Міністерство освіти і науки України
Харківський національний університет радіоелектроніки

Факультет _____*Інфокомунікацій*_____
(повна назва)
Кафедра _____*Інформаційно-мережної інженерії*_____
(повна назва)

# КВАЛІФІКАЦІЙНА РОБОТА
## Пояснювальна записка

рівень вищої освіти _____другий (магістерський)_____

_____*Дослідження механізмів безпеки мереж стандарту 802.11*_____
_____
(тема)

Виконав:
студент _2_ курсу, групи ____*ІМІм-22-1*____
_____*Щербак Д.О.*_____
(прізвище, ініціали)

Спеціальність _*172. Телекомунікації та радіотехніка*_
(код і повна назва спеціальності)
Тип програми _____*освітньо-професійна*_____
(освітньо-професійна або освітньо-наукова)
Освітня програма _*Інформаційно-мережна інженерія*_
( повна назва освітньої програми)

Керівник _____*ст.викл. Твердохліб В.В.*_____
(посада, прізвище, ініціали)

Допускається до захисту

Зав. кафедри _____ _____*Безрук В.М.*_____
(підпис) (прізвище, ініціали)

2023 р.

Не містить відомостей, заборонених
до відкритого публікування

Керівник _____ /*В.В.Твердохліб*

Студент _____ / *Д*.О. *Щербак*

Харківський національний університет радіоелектроніки

Факультет *Інфокомунікацій*

Кафедра *Інформаційно-мережної інженерії*

Рівень вищої освіти другий (магістерський)

Спеціальність *172. Телекомунікації та радіотехніка*
(код і повна назва)

Тип програми *Освітньо-професійна*
(освітньо-професійна або освітньо-наукова)

Освітня програма *Інформаційно-мережна інженерія*
(повна назва)

ЗАТВЕРДЖУЮ:

Зав. кафедри _____
(підпис)
«24» *жовтня* 2023 р.

# ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ

студентові *Щербаку Денису Олександровичу*
(прізвище, ім'я, по батькові)

1. Тема роботи *Дослідження механізмів безпеки мереж стандарту 802.11*

затверджена наказом університету від 23 жовтня 2023 р. № 1233 Ст

2. Термін подання студентом роботи до екзаменаційної комісії 24 січня 2024 р.

3. Вихідні дані до роботи *Обгрунтувати тенденцію до постійного зростання обсягів трафіку у мережах WiFi. Дослідити механізми забезпечення захищеності поширених бездротових мереж стандарту 802.11. Розглянути існуючі підходи та інструменти зламу мереж зазначеного стандарту та виявити найбільш продуктивні з них. Реалізувати сценарій зламу ключа WiFi на базі попередньо обраного інструментарію. Запропонувати рекомендації зі збільшення захищеності мереж розглянутого стандарту*

4. Перелік питань, що потрібно опрацювати в роботі *Вступ*

*1 . Специфіка використання безпровідних мереж доступу*

*2. Інструменти та механізми захисту мереж WiFi*

*3. Методи та засоби зламу безпровідних каналів WiFi*

*4. Реалізація процедури зламу пароля wi-fi на базі методу handshake*

*Висновки*

5. Перелік графічного матеріалу із зазначенням креслеників, схем, плакатів, комп'ютерних ілюстрацій (п.5 включається до завдання за рішенням випускової кафедри) _____
*слайди презентації в форматі Power Point (назва та мета роботи, специфіка застосування мереж WiFi, протоколи безпеки WiFi, підходи до зламу мереж WiFi, перехоплення ключа за методом handshake, висновки)*

**КАЛЕНДАРНИЙ ПЛАН**

| № | Назва етапів роботи | Терміни виконання етапів роботи | Примітка |
|---|---|---|---|
| 1 | Вступ | 24.10.23-26.10.23 | виконано |
| 2 | Специфіка використання безпровідних мереж доступу | 27.10.23-8.11.23 | виконано |
| 3 | Інструменти та механізми захисту мереж WiFi | 9.11.23-18.11.23 | виконано |
| 4 | Методи та засоби зламу безпровідних каналів WiFi | 19.11.23-27.11.23 | виконано |
| 5 | Реалізація процедури зламу пароля wi-fi на базі методу handshake | 28.11.23-16.12.23 | виконано |
| 6 | Висновки | 17.12.23-19.12.23 | виконано |
| 7 | Оформлення пояснювальної записки | 20.12.23-5.1.24 | виконано |

Дата видачі завдання *24 жовтня* 2023 р.

Студент _____
(підпис)

Керівник роботи _____ *ст. викл. Твердохліб В.В.*
(підпис) (посада, прізвище, ініціали)

# РЕФЕРАТ

Пояснювальна записка: 60 с., 17 рис., 21 джерело, 2 додатки

WIFI, WPS, BSSID, WPA2, WPA-PSK, CCMP, KALI LINUX, БЕЗДРОТОВІ МЕРЕЖІ, МЕРЕЖЕВА БЕЗПЕКА

Об'єкт дослідження – інструменти забезпечення захисту мереж стандарту 802.11.

Мета роботи – виявлення недоліків у використанні стандартизованих методів захисту бездротових мереж WiFi.

Обгрунтовується значимість роль WiFi, як невід’ємної складової сучасного інформаційного простору. Виконується огляд протоколів та інструментів безпеки мереж сімейства стандартів 802.11. Виявляються недоліки існуючих захисних механізмів. Досліджуються інструменти зламу паролів мереж зазначеного стандарту.

# THE ABSTRACT

Explanatory note: 60 p., 17 fig., 21 source, 2 apps.

WIFI, WPS, BSSID, WPA2, WPA-PSK, CCMP, KALI LINUX, WIRELESS NETWORKS, NETWORK SECURITY

The object of research is the tools for ensuring the protection of networks of the 802.11 standard.

The purpose of the work is to identify the shortcomings of the use of standardized methods of protecting WiFi wireless networks.

The significance of the role of WiFi as an integral component of the modern information space is substantiated. An overview of protocols and network security tools of the 802.11 family of standards is performed. The shortcomings of the existing protective mechanisms are revealed. Tools for cracking passwords of networks of the specified standard are being studied.

ЗМІСТ

С.

# ПЕРЕЛІК СКОРОЧЕНЬ

RC4 – (Rivest cipher 4) – потоковий алгоритм шифрування;
WEP – (Wired Equivalent Privacy) – протокол безпеки безпровідних мереж WiFi;
WPA, WPA2 – (Wi-Fi Protected Access) – протокол безпеки безпровідних мереж WiFi;
ICV – (Integrity Check Value) – контрольна сума;
LTE – (Long Term Evolution) – технологія високошвидкісної передачі даних мобільними мережами 4-го покоління;
LTE-A – (Long Term Evolution Advanced) – технологія високошвидкісної передачі даних мобільними мережами покоління 4,5, розвиток LTE;
PSK – (Public Shared Key) — метод перевірки автентичності клієнта на базі загальних ключів;
TKIP – (Temporary Key Integrity Protocol) – протокол впровадження тимчасових ключів;
HSPA, HSPA+ – (High Speed Packet data Access) – стандарти мобільного зв'язку 3-го покоління;
IMT2020/5G – (International Mobile Telecommunications-2020) — технологія мобільного зв'язку 5-го покоління;
LoRaWAN – (Low Range Wide-area Network) — технологія побудови енергоефективних мереж широкого радіусу дії;
AES – (Advanced Encryption Standard) — симетричний алгоритм блочного шифрування;
EAP – (Extensible Authentication Protocol) — фреймворк аутентифікації, що застосовується у безпровідних мережах і з'єднаннях типу «точка-точка»;
WLC – (Wireless LAN Controller) — контролер бездротової локальної мережі;
LEAP – (Lightweight EAP) – модернізована версія фреймворку аутентифікації, що застосовується у безпровідних мережах і з'єднаннях типу «точка-точка»;
EAP-FAST – (EAP Flexible Authentication by Secure Tunneling) – високонадійна версія протоколу аутентифікації, що застосовується у безпровідних мережах і з'єднаннях типу «точка-точка»;
PAC – (Protected Access Credentials) – захищены облікові дані доступу;
TLS – (Transport Layer Security) – безпечний протокол передавання даних;

PEAP – (Protected Extensible Authentication Protocol) – удосконалена версія протоклу EAP;

MSCHAP – (Microsoft Challenge Handshake Authentication Protocol) – протокол перевірки автентичності з’єднання між клієнтом і сервером;

GTC – (Generic Token) – апаратний пристрій, що генерує одноразові користувацькі паролі;

EAP-TLS – (EAP Transport Layer Security) – захищений реліз протоколу EAP;

PKI – (Public Key Infrastructure) – набір засобів, розподілених служб та компонент, що у сукупності використовуються для рішення криптозадач на базі відкритого та приватного ключів;

WPS – (Wi-Fi Protected Setup) – технологія напівавтоматичного створення мережі Wi-Fi;

CCMP – (Counter Mode with Cipher Block Chaining Message Authentication Code Protocol) - протокол шифрування 802.11i, створений на заміну TKIP.

# ВСТУП

Однією з характерних рис великої кількості сучасних інформаційних систем є присутність сегментів бездротового зв'язку у їх структурі. При цьому, переважна більшість таких сегментів мають спільні риси, такі, як:

- безпровідний сегмент, частіше за все, використовується для забезпечення доступу до Всесвітньої мережі мобільних клієнтів (планшетів, мобільних телефонів, ноутбуків), що належать співробітникам та клієнтім компанії, або відвідувачам;
- технологією побудови безпровідного сегменту є WiFi;
- безпровідна точка доступу, на базі якої мобільні клієнти отримують доступ до мережі, нерідко позиціонується як звичайний кінцевий пристрій, подібний ПК та іншій периферійній інфраструктурі;
- зона покриття, де забезпечується стійкий прийом сигналу WiFi, нерідко перевищує площу, яку займають приміщення компанії-власника мережі, що має безпровідні розширення.

Таким чином, складаються умови для виникнення потенційних ризиків захищеності мережевої інфраструктури, як наслідок того, що [1, 2]:

- усередині приміщень, де розгорнуто інформаційну мережу підприємства, розгорнуто WiFi-модулі внутрішнього (для службових потреб, захищено паролем) та зовнішнього контурів (для сторонніх осіб, пароль відсутній або є загальноновідомим); при цьому, зона стійкого покриття WiFi-модулів внутрішнього контуру може фіксуватися ззовні контрольованих приміщень;
- алгоритми криптографічного захисту, що використовуються для шифрування WiFi-каналу, як свідчить ряд досліджень, не гарантують високий рівень стійкості;
- комутаційне обладнання, що має WiFi-розширення, нерідко не ізолюється у окремий логічний сегмент, що оснащується додатковими засобами захисту від несанкціонованого доступу.

Отже, беручи до уваги усе вище сказане, можна зазначити, що на сьогодні сегменти мережі, що побудовані на базі стандарту WiFi, є потенційно небезпечними для мережевої інфраструктури у цілому [2].

Відтак, для збільшення рівня захищеності інформаційних мереж від зловмисних впливів, що базуються на використанні уразливостей безпровідних мереж, необхідно, щонайменше:

- виявити фактори, що спричинюють виникнення інформаційних ризиків;

- розробити рекомендації, що сприяють усуненню інформаційних ризиків у безпровідних мережах.

Таким чином, дослідження аспектів безпеки безпровідних сегментів мереж на сьогодні є актуальним.

# 1. СПЕЦИФІКА ВИКОРИСТАННЯ БЕЗПРОВІДНИХ МЕРЕЖ ДОСТУПУ

Головні завдання, що вирішують безпровідні мережі доступу сьогодні – це [3]:

- забезпечення бездротової комунікації безпосередньо між окремими пристроями того, щоб забезпечити обмін поточними даними та/або даними управління;
- надання доступу мобільним терміналам до ресурсів Всесвітньої мережі;
- підключення мобільних автоматизованих робочих місць до інфраструктури локальної мережі підприємства - у тому числі формуючи мобільний сегмент пристроїв LAN.

У будь-якому випадку з перелічених, на теперішній час, беручи до уваги поточний стан розвитку мереж, для рішення означених завдань найчастіше застосовується певний перелік безпровідних технологій, які буде розглянуто далі.

## 1.1 Ключові технології забезпечення безпровідного доступу до мережі

Синхронно до зростання кількості абонентських терміналів у глобальному масштабі, збільшення пропускної здатності каналів мереж, розвитку мережевих сервісів та поступового впровадження ряду новітніх технологічних концепцій, зокрема, концепцій Smart City, Safe City, UHD та IoE, суттєвим ином збільшується загальний обсяг кінцевих пристроїв, які можуть отримувати доступ до Всесвітньої мережі каналами безпровідних мереж доступу [4].

Такі пристрої, зазвичай, належать до однієї з наступних категорій, а саме:

- мобільні клієнтські АРМ (ноутбуки, планшети);
- мобільні телефони;
- безпровідні платіжні термінали;
- пристрої IoT (датчики, сенсори, пристрої фото- та відео фіксації, роботизовані вузли та агрегати тощо) [5].

При цьому, частіше за все, комунікації зазначених вище пристроїв з Всесвітньою мережею здійснюються на базі ряду поширених технологій, які за спрямованістю умовно можна розподілити на ряд категорій, наприклад, такі, як [6-9]:

1. WiMax, LTE, LTE-A, HSPA, HSPA+, UMTS – для мобільних телефонів, планшетів та деяких категорій пристроїв IoE.
2. WiFi – для ноутбуків, планшетів , та деякого сегменту платіжних терміналів.
3. LoRaWAN – для сенсорів, датчиків та модулів роботизованих систем.
4. IMT2020/5G та подібні.

