МІНІСТЕРСТВО ОСВІТИ ТА НАУКИ УКРАЇНИ
КРИВОРІЗЬКИЙ ФАХОВИЙ КОЛЕДЖ
ДЕРЖАВНОГО НЕКОМЕРЦІЙНОГО ПІДПРИЄМСТВА
«ДЕРЖАВНИЙ УНІВЕРСИТЕТ «КИЇВСЬКИЙ АВІАЦІЙНИЙ ІНСТИТУТ»
Циклова комісія *комп'ютерних систем та мереж*
(повна назва циклової комісії)

Допустити до захисту
Голова випускової циклової комісії
комп'ютерних систем та мереж
(повна назва циклової комісії)
(підпис) *Ірина КРАВЧУК*
(ім'я, ПРІЗВИЩЕ)
« 10 » 06 2025 р.

КВАЛІФІКАЦІЙНА РОБОТА
(ПОЯСНЮВАЛЬНА ЗАПИСКА)

ВИПУСКНИКА ОСВІТНЬО-ПРОФЕСІЙНОГО СТУПЕНЯ ФАХОВИЙ МОЛОДШИЙ БАКАЛАВР

Тема: *«Підвищення ефективності та надійності бездротової мережі підприємства шляхом модернізації»*

Група: *321* Спеціальність: *123 «Комп'ютерна інженерія»*

Здобувач освіти (підпис) *Михайло ЗАЛІЗНЯК* (ім'я, ПРІЗВИЩЕ)

Керівник роботи (підпис) *Микола РАШЕВСЬКИЙ* (ім'я, ПРІЗВИЩЕ)

Консультант з оформлення пояснювальної записки (підпис) *Оксана ОСАДЧА* (ім'я, ПРІЗВИЩЕ)

Кривий Ріг 2025 р.

КРИВОРІЗЬКИЙ ФАХОВИЙ КОЛЕДЖ
ДЕРЖАВНОГО НЕКОМЕРЦІЙНОГО ПІДПРИЄМСТВА
«ДЕРЖАВНИЙ УНІВЕРСИТЕТ «КИЇВСЬКИЙ АВІАЦІЙНИЙ ІНСТИТУТ»

Відділення *комп'ютерної та програмної інженерії*
Циклова комісія *комп'ютерних систем та мереж*
Освітньо-професійний ступінь *фаховий молодший бакалавр*
Спеціальність *123 «Комп'ютерна інженерія»*

ЗАТВЕРДЖУЮ
Голова випускової циклової комісії
комп'ютерних систем та мереж
(повна назва циклової комісії)
(підпис) *Ірина КРАВЧУК*
(ім'я, ПРІЗВИЩЕ)
« 01 » 03 2025 р.

ЗАВДАННЯ

НА КВАЛІФІКАЦІЙНУ РОБОТУ ЗДОБУВАЧУ ОСВІТИ

Залізняку Михайлу Валентиновичу
(прізвище, ім'я, по батькові)

1.Тема роботи *«Підвищення ефективності та надійності бездротової мережі підприємства шляхом модернізації»*

Керівник роботи *Рашевський Микола Олександровия, к.ф.-м.н., доцент*
(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)

затверджені наказом по коледжу від « *04* » *04* 2025 року № *50-ст*

2. Строк подання здобувачем освіти роботи з _____ по _____

3. Вихідні дані до роботи *організація процесу захисту мереж, технології, стандарти та специфікації комп'ютерних мереж*

4. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити)
Комп'ютерна мережа та методи її захисту, огляд концепції політики інформаційної безпеки, захист даних під час передачі, проектування захищеної комп'ютерної мережі

5. Перелік графічного матеріалу (з точним зазначенням обов'язкових креслень)

Презентація Microsoft PowerPoint

6. Консультанти розділів роботи (проекту)

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв

7. Дата видачі завдання _____

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів кваліфікаційної роботи	Строк виконання етапів роботи	Примітка
1	*Узгодження технічного завдання з керівником кваліфікаційної роботи*	*24.03.2025-27.03.2025*	*виконано*
2	*Ознайомлення з предметною областю та постановкою задачі дипломного проектування*	*05.04.2025-08.04.2025*	*виконано*
3	*Вивчення спеціальної літератури та відповідної технічної документації*	*09.04.2025-28.04.2025*	*виконано*
4	*Огляд засобів та методів побудови локальних комп'ютерних мереж*	*29.04.2025-04.05.2025*	*виконано*
5	*Аналіз комп'ютерних мережевих технологій*	*12.05.2025-25.05.2025*	*виконано*
6	*Розробка проекту захищеної мережі*	*26.05.2025-01.06.2025*	*виконано*
7	*Оформлення пояснювальної записки*	*02.06.2025-06.06.2025*	*виконано*
8	*Попередній захист кваліфікаційної роботи*	*09.06.2025-13.06.2025*	*виконано*
9	*Захист кваліфікаційної роботи*		

Здобувач освіти _____ *Михайло ЗАЛІЗНЯК*
(підпис) (ім'я, ПРІЗВИЩЕ)

Керівник роботи _____ *Микола РАШЕВСЬКИЙ*
(підпис) (ім'я, ПРІЗВИЩЕ)

Звіт подібності

метадані

Назва організації

Ukrainian national aviation university

Заголовок

ЗАЛІЗНЯК _Проверка

Автор / Науковий керівник / Експерт

ЗАЛІЗНЯК

Підрозділ

Криворізький Фаховий коледж

Обсяг знайдених подібностей

Коефіцієнт подібності визначає, який відсоток тексту по відношенню до загального обсягу тексту було знайдено в різних джерелах. Зверніть увагу, що високі значення коефіцієнта не автоматично означають плагіат. Звіт має аналізувати компетентна / уповноважена особа.

2.64% 2.64% КП 1

0.98% 0.98% КЦ

25 **9759** **77743**

Тривога

У цьому розділі ви знайдете інформацію щодо текстових спотворень. Ці спотворення в тексті можуть говорити про МОЖЛИВІ маніпуляції в тексті. Спотворення в тексті можуть мати навмисний характер, але частіше характер технічних помилок при конвертації документа та його збереженні, тому ми рекомендуємо вам підходити до аналізу цього модуля відповідально. У разі виникнення запитань, просимо звертатися до нашої служби підтримки.

Заміна букв	0
Інтервали	0
Мікропробіли	0
Білі знаки	0
Парафрази (SmartMarks)	22

Подібності за списком джерел

Нижче наведений список джерел. В цьому списку є джерела із різних баз даних. Колір тексту означає, в якому джерелі він був знайдений. Ці джерела і значення Коефіцієнту Подібності не відображають прямого плагіату. Необхідно відкрити кожне джерело і проаналізувати зміст і правильність оформлення джерела.

10 найдовших фраз

Колір тексту

РЕФЕРАТ

Пояснювальна записка до кваліфікаційної роботи «Підвищення ефективності та надійності бездротової мережі підприємства шляхом модернізації» містить: 75 сторінок, 40 рисунків, 3 таблиці, використано 13 ресурсів.

КОМП'ЮТЕРНА МЕРЕЖА, БЕЗДРОТОВА МЕРЕЖА, WI-FI, BLUETOOTH, WEP, WPA2, WPA3, КІБЕРБЕЗПЕКА, ШИФРУВАННЯ, АВТЕНТИФІКАЦІЯ, АТАКИ, РУКОСТИСКАННЯ, РАДІОВИПРОМІНЮВАННЯ, ЗАХИСТ ІНФОРМАЦІЇ.

Кваліфікаційна робота присвячена дослідженню захищених від радіовипромінювання комп’ютерних мереж**,** що є актуальним в умовах інтеграції бездротових технологій та зростання кіберзагроз. У роботі проаналізовано сутність, класифікацію та методи захисту комп'ютерних мереж, з особливим акцентом на специфіку захисту даних при передачі по радіоканалу**.**

У роботі систематизовано поширені способи злому *Wi-Fi* мереж**,** зокрема моніторинг радіоефіру, перехоплення *WPA*/*WPA*2 рукостискань, атаки грубою силою, словникові та маскові атаки, вразливість *WPS* та методи соціальної інженерії.

Результатом дослідження є всебічний аналіз сучасного стану безпеки бездротових комп'ютерних мереж**,** виявлення їхніх основних вразливостей, пов'язаних з радіовипромінюванням, та оцінка ефективності існуючих методів захисту. Запропоновано використання сучасних стандартів шифрування (*WPA*3)**,** комплексне налаштування безпеки мережевого обладнання та підвищення обізнаності користувачів як ключові елементи забезпечення надійного захисту даних в умовах активного радіообміну.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СКОРОЧЕНЬ, ТЕРМІНІВ

LAN – локальна обчислювальна мережа

КМ – комп’ютерна мережа

EOM – електронна обчислювальна машина

ОС – операційна система

PAN – персональна мережа

ВСТУП

Актуальність теми. У сучасному світі, що характеризується стрімким розвитком інформаційних технологій та повсюдним використанням комп'ютерних мереж, питання їхньої безпеки та стабільності функціонування набувають першочергового значення. Дедалі більшого поширення набувають бездротові технології, які, з одного боку, надають значні переваги у гнучкості та доступності, але, з іншого боку, створюють нові виклики у сфері інформаційної безпеки. Одним із таких викликів є проблема радіовипромінювання, яке супроводжує роботу будь якого електронного та мережевого обладнання. Це випромінювання може бути не лише джерелом електромагнітних перешкод, що порушують коректну роботу інших пристроїв, а й

потенційним каналом витоку конфіденційної інформації через побічні електромагнітні випромінювання та наведення (ПЕМІ). В умовах зростаючої кількості кіберзагроз, атак на конфіденційність та цілісність даних, а також необхідності дотримання нормативних вимог щодо електромагнітної сумісності та безпеки для здоров'я, аналіз та розробка методів захисту комп'ютерних мереж від радіовипромінювання є критично важливим завданням.

Мета роботи. Метою кваліфікаційної роботи є проведення комплексного аналізу існуючих підходів та методів захисту комп'ютерних мереж від радіовипромінювання, а також розробка рекомендацій щодо підвищення їхньої захищеності.

Завдання роботи. Для досягнення поставленої мети було визначено наступні завдання:

1. Проаналізувати основні джерела та механізми радіовипромінювання в комп'ютерних мережах.

2. Дослідити ключові загрози інформаційній безпеці, пов'язані з побічними електромагнітними випромінюваннями та електромагнітними перешкодами. 3. Систематизувати та оцінити існуючі методи та технології захисту комп'ютерних мереж від радіовипромінювання.

4. Розглянути застосовні нормативні документи та стандарти у сфері електромагнітної сумісності та безпеки.

5. Сформулювати практичні рекомендації щодо проектування, впровадження та експлуатації захищених від радіовипромінювання комп'ютерних мереж.

Об'єкт дослідження. Об'єктом дослідження є процеси функціонування комп'ютерних мереж у частині генерації та сприйняття радіовипромінювань. Предмет дослідження. Предметом дослідження є методи та засоби захисту комп'ютерних мереж від побічних електромагнітних випромінювань та зовнішніх електромагнітних впливів.

Методи дослідження. У процесі виконання роботи використовувались методи системного аналізу, порівняльного аналізу, метод узагальнення та систематизації наукової та технічної літератури, а також елементи моделювання для оцінки поширення радіосигналів та їхнього впливу.

Наукова новизна. Наукова новизна роботи полягає у систематизації та

комплексному аналізі сучасних підходів до захисту комп'ютерних мереж від радіовипромінювання з урахуванням специфіки сучасних бездротових технологій, а також у формулюванні узагальнених рекомендацій для практичного застосування.

Практична цінність. Практична цінність роботи полягає у можливості використання отриманих результатів та розроблених рекомендацій ІТ-фахівцями, інженерами з безпеки та системними адміністраторами для підвищення захищеності та надійності комп'ютерних мереж, особливо в установах, що працюють з конфіденційною інформацією або в умовах підвищених вимог до електромагнітної сумісності.

РОЗДІЛ 1
КОМП'ЮТЕРНА МЕРЕЖА ТА СПОСІБ ЇЇ ЗАХИСТУ

1.1 Комп'ютерні мережі. Основні умови класифікації

Комп'ютерна мережа (*Computer Network*) являє собою сукупність апаратних та програмних компонентів, що дозволяють різним пристроям (комп'ютерам, серверам, принтерам, мобільним пристроям тощо) обмінюватися даними та спільно використовувати ресурси. В основі функціонування будь-якої комп'ютерної мережі лежить принцип зв'язку, що дає змогу передавати інформацію від одного вузла до іншого. Сучасні комп'ютерні мережі є складною, динамічною системою, що відіграє ключову роль у функціонуванні бізнесу, наукових досліджень, освіти та повсякденного життя.

