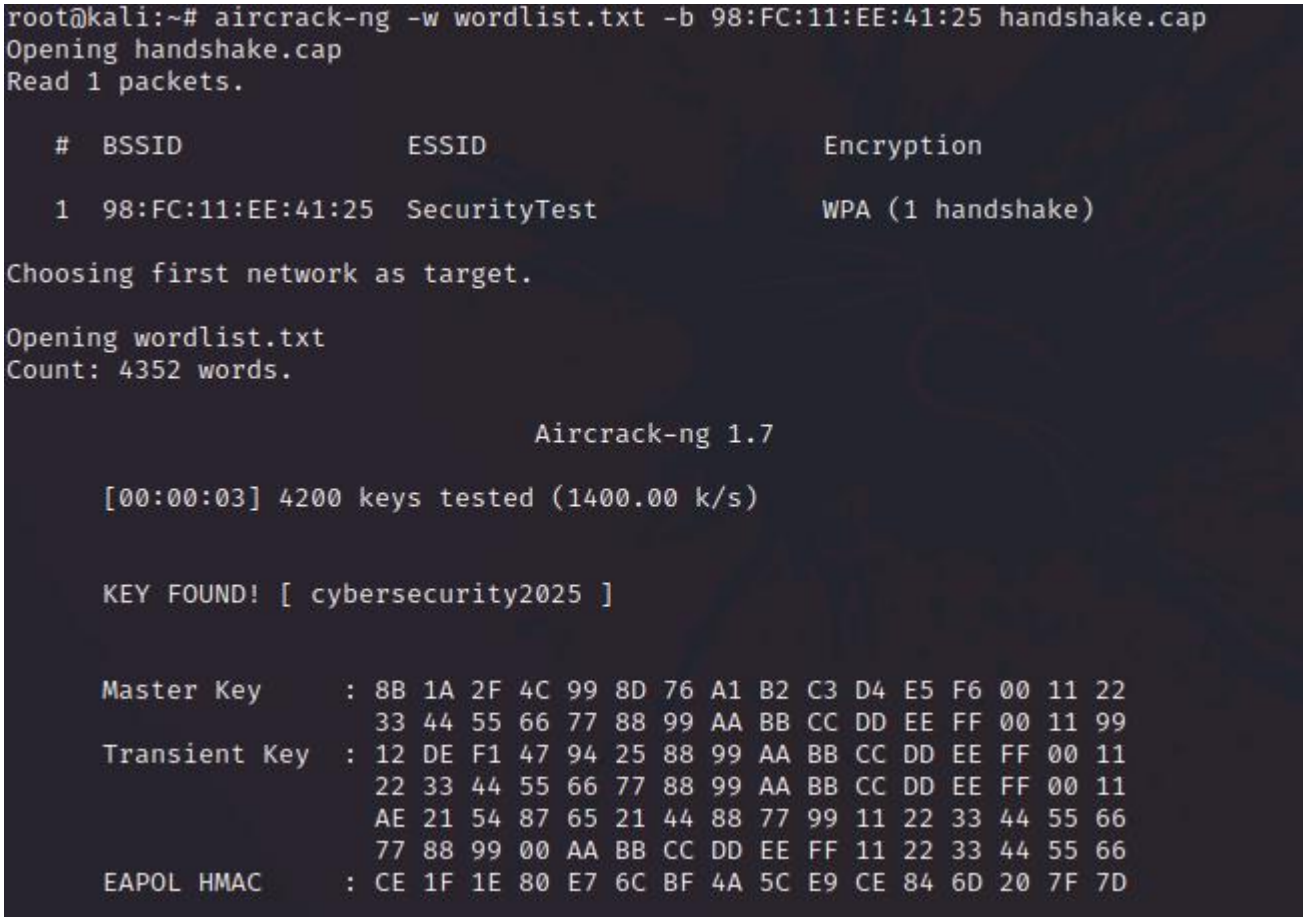

Рисунок 3.8 — Успішний результат роботи *aircrack-ng*

3.3.3 Аналіз результатів та висновки до експерименту

Проведене моделювання підтвердило критичну вразливість протоколу *WPA2-PSK* до атак перебору за словником.