Тут технології першої з зазначених категорій, що належать до поколінь 3G, 4G та 4,5G, характеризуються значними сумарними площами покриття [8, 9]. Стійкий прийом у мережах, побудованих на базі даних технологій, може забезпечуватися навіть за умови віддалення клієнта на відстань від кількох сотень метрів, або кількох кілометрів (в умовах міста) до десятків кілометрів (відкрита територія, за умови відсутності забудови та суттєвих перепадів висот).

Разом з тим, для них є характерною значна різниця потенційно можливих та реальних швидкостей передавання даних.

Це, у свою чергу, є наслідком [8]:

- специфіки розповсюдження радіосигналу в умовах складного ландшафту та в умовах суцільної забудови;
- охоплення одним антенним комплектом значної території;
- територіально нерівномірного та не прогнозованого у часі розподілу навантаження.

При цьому, мережі WiFi, порівняно з мережами, утвореними на базі технологій, розглянутих вище, характеризуються меншими масштабами покриття, що забезпечуються одним антенним комплектом [3].

Залежно від стандарту WiFi, допустимим є віддалення безпровідного клієнтського пристрою на відстань, що не перевищує 30-100 метрів від точки доступу.

З зазначених причин, а також завдяки апріорі вищим швидкостям передачі даних навіть у найбільш ранніх стандартах (до 54 Мбіт/с для 802.11a та до 11 Мбіт/с для випадку 802.11b), випадки мережевих колапсів тут зустрічаються набагато рідше.

Говорячи ж про технології 5 покоління – наприклад, IMT2020/5G та подібні, слід зазначити, що сьогодні більшість з них знаходяться на стадії «реалізованої концепції» [9].

Так, зокрема, для IMT2020/5G існує широка лінійка стандартизованих сумісних пристроїв. Проте мережі IMT2020/5G сьогодні утілено на обмежених територіях, де проводиться тестування їх особливостей.

Однак, не дивлячись на це, мережі як IMT2020/5G, так і будь-яких інших стандартів п’ятого покоління (5G), мають ряд суттєвих переваг, що у перспективі спричинить їх глобальне використання.

Це, зокрема:

- високі швидкості обміну даними (до 1 Гб/сек у режимі uplink та до 10 Гб/сек у режимі downlink для клієнта);
- висока абонентська ємність (підтримується порядку до $10^6$ з’єднань на 1 км$^2$);
- значно краща, порівняно з 4,5G та 4G, енергоефективність пристроїв.

У свою чергу, LoRaWAN являє собою енергоефективна технологія, з використанням якої забезпечується взаємозв’язок між модулями, пристроями та системами, що належать до мереж IIoT (Industrial Internet of Things) [5].

У мережі LoRaWAN радіус покриття може сягати від 1 до 15 км. При цьому, забезпечується швидкість обміну даними на рівні від 0,3 до 50 кбіт/с, що є достатнім для збору телеметричної інформації та передавання команд управління.

На сьогодні, у силу існуючої специфіки технології, її використання у суто «побутовому» форматі майже повністю відсутнє.

Виключенням є окремі системи дистанційного збору даних з побутових лічильників.

У підсумку, зазначимо, що основна маса даних, які передаються сьогодні безпровідними каналами, відноситься до мереж, реалізованих на базі 3G, 4G, 4,5G та WiFi.

## 1.2 Особливості динаміки зміни обсягів трафіку у безпровідних мережах

Обсяг даних, що передавалися мережами доступу першого (gprs) та другого (edge) поколінь, які надавалися операторами мобільного зв’язку, на

початку 2000-х років у цілому складав не більш, ніж приблизно 5 відсотків з усього загальносвітового трафіку, як наслідок низьких швидкостей обміну даними.

Одночасно з цим, за даними різних джерел [4, 10], загальна відсоткова частка WiFi-трафіку також не перевищувала зазначеного показника. Причиною цьому є незначна розповсюдженість терміналів, що мали підтримку WiFi.

Отже, на період 2000-2003 років, загальносвітова статистика розподілу трафіку провідних мереж та мереж безпровідного доступу була такою, як показано рис. 1.1.

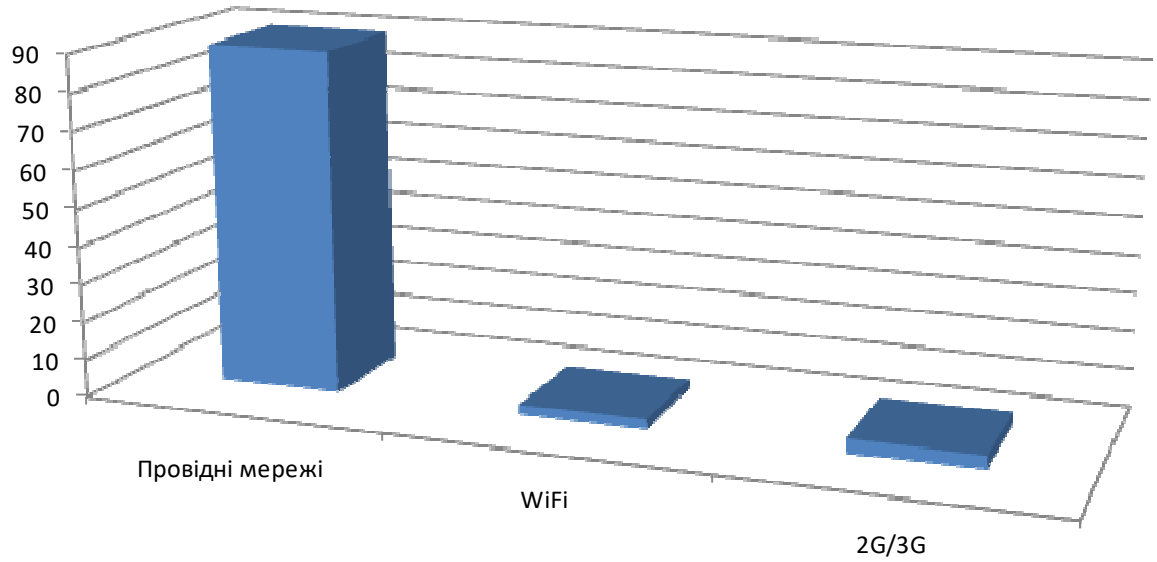


Рисунок 1.1 – Відсоткові частки трафіку мереж WiFi, 2G/3G та мереж провідного сегменту (2000-2003 роки)

Протягом кількох наступних років величина відсоткової частка WiFi-трафіку дещо зросла, але таке зростання не мало гостро вираженого характеру.

Зокрема, необхідно зазначити, що застосовуваність пристроїв стандарту 802.11a у цілому суттєво обмежувалась чутливістю каналу до перешкод, як наслідок обраного способу кодування сигналу на роботи у діапазоні 5 ГГц.

У свою чергу, впровадження стандарту 802.11b, що був спрямований виправити недоліки попереднього 802.11a, кардинальним чином не вплинуло

на зростання трафіку WiFi-мереж на тлі повільного зростання кількості терміналів.

У даному разі така закономірність пояснювалася [3]:

- несумісністю пристроїв 802.11a та 802.11b;
- зниженням реальних показників бітової швидкості у стандарті 802.11b. Так, пікова швидкість за відсутності стороннього навантаження, завад та перешкод не перевищувала 5 Мбіт/с при 11 Мбіт/с канальної швидкості.

При цьому, слід розуміти, що реальна стабільна швидкість, що має місце у звичайних умовах була суттєво нижчою та сягала позначки у 1 – 1,5 Мбіт/с.

Разом з тим, з впровадженням та розповсюдженням мереж на базі технологій 3G, відсоток трафіку мобільних мереж доступу суттєвим чином зріс.

Зокрема, за станом на 2015 рік, використання технологій мобільного доступу дозволяло передавати не менш, ніж 60% безпровідного трафіку у загальносвітовому масштабі [8] (рис. 1.2).

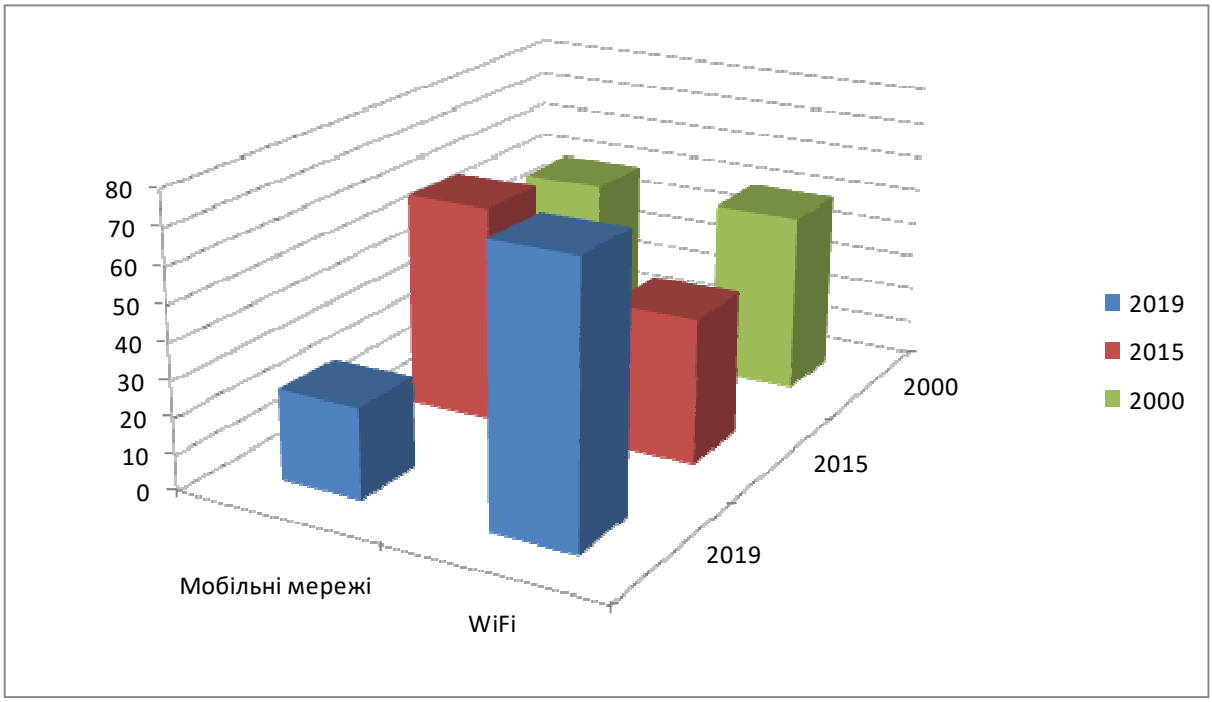


Рисунок 1.2 – Динаміка зміни обсягів трафіку у безпровідних мережах

Водночас, розповсюдження безпровідних пристроїв з підтримкою стандартів 802.11n (55-220 Мбіт/с залежно від кількості антен), 802.11ac (близько 200 Мбіт/с для однієї антени) змінило розподіл трафіку на користь WiFi.

При цьому, одним з найважливіших чинників тут можна вважати не лише покращені швидкісні показники стандартів, але також сумісність пристроїв та зменшену чутливість каналів до екрануючого впливу різного роду перешкод.

Так, за даними дослідження фахівців Juniper Research [10], з початку 2019 року та до сьогоднішнього часу відсоткова частка WiFi- трафіку знаходиться на рівні, що є не нижчий, ніж 75% від загального обсягу безпровідного трафіку.

У свою чергу, на період 2021-2022 років існуюче відношення сумарного трафіку мобільних мереж до трафіку WiFi, у сутності, не зазнало суттєвих змін.

Це зумовлюється тим, що:

- з одного боку, мало місце впровадження мереж 4G та 4,5G та ріст обсягу їх клієнтів;
- з іншого боку, розроблено та поширено стандарт 802.11ax, що дозволяє досягти реальних швидкостей порядку 1 Гбіт/с на одну антену точки доступу.

Окрім цього, сьогоднішній широкій розповсюдженості WiFi-мереж сприяли такі фактори, як [8]:

- дешевизна обладнання; так, вартість безпровідної точки доступу у середньому на 2-3 порядки є меншою у ціні порівняно з обладнанням мобільних мереж;
- легкість реалізації процедур розгортання та налаштування безпровідних сегментів;
- відсутність у багатьох країнах обов’язкової сертифікації обладнання WiFi (яке може виконувати роль точки доступу), що створює сегменти радіусом 100 м.

Слід також додати, що на сьогодні розповсюдженню мереж сімейства стандартів 802.11 додатково сприяє те, що:

- майже усі моделі клієнтських терміналів (планшети, ноутбуки, мобільні телефони та стаціонарні ПК) комплектуються WiFi-модулями за замовчуванням;

- більшість виробників ноутбуків сьогодні фактично взагалі відмовляються від стандартних RJ-45 інтерфейсів для зменшення підсумкових габаритів пристрою (натомість може використовуватися з'єднувач USB/RJ-45);
- WiFi-модулями оснащується побутова техніка як для розширення можливостей керування, так і для можливості інтеграції пристроїв у структуру IoT.

Ще одним фактором розповсюдженості WiFi-мереж є низький рівень потужності випромінювання передавача точки доступу, а також використання їх як:

- маркетингового ходу з боку закладів громадського харчування, торгівельних центрів тощо;
- засобу забезпечення відносно дешевим та стабільним зв'язком співробітників, клієнтів та відвідувачів – з боку підприємств та закладів різного профілю.

Тобто, фактичнв поширеність WiFi-мереж на сьогодні є надзвичайно високою.

Врешті решт, ще одним беззаперечний фактором впливу є сучасні показники продуктивності даних мереж, як показано таблицею 1.1 [].

При цьому, слід обов'язково також брати до уваги, що, як наслідок принципів побудови WiFi-взаємодії, існує суттєва розбідність між показниками канальних та реальних показників швидкостей, що у більшій чи у меншій мірі однаково є справедливим для кожного стандарту сімейства 802.11.

Разом з тим, приблизна кількість точок доступу у світі складає близько $10{,}5 \times 10^6$ одиниць.