Класифікація комп'ютерних мереж здійснюється за низкою основних критеріїв, що дозволяють систематизувати їх за різними ознаками та розуміти їхні функціональні можливості, архітектурні особливості та сфери застосування. Основні умови класифікації комп'ютерних мереж:

1. За географічним охопленням (масштабом): Цей критерій є одним з найпоширеніших і визначає фізичну територію, яку охоплює мережа. - персональні мережі (*PAN - Personal Area Network*): мережі, що охоплюють невелику фізичну область навколо однієї особи, як правило, на відстані до 10 метрів (рисунок 1.1). Використовуються для з'єднання персональних пристроїв (смартфон, навушники,

принтер, планшет) через *Bluetooth*, *USB*, *IrDA*. - локальні мережі (*LAN - Local Area Network*): мережі, що об'єднують пристрої на відносно невеликій географічній території, такій як офіс, будинок, будівля або група прилеглих будівель (рисунок 1.2). Характеризуються високою швидкістю передачі даних та обмеженою кількістю користувачів. Типові технології: *Ethernet*, *Wi-Fi*.

- міські мережі (*MAN - Metropolitan Area Network*): мережі, що охоплюють територію міста або великого міського району. Зазвичай використовуються для

з'єднання кількох локальних мереж (рисунок 1.3). Часто належать до комунальних або корпоративних структур.

- глобальні мережі (*WAN - Wide Area Network*): мережі, що охоплюють великі географічні території, такі як регіон, країна або весь світ. Вони з'єднують локальні та міські мережі (рисунок 1.4) через великі відстані, використовуючи різні технології зв'язку (оптоволокно, супутниковий зв'язок). Прикладом *WAN* є мережа Інтернет.

- глобальні мережі зберігання (*GAN - Global Area Network*): використовуються для зв'язку між мережами по всьому світу, але, як правило, відносяться до корпоративних мереж.

Рисунок 1.1 – Приватна мережа

Рисунок 1.2 – Локальна мережа

Рисунок 1.3 – Міська мережа

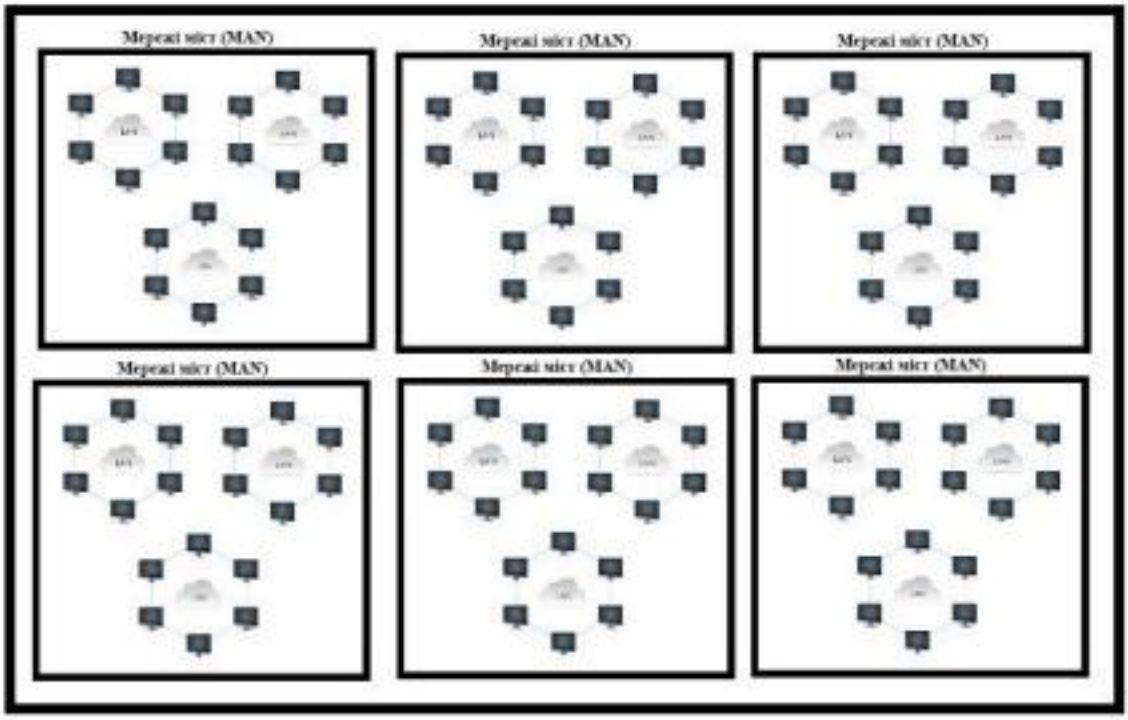

Рисунок 1.4 – Глобальна мережа

2. За топологією (логічною/фізичною структурою): топологія визначає спосіб фізичного або логічного з'єднання пристроїв у мережі:

- Шина (*Bus*): Всі пристрої підключені до одного спільного кабелю. Простота, але вразливість до обривів.

- Зірка (*Star*): Всі пристрої підключені до центрального пристрою (хаба, комутатора). Надійність (вихід з ладу одного пристрою не впливає на інших), але залежність від центрального елемента.

- Кільце (*Ring*): Пристрої з'єднані послідовно по колу, утворюючи замкнене кільце. Дані передаються в одному напрямку.

- Дерево (*Tree*): Комбінація кількох топологій "зірка", з'єднаних між собою шиною.

- Сітка (*Mesh*): Кожен пристрій з'єднаний з кожним іншим пристроєм. Висока надійність і відмовостійкість, але складна та дорога реалізація. - Гібридна: Комбінація декількох базових топологій.

3. За принципом взаємодії між вузлами:

- Клієнт-сервер (*Client-Server*): Мережа, де деякі комп'ютери (сервери) надають ресурси та послуги (файли, принтери, веб-сервіси), а інші комп'ютери (клієнти)

звертаються до цих ресурсів.

- Однорангова (*Peer-to-Peer*, *P2P*): Кожен комп'ютер у мережі може виступати як клієнтом, так і сервером, надаючи та отримуючи ресурси. Часто використовується для обміну файлами.

4. За типом передачі даних (середовищем):

- Дротові мережі: Використовують фізичні кабелі для передачі даних (вита пара, оптоволокно, коаксіальний кабель).

- Бездротові мережі: Використовують радіохвилі, інфрачервоне випромінювання або інші бездротові технології для передачі даних (*Wi-Fi*, *Bluetooth*, *LTE*, 5*G*).

5. За організацією управління:

- Централізовані: Мережа, управління якою здійснюється з одного центрального вузла.

- Децентралізовані: Управління мережею розподілено між кількома вузлами.

Ці класифікації допомагають детально аналізувати архітектуру та функціонування комп'ютерних мереж, що є важливою передумовою для розуміння способів їх захисту, зокрема, від радіовипромінювання.

1.1.1 Класифікація за сферою застосування

Класифікація комп'ютерних мереж за сферою застосування дозволяє виділити їхній функціональний фокус та призначення, відображаючи, яким чином вони використовуються для вирішення конкретних завдань або обслуговування певних категорій користувачів.

Корпоративні мережі (*Enterprise Networks*): Призначені для забезпечення внутрішнього обміну даними, спільного використання ресурсів та підтримки бізнес-процесів в межах однієї організації, компанії або корпорації. Характеризуються високими вимогами до безпеки, надійності, масштабованості та централізованого управління. Можуть включати *LAN*, *MAN*, *WAN* сегменти.

Мережі провайдерів послуг (*Service Provider Networks*): Мережі, що належать телекомунікаційним компаніям та інтернет-провайдерам, які надають послуги зв'язку (доступ до Інтернету, телефонія, *VPN*, хостинг) кінцевим користувачам та іншим підприємствам. Ці мережі є високопродуктивними, відмовостійкими та мають

розгалужену інфраструктуру.

Домашні мережі (*Home Networks*): Невеликі мережі, що використовуються в межах одного будинку чи квартири для підключення персональних комп'ютерів, смартфонів, смарт-телевізорів, ігрових консолей та інших пристроїв до Інтернету та спільного використання файлів або принтерів. Зазвичай це простіші за налаштуванням *LAN* або *WLAN*.

Мережі центрів обробки даних (*Data Center Networks*, *DCN*): Спеціалізовані високошвидкісні мережі, призначені для з'єднання тисяч серверів та пристроїв зберігання даних у межах центру обробки даних. Вони оптимізовані для забезпечення низької затримки, високої пропускної здатності та відмовостійкості, що критично важливо для хмарних сервісів та великих обчислювальних навантажень.

Промислові мережі (*Industrial Networks*): Використовуються для автоматизації та контролю виробничих процесів, підключення промислових контролерів (*PLC*), сенсорів, виконавчих механізмів. Характеризуються підвищеною стійкістю до зовнішніх впливів (шум, температура, електромагнітні перешкоди) та використанням специфічних протоколів (наприклад, *Modbus*, *Profibus*, *Ethernet/IP*).

Безпровідні сенсорні мережі (*Wireless Sensor Networks*, *WSN*): Мережі, що складаються з великої кількості розподілених, автономних сенсорних вузлів, які збирають дані про навколишнє середовище (температура, вологість, тиск, світло тощо) і передають їх до центрального вузла. Використовуються в моніторингу навколишнього середовища, сільському господарстві, "розумних" містах.

1.1.2 Топологічна класифікація

Топологія комп'ютерної мережі описує фізичне або логічне розташування з'єднань між вузлами (пристроями) та шляхи, якими дані можуть передаватися. Вибір топології суттєво впливає на продуктивність, надійність, масштабованість та вартість мережі.

Шина (*Bus Topology*): Всі вузли підключаються до одного спільного комунікаційного кабелю (шини). Дані, надіслані одним вузлом, поширюються по всій шині і приймаються лише тим вузлом, якому вони адресовані.

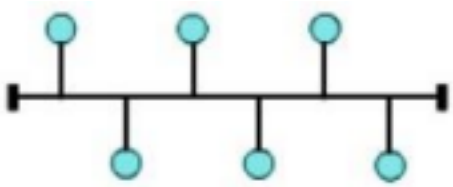

Рисунок 1.5 – Топологія шина

Переваги: Простота реалізації, економія кабелю.

Недоліки: Низька надійність (один обрив кабелю виводить з ладу всю мережу), низька продуктивність при великому трафіку, складнощі у виявленні несправностей.

Зірка (*Star Topology*): Кожен вузол мережі підключається окремим кабелем до центрального пристрою (хаба, комутатора або маршрутизатора).

Рисунок 1.7 – Зірчаста топологія

Переваги: Висока надійність (вихід з ладу одного вузла не впливає на інші), легкість додавання/видалення вузлів, простота виявлення несправностей. Недоліки: Залежність від центрального пристрою (його збій призводить до відмови всієї мережі), більша витрата кабелю.

Кільце (*Ring Topology*): Вузли з'єднані послідовно по колу, утворюючи замкнене кільце. Дані передаються в одному напрямку від одного вузла до наступного, поки не досягнуть адресата.

Переваги: Відносно проста реалізація, кожен вузол є повторювачем сигналу. Недоліки: Один збій у кабелі або вузлі може порушити роботу всієї мережі (хоча існують подвійні кільця для підвищення надійності), складнощі в додаванні/видаленні вузлів.

Сітка (*Mesh Topology*): Кожен вузол мережі має пряме з'єднання з кожним іншим вузлом.

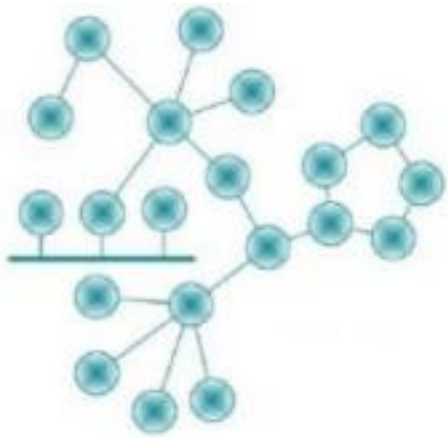

Рисунок 1.8 – Змішана (сітчата) топологія

Переваги: Надзвичайно висока надійність та відмовостійкість (багато резервних шляхів), висока пропускна здатність.

Недоліки: Дуже складна та дорога реалізація (велика кількість кабелів та портів), складності в адмініструванні. Часто використовується для зв'язку маршрутизаторів у глобальних мережах.

Дерево (*Tree Topology*): Ієрархічна структура, що є комбінацією кількох топологій "зірка", з'єднаних між собою сегментами, схожими на шину. Має кореневий вузол, від якого відгалужуються інші вузли та групи вузлів. Переваги: Гнучкість, масштабованість, легкість розширення.

Недоліки: Залежність від центральних сегментів, які при збої можуть ізолювати великі частини мережі.

Гібридна топологія (*Hybrid Topology*): Поєднує дві або більше різних базових топологій для створення більш складної та оптимізованої структури, що використовує переваги кожної з них.

1.1.3 Класифікація відповідно до використовуваного протоколу

Комп'ютерні мережі також класифікуються за основними протоколами, які використовуються для організації обміну даними. Протокол – це набір правил і процедур, що визначають, як дані форматуються, передаються, отримуються та інтерпретуються.

Ethernet (*IEEE* 802.3): Найпоширеніший стандарт для дротових локальних мереж (*LAN*). Використовує кадри для передачі даних і різні швидкості (*Fast Ethernet*, *Gigabit Ethernet*, 10 *Gigabit Ethernet* тощо). Забезпечує високу швидкість передачі

даних і надійність.