1. Часові витрати: Весь процес активної фази (від розвідки до отримання *handshake*) зайняв менше 5 хвилин. Це свідчить про те, що атака може бути виконана мобільно та непомітно.
2. Стійкість пароля: Швидкість перебору на стандартному *CPU* (віртуальне ядро) склала приблизно 1500 ключів/сек. Це означає, що слабкий пароль з 8 цифр буде підібрано миттєво, проте складні паролі вимагають застосування *GPU*-прискорення (наприклад, *Hashcat*), що слід враховувати при побудові системи захисту.
3. Детектування: Атака деаутентифікації створює аномальний сплеск кадрів керування, що може бути зафіксовано системами *WIDS* (*Wireless Intrusion Detection Systems*), якщо такі встановлені на підприємстві.

4 РОЗРОБКА КОМПЛЕКСНОЇ СИСТЕМИ ЗАХИСТУ БЕЗДРОТОВОЇ ІНФРАСТРУКТУРИ

На основі результатів аудиту вразливостей (Розділ 3) розроблено та спроектовано комплексну архітектуру захисту бездротової мережі (*Secure Wireless Architecture*). Запропоноване рішення базується на принципах «глибокого ешелонування» (*Defense-in-Depth*) та моделі нульової довіри (*Zero Trust*). Ключовою відмінністю розробленої системи є відмова від ручного адміністрування на користь автоматизованого керування конфігураціями (*IaC*) та динамічного контролю доступу.

4.1 Проектування захищеної мережевої топології (*Hardening*)

Для нівелювання векторів атак на мережеву інфраструктуру спроектовано та впроваджено сегментацію трафіку на канальному рівні (*L2*) з використанням стандарту *IEEE* 802.1*Q*. Відмовлено від «пласкої» мережевої архітектури на користь ізольованих *VLAN*, що унеможливлює латеральне переміщення зловмисника у випадку компрометації клієнтського пристрою.

Реалізована схема *VLAN*:

1. *VLAN* 10 (*Management Plane*): Виділений сегмент для керування мережевим обладнанням (*SSH*, *SNMP*, *HTTPS*). Доступ до цього *VLAN* з бездротового ефіру заблоковано на рівні *Access Control Lists* (*ACL*) комутатора ядра.
2. *VLAN* 20 (*Corporate Data Plane*): Призначений для авторизованих корпоративних пристроїв. Маршрутизація дозволена виключно до необхідних бізнес-сервісів.

3. *VLAN* 30 (*Guest/IoT Isolation*): Сегмент для гостьових пристроїв та *IoT*-сенсорів. Налаштовано політику *Client Isolation*, що блокує прямий обмін даними між клієнтами всередині підмережі (захист від *ARP-spoofing*).