При цьому, сумарний трафік при цьому складає порядку $115 \times 10^{18}$ байт на місяць.

Таким чином, з огляду на все вищезазначене, найбільш доцільно далі вести дослідження особливостей побудови та аспектів безпеки мереж саме WiFi.

Таблиця 1.1 – Ключові параметри стандартів WiFi

| | 802.11 | 802.11b | 802.11a | 802.11g | 802.11n | 802.11ac | 802.11ax |
|---|---|---|---|---|---|---|---|
| Рік | 1997 | 1999 | 1999 | 2003 | 2009 | 2014 | 2017-2019 |
| Частота | 2,4 GHz | 2,4 GHz | 5 GHz | 2,4 GHz | 2,4 GHz/ 5 GHz | 5 GHz | 2,4 GHz/ 5 GHz |
| Частотні канали | 20 MHz | 20 MHz | 20 MHz | 20 MHz | 20/40 MHz | 20/40/80/160 MHz | 20/40/80/160 MHz |
| Пікова канальна швидкість | 2 Мбіт/с | 11 Мбіт/с | 108 Мбіт/с | 54 Мбіт/с | 150-600 Мбіт/с | 0,433-6,77 Гбіт/с | 0,433-10 Гбіт/с |
| Пікова реальна швидкість | Близько 1 Мбіт/с | 5 Мбіт/с | 40 Мбіт/с | 24 Мбіт/с | 220 Мбіт/с | понад 200 Мбіт/с | понад 400 Мбіт/с |
| Модуляція | DSSS, FHSS | DSSS, CCK | OFDM | OFDM | OFDM | OFDM | OFDM, OFDMA |
| Тип кодування | DQPSK | CCK | 64-QAM, 3/4 | 64-QAM, 3/4 | 64-QAM, 5/6 | 256-QAM, 5/6 | 1024-QAM, 5/6 |
| Макс. кількість тонів OFDM | - | - | 64 | 64 | 128 | 512 | 2048 |
| Рознесення субтонів | - | - | 312,5 КГц | 312,5 КГц | 312,5 КГц | 312,5 КГц | 78,125 КГц |

## 1.3 Типова схема побудови безпровідного сегменту WiFi мережі

Частіше за все зв'язок кінцевого пристрою – безпровідного терміналу з об’єктом інформаційної взаємодії реалізується за однією зі схем, що зображені на рис. 1.3 та 1.4 [6, 11].

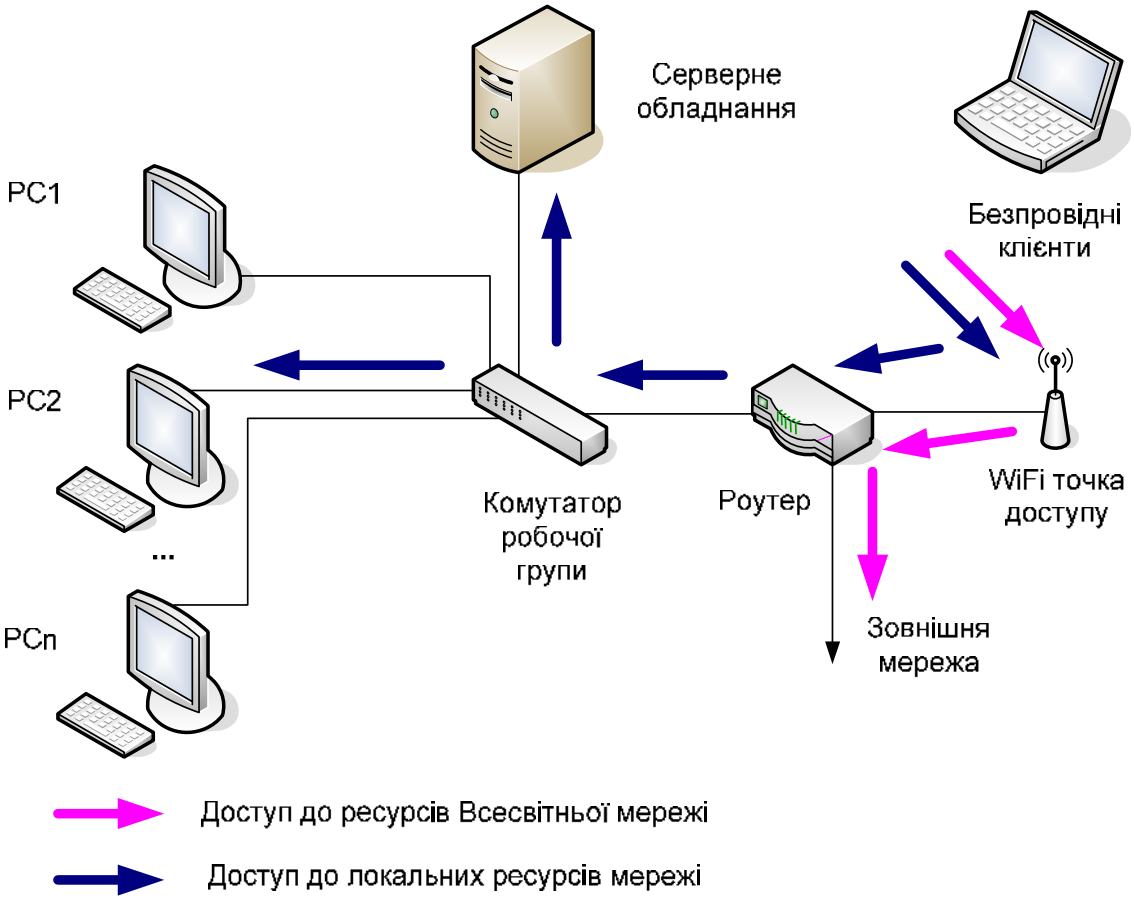


Рисунок 1.3 – Схематичне зображення можливих сценаріїв доступу до ресурсів каналами WiFi у межах типової мережі

У загальному випадку, мобільний клієнт користується мобільною точкою доступу у якості транзитного пристрою для входу до ресурсів всесвітньої мережі.

При цьому, маршрутизатор (що реалізує роль і бездротової точки доступу також) чітко розмежовує внутрішній трафік та трафік мобільних клієнтів.

Зазвичай такий сценарій реалізується у випадку, коли безпровідний сегмент налаштовується для надання доступу до мережі Інтернет у публічних місцях.

Ризики, які існують у даному випадку, пов’язані з наступними загрозами [11, 12]:

- можливістю перехоплення зловмисником трафіку WiFi-каналу після підбору пароля;
- можливістю доступу зловмисника до внутрішніх мережевих ресурсів.

У другому випадку зазначені ризики може бути нівельовано за рахунок ізоляції точки доступу в окремий сегмент, додатково відмежований від іншої мережі екраном (рис. 1.4).

Разом з тим, у випадку, коли хоча б деяка частина внутрішніх клієнтів мережі поєднується у WiFi- сегмент, тоді зловмисник, теоретично, отримавши пароль точки доступу може, окрім перехоплення та розшифрування трафіку, щонайменше мати доступ до відкритих ресурсів таких клієнтів.

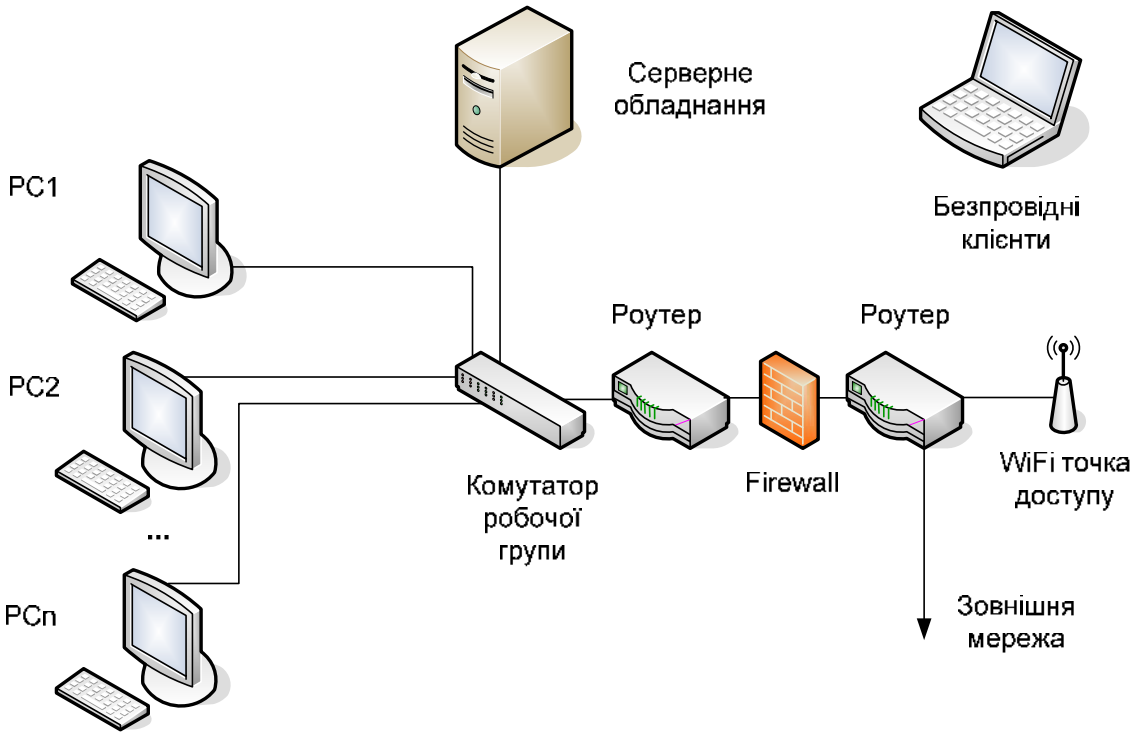


Рисунок 1.4 – Виокремлення точки доступу в ізольований сегмент мережі

Звідси виходить, що  зазначених умовах найвищі ризики безпеки мереж WiFi зумовлені можливістю зламу паролю.

Далі виконаємо аналіз таких ризиків, дослідивши принципи та механізми захисту мереж WiFi.

# 2. ІНСТРУМЕНТИ ТА МЕХАНІЗМИ ЗАХИСТУ МЕРЕЖ WIFI

## 2.1 Базові принципи захисту мереж та сегментів WiFi

Незалежно від того, на базі якого саме стандарту функціонує та чи інша мережа WiFi, питання її безпеки регулюються та наступних технологічних рівнях, а саме [12-16]:

- рівень аутентифікації;
- рівень шифрування даних.

Для того, щоб оцінити фактичний рівень захищеності мереж WiFi, спочатку необхідно виконати огляд інструментарію та механізмів, що містить кожен з зазначених рівнів.

## 2.2 Рівень шифрування даних WiFi

У рамках стандарту 802.11 передбачено ряд протоколів безпеки, що мають у своєму складі алгоритми шифрування, серед яких такі протоколи, як [12]:

- WEP (Wired Equivalent Privacy - секретність, еквівалентна провідним мережам);
- WPA;
- WPA2.

### 2.2.1 Шифрування на базі криптографічних механізмів у складі алгоритму WEP

Процес шифрування з використанням WEP передбачає створення потокового шифру, в основі якого знаходиться криптографічний алгоритм RC4 [12, 15].

У свою чергу, потоковий шифр, який генерує RC4, складається за модулем 2 з вихідними відкритими даними. Результатом цього є шифрограма вихідного повідомлення.

Вибір RC4 зумовлено, по перше, простотою реалізації а по-друге - його високою швидкістю.

В його основі – генератор гамми (псевдовипадкової послідовності) та суматор за модулем 2.

Сам процес шифрування WEP ілюструється схемою, зображеною на рис.2.1, та включає у себе такі технологічні етапи:

1. Обчислення хешу з фрейму вихідних даних на базі алгоритму CRC-32. У результаті отримується величина ICV (Integrity Check Value), що дозволяє контролювати цілісність вихідної інформації.

2. «Змішування» ключа а також вектору ініціалізації (IV) з використанням алгоритму RC4 для отримання ключового потоку.

Тут вектор ініціалізації являє собою 24-розрядне число, яке доповнює ключ для того, щоб гарантувати зміну ключового потоку. У свою чергу, використовуються ключі довжиною від 40 до 104 біт.