Wi-Fi (*IEEE* 802.11): Набір стандартів для бездротових локальних мереж (*WLAN*). Дозволяє пристроям підключатися до мережі без фізичного кабелю за допомогою радіохвиль. Має різні версії (802.11*a*/*b*/*g*/*n*/*ac*/*ax* - *Wi-Fi* 6), що відрізняються швидкістю, діапазоном та ефективністю.

Bluetooth (*IEEE* 802.15.1): Стандарт бездротового зв'язку для формування персональних мереж (*PAN*) на невеликих відстанях (до 10-100 метрів).

Використовується для підключення периферійних пристроїв, гарнітур, мобільних телефонів.

FDDI (*Fiber Distributed Data Interface*): Високошвидкісний стандарт локальних мереж, що використовує оптоволоконний кабель і топологію подвійного кільця. В основному застосовувався в корпоративних мережах до поширення *Gigabit Ethernet*.

ATM (*Asynchronous Transfer Mode*): Технологія комутації та мультиплексування, що передає дані у фіксованих за розміром комірках. Була розроблена для підтримки інтеграції голосу, відео та даних, часто використовувалася в глобальних мережах провайдерів.

TCP/*IP* (*Transmission Control Protocol*/*Internet Protocol*): Набір протоколів, що є основою функціонування Інтернету та більшості сучасних комп'ютерних мереж. *TCP* відповідає за надійну доставку даних, *IP* – за адресацію та маршрутизацію пакетів.

IPX/*SPX* (*Internetwork Packet Exchange*/*Sequenced Packet Exchange*): Застарілий набір протоколів, що використовувався в мережах *Novell NetWare*. *NetBIOS*/*NetBEUI*: Протоколи, що використовувалися в невеликих мережах *Microsoft*.

1.1.4 Система класифікації комп'ютерних мереж

Система класифікації комп'ютерних мереж є багатовимірною і дозволяє повною мірою описати будь-яку мережеву інфраструктуру, враховуючи її різні характеристики. Жодна окрема класифікація не є вичерпною; навпаки, вони доповнюють одна одну, надаючи комплексне розуміння архітектури та функціоналу мережі.

Комплексна система класифікації допомагає:

Зрозуміти призначення мережі: Залежно від географії та сфери застосування.

Оцінити продуктивність та надійність: Виходячи з топології та використовуваних протоколів.

Спланувати безпеку: Знаючи тип мережі та її уразливості.

Вибрати відповідне обладнання та технології: Виходячи з вимог до масштабу, швидкості та функціональності.

Наприклад, мережа може бути класифікована як:

Корпоративна *LAN* на базі *Ethernet* (*IEEE* 802.3) з топологією "зірка" та використанням протоколів *TCP*/*IP*.

Домашня *WLAN* (*Wi-Fi* 6, *IEEE* 802.11*ax*) з гібридною топологією та клієнт серверною взаємодією.

Така детальна класифікація є фундаментом для подальшого аналізу способів захисту комп'ютерних мереж, зокрема від специфічних загроз, таких як радіовипромінювання, що є центральною темою даної роботи. Розуміння структури та функціонування мереж дозволяє ефективно ідентифікувати потенційні вразливості та розробляти адекватні заходи захисту.

1.2 Програмно-технічні та програмні методи захисту

1.2.1 Захист комп'ютера від вірусів

Забезпечення безпеки комп'ютерних мереж та інформації, що в них циркулює, є багатогранним завданням, яке вимагає застосування комплексного підходу. Окрім загроз, пов'язаних з радіовипромінюванням, існують численні ризики, пов'язані з програмними вразливостями, несанкціонованим доступом, шкідливим програмним забезпеченням та людським фактором. Для протидії цим загрозам використовуються різноманітні програмно-технічні та програмні методи захисту, що доповнюють фізичні заходи безпеки.

Шкідливе програмне забезпечення (ШПЗ), або малваре (*malware*), до якого відносяться віруси, троянські програми, хробаки, програми-вимагачі (*ransomware*) та шпигунське ПЗ, є однією з найпоширеніших та найнебезпечніших загроз для комп'ютерних систем та мереж. Вони можуть спричиняти пошкодження даних, крадіжку інформації, порушення роботи систем та інші небажані наслідки. Захист від

вірусів та іншого ШПЗ реалізується за допомогою комплексних заходів:

Антивірусне програмне забезпечення (*Antivirus Software*): Основа захисту від ШПЗ. Сучасні антивірусні програми використовують різні методи виявлення: - Сигнатурний аналіз: порівняння файлів з базою відомих вірусних сигнатур.

- Евристичний аналіз: виявлення підозрілої поведінки програм, яка може свідчити про наявність нового або невідомого вірусу.

- Проактивний захист (поведінковий аналіз): Моніторинг активності програм у реальному часі та блокування підозрілих дій.

- Хмарні технології: використання хмарних баз даних вірусів та аналітичних сервісів для швидкого реагування на нові загрози. - Фаєрволи (*Firewalls*): мережеві екрани, що контролюють вхідний та вихідний трафік на основі встановлених правил. Хоча основна їхня функція – запобігання несанкціонованому доступу, вони також можуть блокувати спроби завантаження шкідливих файлів або зв'язок зараженого комп'ютера з командними серверами зловмисників.

- Системи виявлення та запобігання вторгненням (*IDS*/*IPS* - *Intrusion Detection*/*Prevention Systems*): моніторять мережевий трафік та системні події на предмет ознак атаки або шкідливої активності, а у випадку *IPS* можуть автоматично блокувати виявлені загрози.

- Регулярні оновлення програмного забезпечення: своєчасне встановлення оновлень операційних систем, додатків та антивірусних баз дозволяє закривати відомі вразливості, які можуть бути використані ШПЗ.

- Резервне копіювання даних: регулярне створення резервних копій критично важливої інформації дозволяє відновити дані у випадку їх пошкодження або шифрування програмами-вимагачами.

- Обізнаність користувачів: навчання персоналу правилам безпечного поводження з електронною поштою, посиланнями та завантаженнями з Інтернету значно знижує ризик зараження.

1.2.2 Запобігання несанкціонованому доступу

Несанкціонований доступ (НСД) полягає у отриманні доступу до інформаційних ресурсів, систем або мереж без належного дозволу. Це може призвести до крадіжки, спотворення або знищення даних, а також до порушення роботи системи. Запобігання НСД базується на комплексі організаційних та технічних заходів:

1) Автентифікація та авторизація:

- надійна автентифікація: використання складних паролів, багатофакторної автентифікації (*MFA*), біометричних методів.

- авторизація: надання користувачам лише тих прав доступу, які необхідні їм для виконання службових обов'язків (принцип мінімальних привілеїв). 2) Контроль доступу:

- фізичний контроль: обмеження доступу до приміщень з мережевим обладнанням.

- логічний контроль: розмежування доступу до файлів, папок, мережевих ресурсів, застосування списків контролю доступу (*ACL*).

- фаєрволи (*Firewalls*): ключовий компонент для фільтрації мережевого трафіку, блокування небажаних з'єднань та запобігання несанкціонованому доступу ззовні. Вони можуть бути програмними (на кінцевих пристроях) або апаратними (на периметрі мережі).

- системи виявлення та запобігання вторгненням (*IDS*/*IPS*): моніторинг мережевої активності на наявність спроб НСД та їх блокування. 3) Шифрування: Зашифровані дані стають нечитабельними для осіб, які не мають ключа

дешифрування, навіть у випадку несанкціонованого доступу до них. 4) Системи керування ідентифікацією та доступом (*IAM - Identity and Access Management*): Централізовані системи для управління обліковими записами, ролями та правами доступу користувачів.

5) Регулярний аудит та моніторинг: Відстеження системних журналів (логів) на предмет підозрілої активності, моніторинг доступу до критичних ресурсів.

1.2.3 Захист інформації під час віддаленого доступу

Віддалений доступ до корпоративних ресурсів стає нормою, але несе в собі значні ризики, оскільки дані передаються через потенційно незахищені публічні мережі (Інтернет). Захист інформації в таких умовах вимагає особливих підходів:

- Віртуальні приватні мережі (*VPN - Virtual Private Network*): Є основним засобом захисту віддаленого доступу. *VPN* створює зашифрований "тунель" через публічну мережу, забезпечуючи конфіденційність, цілісність та автентифікацію переданих даних. Це дозволяє користувачам працювати з корпоративними ресурсами так, ніби вони знаходяться у внутрішній мережі. (Детальніше про *VPN* буде розглянуто в інших розділах).

- *SSL*/*TLS* (*Secure Sockets Layer*/*Transport Layer Security*): Протоколи шифрування, що використовуються для захисту комунікацій між веб-браузером та веб-сервером (*HTTPS*), а також для захисту інших протоколів (наприклад, пошти, *FTP*). Забезпечують конфіденційність та цілісність даних на рівні додатків.

- Багатофакторна автентифікація (*MFA*): Обов'язкове використання *MFA* для віддаленого доступу значно підвищує безпеку, вимагаючи від користувача надати два або більше різних доказів своєї ідентичності (наприклад, пароль + код з телефону).

- Захищені шлюзи (*Secure Gateways*): Спеціалізовані пристрої або програмне забезпечення, що контролюють та захищають трафік, який проходить між внутрішньою мережею та зовнішнім світом, забезпечуючи шифрування, фаєрвол-

функції та запобігання вторгненням.

- Ізоляція та сегментація мережі: Розподіл корпоративної мережі на окремі сегменти з різними рівнями доступу. Віддалені користувачі отримують доступ лише до необхідних їм сегментів.

1.2.4 Адміністративні заходи

Адміністративні заходи є основою будь-якої системи інформаційної безпеки, оскільки вони визначають правила, процедури та відповідальність персоналу. Вони доповнюють програмно-технічні засоби та забезпечують їхнє ефективне функціонування.

Політики безпеки: Розробка та впровадження чітких політик інформаційної безпеки, що регламентують правила використання мережевих ресурсів, парольну політику, правила роботи з конфіденційною інформацією, процедури реагування на інциденти безпеки.

Навчання та підвищення обізнаності персоналу: Регулярне проведення тренінгів та інструктажів для співробітників щодо основ кібербезпеки, правил поводження з інформацією, розпізнавання фішингових атак та інших загроз. Людський фактор є однією з головних вразливостей, тому обізнаність є критичною.

Управління доступом та ролями: Чітке визначення ролей та прав доступу для кожного співробітника, регулярний перегляд та коригування цих прав відповідно до зміни посадових обов'язків.

Аудит та моніторинг: Регулярне проведення внутрішніх та зовнішніх аудитів безпеки, моніторинг системних журналів та мережевої активності для виявлення підозрілих подій та порушень політик безпеки.

Планування безперервності бізнесу та відновлення після збоїв (*BCP*/*DRP*): Розробка планів дій на випадок серйозних збоїв, кібератак або природних катастроф для забезпечення швидкого відновлення функціонування мережі та доступу до даних.

Контроль фізичного доступу: Обмеження доступу до серверних приміщень, мережевого обладнання та носіїв інформації.

1.3 Висновок до розділу 1

У першому розділі кваліфікаційної роботи було проведено всебічний аналіз комп'ютерних мереж, починаючи від їхньої сутності та основних принципів функціонування, до детальної класифікації за різними критеріями, такими як

географічне охоплення, топологія, використовувані протоколи та сфера застосування. Визначено, що комп'ютерні мережі є складною та динамічною системою, життєво необхідною для сучасного суспільства.

Особливу увагу було приділено програмно-технічним та програмним методам захисту, які є невід'ємною частиною забезпечення кібербезпеки мереж. Розглянуто основні підходи до захисту від вірусів та шкідливого програмного забезпечення, методи запобігання несанкціонованому доступу, особливості захисту інформації під час віддаленого доступу, а також важливість адміністративних заходів. Ці методи створюють базовий рівень захисту інформації на логічному та програмному рівнях.

Однак, незважаючи на ефективність розглянутих методів, виявлено, що вони не повністю покривають усі потенційні канали витоку інформації та впливу загроз. Зокрема, питання захисту від побічних електромагнітних випромінювань, яке є центральною темою даної роботи, залишається поза сферою їхнього прямого впливу. Це підкреслює необхідність подальшого дослідження та впровадження специфічних рішень, спрямованих на нейтралізацію загроз, пов'язаних з радіовипромінюванням, що буде детально розглянуто у наступних розділах роботи.

РОЗДІЛ 2
ЗАХИСТ ДАНИХ ПІД ЧАС ПЕРЕДАЧІ

2.1 Способи передачі інформації та способи її захисту

Передача інформації є фундаментальною функцією будь-якої комп'ютерної мережі. Вона здійснюється за допомогою різних фізичних середовищ та технологій, кожна з яких має свої особливості, переваги, недоліки та, що найважливіше, власні вразливості. Розуміння цих способів передачі є ключовим для розробки адекватних методів захисту.

Основні способи передачі інформації:

1) Дротова передача (*Wired Transmission*):

- Вита пара (*Twisted Pair*): Найпоширеніший тип кабелю (*UTP*, *STP*) для локальних мереж *Ethernet*. Дані передаються електричними сигналами. Способи захисту: Екранування кабелю (*STP*) для зменшення електромагнітних перешкод та випромінювань, правильне заземлення, фізичний захист кабельних трас, шифрування даних на мережевому та вищих рівнях (*VPN*, *SSL*/*TLS*).