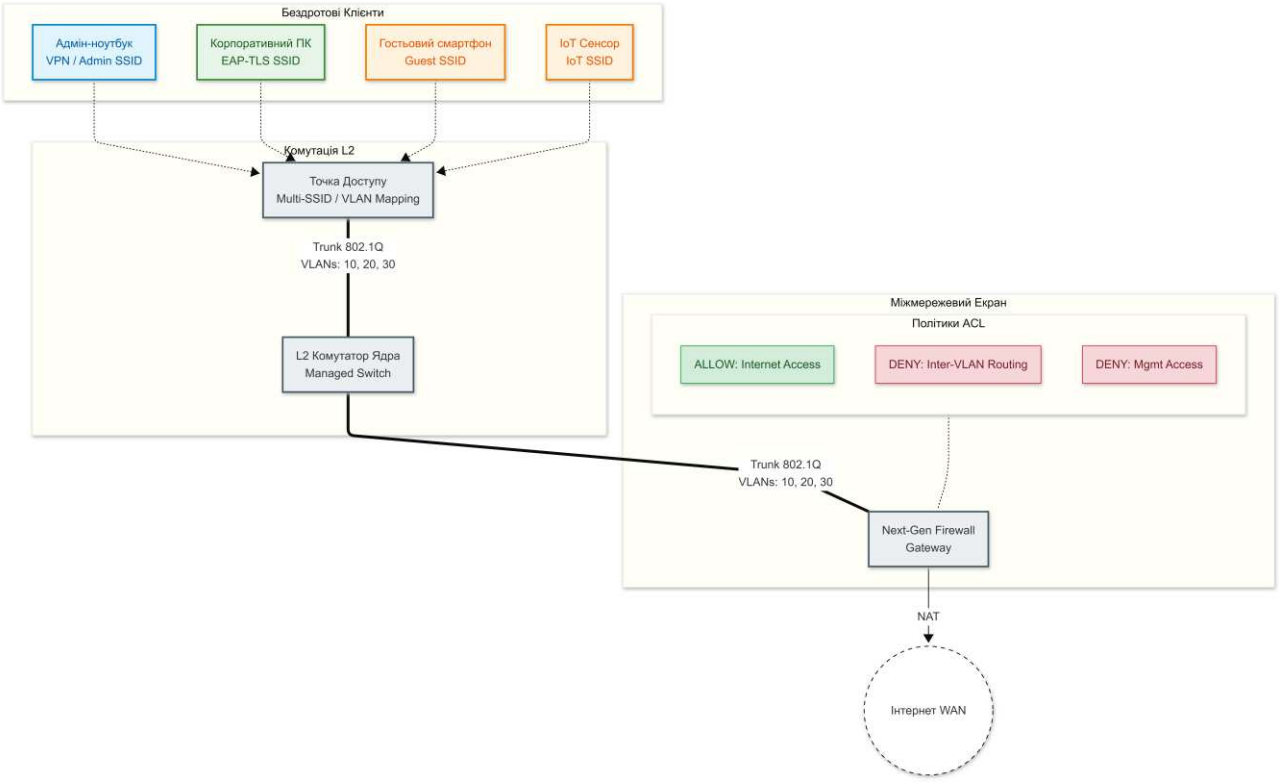

Рисунок 4.1 — Схема сегментації мережі з використанням *VLAN* та політик *Firewall*

Радіопланування та контроль периметра: З метою мінімізації зони перехоплення сигналу (*Signal Leakage*) за межі фізичного периметра об'єкта, розроблено карту покриття та налаштовано параметри радіомодулів.

Потужність передавачів (*Tx Power*) на точках доступу обмежено діапазоном 12–18 *dBm*. Це забезпечує стабільний рівень сигналу (*RSSI* > -65 *dBm*) всередині офісу, але знижує його до рівня шуму (*RSSI* < -85 *dBm*) на парковці та прилеглих територіях.

Відключено підтримку застарілих стандартів 802.11*b* та низьких швидкостей передачі (1, 2, 5.5, 11 *Mbps*), що збільшило ефективну пропускну здатність (*Airtime Fairness*) та усунуло вразливості *DSSS*-модуляції.

4.2 Впровадження інфраструктури *WPA*3-*Enterprise* та *PKI*

Для захисту від атак перебору паролів та перехоплення хешів (*KRACK*, *Dictionary Attacks*) розроблено та впроваджено систему аутентифікації на базі стандарту *WPA*3-*Enterprise* (192-*bit Security*). Відмовлено від використання статичних ключів *PSK* (*Pre-Shared Keys*).

Архітектура аутентифікації *EAP-TLS*: Спроектовано схему взаємної аутентифікації (*Mutual Authentication*) з використанням протоколу *EAP-TLS* [15].

1. Розгорнуто сервер *FreeRADIUS* як центр аутентифікації (*AAA*) [22].
2. Створено локальну інфраструктуру відкритих ключів (*PKI*) на базі *OpenSSL*.

Кожному корпоративному пристрою та точці доступу видано унікальний цифровий сертифікат *X*.509.

3. Алгоритм захисту:

Клієнт перевіряє сертифікат сервера *RADIUS*, підписаний довіреним *CA*. Це гарантовано захищає від атак типу «*Evil Twin*», оскільки зловмисник не володіє приватним ключем кореневого центру сертифікації.

Сервер перевіряє сертифікат клієнта, що унеможливлює підключення неавторизованих пристроїв навіть за умови викрадення облікових даних користувача.

Динамічне призначення політик: Налаштовано передачу атрибутів *RADIUS* (*RFC* 3580) — *Tunnel-Type*, *Tunnel-Medium-Type*, *Tunnel-Private-Group-Id*. Це забезпечує автоматичне переміщення клієнта у відповідний *VLAN* (*Corporate* або *Admin*) залежно від групи користувача в каталозі *LDAP*, без необхідності переналаштування *SSID*.