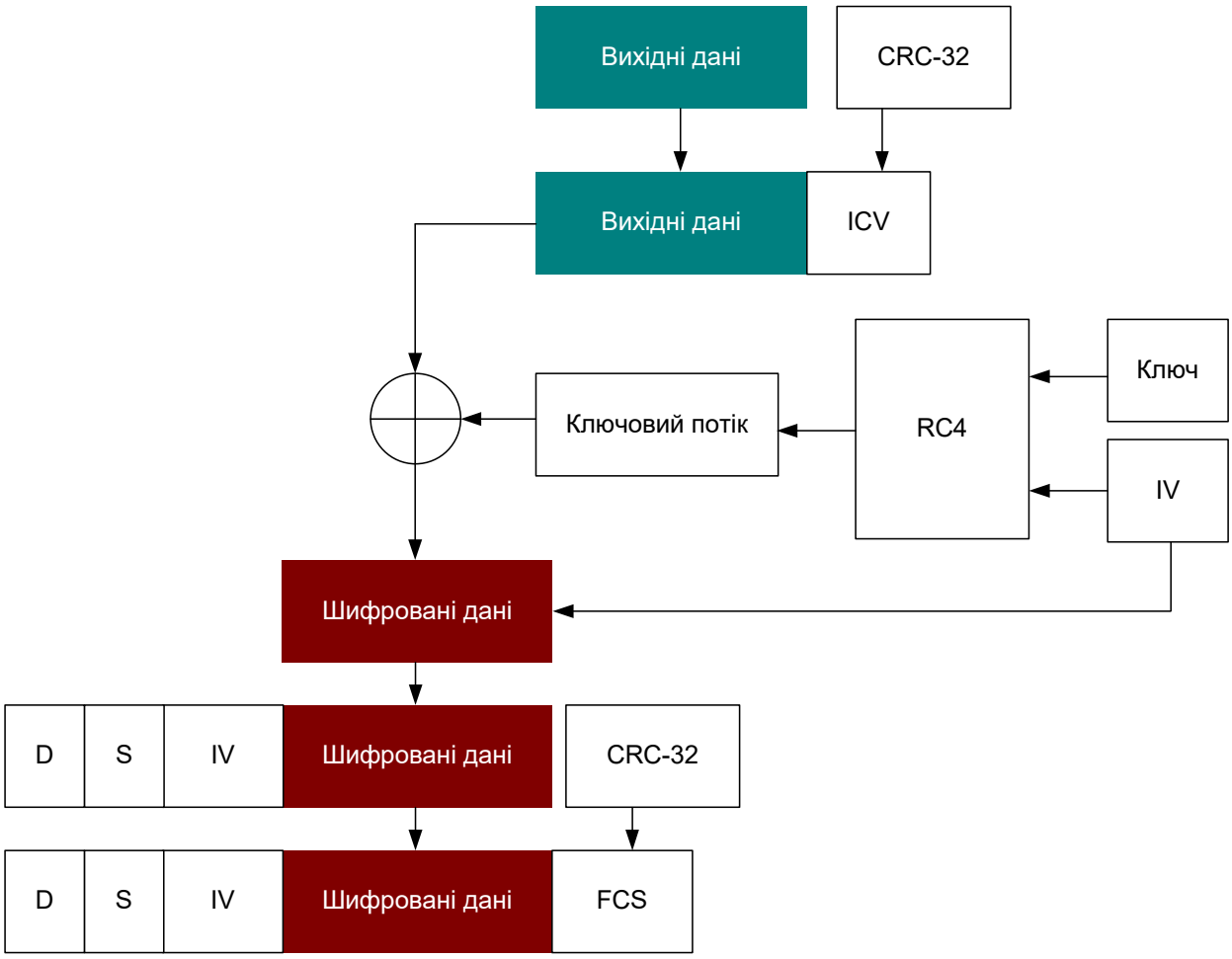


Рисунок 2.1 – Схема реалізації процесу WEP-шифрування

При цьому, якщо введений ключ залишається незмінним, то вектор ініціалізації має змінюватися для кожного фрейму. Завдяки цьому може бути уникнено ситуації, когда одинакові дані з однаковим ключем завжди формуватимуть один и той же ключовой потік, що суттєво знижує захищеність шифру [11].

3. Складання за модулем 2 сегменту даних, утвореного вихідним фреймом разом зі значенням ICV, з ключовим потоком. У результаті отримується шифрованний сегмент інформації.

4. Приєднання до шифрованого сегменту вектора IV у відкритому вигляді.

5. Додавання до утвореної послідовності MAC-адрес джерела (S) та призначення (D).

6. Обробка послідовності, утвореної на етапі 5 з використанням алгоритму CRC-32 для отримання FCS (Frame Check Sequence) — контрольної суми фрейму. Отримана величина записується у поле FCS.

На момент розробки, алгоритм забезпечував прийнятну стійкість.

Разом з тим, на сьогодні WEP, хоча і підтримається за замовчуванням майже усіма пристроями 802.11, вважається застарілим.

До недоліків WEP можна віднести як його власні, так і такі, що зумовлені недосконалістю RC4, а саме:

- невелика довжина ключа (WEP);
- використання гамм, які не є глобально унікальними, як наслідок недосконалого механізму їх генерування (RC4);
- корельованість першого байту ключового потоку з першими трьома байтами ключа (RC4);
- архітектура алгоритму є нестійкою до атаки на базі статистичного аналізу в умовах сучасних обчислювальних потужностей (WEP).

У цілому, головна ідея WEP базується на тому, що підбір паролю в умовах постійної зміни ключового потоку є завданням підвищеної складності.

Разом з тим, в умовах, коли зловмисник має можливість захоплення пакетів, та має у розпорядженні суттєві обчислювальні ресурси, стандартизована 24-розрядна довжина IV є недостатньою для забезпечення стійкості.

У таких умовах під час збору фреймів можна зібрати множину таких, для яких IV є однаковими.

Отже, незважаючи на складність ключа, розкриття шифрограми є можливим після виконання статистичного аналізу великої кількості перехоплених фреймів.

При цьому, час зламу шифрограми на базі WEP може складати від кількох десятків хвилин, до кількох хвилин залежно від зібраної статистики на наявних обчислювальних ресурсів.

Для усунення виявлених недоліків WEP згодом було розроблено сімейство стандартів WPA (Wi-Fi Protected Access).

### 2.2.2 Шифрування на базі криптографічних механізмів алгоритмів сімейства WPA

Одна з головних відмінностей алгоритмів WPA-архітектури від попереднього алгоритму WEP полягає у застосуванны протоколу TKIP (Temporary Key Integrity Protocol) – протокол впровадження тимчасових ключів [12, 13].

Протокол TKIP передбачає використання дворівневої системи векторів ініціалізації. При цьому, реалізація процесу створення ключа для формування ключового потоку виконується протягом двох фаз, як показано схемою на рис.2.2.

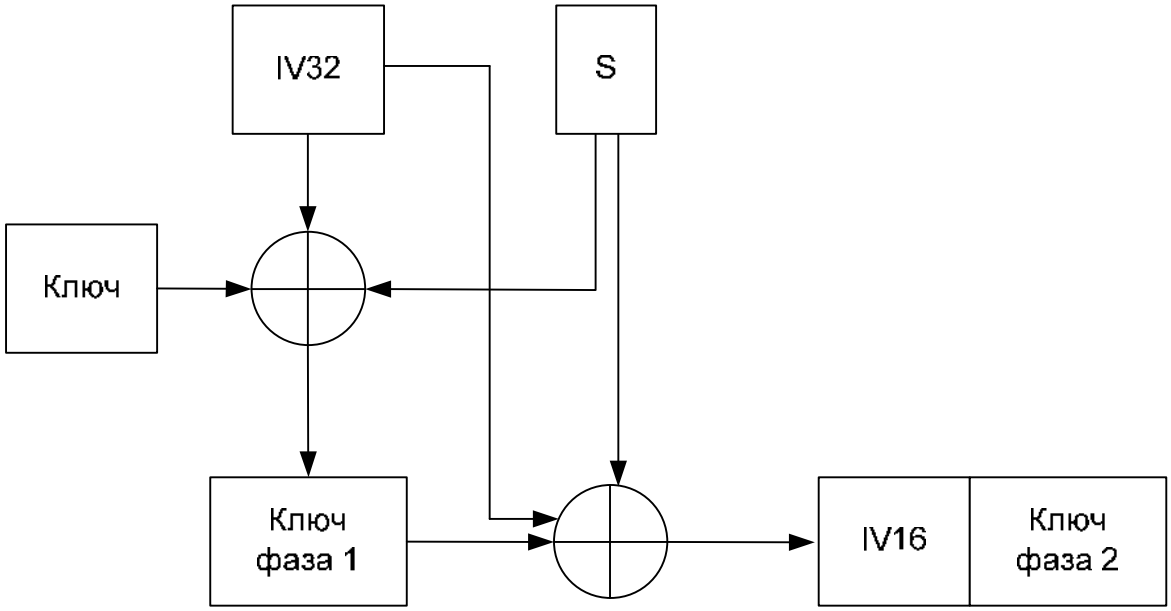


Рисунок 2.2 – Схема формування ключового потоку WPA

Процедура формування ключового потоку у даному випадку містить такі кроки, як:

1. Формування ключа перщої фази. Для цього виконується складання за модулем 2 вихідного ключа, старших 32 разрядів вектора ініціалізації (IV32) та MAC-адреси джерела (S).

2. Складання за модулем 2 ключа першої фази зі старшими 32 розрядами вектору (IV32) та MAC-адресою джерела (S).

Результатом є 128-розрядна послідовність, де перші 16 розрядів являють собою «молодший» вектор ініціалізації а інші 112 — т.з. пофреймовий ключ.

У свою чергу, саме пофреймовий ключ далі буде використано для формування ключового потоку.

Сутність такої схеми полягає у наступному.

У ході роботи алгоритму для кожного нового фрейму буде збільшуватися значення молодшого вектору ініціалізації.

Після того ж, як усі можливі комбінації вектору (яких не більш, ніж $2^{16}$, тобто, 65536) було використано, виконується збільшення старшого вектору ініціалізації після чого виконується процедура формування нового ключа, як було зазначено схемою на рис. 2.2.

Відтак, за рахунок виконання змін ключа обсяг статистичних даних, достатній для реалізації зламу шифру, не встигає сформуватися.

Слід зауважити, що потенційна результативність процесу зламу визначається, у перш чергу, обсягом зібраних фреймів і значно менш суттєво - наявною обчислювальною потужністю, що є першочергово важливим, наприклад, для атак методом підбору (brootforce).

У рамках WPA2 використовується CCMP (Counter Mode with Cipher Block Chaining Message Authentication Code Protocol), що являє собою протокол блочного шифрування з кодом аутентичності повідомлення (MAC) та режимом зчіплення блоків і лічильника, який було створено для заміни протоколу TKIP, що, у свою чергу, використовувався у рамках WPA та WEP та являв собою одну з ключових компонент їх безпеки.

На відміну від TKIP, протокол CCMP базується на використанні AES (Advanced Encryption Standard) – симметричного алгоритму блочного шифруваняя (размір блоку 128 біт, ключі довжиною 128, 192, та 256 біт відповідно) [7].

З огляду на використання AES, теоретично WPA2 може вважатися надійним протоколом.

Разом з тим, на сьогодні виявлено значну кількість уразливостей CCMP, що суттєвим зменшує захищеність протоколу. Зокрема, серед таких виявлених уразливостей одна з найбільш відомих – Hole196, яка, у свою чергу, відома ще з 2010 року [13].

## 2.3 Рівень аутентифікації WiFi

У загальному випадку, аутентифікація клієнта зазвичай включає у себе відправлення запиту, отримання відповіді, залежно від якої далі приймається рішення про надання доступу [6, 7].

Окрім того, додатково можливе використання процедури обміну ключами сесії, або ключами шифрування тощо.

У цілому, кожен метод аутентифікації може мати унікальні механізми та способи передачі між клієнтом і точкою доступу.

Зараз використовується велика кількість методів аутентифікації користувачів безпровідної мережі WiFi у ході підключення, як додатковий механізм безпеки. Такі методи впроваджувалися:

- як для різноманітних бездротових технологій, так і бездротового устаткування;
- синхронно до виявлення слабких місць у системі безпеки існуючого інструментарію.

Розглянемо далі найбільш поширені з них.

### 2.3.1 Відкрита аутентифікація

Стандартом 802.11 у його базисному варіанті використовується лише два варіанти аутентифікації клієнта, а саме [16]:

- Open Authentication;
- WEP-аутентифікація.

Тут Open Authentication передбачає відкритий доступ до WLAN.

При цьому, єдина вимога полягає у тому, що клієнт до того, як почати користування мережею стандарту 802.11, має відправити запит щодо аутентифікації для подальшого з’єднання з AP (точкою доступу). У цьому випадку яких-небудь даних з боку клієнту не вимагається.

У свою чергу, Open Authentication використовується у тих випадках, коли клієнт підтримує стандарт 802.11.

У цьому, власне, і полягає ідея Open Authentication - перевірити, що клієнт є допустимим пристроєм стандарту 802.11. При цьому, процедура аутентифікації особи користувача проводиться іншими передбаченими стандартом засобами безпеки.

Як правило, мережі, де використовується Open Authentication, можна зустріти, наприклад, у громадських місцях. У мережах зазначеного типу частіше за все виконання процедури аутентифікації здійснюєьбся через веб-інтерфейс.

У такому разі клієнт підключається до мережі негайно, однак, попередньо повинен відкрити веб-браузер для того, щоб прочитати та далі вже прийняти умови користування сервісом а також ввести основні облікові дані.

Після виконання зазначених операцій клієнт отримує доступ до мережі. Необхідно також зазначити, що майже усі операційні системи клієнтів у цьому разі видають попередження про те, що дані, які передаються через мережу, не будуть гарантовано захищені.

### 2.3.2 WEP-аутентифікація

Як зазначалося вище, WEP являє собою механізм безпеки, що використовує загальний ключ [13, 14].

Тобто, один і той самий ключ повинен бути як у відправника, так і одержувача. При цьому, такий ключ розміщується на бездротових пристроях заздалегідь.

У цілому, можна сказати, що WEP-ключ також застосовується не лише як безпосередньо механізм шифрування даних, але і як додатковий метод аутентифікації.

Тобто, у разі, якщо клієнт надсилатиме неправильний ключ WEP, йому не буде недано можливість здійснювати підключення до обраної точки доступу.

У свою чергу, точка доступу перевіряє знання клієнтом ключа WEP, надсилаючи йому випадкову фразу виклику.

Клієнт шифрує фразу виклику за допомогою WEP та повертає результат точці доступу.

Далі точка доступу порівнює шифрування клієнта зі своїми власними, щоб переконатися в ідентичності двох ключів WEP.

Раніше зазначалося, що довжина WEP-ключів знаходиться у діапазоні від 40 до 104 біт.

Очевидно, що ключі більшої довжини здатні забезпечити більш надійне шифрування.

Разом з тим, на сьогодні як шифрування WEP, так і аутентифікація з використанням загального ключа WEP є досить слабкими методами захисту мережі.

### 2.3.3 Аутентифікація 802.1x/EAP

За наявності тільки Open Authentication і WEP, доступних у стандарті 802.11, існувала необхідність у більш надійному методі аутентифікації [12].