- Оптоволоконний кабель (*Fiber Optic*): Використовує світлові імпульси для передачі даних. Забезпечує надзвичайно високу швидкість, велику відстань передачі та високу стійкість до електромагнітних перешкод.

Способи захисту: Фізичний захист кабелю (складно перехопити без розриву), шифрування даних. Захист від радіовипромінювання для оптоволокна не є актуальним, оскільки світлові сигнали не створюють електромагнітних випромінювань, що можуть бути перехоплені традиційними методами ПЕМІ.

- Коаксіальний кабель (*Coaxial Cable*): Історично використовувався в мережах *Ethernet* та кабельному телебаченні.

Способи захисту: Екранування, фізичний захист, шифрування.

2) Бездротова передача (*Wireless Transmission*):

- Радіохвилі (*Radio Waves*): Найпоширеніший спосіб бездротової передачі (*Wi-Fi*, *Bluetooth*, мобільний зв'язок). Дані передаються у вигляді електромагнітних хвиль у радіочастотному діапазоні.

Способи захисту:

· Шифрування даних: (*WEP*, *WPA*/*WPA*2/*WPA*3 для *Wi-Fi*; різні алгоритми для *Bluetooth*) – критично важливо для конфіденційності.

· Автентифікація: Контроль доступу до мережі (паролі, сертифікати, 802.1*X*).

· Зміна частот (*Frequency Hopping Spread Spectrum* - *FHSS*) та поширення спектра (*Direct Sequence Spread Spectrum* - *DSSS*): Технології, що ускладнюють перехоплення та глушіння сигналу.

· Управління потужністю передавача: Зменшення потужності до необхідного

мінімуму для обмеження зони розповсюдження сигналу. · Направлені антени: Фокусування сигналу в певному напрямку для зменшення розсіювання.

· Екранування та поглинання: Використання спеціальних матеріалів та конструкцій для приміщень, що блокують або поглинають радіовипромінювання (актуально для захисту від ПЕМІ).

- Інфрачервоне випромінювання (*Infrared*): Використовується для зв'язку на коротких відстанях (пульти ДУ, застарілі технології обміну даними між пристроями).

Способи захисту: фізичне обмеження зони дії, шифрування.

- Мікрохвильовий зв'язок (*Microwave*): використовується для зв'язку "точка-точка" на значні відстані (радіорелейні лінії).

Способи захисту: Направленість антен, шифрування.

Загальні принципи захисту даних під час передачі:

- Конфіденційність (*Confidentiality*): забезпечення того, що інформація доступна лише авторизованим особам. Основний механізм – шифрування, що перетворює дані у нечитабельний формат.

- Цілісність (*Integrity*): гарантування того, що дані не були змінені або пошкоджені під час передачі. Забезпечується за допомогою контрольних сум, хеш функцій та цифрових підписів.

- Доступність (*Availability*): забезпечення безперебійного та своєчасного доступу до інформації для авторизованих користувачів. Захист від атак типу "відмова в обслуговуванні" (*DoS*/*DDoS*), резервування каналів.

- Автентифікація (*Authentication*): підтвердження особистості користувача або пристрою, що намагається отримати доступ до мережі.

- Авторизація (*Authorization*): надання автентифікованим користувачам певних прав доступу до ресурсів.

У контексті даної роботи, особлива увага приділяється бездротовим технологіям, оскільки саме вони є джерелом та приймачем радіовипромінювань, що несуть потенційні загрози. Наступні підрозділи зосередяться на конкретній бездротовій технології – *Bluetooth*, як прикладі, що вимагає детального аналізу захисту від радіовипромінювання.

2.2 Технологія *Bluetooth* та її захист

2.2.1 Загальна характеристика та застосування *Bluetooth*

Bluetooth – це бездротова технологія короткого радіусу дії (стандарт *IEEE* 802.15.1), розроблена для створення персональних мереж (*PAN*) або так званих "пікомереж" (*piconets*). Її основне призначення – забезпечити швидкий та зручний обмін даними між різноманітними електронними пристроями без використання кабелів. Технологія оперує в неліцензованому промисловому, науковому та медичному (*ISM*) діапазоні частот – 2.400-2.4835 ГГц.

Bluetooth дозволяє підключати такі пристрої як:

- бездротові гарнітури та навушники;

- мобільні телефони та смартфони;

- ноутбуки та планшети;

- клавіатури, миші, принтери;

- розумні годинники та інші пристрої "Інтернету речей" (*IoT*); -

автомобільні системи "*hands-free*".

2.2.2 Переваги технології *Bluetooth*

Основними перевагами *Bluetooth* є:

- Бездротова зручність: усуває потребу в кабелях, спрощуючи підключення та використання пристроїв.

- Низьке енергоспоживання: особливо в режимі *Bluetooth Low Energy* (*BLE*), що робить його придатним для малопотужних пристроїв та сенсорів, що живляться від батарей.

- Глобальний стандарт: широко підтримується більшістю електронних пристроїв по всьому світу, забезпечуючи сумісність.

- Простота підключення (*Pairing*): процес встановлення з'єднання між пристроями зазвичай є інтуїтивно зрозумілим.

- Доступність (*ISM*-діапазон): використовує неліцензований радіочастотний спектр, що дозволяє виробникам впроваджувати технологію без додаткових ліцензійних витрат.

- Висока стійкість до перешкод: використовує технологію адаптивної псевдовипадкової перебудови робочої частоти (*Adaptive Frequency Hopping*, *AFH*), що дозволяє пристроям уникати зайнятих або зашумлених каналів у діапазоні 2.4 ГГц, підвищуючи надійність з'єднання.

- Компактність та інтеграція: може бути легко інтегрований у мініатюрні пристрої.

2.2.3 Недоліки технології *Bluetooth*

Основними недоліками *Bluetooth* є:

- Обмежений радіус дії: зазвичай до 10-100 метрів (залежно від класу пристрою та оточення), що обмежує його застосування для локальних зв'язків. -

Відносно низька швидкість передачі даних: Хоча версії постійно покращуються, *Bluetooth* зазвичай поступається *Wi-Fi*за пропускною здатністю для передачі великих обсягів даних.

- Безпекові вразливості: незважаючи на вбудовані механізми безпеки, історично

існували та продовжують виявлятися вразливості, пов'язані з процесами сполучення, автентифікації та шифрування. Це може призвести до несанкціонованого доступу, перехоплення даних та атак типу "відмова в обслуговуванні".

- Перешкоди від інших пристроїв: діапазон 2.4 ГГц є дуже завантаженим (*Wi-Fi*, мікрохвильові печі, інші бездротові пристрої), що може спричиняти взаємні перешкоди, незважаючи на *AFH*.

- Складність керування великими мережами: *Bluetooth* не призначений для створення великих та складних мереж. Управління кількома десятками пристроїв може бути незручним.

2.2.4 Захист *Bluetooth*: механізми безпеки

Безпека в *Bluetooth* реалізується на різних рівнях, щоб забезпечити конфіденційність, цілісність, автентифікацію та авторизацію даних. Основні механізми безпеки, що вбудовані в стандарт *Bluetooth*, включають:

- Автентифікація: перевірка ідентичності пристроїв, що намагаються встановити з'єднання. Це запобігає підключенню неавторизованих пристроїв. - Авторизація: надання певних прав доступу автентифікованим пристроям до ресурсів або сервісів.

- Шифрування: захист конфіденційності даних шляхом їх кодування перед передачею та дешифрування при отриманні.

- Цілісність даних: Ввикористання контрольних сум та криптографічних хешів для гарантування того, що дані не були змінені під час передачі.

Ці механізми працюють спільно під час різних фаз життєвого циклу з'єднання *Bluetooth* – від виявлення пристроїв до передачі даних.

2.2.5 Процес сполучення (затвердження) та автентифікація Процес сполучення (*pairing*) є фундаментальним для безпеки *Bluetooth*. Він встановлює

довірені відносини між двома пристроями, що дозволяє їм безпечно спілкуватися в майбутньому без повторної автентифікації. Існує кілька методів сполучення, які еволюціонували з версіями стандарту:

- *Legacy Pairing* (*Bluetooth* 2.0 і раніше): Зазвичай використовував *PIN*-код, який вводився на обох пристроях. Був вразливий до атак перебору (*brute-force*) для простих *PIN*-кодів.

- *Secure Simple Pairing* (*SSP*, *Bluetooth* 2.1 + *EDR* і вище): Значно покращив безпеку та зручність. *SSP* має чотири режими:

- *Just Works*: Автоматичне сполучення без введення *PIN*-коду (для пристроїв без інтерфейсу введення, наприклад, гарнітур). Надає захист від пасивного прослуховування, але вразливий до *MiTM*-атак.

- *Numeric Comparison*: Обидва пристрої відображають 6-значний код, і користувач підтверджує його збіг. Захищає від *MiTM*-атак.

- *Passkey Entry*: Користувач вводить 6-значний *PIN*-код, який відображається на одному пристрої, на іншому. Використовується для пристроїв з клавіатурою, але без дисплея.

- *Out of Band* (*OOB*): Використовує сторонній канал (наприклад, *NFC*) для обміну інформацією для сполучення, що забезпечує високий рівень безпеки та стійкість до *MiTM*-атак.

Після успішного сполучення генерується та зберігається довготривалий ключ зв'язку (*link key*). Цей ключ використовується для:

- ввтентифікації: перевірки ідентичності пристроїв при кожному подальшому підключенні без повторного сполучення;

- генерації сесійних ключів: для шифрування даних під час сесії.

2.2.6 Спосіб шифрування (кодування) даних у *Bluetooth*

Шифрування даних у *Bluetooth* забезпечує конфіденційність переданої інформації. Механізми шифрування також еволюціонували з версіями стандарту: - Шифрування в *Legacy Bluetooth*: Використовувалися потокові шифри (*E*0) з ключами довжиною до 128 біт. Однак, ранні реалізації були вразливі, особливо при коротких ключах або неправильному використанні. - Шифрування в *Bluetooth Core Specification* (з версії 2.1 + *EDR*): Використовується шифрування на основі алгоритму *AES* (*Advanced Encryption Standard*) зі 128-бітними ключами, що є значно надійнішим. Для генерації сесійних ключів використовується алгоритм, що базується на довготривалому ключі зв'язку (*link key*), отриманому під час сполучення.

Процес шифрування зазвичай включає:

- Генерація сесійного ключа: довготривалий ключ зв'язку (*link key*) та інші параметри використовуються для генерації тимчасового сесійного ключа, який діє протягом однієї сесії зв'язку.

- Шифрування пакета даних: кожен пакет даних шифрується за допомогою сесійного ключа перед передачею.

- Дешифрування: отримуючий пристрій використовує той самий сесійний ключ для дешифрування пакета.

- Шифрування у *Bluetooth* є обов'язковим для багатьох профілів і забезпечує захист від пасивного прослуховування.

2.2.7 Безпека *Bluetooth*: Вразливості та заходи протидії

Незважаючи на вбудовані механізми безпеки, технологія *Bluetooth* не є абсолютно невразливою. Існують відомі атаки та потенційні загрози: - *Bluejacking*: розсилання небажаних повідомлень на *Bluetooth*-пристрої. Не є загрозою безпеці даних, але є формою спаму.

- *Bluesnarfing*: несанкціонований доступ до даних (контакти, календар, файли)

на пристрої-жертві без її відома. Старіші пристрої були більш вразливими.

- *Bluebugging*: несанкціонований віддалений доступ до мобільного телефону через *Bluetooth*, що дозволяє здійснювати дзвінки, надсилати повідомлення та отримувати доступ до даних.

- Атаки "людина посередині" (*MiTM*): у деяких режимах сполучення (особливо "*Just Works*") або при відсутності належного підтвердження *PIN*-коду зловмисник може вклинитися в з'єднання та перехоплювати/модифікувати дані.

- Атаки перебору (*Brute-force*) на *PIN*-коди: для старих версій *Bluetooth* та простих *PIN*-кодів існує ризик їх перебору.

- Вразливості реалізації: будь-яке програмне забезпечення може містити помилки. Вразливості можуть бути виявлені в конкретних реалізаціях *Bluetooth* стеку на пристроях.

- Атаки на адаптивну перебудову частоти (*AFH*): теоретично можливі атаки, спрямовані на перешкоджання ефективній роботі *AFH*, щоб змусити пристрої використовувати вразливі або зашумлені канали.

Заходи протидії та рекомендації для підвищення безпеки *Bluetooth*: - Використання сучасних версій *Bluetooth*: віддавати перевагу пристроям з *Bluetooth* 2.1 + *EDR* (*SSP*) і вище, особливо *Bluetooth* 4.0 (*BLE*) та *Bluetooth* 5.0+, які мають значно покращені механізми безпеки (наприклад, *AES*-128 шифрування, покращені методи сполучення).

- Завжди підтверджувати сполучення: не ігнорувати запити на підтвердження *PIN*-коду або числових порівнянь під час сполучення. - Використовувати складні *Passkey*: якщо доступний режим *Passkey Entry*, використовувати складні, випадкові послідовності.