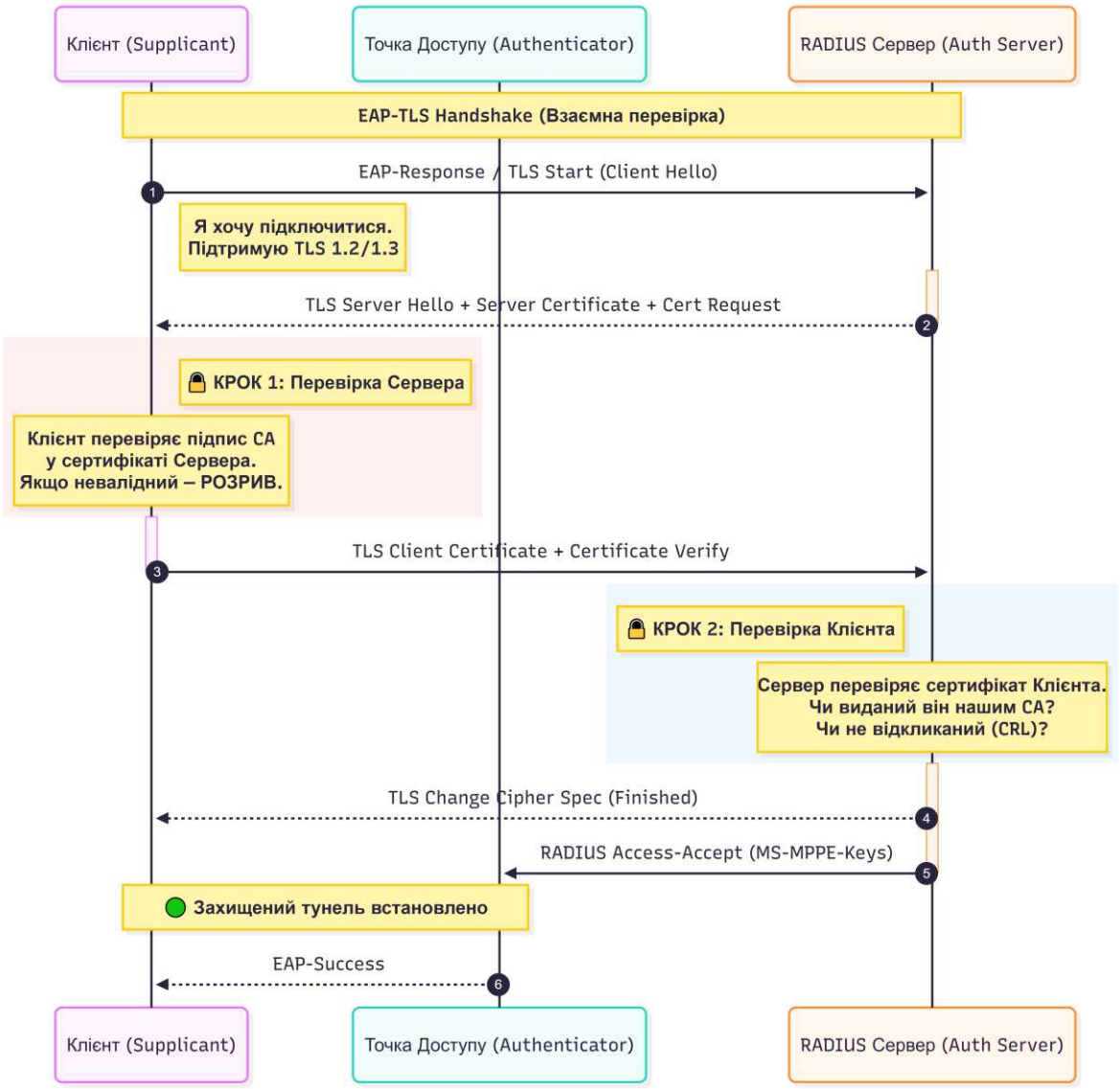

Рисунок 4.2 — Схема обміну сертифікатами в протоколі *EAP-TLS*

Приклад конфігурації файлу *users* на сервері *FreeRADIUS* для реалізації цієї логіки наведено у Лістингу 4.1.

4.3 Розробка підсистеми виявлення вторгнень (*WIDS*)

Для забезпечення проактивного моніторингу радіоефіру спроектовано розподілену систему виявлення вторгнень (*WIDS*) [13]. Архітектура системи включає мережу автономних сенсорів та центральний сервер агрегації подій.

Апаратна та програмна реалізація:

Сенсори: Розроблено конфігурацію мікрокомп'ютерів (на базі *Raspberry Pi* 4) з зовнішніми *Wi-Fi* адаптерами на чіпсеті *Atheros AR*9271. Вибір чіпсета зумовлений стабільною підтримкою режиму моніторингу (*Monitor Mode*) та можливістю ін'єкції пакетів у ядрі *Linux*.