При цьому, замість того, щоб вбудувати додаткові методи аутентифікації до вже існуючих у стандарті 802.11, була впроваджено більш гнучку та масштабовану структура аутентифікації, а саме - розроблено протокол аутентифікації (EAP - Extensible Authentication Protocol). Як видно з його назви, EAP є розширюваним і не обмежується єдиним методом аутентифікації.

Натомість EAP визначає набір спільних функцій, які застосовують конкретні методи аутентифікації користувачів.

Також особливістю EAP є можливість інтеграції зі стандартом керування доступом на основі портів стандарту IEEE 802.1X.

При цьому, коли порт стандарту 802.1X увімкнений, він обмежує доступ до мережного носія доти, доки клієнт не пройде процедуру аутентифікації. Це, у свою чергу означає, що бездротовий клієнт має змогу зв'язуватися з точкою доступу, але при цьому не зможе передавати дані в іншу частину мережі, доки процес аутентифікації не буде успішно завершено.

Зазначимо також, що якщо у випадках Open Authentication та WEP процедура аутентифікації бездротових клієнтів виконується локально на точці доступу, то у рамках стандарту 802.1X даний принцип не використовується.

Натомість, у даному випадку клієнт використовує відкриту аутентифікацію для організації зв'язку з точкою доступу, а після цього

фактичний аутентифікаційний процес реалізується на виділеному сервері аутентифікації.

Так, на рис. 2.3 показано тристоронню схему стандарту 802.1X.

У складі зазначеної схеми присутні такі об’єкти, як:

- клієнт, яким є будь-який пристрій WiFi, що надсилає запит на доступ;
- аутентифікатор, що являє собою мережевий пристрій, який забезпечує доступ до мережі (зазвичай це контролер бездротової локальної мережі (WLC));
- сервер аутентифікації (AS), що являє собою пристрій, який приймає облікові дані користувача і може або надавати, або забороняти доступ до мережі на основі бази даних користувачів та політик (зазвичай сервер RADIUS) [12, 15-17].

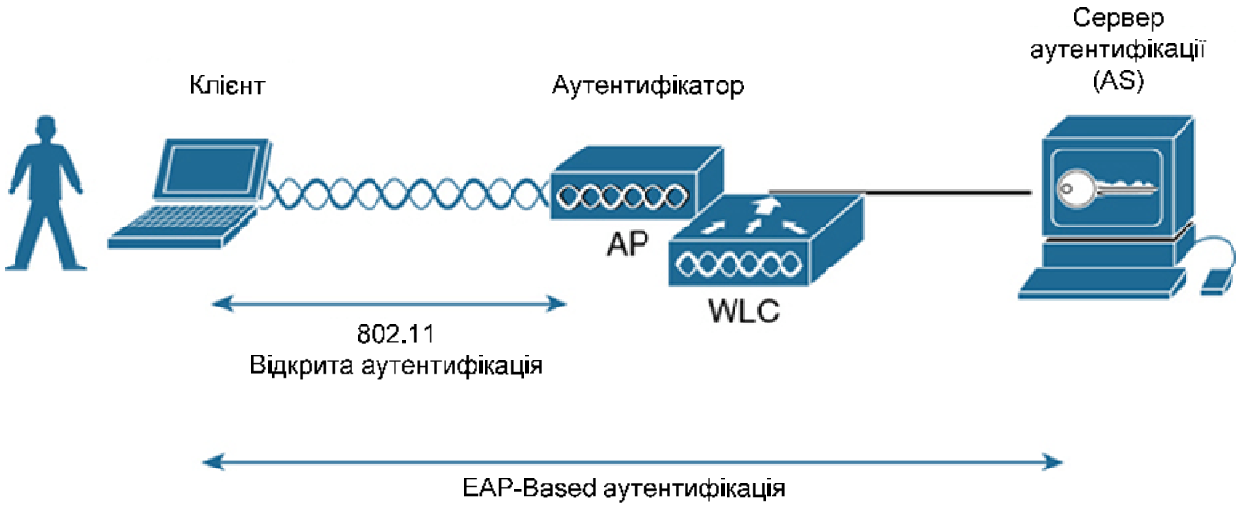


Рисунок 2.3 – Трьохстороння схема аутентифікації стандарту 802.1X

На рисунку 2.3 клієнт з’єднується з точкою доступу через безпровідний канал, тут AP є аутентифікатором.

При цьому, первинне підключення реалізується згідно зі стандартом Open Authentication 802.11.

У свою чергу, точка доступу з’єднана з WLC, який далі підключено до сервера аутентифікації (AS). Зазначена схема є базисом для виконання аутентифікації на основі EAP.

У даному випадку контролер бездротової локальної мережі є посередником у процесі аутентифікації клієнта, контролюючи доступ користувачів за допомогою стандарту 802.1X, взаємодіючи із сервером аутентифікації за допомогою платформи EAP.

На сьогодні протокол захисту EAP має ряд реалізацій. Розглянемо найбільш поширені з них.

LEAP

Даний метод безпровідної аутентифікації Lightweight EAP (LEAP), який свого часу було розроблено Cisco, дозволяє усунути ключові недоліки протоколу WEP [12].

Для аутентифікації клієнт повинен надати системі облікові дані користувача та пароля. Після цього, у процесі встановлення з'єднання, сервер аутентифікації і клієнт виконують процедуру обміу т.з. челендж-повідомленнями, які потім шифруються і повертаються. Це і забезпечує взаємну автентифікацію.

Аутентифікація між клієнтом та AS здійснюється лише за умови попередньо успішн виконаної процедури розшифрування челендж-повідомлень.

На сьогодні LEAP вважається застарілим протоколом а відтак - застосовується виключно у межах WEP-мереж. З причини недостатньої надійності механізмів шифрування челендж-повідомлень на теперішній момент є вразливим.

EAP-FAST

Ще однією реалізацією EAP, розробленою компанією Cisco, є EAP-FAST (Flexible Authentication by Secure Tunneling). Даний механізм, на відміну від попередньо розглянутих, у цілому вважається достатньо надійним [12, 17].

У рамках EAP-FAST передбачено захист облікових даних доступу (PAC), що передаються між AS і клієнтом, шляхом попереднього їх шифрування.

Тут PAC - це форма загального секрету, який генерується AS і використовується для взаємної аутентифікації.

Аутентифікація за методом EAP-FAST включає у себе ряд фаз, що виконуються послідовно:

- Фаза 0: PAC створюється або готується та встановлюється на клієнті;

- Фаза 1: після того, як клієнт та AS аутентифікували один одного, узгоджуються параметри безпечного тунеля транспортного рівня (TLS).
- Фаза 2: кінцевого користувача може бути аутентифіковано через TLS тунель для додаткової безпеки.

Слід звернути увагу на те, що у ході аутентифікації EAP-FAST мають місце два окремих процеси аутентифікації, а сакме:

- між AS і клієнтом;
- з кінцевим користувачем.

Зазначені процеси є вкладеними: зовнішня аутентифікація виконується поза тунелем TLS, тоді як внутрішня - усередині тунелю.

Цей метод, оскільки базується на засадах EAP, також потребує сервера RADIUS.

PEAP

Аналогічно до методу EAP-FAST, захищений метод EAP (PEAP) використовує внутрішню та зовнішню аутентифікацію, проте AS надає цифровий сертифікат для аутентифікації себе з клієнтом у зовнішній аутентифікації [12, 17].

Якщо клієнт успішно ідентифікується AS, далі між ним та AS створюється тунель TLS, який буде використовуватися для внутрішньої аутентифікації клієнта та обміну ключами шифрування.

У рамках PEAP використовується цифровий сертифікат AS, що складається з даних у стандартному форматі, які ідентифікують власника та "підписані", або підтверджені третьою стороною.

У даному випадку третя сторона - центр сертифікації (CA), яка є відомою, та користується довірою як з боку AS, так і з боку заявника.

Відтак, тут заявник також повинен мати сертифікат CA виключно тільки для того, щоб він міг перевірити той сертифікат, який він отримує від AS.

Окрім зазначеного, сертифікат також використовується для передачі ключа відкритого типу, який може бути використаний для розшифровування повідомлень AS.

Необхідно також зазначити про те, що лише AS має сертифікат PEAP. Це, у свою чергу, означає, що клієнт може легко підтвердити справжність AS.

При цьому, клієнт не має, або не використовує свій власний сертифікат, тому він повинен бути аутентифікованим у тунелі TLS за допомогою одного з наступних двох методів:

- MSCHAPv2;
- GTC (універсальна маркерна карта): апаратний пристрій, який генерує одноразові паролі для користувача, або вручну згенерований пароль.

EAP-TLS

EAP-TLS, як ще одна реалізація протоколу EAP, базується на використанні цифрового сертифікату на AS як надійний метод для аутентифікації сервера RADIUS.

При цьому, отримати та встановити сертифікат на одному сервері нескладно, але, водночас, клієнтам залишається ідентифікувати себе іншими способами.

У свою чергу, безпека транспортного рівня EAP (EAP-TLS) додатково посилює захист, вимагаючи сертифікати на AS на кожному клієнтському пристрої.

За допомогою EAP-TLS виконується обмін сертифікатами між AS та клієнтом, що, таким чином, надає можливість їм аутентифікувати один одного.

Далі, після виконання взаємної аутентифікації, будується TLS-тунель, який, у свою чергу. надає змогу безпечного обміну матеріалами ключа шифрування.

На сьогодні EAP-TLS вважається найбільш безпечним методом бездротової аутентифікації, проте, у ході його реалізації виникають певні складнощі.

Так, так само, як і AS, кожен бездротовий клієнт повинен отримати та встановити сертифікат.

Разом з тим, цілком очевидно, що реалізація процедури встановлення сертифікатів вручну на сотні чи тисячі клієнтів є досить складною проблемою.

Тому можливою альтернативою у цьому разі є впровадження інфраструктури відкритих ключів (PKI).

У свою чергу, PKI здатна безпечно та ефективно надавати сертифікати та відкликати їх, коли клієнт або користувач більше не матиме доступу до мережі.

Водночас, впровадження PKI, зазвичай, потребує створення власного центру сертифікації, або, щонайменше - побудови довірчих відносин зі стороннім центром сертифікації, який може надавати сертифікати клієнтам.

# 3. МЕТОДИ ТА ЗАСОБИ ЗЛАМУ БЕЗПРОВІДНИХ КАНАЛІВ WIFI

## 3.1 Поширені методи реалізації зламу WiFi-мереж

У цілому, якщо узагальнити досвід успішних атак на WiFi – з'єднань, можемо виокремити ряд типових методів їх реалізації а саме [1, 12, 14]:

- ручний підбір пароля;
- підбір пароля засобами brootforce;
- підбір WPS-коду;
- фішинг;
- використання баз паролів;
- перехоплення «рукостискань» (handshake) з наступним розшифруванням.

Виконаємо огляд найбільш поширених методів серед зазначених для того, щоб обрати з них найбільш продуктивний для успішного зламу мережі WiFi.

### 3.1.1 Метод підбору WPS-коду

Можливість реалізації зазначеного методу зумовлена тим, що ряд роутерів/точок доступу дозволяють у спрощеному режимі налагодити канал на базі WPS [11].

При цьому, для під'єднання до таких мереж потрібно лише ввести ПІН-код, який характеризується такими параметрами:

- є обмеженим до 8 символів;
- формується виключно з цифр.

Таким чином, у цьому разі може бути реалізовано повний перебір ключів WEP за досить стислий термін.

Окрім цього, у ході дослідження можливостей зламу WEP було знайдено кореляцію,що дає змогу виконувати процес підбору попарно. Так, спочатку підбираються перші 4 цифры а далі - інші 4 цифры.

Зрозуміло, що за таких умов процес повного перебору суттєво прискорюється.

У даному випадку точку доступу при відкритому WPS гарантовано може бути зламано протягом декількох годин.

Існує також інший варіант реалізації атаки даного типу, а саме – застосування кодів за замовчуванням. Тут мається на увазі ключі, які виробник пристроїв розміщує на задній панелі пристрою.

При цьому, велика кількість пристроїв має однаковий встановлений ПІН-код.

З іншого боку, створено велику кількість програмних засобів, що мають у собі бази таких ПІН-кодів. Отже. Процес зламу WiFi-мережі може суттєво спрощуватися.

### 3.1.2 Метод фішингу

Використання фішингу для зламу пароля WiFi може бути реалізовано за рядом сценаріїв. Найбільш широкого застосування набули такі з них, як [6]:

1. Нова точка доступу.

У даному разі зловмисник створює нову точку доступу з іменем, аналогічним імені точки, що атакується. За умови фізичного розміщення нової точки на незначному віддаленні від вже існуючої, рівень сигналу для користувачів буде достатньо високим.

Даний фактор, та також знайоме ім’я точки доступу, врешті решт приведуть до того, хоча б один користувач буде робити спроби під’єднатися до неї, попередньо вводячи пароль «справжньої» точки доступу, який і буде зчитано зловмисником.

Метод можна вважати відносно ефективним, проте його ефективність не є гарантованою – процес отримання паролю може тривати досить довгий час.

2. Спливаючі вікна

У рамках реалізації даного методу користувачеві у браузер вивантажуються вікна, які пропонують виконати термінове оновлення браузеру, для чого потрібно ввести пароль Wi-Fi, як це показано на рисунку 3.1.

Даний метод є суттєво менш продуктивним, порівняно з попередньо розглянутим, що є наслідками:

- зростання рівня обізнаності користувачів з базових питань інформаційної безпеки;
- технічної складності реалізації методу.

3. Використання спеціалізованих програмних засобів.

Розглянемо приклад реалізації даного методу на прикладі застосування утиліти Wifiphisher.

Метод є автоматизованою версією нової точки доступу.