- Вимкнути *Bluetooth*, коли він не використовується: зменшує вікно для потенційних атак.

- Оновлювати прошивку пристроїв: регулярні оновлення можуть виправляти відомі вразливості в реалізації *Bluetooth*-стеку.

- Обмежити видимість пристрою: деякі пристрої дозволяють бути "невидимими" для інших пристроїв, якщо вони не перебувають у режимі сполучення.

- Уникати публічних режимів сполучення: за можливості не використовувати режим "*Just Works*" у середовищах з високим ризиком. - Використання *VPN* поверх *Bluetooth*: хоча це не прямий захист протоколу *Bluetooth*, для передачі критично важливих даних, особливо в корпоративному середовищі, можна використовувати *VPN*-з'єднання, тунельоване через *Bluetooth* з'єднання, що додасть ще один рівень шифрування та автентифікації. Аналіз цих аспектів безпеки *Bluetooth* показує, що, хоча технологія надає зручність та функціональність, її захищеність вимагає уважного налаштування та розуміння потенційних ризиків, особливо в контексті можливих побічних випромінювань та їх перехоплення.

2.3 Бездротовий доступ до Інтернет

2.3.1 Параметри безпеки маршрутизатора

Бездротовий доступ до Інтернету, що базується переважно на технології *Wi-Fi* (*IEEE* 802.11), став повсюдним та є невід'ємною частиною сучасних комп'ютерних мереж. Однак зручність бездротового зв'язку привносить і значні ризики для безпеки, оскільки дані передаються по радіоефіру і можуть бути легко перехоплені зловмисниками. Захист бездротових мереж є критично важливим завданням, що вимагає належного налаштування обладнання та використання надійних протоколів шифрування.

Бездротовий маршрутизатор (*Wi-Fi* роутер) є центральним елементом

домашньої або офісної бездротової мережі, і його правильне налаштування безпеки є першочерговим кроком до захисту всієї мережі.

Основні параметри безпеки, які необхідно конфігурувати на маршрутизаторі: - Зміна стандартних облікових даних адміністратора: перший і найважливіший крок. Більшість маршрутизаторів поставляються з типовими іменами користувачів та паролями (наприклад, *admin*/*admin*, *admin*/*password*). Їх необхідно негайно змінити на унікальні та складні комбінації.

- Вибір надійного протоколу шифрування: використання найновіших і найбезпечніших стандартів шифрування (*WPA*2 або *WPA*3) замість застарілих (*WEP*, *WPA*) є обов'язковим.

- Використання складного пароля для *Wi-Fi* мережі (*Pre-Shared Key - PSK*): пароль (ключ) доступу до бездротової мережі має бути довгим, містити комбінацію великих і малих літер, цифр та спеціальних символів.

- Вимкнення *WPS* (*Wi-Fi Protected Setup*): функція *WPS*, призначена для спрощення підключення пристроїв, має відомі вразливості, які можуть бути використані для злому пароля мережі. Рекомендується її вимкнення.

- Вимкнення віддаленого управління: доступ до налаштувань маршрутизатора ззовні локальної мережі має бути вимкнений, щоб запобігти несанкціонованій конфігурації.

- Оновлення прошивки маршрутизатора: регулярне оновлення програмного забезпечення маршрутизатора (прошивки) виправляє виявлені вразливості та покращує безпеку.

- Вимкнення широкомовлення *SSID* (*Service Set Identifier*): приховування назви мережі (*SSID*) робить її менш помітною для випадкових сканувань, хоча не є надійним методом захисту від цілеспрямованих атак.

- Фільтрація за *MAC*-адресами (*MAC Address Filtering*): дозволяє дозволяти підключення лише пристроям з певними, заздалегідь визначеними *MAC*-адресами. Цей метод не є надійним захистом, оскільки *MAC*-адреси легко підробити (спуфінг), але може створити додатковий бар'єр для випадкових зловмисників.

2.3.2 Конфіденційність, еквівалентна дротовому зв'язку (*WEP*) *WEP* (*Wired Equivalent Privacy*) був першим протоколом безпеки, розробленим для бездротових мереж *IEEE* 802.11 з метою забезпечити рівень конфіденційності, еквівалентний дротовим мережам. Він був впроваджений у 1999 році та використовував симетричний алгоритм шифрування *RC*4. Принцип роботи: *WEP* використовував статичний ключ шифрування, який вручну встановлювався на маршрутизаторі та на всіх клієнтських пристроях. Для шифрування даних до статичного ключа додавався вектор ініціалізації (*IV*), який змінювався для кожного пакета.

Недоліки та вразливості *WEP*:

- Короткий *IV*: вектор ініціалізації був занадто коротким (24 біти) і передавався у відкритому вигляді. Це призводило до швидкого повторення комбінацій ключів та дозволяло зловмисникам збирати достатньо даних для криптоаналізу.

- Статичний ключ: використання одного і того ж статичного ключа для всіх пристроїв мережі спрощувало атаку.

- Відсутність механізмів управління ключами: процес зміни ключів був ручним та незручним, тому ключі рідко змінювалися.

- Вразливість алгоритму *RC*4: виявлені слабкості в алгоритмі *RC*4 при його використанні з повторюваними ключами.

- Відсутність надійного захисту цілісності: контрольні суми були легко підроблюваними, дозволяючи зловмисникам змінювати пакети. Через ці фундаментальні вразливості, *WEP* був визнаний небезпечним і є вкрай небажаним для використання в сучасних мережах.

2.3.3 *WPA*, як перехідний етап між *WEP* та *WPA*2. *WPA* (*Wi-Fi Protected Access*)

Був представлений у 2003 році як проміжне рішення для усунення найсерйозніших недоліків *WEP* без необхідності заміни апаратного забезпечення. *WPA* покращив безпеку за рахунок використання протоколу *TKIP* (*Temporal Key*

Integrity Protocol) для динамічної зміни ключів та посилення захисту цілісності повідомлень, а також включив кращі механізми автентифікації. Однак, *TKIP* все ще містив елементи вразливого *RC*4, і хоча *WPA* був значним покращенням порівняно з *WEP*, він все ще не був повністю захищеним.

2.3.4 *Wi-Fi Protected Access* 2 (*WPA*2)

*WPA*2 (*Wi-Fi Protected Access* 2) був офіційно представлений у 2004 році (стандарт *IEEE* 802.11*i*) і став значним кроком уперед у безпеці бездротових мереж, усунувши більшість вразливостей *WEP* та *WPA*.

Основний алгоритм шифрування: *WPA*2 використовує *AES* (*Advanced Encryption Standard*) з режимом лічильника та *CBC-MAC* (*CCMP - Counter Mode with Cipher Block Chaining Message Authentication Code*) для шифрування та забезпечення цілісності даних. *AES* є набагато надійнішим криптографічним алгоритмом порівняно з *RC*4.

Динамічні ключі: Для кожної сесії та кожного пакету використовуються унікальні ключі, що значно ускладнює криптоаналіз.

Захист цілісності: *CCMP* забезпечує надійний захист цілісності даних, запобігаючи модифікації пакетів зловмисниками.

Режими роботи *WPA*2:

- *WPA*2-*Personal* (*WPA*2-*PSK*): Використовується для домашніх та малих офісних мереж. Для автентифікації використовується один загальний попередньо узгоджений ключ (*Pre-Shared Key - PSK*), який вводиться вручну на кожному пристрої.

- *WPA*2-*Enterprise* (*WPA*2-802.1*X*): Призначений для корпоративних мереж. Вимагає використання сервера автентифікації (*RADIUS*-сервера) для централізованої автентифікації користувачів за логінами, паролями або сертифікатами. Це значно підвищує безпеку, оскільки кожен користувач має унікальні облікові дані.

Незважаючи на те, що у 2017 році в *WPA*2 була виявлена вразливість *KRACK* (*Key Reinstallation Attack*), яка дозволяла перехоплювати дані під час встановлення

з'єднання, вона була виправлена виробниками через оновлення прошивок, і *WPA*2 залишається надійним протоколом безпеки за умови своєчасних оновлень.

2.3.5 Захищений доступ *Wi-Fi* 3 (*WPA*3)

*WPA*3 (*Wi-Fi Protected Access* 3) є новітнім стандартом безпеки для бездротових мереж, представленим у 2018 році, який покликаний замінити *WPA*2 і надати ще вищий рівень захисту, особливо в умовах зростання кількості *IoT* пристроїв та публічних *Wi-Fi* мереж.

Основні покращення *WPA*3:

- *SAE* (*Simultaneous Authentication of Equals*): замість *PSK* у *WPA*3-*Personal* використовується протокол обміну ключами *SAE*, який забезпечує кращий захист від атак грубої сили (*brute-force*) на паролі та відключає їх перехоплення в офлайн режимі. *SAE* гарантує "форвардну секретність" (*forward secrecy*), що означає, що навіть якщо хакер отримає ключ сесії, він не зможе розшифрувати попередній трафік.

- Покращений захист у публічних мережах (*Enhanced Open*): у публічних незапаролених мережах *WPA*3 забезпечує індивідуальне шифрування трафіку між пристроєм та точкою доступу за допомогою *Opportunistic Wireless Encryption* (*OWE*). Це захищає від пасивного прослуховування, навіть якщо мережа не вимагає пароля.

- 192-бітове шифрування (*Suite B Cryptography*): для *WPA*3-*Enterprise* передбачається використання 192-бітового шифрування, що відповідає найвищим стандартам безпеки, зокрема для державних та військових потреб.

- Спрощене налаштування пристроїв без дисплея: *WPA*3 спрощує підключення пристроїв без графічного інтерфейсу або клавіатури, зберігаючи при цьому високий рівень безпеки.

*WPA*3 є найбезпечнішим на сьогоднішній день протоколом для *Wi-Fi* мереж, і його впровадження є рекомендованим кроком для максимального захисту бездротового зв'язку.

2.3.6 *WPA*2 – оптимальний стандарт безпеки

*WPA*2 став де-факто стандартом безпеки для бездротових мереж протягом багатьох років і залишається надійним вибором у більшості випадків, якщо *WPA*3 ще не підтримується всім обладнанням.

Таблиця 2.1 – Порівняльний аналіз *WPA* та *WPA*2

Характеристика	Стандарт	
	WPA	WPA2
Рік випуску	2003	2004
Метод шифрування	Temporal Key Integrity Protocol (TKIP)	Advanced Encryption Standard (AES)
Рівень безпеки	Вище, ніж WEP, пропонує базовий рівень безпеки	Вище, ніж WPA, пропонує підвищений рівень безпеки
Підтримка пристроїв	Може підтримувати більш старе ПО	Сумісний тільки з новішим ПО
Довжина пароля	Допускається коротший пароль	Потрібно більш довгий пароль
Використання в компаніях	Нема версії для компаній	Є версія для компаній
Необхідні обчислювальні потужності	Мінімальні	Потрібно більше потужностей

Основні причини вибору *WPA*2:

- Високий рівень безпеки: використання алгоритму шифрування *AES* та протоколу *CCMP* забезпечує значно вищий рівень захисту конфіденційності та цілісності даних порівняно з *WEP* та *WPA*. Він стійкий до більшості відомих атак.

- Широка сумісність: переважна більшість сучасних пристроїв (ноутбуки, смартфони, планшети, розумні пристрої) та бездротових маршрутизаторів підтримують *WPA*2, що робить його універсальним рішенням.

- Підтримка "*Personal*" та "*Enterprise*" режимів: гнучкість для використання як у малих мережах з попередньо узгодженим ключем, так і у великих корпоративних мережах з централізованою автентифікацією.

- Стійкість до більшості відомих криптографічних атак: незважаючи на виявлення *KRACK*, *WPA*2 залишається надійним, якщо пристрої отримують оновлення прошивки, що усувають цю вразливість.

Загалом, *WPA2* є мінімальним рекомендованим стандартом безпеки для будь якої бездротової мережі сьогодні, забезпечуючи значний рівень захисту від несанкціонованого доступу та перехоплення даних.

2.4 Техніки злому

Успішний захист комп'ютерних мереж вимагає глибокого розуміння не лише принципів їх функціонування та засобів захисту, а й методів, які використовують зловмисники для компрометації систем та доступу до інформації. Аналіз технік злому дозволяє виявити вразливості та розробити ефективні контрзаходи. Особлива увага в контексті даної роботи приділяється технікам, що стосуються бездротових мереж, оскільки їхня відкритість до радіоефіру робить їх особливо вразливими до певних видів атак.

2.4.1 Незахищені мережі

Незахищені мережі – це бездротові мережі, які не використовують жодних протоколів шифрування або автентифікації (наприклад, мережі з вимкненим *WEP*/*WPA*/*WPA2*/*WPA3*). До них також можна віднести "відкриті" громадські *Wi-Fi* точки доступу, які, хоча і є загальнодоступними, часто не забезпечують жодного захисту даних, що через них передаються.

Рисунок 2.1 – Шифрування Ключем

Принцип вразливості: у незахищеній мережі весь трафік передається у

відкритому вигляді. Будь-який зловмисник, що знаходиться в радіусі дії сигналу, може легко перехопити (прослухати) всі дані, що передаються між пристроєм користувача та точкою доступу. Це включає логіни, паролі, особисті повідомлення, конфіденційні документи та іншу чутливу інформацію.