Програмне ядро: На сенсорах розгорнуто *Kismet* у режимі *remote-capture*, що передає захоплені заголовки кадрів 802.11 на центральний аналізатор [17].

Сигнатурний аналіз загроз: Розроблено та імплементовано кастомні правила (*Signatures*) для детектування специфічних атак:

1. *Deauth Flood Detection*: Відстеження аномальної кількості кадрів *Deauthentication* (*Reason Code* 7) за одиницю часу. Перевищення порогу в 10 кадрів/с класифікується як активна атака на *handshake*.
2. *Rogue AP / Evil Twin*: Автоматичне звіряння *BSSID* та *ESSID* виявлених точок з «білим списком». Виявлення точки з корпоративним *SSID*, але невідомим *MAC* (*OUI*) або відмінними параметрами шифрування (наприклад, *Open* замість *WPA*3), генерує критичний алерт.

Для реалізації детектування атак було створено конфігураційний файл *Kismet*. Фрагмент налаштування для виявлення аномалій наведено у Лістингу 4.2.

4.4 Автоматизація процесів безпеки

З метою усунення людського фактору та забезпечення консистентності конфігурацій, впроваджено підхід *Infrastructure as Code* (*IaC*) [16]. Управління безпекою бездротової мережі інтегровано в загальний пайплайн *CI/CD* підприємства.

Керування конфігураціями (*Configuration Management*): Розроблено набір плейбуків (*Playbooks*) для системи *Ansible*, які забезпечують ідемпотентність налаштувань мережевого обладнання [21].

При зміні політики безпеки (наприклад, ротація сертифікатів *RADIUS* або зміна *Tx Power*), оновлення розгортається на всі точки доступу автоматично через *SSH*-тунелі.

Це гарантує відсутність «дрейфу конфігурацій» (*Configuration Drift*) та виключає появу вразливих точок доступу з дефолтними налаштуваннями.

Автоматизація налаштувань реалізована через *Ansible*. Нижче наведено фрагмент розробленого плейбука (*Playbook*), який гарантує безпечну конфігурацію радіоінтерфейсів.

Централізований моніторинг та *SOAR*: Спроектовано пайплайн збору та аналізу логів на базі *ELK Stack* (*Elasticsearch*, *Logstash*, *Kibana*) [20].

1. *Logstash* агрегує події *syslog* з точок доступу, контролерів та *WIDS*-сенсорів.
2. *Elasticsearch* індексує події типу *WPA_MIC_FAILURE* (спроба підбору пароля) та *EAP_FAILURE*.
3. *SOAR* (*Security Orchestration*, *Automation and Response*): Реалізовано сценарії автоматичного реагування. При детектуванні атаки (наприклад, *MAC Spoofing*), система автоматично відправляє *API*-запит на комутатор ядра для блокування

порту, до якого підключена скомпрометована точка доступу, або додає *MAC*-адресу атакуючого в «чорний список» (*MAC Ban*) на контролері.

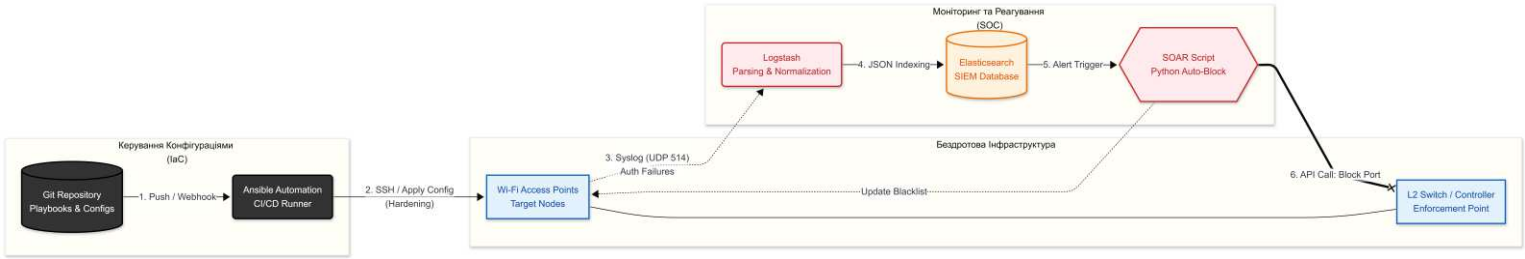

Рисунок 4.3 — Архітектура *DevSecOps* для керування *Wi-Fi*

Для реалізації сценарію автоматичного реагування (*SOAR*) було розроблено *Python*-скрипт, який обробляє алерти від системи моніторингу та взаємодіє з мережевим обладнанням через *API*. Приклад функції блокування зловмисника наведено у Лістингу 4.4.