Порядок дій при цьому є наступним:

- обирається точка доступу для атаки, її налаштування, такі, як назва, канал і т.д., копіюються.
- створюється клон «Злий Двійник» точки, що атакується. Зовні спостерігається повна її подібність з оригінальною за винятком того, що під'єднання до неї є можливим без паролю;
- використовується примусова деаутентифікація користувачів, що фактично є відлученням від оригінальної точки доступу.
- здійснюється безперервне пригнічення радіоканалу оригінальної точки (потрібен додатковий WiFi-адаптер);
- після підключення користувача до «Злого Двійника», його тим чи іншим способом спонукається до введення паролю WiFi (наприклад, для оновлення прошивки);
- одержаний таким чином пароль стає доступним зловмиснику.

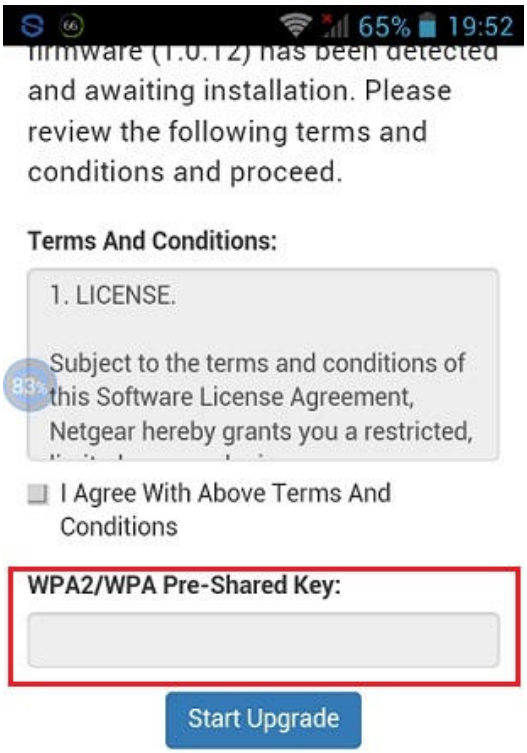


Рисунок 3.1 – Приклад сторінки з запитом на ввід паролю для оновлення браузеру

Метод відзначається легкістю реалізації та не вимагає від користувача специфічних знань.

Головна вимога для того, щоб ним можливо було скористатися – мати у розпорядженні два безпровідних адаптери.

Разом з тим, як і у попередніх випадках, метод не є гарантованим, а його результативність зумовлена виключно людським фактором.

### 3.1.3 Підбір паролю

У чистому вигляді метод є одним з найменш продуктивних.

При цьому, якщо навіть перебір паролів здійснювати за допомогою спеціалізованих програмних засобів у форматі brootforce-атаки, це не гарантує результативність усієї процедури, оскільки існує ризик блокування запитів бездротового адаптеру зловмисника.

Така можливість існує, якщо для захисту WiFi-з'єднань використовуються засоби, що здатні обмежувати кількість запитів (а саме – спроб введення паролю) в одиницю часу.

У даному випадку можливі такі варіанти перебігу подій, як зазначено далі, а саме:

- суттєве уповільнення процесу підбору паролів (а відтак – його реалізація не матиме сенсу);
- успішний підбір пароля;
- превентивне блокування безпровідної точки доступу на рівні MAC-адреси з необхідністю її зміни для можливості продовжити атаку.

Таким чином, даний метод також не є гарантовано результативним.

### 3.1.4 Метод, що базується на використанні баз паролів

Даний метод відноситься до категорії словникових [7, 11].

В основі методу лежить твердження про те, що деякі фрази, невеликі словосполучення та цифрово-літерні комбінації мають дуже високу частоту використання у якості паролів (рис.3.2).

Це, зазвичай:

- дата народження у різних форматах;
- ім'я власника, поєднане з роком його народження;
- крилаті вислови (per espera ad astra, hoho homini lupus est, sol lucet omnibus) у варіантах – з пробілами, та без;

- імена відомих кінематографічних/літературних героїв та персонажів у різному форматі написання;
- специфічні цифрово-літерні комбінації;
- специфічні слова, назви та терміни, що з тих чи інших причин у побутовому лексиконі майже не вживаються (синхрофазотрон, кінематографістика, Ейяфьядлайокудль та ін.).

До того ж, значний відсоток користувачів пароль від поштової скриньки застосовує і для налаштування месенджерів, і для точки доступу WiFi.

Якщо ж говорити про мережі WEP, де можливим було використання паролів менше 8 символів, то серед паролів, які використовуються там, можна знайти «QWERTY», «12345» тощо.

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| 1 | 123456 | 6 | 1234567890 | 11 | qwertyuiop | 16 | 7777777 | 21 | google |
| 2 | 123456789 | 7 | 1234567 | 12 | mynoob | 17 | 1q2w3e4r | 22 | 1q2w3e4r5t |
| 3 | qwerty | 8 | password | 13 | 123321 | 18 | 654321 | 23 | 123qwe |
| 4 | 12345678 | 9 | 123123 | 14 | 666666 | 19 | 555555 | 24 | zxcvbnm |
| 5 | 111111 | 10 | 987654321 | 15 | 18atcskd2w | 20 | 3rjs1la7qe | 25 | 1q2w3e |

Рисунок 3.2 – Перелік з 25 паролів, що найчастіше використовувалися у мережах на базі WEP

Також, значний відсоток баз паролів складають так звані скомпрометовані паролі – тобто, ті, які раніше було зламано.

При цьому, атака з використанням бази паролів може розглядатися як різновид brootforce-атаки, у ході якої реалізується не повний перебір паролів, а їх обмеженої множини, отриманої з однієї або кількох баз.

Результативність даного методу можна вважати відносно високою лише для випадків, коли питаннями безпеки WiFi опікуються особи, що не мають відповідної кваліфікації, або хоча б обмежених знань з інформаційної безпеки.

Отже, розглянутий метод також не може гарантувати злам WiFi-мережі.

3.1.5 Метод handshake

Якщо розглядати даний метод суто з технічної точки зору, тоді зазначимо, що handshake (рукостискання) у безпровідних мережах — це процес обміну даними, що має місце між точкою доступу та клієнтом у момент його підключення. Обмін інформацією реалізується у ході кількох стадій. Зазначений процес є стандартизованим [12].

У свою чергу, з практичної точки зору достатньо знати наступне:

1. Handshake може бути захоплено у ході підключення клієнта, який використовує валідний пароль, до безпровідної точки доступу.

2. Handshake містить у собі достатній обсяг інформації для розшифрування паролю.

При цьому, процедура виокремлення паролю з рукостискання виконується методом перебору (brootforce-підхід).

Разом з тим, handshake має ключові відмінності з прямим методом підбору на базі brootforce, а саме:

- у ході реалізації «класичного» brootforce, виконуються спроби підключення до точки доступу, кожен раз – з новим паролем;
- у випадку методу «хендшейк» виконується захоплення даних, попередньо шифрованих з використанням реального паролю. Процес підбору виконується у offline-режимі.

Для підбору паролю може бути використано або процесорна потужність, або зовнішні сервіси, або можливості GPU, використовуючи CUDA.

При цьому, на відміну від brootforce, кожного ражу не здійснюється звернення до точки доступу. Наслідком цього є:

- суттєве заощадження часу за рахунок відсутності необхідності підключення для перевірки кожного чергового паролю;
- мінімізація, або повна відсутність ймовірності блокування точки доступу системою безпеки атакованої мережі.

Водночас, як свідчить статистика [12-15], за умови перехоплення достатньої кількості векторів ініціалізації, WiFi-мережу на базі WPA/WPA2 може бути гарантовано зламано.

Отже, розглянувши найбільш поширені методи зламу паролів у мережах WiFi, можемо зробити попередній висновок про те, що:

- гарантований злам WiFi-мережі серед розглянутих - забезпечують виключно хендшейк-методи;

- результативність методів фішингу та таких, що орієнтуються на підбір паролів, суттєвим чином залежить від «якості» пароля атакованої точки доступу;

- у випадку мультизвернень до точки доступу, можливе або тимчасове, або повне блокування адаптеру зловмисника на рівні MAC-адреси, що вимагає або за діяння нового апаратного пристрою, або маскування існуючого MAC.

Таким чином, ураховуючи вищезазначене, найбільш результативним методом для зламу паролів WiFi є метод handshake.

Виконаємо дослідження засобів, що дозволяють реалізувати метод handshake для зламу паролів WiFi.

## 3.2 Огляд інструментів для реалізації зламу WiFi-з'єднання

На сьогоднішній час для зламу паролів WiFi існує велика кількість програмних засобів. Це є прямим наслідком того, що уразливості як WEP, так і WPA, є широковідомими. Розглянемо деякі з них.

### 3.2.1 Aircrack-ng

Програмний засіб Aircrack-ng реалізовано як у Windows-оточенні, так і для використанні у середовищі Linux [18].

Дана утиліта орієнтована на злам WEP та WPA/WPA2 паролів.

Тут передбачено можливість використання атак Pychkine-Tews-Weinmann та KoreK. Обидва методи базуються на виявленні статистичних закономірностей та є більш ефективними, ніж атака FMS, що вже отримала статус класичного методу.

Утиліта Aircrack-ng має у своєму складі ряд компонентів, а саме:

- Airmon-ng, що використовується для налаштування безпровідного мережевого адаптеру. Для коректної роботи утиліти необхідно використовувати Wi-Fi адаптер з можливістю підтримки режиму моніторинга (Monitor mode);

- Airodump-ng, завданням якої є захоплення кадрів. У сутності, компонента виконує прийом та обробку усіх захоплених адаптером пакетів безпровідної мережі, виводить дані щодо параметрів даних мереж та зберігає дані, необхідні для підбору ключів до цих мереж;

- Aireplay-ng, що генерує трафік.

- однойменна компонента Aircrack-ng, яка виконує злам, використовуючи при цьому дані, попередньо зібрані компонентою airodump-ng;

- airdecap-ng, для дешифрування захоплених пакетів.

Тобто, Aircrack-ng є, власне, пакетом засобів, а також ім'ям однієї з компонент.

### 3.2.2 CoWPAtty

Засіб CoWPAtty орієнтований на роботу у Linux-оточенні, а також Mac OS, Windows та Android [12, 19].

У його основі – механізми автоматизація атаки за словником для WPA-PSK.

Як і Aircrack-ng , утиліта запускається з командного рядку. При цьому, у якості головного параметру має задаватися перелік слів, що забезпечує ймовірність знаходження парольної фрази.

Перевагою даного засобу є його безумовна продуктивність.

До недоліків можна віднести складність ряду функцій для розуміння, та складність процесу встановлення.

### 3.2.3 Void11

Утиліта Void11, у сутності, не є самостійним засобом зламу. Зазвичай вона використовується паралельно з іншим засобом, який, власне, виконує підбір паролю, у якості допоміжного [19].

Void11 деаутентифікує клієнтів безпровідної мережі, подібно тому, як ще здійснює Wifiphisher, та інші схожі засоби. Пояснимо доцільність його використання наступним прикладом.

Припустимо, що у поточний час активовано утиліту Airodump-ng (рис.3.3).

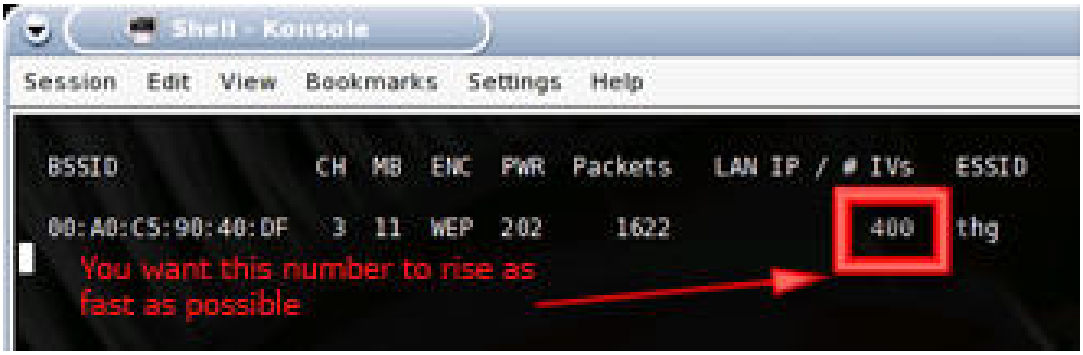


Рисунок 3.3 - Процес захоплення пакетів безпровідного каналу за допомогою Airodump-ng

На рис. 3.3 MAC-адреса точки доступу, яка у поточний час атакується, відображується у лівій колонці поруч з заголовком BSSID.

У цей час значення лічильників кількості захоплених пакетів (Packet count), а також векторів ініціалізації (IV count), постійно зростатиме. Така закономірність є справедливою навіть для випадку незавантаженої, або – недостатньо завантаженої мережі.

Разом з тим, у нашому випадку має значення швидкість росту IV count, так як зростання Packet count може взагалі не мати відношення до процесу зламу.

Дана обставина, у свою чергу, пояснюється тим, що значна кількість пакетів є не що інше, як об’яви точки доступу, що за замовчуванням надсилаються з частотою 10 пакетів/с.

У свою чергу, відомості, що надає лічильник IV, опосередковано сповіщують про перебіг процесу зламу.

При цьому, гарантований злам мережі на базі протоколу WEP з ключем довжиною 64 біта потребує наявності від 50000 до 200000 векторів

ініціалізації, тоді як для випадку 128-бітного ключа WEP - від 200000 до 700000 [12, 19].

З іншого боку, у реальних умовах, за випадку звичного режиму роботи мережі зростання величини IV може відбуватися досить повільно.

У такому випадку для збору достатньої кількості векторів ініціалізації може знадобитися суттєвий проміжок часу – від кількох годин, до кількох діб.

Водночас, дієвим способом прискорення росту значення IV є завантаження атакованої мережі.

Оскільки знаходячись поза її межами, повністю відсутня можливість, наприклад, налагодити передавання великої кількості файлів між тими чи іншими внутрішніми вузлами, або надсилання великої кількості ping-запитів, дієвим є спосіб завантаження мережі, який реалізується з використанням утиліти Void11.