Техніка експлуатації: для перехоплення даних достатньо використовувати прості інструменти мережевого аналізу (пакетні аналізатори, наприклад, *Wireshark*) або спеціалізовані утиліти для бездротових мереж.

Захист: єдиний ефективний захист – це відмова від використання незахищених мереж. Якщо використання такої мережі неминуче, необхідно застосовувати додаткові рівні шифрування, такі як *VPN* або *SSL*/*TLS* (*HTTPS*) для захисту конкретних сесій.

2.4.2 Ручний вибір

"Ручний вибір" або "ручне підключення" до мережі відноситься до процесу, коли користувач вручну обирає зі списку доступних бездротових мереж (*SSID*) ту, до якої він бажає підключитися. Хоча це не є технікою злому безпосередньо, цей процес може бути використаний зловмисниками для здійснення атак або введення в оману користувача.

Принцип вразливості: зловмисник може створити підроблену точку доступу (так звану "злу двійнятку" - *Evil Twin*) з *SSID*, що імітує легітимну мережу (наприклад, "*Free Wi-Fi*", "*Starbucks Wi-Fi*" або назву корпоративної мережі). Користувач, здійснюючи ручний вибір, може помилково підключитися до цієї підробленої мережі.

Техніка експлуатації: після підключення користувача до "злісної двійнятки", зловмисник отримує можливість перехоплювати весь трафік, перенаправляти користувача на фішингові сайти, збирати облікові дані або впроваджувати шкідливе ПЗ.

Захист: завжди перевіряйте легітимність точки доступу (наприклад, уточнюйте назву у адміністратора або персоналу закладу). Віддавайте перевагу

мережам із надійним шифруванням (*WPA*2/*WPA*3) та використовуйте *VPN* для захисту даних у публічних мережах.

2.4.3 Брутфорс (*Brute-force*)

Атака "брутфорс" (груба сила) – це метод злому паролів, який полягає у систематичному переборі всіх можливих комбінацій символів до тих пір, поки не буде знайдено правильний пароль. Ця техніка є універсальною і застосовується для зламу паролів до *Wi-Fi* мереж, облікових записів, файлів тощо.

Принцип вразливості: залежить від слабкості або відсутності механізмів захисту від багаторазових спроб входу (наприклад, блокування облікового запису після кількох невдалих спроб). Для *Wi-Fi* мереж, особливо тих, що використовують *WPA*/*WPA*2-*PSK*, атака може бути проведена в офлайн-режимі після перехоплення "рукостискання" (див. 2.4.4).

Техніка експлуатації: використовуються спеціалізовані програми (наприклад, *Aircrack-ng* для *Wi-Fi*), які автоматизують перебір паролів. Ефективність атаки значно зростає при використанні словників паролів або при слабких, коротких паролях.

Захист: використання довгих та складних паролів (12+ символів, комбінації літер, цифр, спецсимволів). Для *WPA*3-*Personal* протокол *SAE* значно ускладнює офлайн-атаки перебору. Використання *WPA*2-*Enterprise* з 802.1*X* або *WPA*3-*Enterprise* є найкращим захистом.

2.4.4 Перехоплення «рукостискання» (*Handshake Interception*) Перехоплення "рукостискання" є однією з основних технік для зламу паролів *WPA*/*WPA*2-*PSK* мереж. "Рукостискання" (4-*way handshake*) – це послідовність обміну пакетами між клієнтом і точкою доступу під час автентифікації, що використовується для генерації сесійного ключа.

Принцип вразливості: Хоча сам ключ *PSK* не передається у відкритому вигляді, інформація, що передається під час "рукостискання", містить достатньо даних для того, щоб зловмисник міг спробувати відновити *PSK*, використовуючи

атаки брутфорс або словникові атаки в офлайн-режимі. Зловмисник не потребує активного втручання; достатньо пасивного прослуховування.

Техніка експлуатації: Зловмисник використовує бездротовий адаптер у режимі моніторингу та спеціалізоване програмне забезпечення (наприклад, *Aircrack-ng*) для:

1) Виявлення цільової *Wi-Fi* мережі та активного клієнта.

2) Надсилання "де-автентифікаційних" пакетів клієнту, щоб змусити його

відключитися та повторно підключитися до мережі.

3) Перехоплення пакетів "рукостискання" під час повторної автентифікації. 4) Після перехоплення "рукостискання", *PSK* перебирається в офлайн режимі за допомогою словників або брутфорсу.

Захист: Використання складних та довгих паролів для *Wi-Fi*, які неможливо знайти у словниках або перебрати. Перехід на *WPA*3-*Personal* з протоколом *SAE*, який забезпечує стійкість до таких офлайн-атак. Для корпоративних мереж – використання *WPA*2/*WPA*3-*Enterprise* з 802.1*X*, де кожен користувач має унікальні облікові дані.

2.4.5 Код WPS (Wi-Fi Protected Setup)

WPS (*Wi-Fi Protected Setup*) – це функція, розроблена для спрощення підключення пристроїв до бездротової мережі шляхом введення короткого 8-значного *PIN*-коду, натискання кнопки на маршрутизаторі або використання *NFC*. Однак ця зручність приховує серйозну вразливість.

Принцип вразливості: *PIN*-код *WPS* складається з 8 цифр, але фактично перевіряється по частинах: перші 4 цифри та останні 3 (восьма є контрольною сумою). Це означає, що замість 10^8(100 мільйонів) можливих комбінацій, зловмиснику потрібно перебрати лише 10^4(10 тисяч) для першої половини та 10^3 (тисячу) для другої, що значно скорочує час атаки.

Техніка експлуатації: Спеціалізовані інструменти (наприклад, *Reaver*) можуть автоматизувати цей процес, дозволяючи зловмиснику зламати *PIN*-код

WPS протягом кількох годин (іноді хвилин) і, як наслідок, отримати доступ до *PSK* мережі.

Захист: Категорично рекомендується вимикати функцію *WPS* на бездротовому маршрутизаторі, якщо вона не використовується, або якщо її використання не є критично необхідним. Багато сучасних маршрутизаторів дозволяють це зробити через веб-інтерфейс налаштування.

2.4.6 Шахрайство з персональними даними (Фішинг/Соціальна інженерія)

Шахрайство з персональними даними, або фішинг, є методом соціальної

інженерії, спрямованим на виманювання конфіденційної інформації (логінів, паролів, даних кредитних карток) у довірливих користувачів. Ця техніка не є чисто технічним зломом, але часто використовується у комбінації з іншими атаками.

Принцип вразливості: Людський фактор – довіра, необізнаність, стрес, бажання допомогти. Зловмисники експлуатують психологічні аспекти, а не технічні вразливості.

Техніка експлуатації:

- Фішингові електронні листи: надсилання підроблених листів, що імітують відомі компанії, банки або сервіси, з посиланнями на фальшиві веб-сайти, де користувач вводить свої дані.

- "Злі двійнятки" *Wi-Fi*: (як згадано в 2.4.2) створення підроблених точок доступу, які перенаправляють користувача на фейкову сторінку входу в систему або збирають дані.

- Голосовий фішинг (*Vishing*) та *SMS*-фішинг (*Smishing*): спроби виманити інформацію через телефонні дзвінки або текстові повідомлення. Захист:

- Навчання та підвищення обізнаності користувачів: навчання персоналу розпізнавати ознаки фішингу.

- Багатофакторна автентифікація (*MFA*): значно ускладнює використання викрадених облікових даних.

- Антивірусне ПЗ та фільтри спаму: допомагають блокувати фішингові листи та шкідливі посилання.

- Особиста обережність: завжди перевіряти *URL*-адреси, відправників листів та не вводити конфіденційні дані на сумнівних сайтах.

-

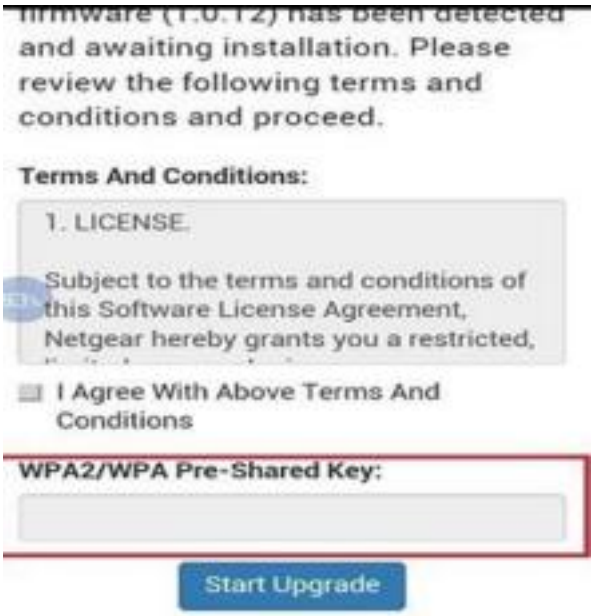

Рисунок. 2.3 – Приклад повідомлення про повторне введення пароля

2.4.7 База паролів

База паролів або словники паролів використовуються в комбінації з атаками брутфорс або для словникових атак. Це набори заздалегідь підготовлених або зібраних паролів, які використовують зловмисники для швидшого підбору.

Принцип використання: Замість повного перебору всіх можливих комбінацій, що є надзвичайно ресурсоємним, атакуючий спочатку намагається використати найпоширеніші паролі, слова зі словника, а також раніше скомпрометовані паролі, які публікуються у великих базах даних.

Техніка експлуатації: Після перехоплення хешованих паролів (наприклад, "рукостискання" *WPA2-PSK*) або отримання доступу до бази даних хешів, атакуючий використовує програми для "розшифровки" (крекінгу) цих хешів, порівнюючи їх з хешами слів зі словника або згенерованими хешами поширених паролів.

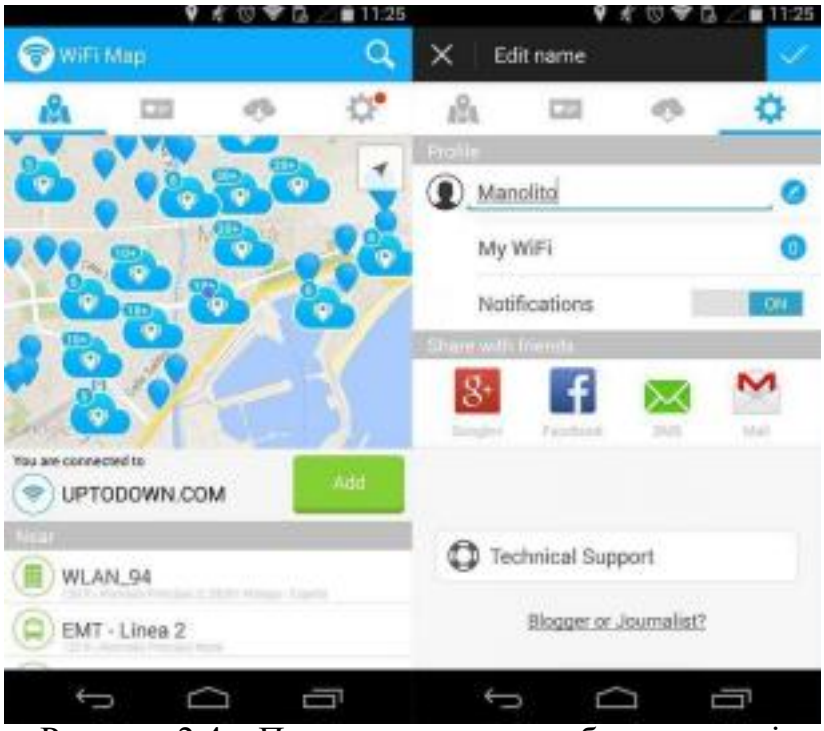

Рисунок 2.4 – Приклад програми з базою паролів

Захист: використання унікальних, складних та довгих паролів, які не є словами зі словників, поширеними фразами або особистою інформацією. Регулярна зміна паролів. Використання *WPA3-Personal*, який забезпечує кращий захист від офлайн-атак зі словниками.

2.4.8 Злом роутерів

Злом роутерів (маршрутизаторів) – це компрометація самого мережевого пристрою, що дозволяє зловмиснику отримати повний контроль над ним та всією мережею, яку він обслуговує.

Принцип вразливості:

- Стандартні/слабкі облікові дані: Використання заводських або легко підбираних імен користувачів та паролів для доступу до адміністративного інтерфейсу маршрутизатора.

- Вразливості прошивки: Наявність відомих або невідомих (0-*day*) вразливостей у програмному забезпеченні маршрутизатора, які дозволяють виконувати довільний код або отримувати несанкціонований доступ.

- Відкриті порти та сервіси: Наявність відкритого доступу до інтерфейсу управління маршрутизатором ззовні локальної мережі.

Техніка експлуатації:

- Брутфорс/словникові атаки: Підбір паролів доступу до адміністративного інтерфейсу.

- Експлуатація вразливостей: Використання публічно доступних експлойтів для відомих вразливостей у прошивці маршрутизатора (наприклад, через веб-інтерфейс, *SNMP*, *Telnet*).