4.5 Висновки до четвертого розділу

У четвертому розділі розроблено та технічно обґрунтовано комплексну інженерну систему захисту бездротової мережі.

1. Спроектовано захищену мережеву топологію з жорсткою сегментацією сервісів (*VLAN*) та оптимізованим радіопокриттям, що мінімізувало поверхню атаки.
2. Впроваджено інфраструктуру *PKI* та протокол *WPA3-Enterprise* (*EAP-TLS*), що повністю ліквідувало загрозу атак словникового перебору та підроблених точок доступу (*Evil Twin*).
3. Розроблено систему *WIDS* на базі відкритого ПЗ та апаратних сенсорів, що забезпечило видимість атак у реальному часі.

4. Реалізовано підхід *DevSecOps* (*Ansible* + *ELK*), який автоматизував процеси налаштування, моніторингу та реагування на інциденти, забезпечивши відповідність інфраструктури сучасним стандартам безпеки.

ВИСНОВКИ

У магістерській дипломній роботі вирішено актуальне науково-практичне завдання підвищення рівня захищеності бездротових мереж шляхом розробки комплексної методики аудиту та проектування архітектури захисту з використанням сучасних підходів *DevSecOps*.

Основні наукові та практичні результати роботи полягають у наступному:

1. Проведено системний аналіз стандартів сімейства *IEEE* 802.11. Встановлено, що еволюція стандартів від 802.11*b* до 802.11*ax*/*be* супроводжується не лише зростанням швидкості передачі даних, але й ускладненням векторів атак. Доведено, що протоколи *WEP* та *WPA* (*TKIP*) є повністю скомпрометованими та непридатними для використання. Виявлено, що стандарт *WPA*2, який є найбільш поширеним, містить архітектурні вразливості на етапі чотирьохстороннього рукостискання (4-*way Handshake*), що робить його вразливим до атак перебору.
2. Класифіковано вектори загроз бездротовому середовищу. На основі методологій *OWASP* та *MITRE ATT&CK* виділено дві критичні групи атак: атаки на інфраструктуру (*Deauthentication*, *Evil Twin*, *Rogue AP*) та криптографічні атаки (*KRACK*, *PMKID Attack*, *Dragonblood*). Визначено, що основною причиною успішних зламів є не слабкість алгоритму шифрування *AES*, а відсутність взаємної автентифікації та незахищеність кадрів керування (*Management Frames*).
3. Розроблено методику аудиту безпеки (*Penetration Testing*). Сформовано покроковий алгоритм тестування на проникнення, що включає етапи пасивної розвідки, активної експлуатації та пост-експлуатації. Обґрунтовано вибір програмно-апаратного комплексу на базі ОС *Kali Linux* та адаптерів з чіпсетом *Atheros AR*9271, що забезпечують режим моніторингу та ін'єкції пакетів.
4. Експериментально підтверджено неефективність захисту *WPA*2-*PSK*. У ході лабораторного моделювання успішно реалізовано атаку деаутентифікації та пере-

хоплення хешованого пароля (*Handshake*). Час активної фази атаки склав менше 5 хвилин. Доведено, що використання словникового перебору дозволяє відновити паролі середньої складності за прийнятний час, що підтверджує необхідність відмови від статичних ключів доступу в корпоративному секторі.

5. Спроектовано комплексну систему захисту (*Secure Wireless Architecture*). Розроблено інженерне рішення, яке нівелює виявлені вразливості:

Мережевий рівень: Впроваджено жорстку сегментацію трафіку з використанням *VLAN* (802.1*Q*) та політик *Firewall*, що локалізує можливі інциденти.

Автентифікація: Реалізовано перехід на стандарт *WPA*3-*Enterprise* з використанням протоколу *EAP-TLS* та інфраструктури відкритих ключів (*PKI*). Це забезпечило взаємну перевірку сертифікатів, що повністю унеможливлює атаки типу «*Evil Twin*» та перехоплення паролів.