Для запуску Void11 знадобиться інша робоча станція, оснащена безпровідним адаптером.

На базі іншої робочої станції активується утиліта, яка реалізує сценарій деаутентифікації активних користувачів, яких подано наступним лістингом команд:

```
switch-to-hostap
cardctl eject
cardctl insert
iwconfig wlan0 channel [номер каналу мережі, що
атакується]
iwpriv wlan0 hostapd 1
iwconfig wlan0 mode master
void11_penetration -D -s [MAC-адреса клієнта] -B [MAC-
адреса точки доступу] wlan0
```

Деаутентифікація безпровідних клієнтів від точки доступу є нічим іншим, як їх від’єднанням.

Відтак, після кожного від’єднання безпровідний клієнт буде автоматично намагатися здійснити підключення до точки доступу, тобто, повторити асоціацію.

При цьому, зрозуміло, що під час кожної такої спроби генеруватиметься трафік, що і сприятиме навантаженню мережі без фізичного доступу до неї.

Подібні атакі отримали назву атаки деаутентифікації, атаки відключення чи "deauth attack".

### 3.2.4 Типізовані скриптові рішення

Існує велика кількість командних сценаріїв, що дозволяють реалізувати процес зламу WEP/WPA шифрування у мережах WiFi.

Одним з найбільш відомих скрипкових рішень на сьогодні може вважатися Wifite [20].

На базі подібних рішень у цілому аналогічним чином, як було розглянуто вище, може бути побудовано процес зламу механізмів шифрування у мережах WiFi.

При цьому, підсумкову результативність даного підходу можемо вважати аналогічною тим підходам, що є властивими іншим розглянутим підходам.

Разом з тим, типізовані скриптові рішення мають ряд недоліків, серед яких:

- суттєвий відсоток рішень орієнтується на певний алгоритм шифрування WiFi та/або умови зламу;
- успішне використання рішення потребує попереднього достатньо глибокого вивчення логіки роботи пакету скриптів та особливостей їх використання.

Таким чином, беручи до уваги особливості розглянутого інструментарію, для дослідження можливостей зламу мереж WiFi найбільш дієвими засобами можемо вважати мультиутиліту Aircrack-ng у поєднанні з засобом Void11.

Це зумовлено наступними факторами:

- у цілому, процес використання як Aircrack-ng, так і Void11, є формалізованим, відтак – по-перше, не потребує від користувача обов’язкового вивчення логіки (загальної, або детальної) роботи тієї чи іншої компоненти засобу;
- обидва означені засоби мають потужну інформаційну підтримку – починаючи з рекомендацій щодо інсталяції засобів і закінчуючи

рекомендаціями з їх використання та описом можливих проблем і вказівками з їх усунення;

- кожна з утиліт, що входить до складу пакету, зарекомендувала себе як результативний засіб.

# 4. РЕАЛІЗАЦІЯ ПРОЦЕДУРИ ЗЛАМУ ПАРОЛЯ WI-FI НА БАЗІ МЕТОДУ HANDSHAKE

## 4.1 Умови проведення дослідження

Для виконання процедури підбору паролю до Wi-Fi-мережі у ролі платформи обирається Kali Linux на базі VMware [21].

Вибір Kali Linux у даному випадку зумовлено, по-перше, наявністю великої кількості специфічних програмних засобів, у т.ч. утиліт для роботи з бездротовими з'єднаннями, у складі базового дистрибутиву а по-друге – присутністю у системі драйверів майже усіх виробників Wi-Fi-обладнання [12, 18, 19].

При цьому, для дослідження ступеня залежності між обчислювальною потужністю апаратного базису та продуктивністю методу handshake, процедура послідовно виконується з використанням ПК наступних конфігурацій:

- Intel Pentium Dual-Core CPU T4500 2x2,3 GHz, 4 GB RAM;
- Intel Core I5 CPU 6x2,1 GHz, 8 GB RAM.

У свою чергу, для кожної конфігурації ПК процедура виконується за єдиним сценарієм, на базі використання однакового набору утиліт, а саме – пакету Aircrack-ng.

## 4.2 Хід дослідження

Так як обладнання на базі CPU T4500 – ПК у десктоп-версії, для цього випадку буде використано сторонній Wi-Fi-адаптер.

Тому після налаштування та запуску Kali Linux у віртуальному середовищі VMware виконується процес під'єднання та далі - ініціалізації безпровідного Wi-Fi-адаптера, у ролі якого використовується пристрій Ralink 802.11n USB WirelessLanCard.

Для цього виконується наступний перелік дій:
VM →RemovableDevices→Ralink 802.11n USB WirelessLanCard→Connect, як показано на рис.4.1

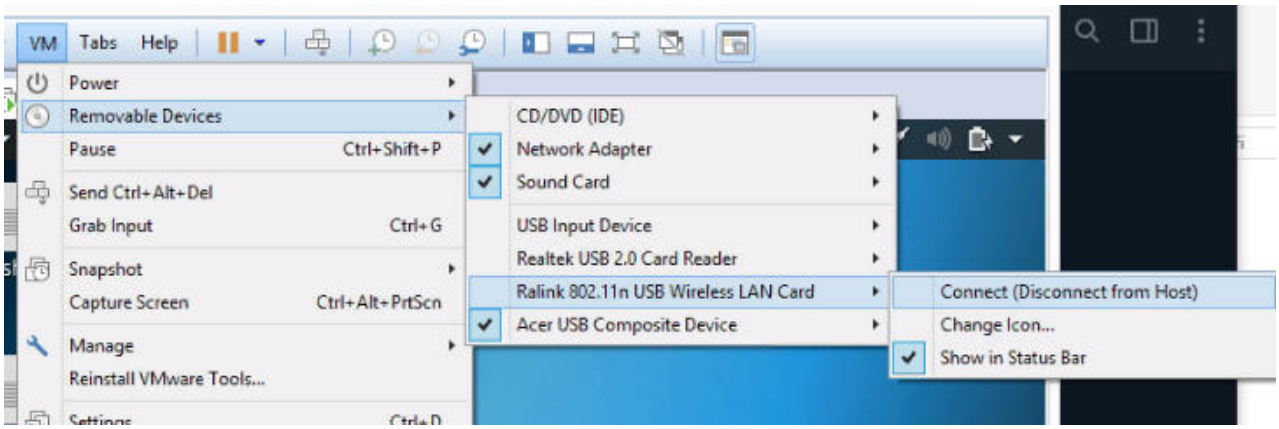


Рисунок 4.1 – Ініціалізація безпровідного адаптеру у системі

Далі, на наступному кроці, необхідно упевнитись у тому, що встановлене безпровідне обладнання є готовим до використання. Для цього достатньо отримати відомості про наявні інтерфейси, що може бути виконано запуском у терміналі команди [18, 19]:

```
airmon-ng
```

У результаті цього бачимо, що пристрій є активним у системі, при цьому йому відповідає інтерфейс wlan0, як показано на рис.4.2.

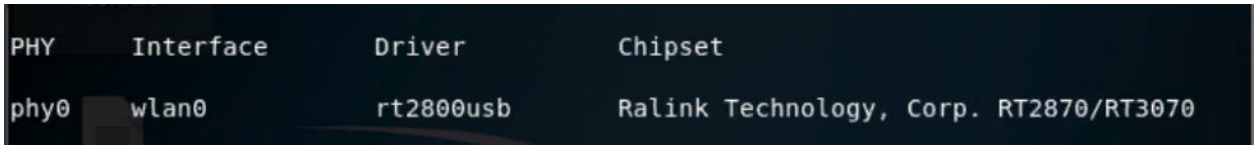


Рисунок 4.2 – Відомості щодо встановленого Wi-Fi-адаптеру

Далі, використовуючи отримані відомості про інтерфейс адаптеру, виконується його переведення у режим моніторингу. У свою чергу, для того, щоб виконати дану операцію, використовується команда вигляду airmon-ngstart [ім'я інтерфейсу]. Відповідно, у нашому випадку маємо:

```
airmon-ngstart wlan0
```

Про те, що тепер Wi-Fi-адаптер функціонує у режимі моніторингу, можна впевнитися, переглянувши у терміналі результат виконання команди (рис.4.3).

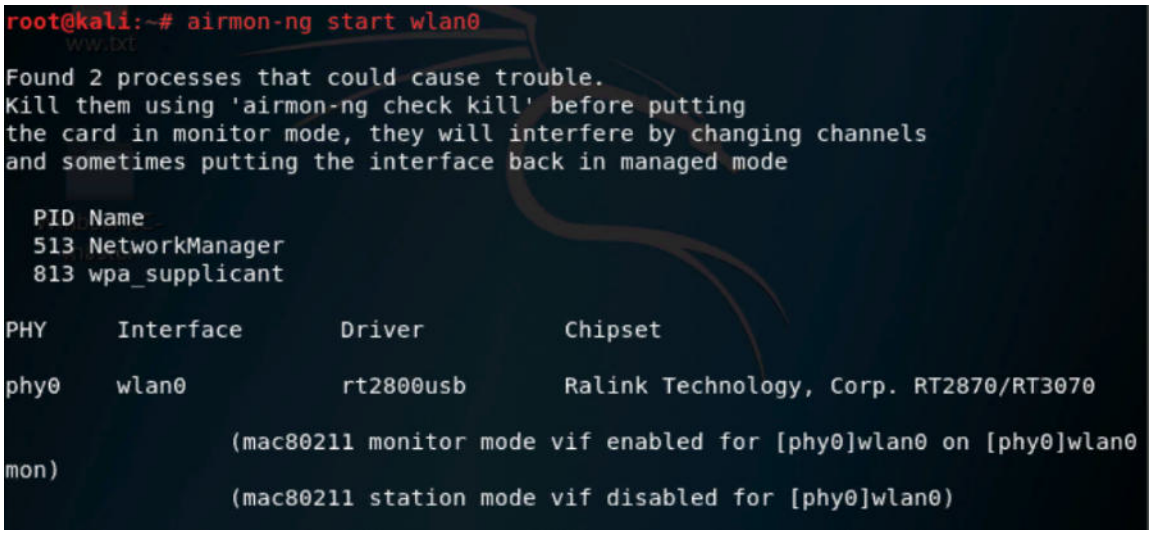


Рисунок 4.3 – Відомості про поточний режим роботи адаптеру

Тепер, у режимі моніторингу, можливо отримати відомості про Wi-Fi-мережі у зоні досяжності. Для цього виконується команда:

```
airodump-ng wlan0 mon
```

Як можна бачити з рис. 4.4, де наведено результати виконання команди, у момент моніторингу зафіксовано велику кількість Wi-Fi-мереж, розгорнутих поряд. Окрім цього, отримано дані відносно:

- BSSID, або ідентифікатори мереж. Тут це – MAC-адреси мережевих адаптерів або точок доступу;
- імен точок доступу;
- використовуваних протоколів безпеки (WPA2);
- алгоритмів шифрування (CCMP);
- алгоритмів аутентифікації (PSK).

Таким чином, отримані відомості свідчать про потенційну вразливість усіх виявлених мереж [12-14].

Далі виконується налаштування утиліти для прослуховування однієї з виявлених мереж, для чого використовується команда вигляду airodump-ng -c [номер цільового каналу] –bssid [цільовий BSSID] -w /root/Desktop/ [інтерфейс моніторингу]. У нашому випадку обирається BSSID 4C:ED:FB:8A:4F:C0. Тоді зазначена команда буде наступною (рис.4.5):

```
airodump-ng -c 6 –bssid 4C:ED:FB:8A:4F:C0 -w
/root/Desktop/ wlan0 mon.
```

Після запуску зазначеної команди утиліта airodump буде виконувати моніторинг вказаної мережі, очікуючи з’єднань з нею з боку легальних користувачів.

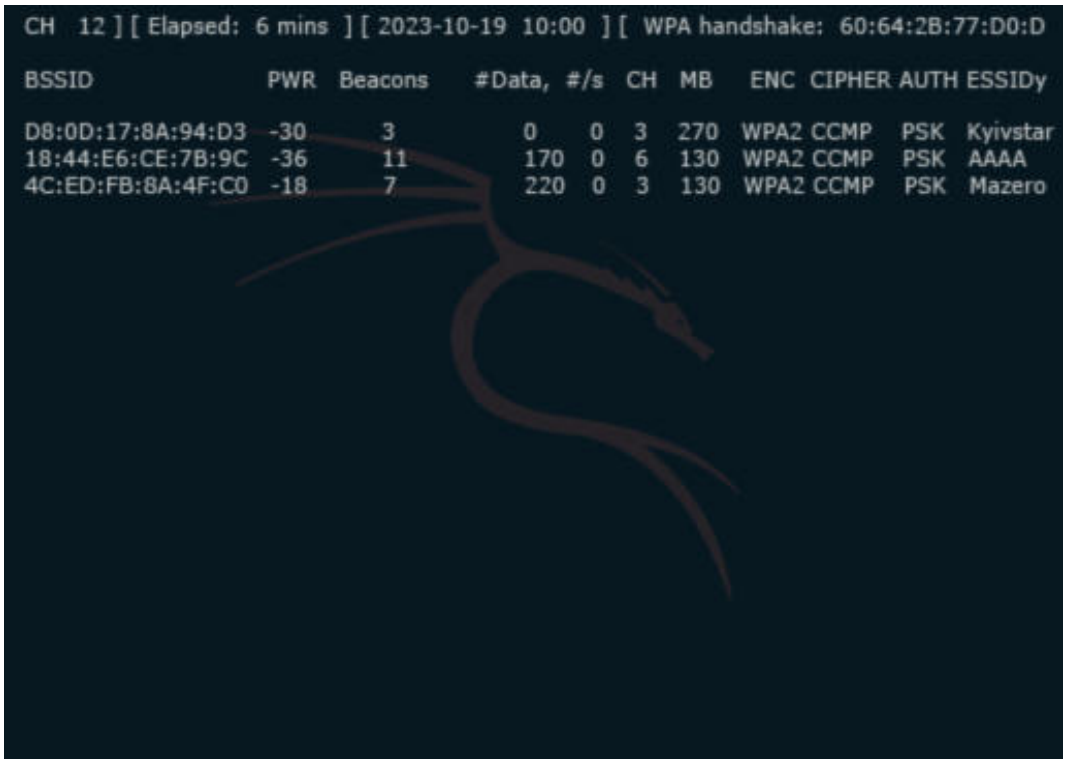


Рисунок 4.4 – Відомості про Wi-Fi-мережі, розгорнуті у зоні досяжності адаптеру


Рисунок 4.5 – Запуск команди прослуховування обраної мережі

Відповідно, після того, як до цільової мережі буде підєднано хоча б одного користувача, розпочнеться процес отримання handshake-файлів.