- Змінений *DNS*: Після зламу маршрутизатора зловмисник може змінити *DNS*-сервери, щоб перенаправляти трафік користувачів на шкідливі сайти. Захист:

- негайна зміна стандартних облікових даних адміністратора; -

регулярне оновлення прошивки маршрутизатора;

- вимкнення віддаленого управління;

- вимкнення невикористовуваних сервісів (*Telnet*, *FTP*);

- використання надійних, складних паролів.

2.4.10 Кібербезпека

Усі розглянуті техніки злому, від перехоплення радіосигналів до соціальної інженерії, підкреслюють багатогранність загроз у сучасному цифровому просторі. Кібербезпека – це не просто набір інструментів, а комплексний підхід, що включає технології, процеси та людський фактор, спрямований на захист інформаційних систем від цих загроз. Ефективна кібербезпека вимагає постійного моніторингу, своєчасного реагування на нові виклики, безперервного навчання персоналу та застосування багаторівневого захисту. Розуміння механізмів злому, описаних вище, є фундаментальною умовою для побудови надійної архітектури безпеки комп'ютерних мереж, здатної протистояти як відомим, так і новим кіберзагрозам, включаючи ті, що пов'язані з радіовипромінюванням.

2.5 Висновок до розділу 2

У другому розділі кваліфікаційної роботи було детально проаналізовано різноманітні аспекти захисту даних під час їхньої передачі, з особливим акцентом на бездротові технології, які за своєю природою є найбільш вразливими до перехоплення через радіовипромінювання.

Спочатку було розглянуто основні способи передачі інформації – дротові та бездротові – та висвітлено специфічні методи їхнього захисту. З'ясовано, що хоча дротові мережі мають вищий ступінь фізичної захищеності від ПЕМІ, бездротові технології, такі як *Wi-Fi* та *Bluetooth*, потребують комплексних заходів безпеки для забезпечення конфіденційності, цілісності та доступності даних.

Поглиблений аналіз технології *Bluetooth* розкрив її переваги у зручності та енергоефективності, а також суттєві недоліки, пов'язані з обмеженим радіусом дії та потенційними безпековими вразливостями. Розглянуто вбудовані механізми захисту *Bluetooth*, такі як процеси сполучення та шифрування, а також описано типові атаки ("*Bluesnarfing*", "*Bluebugging*") та методи протидії. Виявлено, що, незважаючи на вдосконалення стандарту, обізнаність користувачів та правильне налаштування є критично важливими для мінімізації ризиків.

Особлива увага була приділена бездротовому доступу до Інтернету через *Wi Fi*, з акцентом на еволюцію протоколів безпеки. Протокол *WEP* визнано абсолютно застарілим та небезпечним через його фундаментальні криптографічні вразливості. *WPA* (як проміжне рішення) та *WPA*2 (з використанням *AES* та *CCMP*) були представлені як значні покращення, що забезпечили високий рівень захисту протягом багатьох років. Найновіший стандарт *WPA*3 з протоколом *SAE* та розширеним захистом відкритих мереж позиціонується як найнадійніше рішення для сучасних бездротових мереж, усуваючи відомі недоліки попередніх версій. Важливість правильного налаштування параметрів безпеки маршрутизатора підкреслена як перший етап забезпечення захисту *Wi-Fi* мережі.

Нарешті, було розглянуто ряд поширених технік злому, включаючи експлуатацію незахищених мереж, методи "ручного вибору" (злі двійнятки),

брутфорс, перехоплення "рукостискання", атаку на *WPS*, а також методи соціальної інженерії (фішинг) та злом маршрутизаторів. Детальний опис цих технік дозволяє усвідомити багатовекторність загроз та необхідність застосування комплексних,

багаторівневих заходів кібербезпеки, що включають як технічні рішення, так і підвищення обізнаності користувачів.

Таким чином, у цьому розділі було закладено теоретичну базу для розуміння вразливостей бездротових мереж, що виникають під час передачі даних по радіоефіру, та методів їхнього захисту. Отримані знання є основою для подальшого аналізу специфічних загроз, пов'язаних з радіовипромінюванням, та розробки комплексних рішень для захисту комп'ютерних мереж.

РОЗДІЛ 3
СПОСОБИ ВЗЛОМУ МЕРЕЖІ *WI-FI*

3.1 Моніторинг мережі

Моніторинг мережі є першим етапом у більшості атак на *Wi-Fi*. Він передбачає використання спеціалізованого програмного забезпечення та бездротового адаптера, що працює в режимі моніторингу (*monitor mode*), для перехоплення та аналізу радіосигналів у певному діапазоні частот.

Якщо до комп’ютера підключено *USB*-адаптер *Wi-Fi*, **увімкніть його таким чином: Пристрої** → *USB* → **Схема** *MediaTek* 802.11 *n WLAN* (рисунок 3.1).

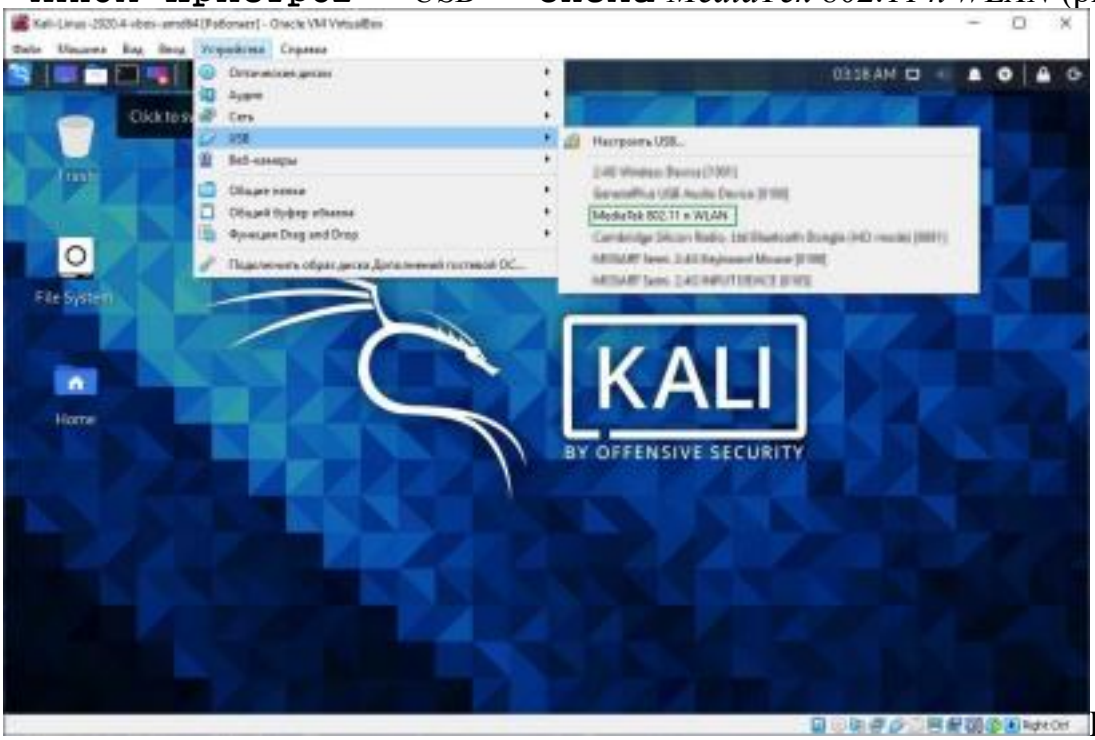

Рисунок 3.1– Бездротовий *USB*-адаптер *Wi-Fi* у *Kali Linux* у *VirtualBox*

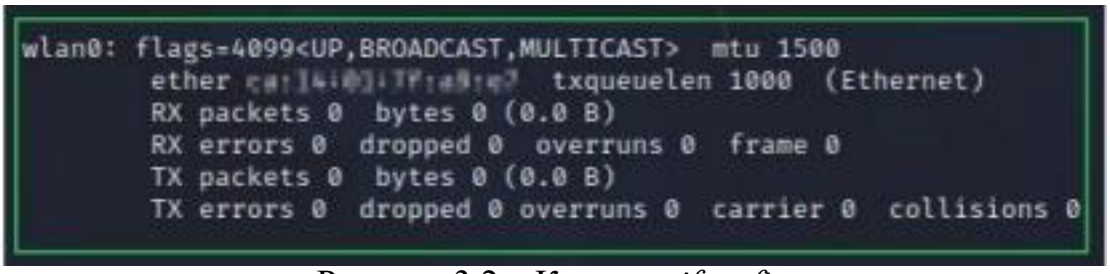

Рисунок 3.2 – Команда *ifconfig*

Щоб дізнатися назву адаптера,потрібно скористатися командою *ifconfig.* У нашому прикладі адаптер називається *w*0 (рисунок 3.2).

На рисунку 3.3 зображено команду, яка використовується для вимкнення непотрібних процесів (для подальших операцій з бездротовим адаптером).

Рисунок 3.3 – Команда *sudo airmon-ng check kill*

Потім переводимо адаптер у режим моніторингу (рисунок 3.4).

Рисунок 3.4 – Перемикання адаптера в режим моніторингу

На рисунку 3.5 показано запуск інструменту *bettercap* в операційній системі *Kali Linux*

Рисунок 3.3 – Команда *bettercap*

На рисунку 3.6 продемонстровано практичне застосування інструменту *Bettercap* у терміналі операційної системи *Kali Linux* для моніторингу доступних бездротових мереж стандарту *Wi-Fi*. Після запуску *Bettercap* з вказанням мережевого інтерфейсу *(--iface wlan0*), що є типовим для бездротового адаптера, активується режим сканування *Wi-Fi* командою *wifi.recon on.*

Рисунок 3.6 – Використання *bettercap* для моніторингу мережі *Wi-Fi* у *Kali Linux*

На рисунку 3.7 представлено розширений результат сканування та моніторингу бездротових мереж, виконаного за допомогою інструменту *Bettercap* у ОС *Kali Linux* (як продовження дій, показаних на рисунку 3.6). Зображення демонструє табличний вивід команди *wifi.show* у консолі *Bettercap*, який надає вичерпну інформацію про виявлені *Wi-Fi* мережі та підключених до них клієнтів.

Рисунок 3.7 – Перегляд виявлених *Wi-Fi* мереж за допомогою *bettercap*

Принцип роботи: У звичайному режимі бездротовий адаптер приймає лише ті

пакети, які адресовані йому. У режимі моніторингу він перехоплює всі пакети, що передаються в радіусі його дії, незалежно від адресата. Це дозволяє зловмиснику "прослуховувати" весь трафік у бездротовому середовищі.

Найпоширеніші інструменти для моніторингу *Wi-Fi* мереж:

- *Airmon-ng*: частина пакету *Aircrack-ng*, використовується для переведення бездротового адаптера в режим моніторингу.

- *Wireshark*: потужний мережевий аналізатор, що дозволяє переглядати та аналізувати перехоплені пакети.

- *Kismet*: інструмент для виявлення та моніторингу бездротових мереж, може відображати інформацію про *SSID*, канали, протоколи безпеки та клієнтів.

Інформація, отримана під час моніторингу, використовується для: - виявлення цільових мереж (*SSID*).

- визначення використовуваного протоколу безпеки (*WEP*, *WPA*/*WPA*2/*WPA*3).

- ідентифікації активних клієнтів.

- перехоплення "рукостискання" (4-*way handshake*) для подальшого зламу пароля.

3.2 Прийняти рукостискання

"Прийняти рукостискання" (*capture the handshake*) – це ключовий етап для зламу паролів *WPA*/*WPA*2-*PSK* мереж. Як було описано в попередньому розділі, "рукостискання" – це процес обміну чотирма пакетами (4-*way handshake*) між клієнтом та точкою доступу під час встановлення з'єднання. Ці пакети містять інформацію, необхідну для генерації сесійного ключа.

Принцип роботи: зловмисник використовує бездротовий адаптер у режимі моніторингу та спеціалізоване програмне забезпечення (наприклад, *Aircrack-ng*) для перехоплення цих чотирьох пакетів.

Методи перехоплення "рукостискання":

- Пасивне очікування: зловмисник просто чекає, поки клієнт підключиться або перепідключиться до мережі. Це може зайняти багато часу. - Деаутентифікація (*Deauthentication attack*): найпоширеніший метод. Зловмисник надсилає пакети деаутентифікації клієнту, щоб змусити його відключитися від мережі. При наступному підключенні клієнта до мережі, відбувається обмін пакетами "рукостискання", які зловмисник перехоплює. Інструменти:

- *Aircrack-ng*: найпопулярніший пакет інструментів для зламу *Wi-Fi*. Включає утиліти для моніторингу (*airmon-ng*), перехоплення пакетів (*airodump-ng*) та зламу паролів (*aircrack-ng*).

- *Reaver*: інструмент для зламу *WPS* (див. 3.5), але також може використовуватися для перехоплення "рукостискання".