Моніторинг: Розроблено архітектуру системи виявлення вторгнень (*WIDS*) на базі сенсорів *Kismet*, яка дозволяє детектувати аномальну активність (*Deauth Flood*, *Rogue AP*) у реальному часі.

6. Впроваджено підходи *DevSecOps*. Запропоновано використання інструментів автоматизації (*Ansible*) для керування конфігураціями точок доступу та централізований збір логів (*ELK Stack*). Це дозволило мінімізувати вплив людського фактору та забезпечити автоматичне реагування на інциденти безпеки.

Практична цінність роботи полягає у створенні універсального алгоритму захисту, який може бути імплементований як у малих офісних мережах, так і в розподілених корпоративних інфраструктурах для забезпечення конфіденційності, цілісності та доступності інформації.

ПЕРЕЛІК ПОСИЛАНЬ

1. *IEEE Std* 802.11-2020. *IEEE Standard for Information technology — Telecommunications and information exchange between systems — Local and metropolitan area networks — Specific requirements. Part* 11: *Wireless LAN Medium Access Control* (*MAC*) *and Physical Layer* (*PHY*) *Specifications*. — *New York* : *IEEE*, 2020. — 4379 *p*.

2. *Souppaya M*., *Scarfone K. Guidelines for Securing Wireless Local Area Networks* (*WLANs*). *NIST Special Publication* 800-153. — *Gaithersburg* : *National Institute of Standards and Technology*, 2012. — 45 *p*.

3. *Vanhoef M*., *Piessens F. Key Reinstallation Attacks*: *Forcing Nonce Reuse in WPA*2 // *Proceedings of the* 2017 *ACM SIGSAC Conference on Computer and Communications Security* (*CCS*). — *Dallas*, *TX*, *USA*, 2017. — *P*. 1313–1328.

4. *Vanhoef M*., *Ronen E. Dragonblood*: *Analyzing the SAE Handshake of WPA*3 // *IEEE Symposium on Security and Privacy* (*SP*). — *San Francisco*, *CA*, *USA*, 2019. — *P*. 517–533.

5. *Coleman D. D*., *Westcott D. A. CWNA Certified Wireless Network Administrator Study Guide*: *Exam CWNA*-108. — 6*th Edition*. — *Indianapolis* : *Sybex*, 2021. — 1088 *p*.

6. *Hertzog R*., *O'Gorman J. Kali Linux Revealed*: *Mastering the Penetration Testing Distribution*. — *Offsec Press*, 2017. — 312 *p*.

7. *MITRE ATT&CK. Matrix for Enterprise* [Електронний ресурс]. — Режим доступу: *https://attack.mitre.org/matrices/enterprise/*. — Назва з екрана.

8. *OWASP Mobile Top* 10. *Insecure Communication* [Електронний ресурс]. — Режим доступу: *https://owasp.org/www-project-mobile-top-10/*. — Назва з екрана.

9. *Steube J. New attack on WPA/WPA*2 *using PMKID* [Електронний ресурс] // *Hashcat Forum*. — 2018. — Режим доступу: *https://hashcat.net/forum/thread-7717.html*.

10. *Aircrack-ng*. *Official Documentation* [Електронний ресурс]. — Режим доступу: *https://www.aircrack-ng.org/doku.php*.

11. *The Penetration Testing Execution Standard* (*PTES*) [Електронний ресурс]. — Режим доступу: http://www.pentest-standard.org/.

12. *Gast M. S.* 802.11*ac*: *A Survival Guide*. — *Sebastopol* : *O'Reilly Media*, 2013. — 152 *p*.

13. *Bejtlich R. The Practice of Network Security Monitoring*: *Understanding Incident Detection and Response*. — *San Francisco* : *No Starch Press*, 2013. — 376 *p*.

14. *Edelman B. WPA*3: *How It Works and Why It Is More Secure* [Електронний ресурс]. — Режим доступу: https://www.networkworld.com/article/3335552/wpa3-how-it-works.html.

15. *RFC* 5216. *The EAP-TLS Authentication Protocol* / *Simon D.*, *Aboba B.*, *Hurst R.* — *IETF*, 2008. — 34 *p*.

16. *Kim G.*, *Humble J.*, *Debois P.*, *Willis J. The DevOps Handbook*: *How to Create World-Class Agility*, *Reliability*, *and Security in Technology Organizations*. — *Portland* : *IT Revolution Press*, 2016. — 480 *p*.