Такі файли, у свою чергу, будуть зберігатися у директорії, заданій командою, а саме - /root/Desktop.

Процес прослуховування цільової мережі утилітою airodump з захопленням пакетів та формування handshake-файлів показано рис.4.6.

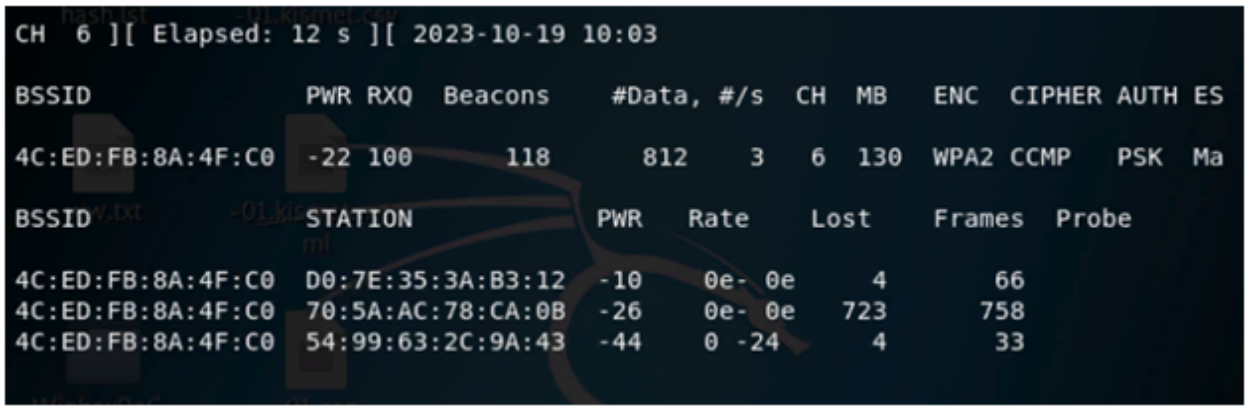


Рисунок 4.6 – Процес збору пакетів цільової мережі

Далі після того, як було зібрано достатню кількість handshake-файлів, виконується аналіз отриманих статистичних даних з виокремленням Wi-Fi-ключа.

З причини достатньо низької кількості користувачів у межах обраної мережі, а також незначної інтенсивності обміну даними між ними, тривалість збору handshake-файлів у нашому випадку складає близько 4 годин.

Сам процес аналізу зібраних статистичних даних ініціюється командою вигляду aircrack-ng -a2 -b [router bssid] -w [path to wordlist] /root/Desktop/*.cap. Тобто, для нашого випадку маємо:

```
aircrack-ng -a2 -b 4C:ED:FB:8A:4F:C0 -w
/root/Desktop/ww.txt /root/Desktop/*.cap
```

Результат аналізу даних handshake та знайдений Wi-Fi-ключ показано на рисунку 4.7


Рисунок 4.7 – Результати обробки handshake-файлів

## 4.3 Рекомендації з безпеки мереж Wi-Fi за результатами виконаного дослідження

У цілому, на сьогодні існує 3 дієвих механізми захисту безпровідної мережі 802.11, а саме [12, 15, 17]:

- налаштування клієнту та AP на використання одного (який не обирається за замовчуванням) SSID;
- встановити дозвіл для AP на зв'язок лише з клієнтами, MAC-адреси яких є відомими AP;
- виконати налаштування клієнтів на аутентифікацію в AP і шифрування трафику.

При цьому, на сьогодні налаштування переважної більшості AP виконується таким чином, що передбачає работу з SSID, який обирається за замовчуванням, без використання переліку «дозволених» MAC-адрес клієнтів та з відомим загальним ключем для аутентифікації та шифрування (чи взагалі без використання зазначених технологічних процедур).

Зазвичай ці параметри наведені не лише у супровідній документації до Wi-Fi-пристроїв, але також є задокументованими в оперативній довідковій системі на Web-узлі виробника.

З одного боку, у даному разі, маючи усі зазначені параметри у розпорядженні, навіть користувачі без відповідного доступу мають змогу як швидко розгорнути безпровідну мережу, так і розпочати роботу з нею.

З іншого боку, у зазначених умовах суттєво спрощується завдання для зловмисника щодо проникнення до мережі. При цьому, існуюча ситуація погіршується тим, що більшість вузлів доступу налаштовано на широкомовну передачу SSID. У зв’язку з цим зловмисних отримує змогу знайти уразливі мережі за стандартним SSID.

Відтак, перший крок у збільшенні захищеності безпровідної мережі полягає у зміні SSID вузла доступу. Разом з тим, необхідно змінити даний параметр на клієнті, щоб забезпечити зв'язок з AP. У даному випадку доцільним є призначення SSID, який матиме сенс для користувачів мережі та її адміністратора, але при цьому жодним чином не ідентифікуватиме мережу серед множини інших SSID, які може бути перехоплено сторонніми особами.

Наступним кроком налаштувань, після зміни SSID, є, за можливості, блокування широкомовної передачі SSID вузлом доступу. Сенс даної операції полягає в утрудненні для зловмисника (разом тим, така можливість певною мірою зберігається) виявлення наявності активної безпровідної мережі та SSID.

Проте, існує перелік модельних рядів AP, для яких можливість блокування широкомовної передачі SSID повністю відсутня. Для зазначених випадків можливим рішенням є збільшення інтервалу широкомовної передачі до максимально можливого значення. Разом з тим, зв'язок з рядом клієнтів може встановлюватися лише за умови виконання широкомовної передачі SSID вузлом доступа. За таких умов адміністратор мережі має експериментально визначити інтервал, щоб вибрати його оптимальне значення.

З точки зору протоколів безпеки WiFi, за можливості використання WPA, зазвичай має бути виконано вибір між WPA, WPA2 та WPA-PSK.

У свою чергу, тут ключовим фактором під час вибору WPA або WPA2, з одного боку, та WPA-PSK — з іншого, є можливість розгортання інфраструктури, що є необхідною WPA та WPA2 для виконання аутентифікації користувачів. Так. у випадку як WPA, так і WPA2 необхідно

розгорнути сервери RADIUS а також, в окремих випадках, додатково PublicKeyInfrastructure (PKI).

Разом з тим, WPA-PSK, як і WEP, функціонує на базі загального ключа, що є відомим як безпровідному клієнту, так і AP. На випадок WPA-PSK може ьбути використано загальний ключ WPA-PSK для реалізації процесів аутентифікації та шифрування, так як для даного протоколу не властиві недоліки WEP.

# ВИСНОВКИ

У відповідності до технічного завдання було виконано дослідження рівня потенційної захищеності трафіку безпровідних мереж. Зокрема:

- обгрунтовано, що найбільший відсоток безпровідного трафіку сьогодні належить мережам WiFi;
- досліджено механізми захисту, які використовуются у мережах WiFi. Сюди відносяться механізми аутентифікації та шифрування даних;
- доведено потенційну уразливість алгоритмів шифрування, задіяних під час формування WiFi-трафіку;
- розглянуто поширені сьогодні методи зламу паролю у мережах WiFi;
- реалізовано атаку на WiFi-з'єднання.

При цьому, виявлено, що:

- найменш надійним алгоритмом шифрування WiFi-з'єднання є WEP, що є наслідком ряду його архітектурних особливостей та постійного зростання обчислювальних можливостей у т.ч. потенційного зловмисника; разом з тим, на час створення алгоритм WEP забезпечував прийнятний рівень захищеності;
- майже завжди під терміном «злам мережі WiFi» мається на у вазі процес реконструкції пароля на базі того чи іншого методу;
- усі поширені методи зламу WiFi так чи інакше може бути зведено до brootforce, методів соціальної інженерії чи handshake-методів;
- результативність методів кожної з груп суттєвим чином залежить від типу шифрування, використаного для захисту каналу, кількості зібраних статистичних даних та складності використаного паролю шифрування;
- як для WEP, так і для усього сімейства WPA (у т.ч. WPA2 та WPA3) найбільш дієвим можна вважати підхід, що базується на використанні handshake-методів;
- за умови збору достатнього обсягу статистичних даних, handshake-методи гарантовано дозволяють виконати злам WiFi-з'єднання.

У свою чергу, для реалізації процесу зламу WiFi-мережі було застосовано пакет утиліт AirCrack.

При цьому, у ролі платформи використано Kali Linux.

За результатами дослідження виявлено, що для зазначених раніше обчислювальних потужностей процес зламу пароля WiFi-мережі, захищеного ключем стандартної довжини, було реалізовано протягом:

- сумарно 4,5 годин (у т.ч. 4 з них – для збору статистичних даних та близько 35 хвилин – на обробку handshake) для ПК на базі Intel Pentium Dual-Core CPU T4500 2x2,3 GHz, 4 GB RAM;
- сумарно 4.1 годин (у т.ч. приблизно 4 з них – для збору статистичних даних та порядку 6 хвилин – на обробку handshake) для ПК на базі Intel Core I5 CPU 6x2,1 GHz, 8 GB RAM.

Таким чином, доведено, що питання захищеності WiFi-сегментів є одними з ключових у забезпеченні захисту інформаційних систем у цілому.

Отже, усі завдання до кваліфікаційної роботи виконано у повному обсязі.

# ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАННЯ

1. Microsoft security report [Електронний ресурс] – Режим доступу: https://microsoft.com/securityinsights.

2. Antivirus and Cybersecurity Statistics & Facts 2021 [Електронний ресурс] – Режим доступу: https://wethegeek.com/antivirus-statistics-facts/.

3. Understanding Wi-Fi 4/5/6/6E/7(802.11 n/ac/ax/be) [Електронний ресурс] – Режим доступу: https://www.duckware.com/tech/wifi-in-the-us.html

4. VNI Service Adoption Forecast [Електронний ресурс] – Режим доступу: https://www.cisco.com/c/dam/assets/sol/sp/vni/sa_tools/vnisa-graphing-tool/vnisa-graphing-tool.html

5. Book LoRaWAN [Електронний ресурс] – Режим доступу: https://www.univ-smb.fr/lorawan/en/free-book/

6. Anderson, Ross J. (2008). Security engineering: a guide to building dependable distributed systems (2 ed.). Indianapolis, IN: Wiley. p. 1040. ISBN 978-0-470-06852-6.

7. Шаньгін В.Ф. Захист інформації в розподілених корпоративних мережах і системах [Текст]: підручник / В.Ф. Шаньгин, А.В. Соколов. – М.: ДМК Пресс, 2002. – 656 с.

8. Colon S. Wireless Networks and Communications. Wiiford Press, 2019. – 229 p.

9. Korowajszuk L. LTE-A, WiMAX 2.2 and WLAN (4G/5G): Network Design, Optimization and Performance Analysis 2nd Edition. Wiley, 2023. – 850 p.

10. Wifi to carry 60 pc of mobile data traffic by 2019 [Електронний ресурс] – Режим доступу: http://www.juniperresearch.com/press/press-releases/wifi-to-carry-60pc-of-mobile-data-traffic-by-2019.

11. Bejtlich R. The Practice of Network Security Monitoring: Understanding Incident Detection and Response / Richard Bejtlich. – San Francisco: Search Press Inc, 2013. – 341p.

12.Coleman David D., Westcott David A. CWNA Certified Wireless Network Administrator Study Guide: Exam CWNA-107, 5th Edition. D. Coleman. – Wiley, 2018. – 1024 p. ISBN: 978-1-119-42578-6.

13.Coleman David D., Westcott David A., Bryan Harkins E. CWSP Certified Wireless Security Professional Study Guide: Exam CWSP-205, 2nd Edition. D. Coleman. – Wiley, 2016. – 696 p. ISBN: 978-1-119-21109-9.

14.Coleman David D., Westcott David A., Miller B., Mackenzie P. CWAP Certified Wireless Analysis Professional Official Study Guide: Exam PW0-270. D. Coleman. – Wiley, 2011. – 696 p. ISBN: 978-1-118-07523-4.

15. Matthew Gast S. 802.11ac: A Survival Guide. O'Reilly Media, Inc, 2003. – 152 p. ISBN: 9781449343149.

16. IEEE 802.11-2016 [Електронний ресурс] – Режим доступу: https://standards.ieee.org/ieee/802.11/5536/

17. Росс Д. Бездротова комп'ютерна мережа Wi-Fi власноруч: інсталяція, налаштування, використання. Наука і техніка, 2009. – 384 с. ISBN: 978-5-94387-575-5.

18. Aircrack-ng [Електронний ресурс] – Режим доступу: https://aircrackng.com/doku.php?id=main

19. How to Hack WPA/WPA2 WiFi Using Kali Linux? [Електронний ресурс] – Режим доступу: https://www.geeksforgeeks.org/how-to-hack-wpa-wpa2-wifi-using-kali-linux/

20. Github - ParrotSec / wifite [Електронний ресурс] – Режим доступу: https://github.com/ParrotSec/wifite

21. Kali Linux | Penetration Testing and Ethical Hacking Linux Distribution [Електронний ресурс] – Режим доступу: https://www.kali.org/