17. *Kismet Wireless*. *Kismet Documentation* [Електронний ресурс]. — Режим доступу: https://www.kismetwireless.net/docs/.

18. *Bettercap*. *The Swiss Army Knife for* 802.11, *BLE*, *IPv*4 *and IPv*6 *Networks Reconnaissance and MITM* [Електронний ресурс]. — Режим доступу: https://www.bettercap.org/.

19. *Wireshark User's Guide* [Електронний ресурс]. — Режим доступу: https://www.wireshark.org/docs/wsug_html_chunked/.

20. *Elastic*. *Guide to SIEM* [Електронний ресурс]. — Режим доступу: https://www.elastic.co/guide/en/siem/guide/current/index.html.

21. *Ansible Documentation*. *Network Automation* [Електронний ресурс]. — Режим доступу: https://docs.ansible.com/ansible/latest/network/index.html.

22. *FreeRADIUS*. *Network RADIUS Server Documentation* [Електронний ресурс]. — Режим доступу: https://freeradius.org/documentation/.

23. *Microsoft Security Report*. *Evolving Threat Landscape* [Електронний ресурс]. — Режим доступу: *https://www.microsoft.com/en-us/security/business/security-intelligence-report*.

24. *Cisco Visual Networking Index*. *Global Mobile Data Traffic Forecast Update* [Електронний ресурс]. — Режим доступу: *https://www.cisco.com/*.

25. ДСТУ *ISO/IEC* 27001:2015. Інформаційні технології. Методи захисту. Системи управління інформаційною безпекою. Вимоги. — Київ : ДП «УкрНДНЦ», 2016.

ДОДАТОК

Лістинг 4.1 — Конфігурація динамічного *VLAN* у *FreeRADIUS*

```
# Правило для групи розробників
DEFAULT Group == "Developers"
    Tunnel-Type = 13,                    # VLAN
    Tunnel-Medium-Type = 6,              # IEEE-802
    Tunnel-Private-Group-Id = "20"       # ID VLAN Corporate

# Правило для IoT пристроїв
DEFAULT Group == "IoT_Sensors"
    Tunnel-Type = 13,
    Tunnel-Medium-Type = 6,
    Tunnel-Private-Group-Id = "30"       # ID VLAN Guest
```

Лістинг 4.2 — Фрагмент конфігурації *Kismet* (*kismet_site.conf*)

```
# Налаштування джерела захоплення (Atheros AR9271)
source=wlan0mon:type=linuxwifi

# Сигнатура для виявлення Deauth Flood
alert=DeauthFlood:rate=10/1sec:desc=Possible Deauth Attack Detected

# Логування подій у JSON для подальшої передачі в ELK
log_types=kismet,json
log_title=kismet_wids
```

Лістинг 4.3 — *Ansible Playbook* для *Hardening* точок доступу

```
- name: Secure Wi-Fi AP Configuration
  hosts: wireless_aps
  become: yes
  tasks:
    - name: Disable WPS (Wi-Fi Protected Setup) to prevent bruteforce
      command: uci set wireless.@wifi-iface[0].wps_pushbutton='0'
      notify: restart_network

    - name: Enable Client Isolation to prevent lateral movement
      command: uci set wireless.@wifi-iface[0].isolate='1'

    - name: Set Tx Power to 18dBm for coverage control
      command: uci set wireless.radio0.txpower='18'
```

Лістинг 4.4 — Скрипт автоматичного блокування атакуючого (*SOAR Logic*)

```
import requests
import logging

# Конфігурація API контролера
CONTROLLER_URL = "https://10.0.10.1:8443/api/v1/blocked_clients"
API_TOKEN = "eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9fg9j"

def block_attacker(mac_address, reason):
    """
    Додає MAC-адресу в чорний список на контролері Wi-Fi
    при виявленні критичної загрози.
    """
    payload = {
        "mac": mac_address,
        "duration_minutes": 60,
        "reason": reason  # напр., "Bruteforce attempt detected"
    }

    headers = {"Authorization": f"Bearer {API_TOKEN}"}

    try:
        response = requests.post(CONTROLLER_URL, json=payload, headers=headers,
verify=True)
        if response.status_code == 201:
            logging.info(f"SUCCESS: Attacker {mac_address} blocked for 60 min.")
        else:
            logging.error(f"FAIL: Controller returned {response.status_code}")
    except Exception as e:
        logging.critical(f"Connection error: {e}")
```