Вибираємо мету - точку доступу *NX*531*J*. Давайте спробуємо провести рукостискання між точкою доступу *NX*531*J* і підключеним до неї пристроєм. Чекаємо відключення клієнта і потім підключаємося, або використовуємо команду деаутентифікації для примусового відключення: *wifi.deauth MAC*-адреса точки доступу

Адреса – унікальний ідентифікатор мережевого пристрою. Його значення береться зі стовпця *BSSID*. У нашому випадку: *wifi.deauth* 90:*c*7:*aa*:*bb*:*cc*:*dd*. Ми повторюємо цю команду, поки не перехопимо рукостискання. *wifi.deauth* * і *wifi.deauth* вимикають усі пристрої на всіх точках доступу (рисунок 3.8).

Рисунок 3.8 – Використання *bettercap* для перехоплення рукостискання в *Kali Linux*

3.3 Чотиристоронє рукостискання

Чотиристоронне рукостискання — це механізм для створення пари ключів переходу *PTK* для захисту трафіку.

Перше рукостискання: точка доступу надсилає клієнту випадковий 32-байтовий *nonce*.

Друге рукостискання: у відповідь клієнт генерує власний випадковий 32-байтовий номер *SNonce*. *ANonce*, *SNonce* та спільний *PMK* (*Pair Master Key*) утворюють *PTK* (*Pair Transition Key*). У другому повідомленні клієнт надсилає *SNonce* та *MIC* (код цілісність повідомлення) точка доступу.

Третє рукостискання: точка доступу генерує свій *PTK*, щоб перевірити значення *MIC* у другому повідомленні. Якщо все вірно, точка доступу надішле клієнту повідомлення про застосування *PTK*.

Четверте рукостискання: клієнт підтверджує за допомогою ключа *PTK*. Найголовніше рукостискання – друге. Окрім цього, потрібне перше та/або третє рукостискання. Найкращими мінімальними варіантами є друга і третя діаграми рукостискання (рисунок 3.9).

Рисунок 3.9 – Чотиристоронняя схема рукостискання між точкою доступу (*AP*) і клієнтом (*STA*)

Файли рукостискань зберігаються в /*root*/*bettercap-wifi-handshakes.pcap*.

Ми копіюємо його в домашній каталог *fig*. (рисунок 3.10)

Рисунок 3.10 – Копіювання до каталогу

Етапи 4-*way handshake*:

1) *AP* (*Access Point*) -> *Client*: *ANonce*: Точка доступу надсилає клієнту випадкове число (*ANonce*).

2) *Client -> AP*: *SNonce*, *MIC*: Клієнт генерує своє випадкове число (*SNonce*), обчислює *MIC* (*Message Integrity Code*) на основі *ANonce*, *SNonce*, *PSK* (*Pre-Shared Key*) та іншої інформації, і надсилає ці дані точці доступу.

3) *AP -> Client*: *MIC*: Точка доступу перевіряє *MIC*, обчислює свій *MIC* та надсилає його клієнту.

4) *Client -> AP*: *MIC*: Клієнт перевіряє *MIC* від точки доступу.

Після успішного завершення "рукостискання", обидва пристрої мають достатньо інформації (*ANonce*, *SNonce*, *PSK*) для генерації сесійного ключа (*PTK - Pairwise Transient Key*), який використовується для шифрування трафіку.

3.4 Вибір правильного методу рукостискання

Вибір правильного методу перехоплення "рукостискання" залежить від ситуації.

Пасивне очікування: Найпростіший метод, але може бути дуже повільним, якщо клієнт рідко перепідключається до мережі.

Деаутентифікація: Найефективніший метод, оскільки дозволяє змусити клієнта перепідключитися негайно. Однак, надсилання пакетів деаутентифікації може бути помічено адміністраторами мережі або системами виявлення вторгнень (*IDS*).

Щоб вибрати цікаві нам рукостискання та експортувати їх в окремі файли, нам потрібна програма для аналізу мережевих протоколів *WireShark*. В *Ubuntu* встановіть графік *WireShark* (рисунок 3.11).

Рисунок 3.11 – Встановлення *WireShark*

Введемо команду *wireshark* у терміналі. Відкриється програма з графічним інтерфейсом. Натисніть *Ctrl+O* і відкрийте файл рукостискання *bettercapwifi handshakes.pcap*

Відфільтруєм дані по мак-адресою *w.addr == 90: c7: aa: bb: cc: dd* і відсортуємо за часом, клікнувши по стовпцю *Time*. Також можна впорядкувати за номером *No* .. Значення *ANonce* і *SNonce* змінюються кожну сесію, тому вибираємо рукостискання, розділені невеликим часовим проміжком (десятки мілісекунд). Рукостискання з різних сесій для злому непридатні (рисунок 3.12).

Рисунок 3.12 – Перегляд рукостискання в *WireShark*

Як бачимо, ми отримали перше, друге і третє рукостискання. Давайте виберемо всі рукостискання *EAPOL*, файл із назвою мережі *SSID* (у нашому випадку це *запит на асоціацію*) і натисніть Файл → Експортувати вказаний пакет (рисунок 3.13).

Рисунок 3.13 – Експорт рукостискання в програму *WireShark*

Відкриється діалогове вікно, у якому ми вибираємо пакети та зберігаємо файл із назвою *hs.pcap fig*. (рисунок 3.14).

Рисунок 3.14 – Збереження рукостискання в *WireShark*

3.5 Отримання пароля

Після успішного перехоплення "рукостискання", зловмисник має файл (зазвичай у форматі *.cap* або *.pcap*), що містить необхідну інформацію для спроби зламу пароля *PSK*.

Методи зламу пароля:

1) Брутфорс (*Brute-force*): Перебір усіх можливих комбінацій символів. Дуже повільний та неефективний для складних паролів.

2) Словникова атака (*Dictionary attack*): Використання великих списків (словників) поширених паролів, слів та фраз. Значно швидший за брутфорс, якщо пароль є поширеним словом або фразою.

3) Атака за маскою (*Mask attack*): Комбінація брутфорсу та словникової атаки. Зловмисник визначає шаблон (маску) пароля (наприклад, "8 символів, починається з великої літери") та перебирає лише ті комбінації, що відповідають цьому шаблону.

Інструменти:

- *Aircrack-ng*: Найпопулярніший інструмент для зламу паролів *Wi-Fi*.

Використовує *CPU* та/або *GPU* для швидкого перебору.

- *Hashcat*: Потужний інструмент для зламу різних типів хешів, включаючи хеші

WPA/*WPA*2. Підтримує використання *GPU* для значного прискорення процесу.

Спочатку перетворюємо файл *hs.pcap* у файл *hs.hccapx* (рисунок 3.15).

Рисунок 3.15 – Перетворення файлу *hs.pcap* у файл *hs.hccapx*

Це потрібно для того, щоб дешифратор *hashcat* міг прочитати файл. Він використовує процесор і/або *DP* для вибору пароля (рисунок 3.16).

Рисунок 3.16 – Перетворення з *.pcap* на *.hccapx* за допомогою утиліти *hashcat*

3.6 Вибір словника

Вибір правильного словника є критично важливим для успішної словникової атаки.

Типи словників:

- Загальні словники: містять найпоширеніші паролі, слова та фрази. - Спеціалізовані словники: містять слова, пов'язані з певною тематикою (наприклад, імена, дати, спортивні терміни).

- Скомпрометовані паролі: списки паролів, які були викрадені з різних веб сайтів та сервісів.

- Створені користувачем словники: словники, створені на основі інформації про ціль (наприклад, ім'я компанії, назва вулиці, імена співробітників). Створіть або завантажте словник і розмістіть його в /*home*/*kali* або /*home*/*USERNAME* для *Ubuntu* (рисунок 3.18).

Рисунок 3.18 – Приклад словника для атаки за словником

Розшифруємо значення опцій:

- *force* - приховати помилки.

- *m2500* - тип зламуваного хешу *WPA-EAPOL-PBKDF2*.

- *a0* - атака по словнику. Можна без цього прапора, так як він працює за замовчуванням.

- */home/kali/hs.hccapx* - файл хешу.

- */home/kali/dic.txt* - словник.

У разі успіху статус злому прийме значення *Cracked* і ми отримаємо пароль (рисунок 3.19).

Рисунок 3.19 – Успішний злом пароля атакою по словнику за допомогою утиліти *hashcat*

Рекомендації:

- Використовуйте декілька словників, комбінуючи загальні та спеціалізовані.

- Спробуйте створити власний словник на основі інформації про ціль. - Використовуйте інструменти для генерації варіацій паролів (наприклад, додавання цифр, символів, зміна регістру).

3.7 Атаки грубою силою та маскою

Атака грубою силою (*Brute-force attack*): перебір усіх можливих комбінацій символів. Надзвичайно повільний та неефективний для складних паролів. Використовується лише тоді, коли немає іншої альтернативи.

Атака за маскою (*Mask attack*): значно ефективніша за брутфорс, якщо відома структура пароля (наприклад, "8 символів, починається з великої літери"). Зловмисник визначає шаблон (маску) пароля та перебирає лише ті комбінації, що відповідають цьому шаблону.

Використовуючи грубу силу, шукайте всі можливі символи. За допомогою маски ми звужуємо виділені символи, наприклад, тільки цифри або тільки цифри і малі літери. Таким чином, організація займає менше часу. Цей підхід зручний, якщо ми маємо приблизне уявлення про те, як людина винайшла шифр. Ви можете застосувати грубу силу маски, включивши всі символи в пошуковий запит.

Щоб атакувати маску, введіть наступну команду (рисунок 3.20): *? 1werty? 2? 2*- вгадайте паролі з невідомими символами.

У цьому випадку завдання спрощуються для економії часу (рисунок 3.20).

Рисунок 3.20 – Атака по масці

Значення опцій:

- *m2500* - тип зламувати хешу. *WPA-EAPOL-PBKDF2*.

- *a3* - атака по масці.

- *1? L* - маска з прописних латинськими літерами (прописна буква L). -

2? D - маска по цифрам.

- *hs.hccapx* - файл хешу.

- *? 1werty? 2? 2* - передбачуваний пароль з невідомими символами. В даному випадку завдання полегшене для економії часу (рисунок 3.21).

Рисунок 3.21 – Успішний злом пароля атакою по масці за допомогою утиліти *hashcat*

Таблиця 3.1 – Словники

?	**СИМВОЛИ**
l (прописна буква *L*)	*abcdefghijklmnopqrstuvwxyz*
u	*ABCDEFGHIJKLMNOPQRSTUVWXYZ*
d	*0123456789*
h	*0123456789abcdef*
H	*0123456789ABCDEF*
s	*!"#$%&'()*+,-./:;<=>?@[\]^_`{|}~*
a	*?l?u?d?s*
b	*0x00 – 0xff*

Рисунок 3.22 – Обчислення за допомогою графічної карти

На рисунку 3.22 показано команду *hashcat* з усіма переліченими вище опціями: *hashcat; -D2; -m2500; -a3; -1?L; -2?d; hs.hccapx; ?1werty?2?2?. -D2*: вказує *hashcat* використовувати графічний процесор (*GPU)* для обчислень, оскільки це значно швидше, ніж використання ЦП (*CPU*) для таких завдань.

Таблиця 3.2 уточнює, яке обладнання може бути використано для злому.

Таблиця 3.2 – Типи обчислювального обладнання для проведення атак

№	Обладнання
1	ЦП
2	*DP*
3	*FPGA*, *DSP*, співпроцесор

У комбінаторної атаці використовуються два словника. Слова з двох словників конкатенуються. Якщо словники містять такі слова: *HAY*

Human

3845

!

то після їх з'єднання отримаємо такий словник:

HAYHAY

HAYHuman

Hello3845

HAY!

HumanHAY

HumanHuman

Human3845

Human!

3845HAY

Запуск комбінаторної атаки зображено на рисунку 3.23.

Рисунок 3.23 – Запуск комбінаторної атаки

Рисунок 3.24 – Успішний злом пароля за допомогою утиліти *hashcat*

3.8 Зберігання паролів

У контексті *Wi-Fi*, пароль (*PSK*) зберігається в точці доступу (маршрутизаторі) у зашифрованому вигляді. Коли клієнт підключається до мережі, він також зберігає пароль (або його хеш) у своєму операційній системі або менеджері бездротових

мереж.

Зберігання на клієнті:

- ***Windows*:** Паролі зберігаються у зашифрованому вигляді в реєстрі. - ***Linux*:** Паролі можуть зберігатися в різних місцях, залежно від використовуваного менеджера мереж (наприклад, *NetworkManager*). - ***Android*:** Паролі зберігаються у файлі /*data*/*misc*/*wifi*/*wpa_supplicant.conf*, але для доступу до нього потрібні права *root*.

Зберігання на точці доступу: пароль (*PSK*) зазвичай зберігається у вигляді хешу. Маршрутизатори використовують різні алгоритми хешування, але часто це варіації *SHA*256.

3.9 Онлайн-сервіс дешифрування хешу

Існують онлайн-сервіси, які пропонують послуги з "розшифровки" (крекінгу) хешів паролів. Вони використовують великі бази даних попередньо обчислених хешів (райдужні таблиці) та розподілені обчислення для прискорення процесу.

Рисунок 3.25 – Результати злому паролів за допомогою сервісу *onlinehashcrack.com*

Платформа *passcrack.online* отримала пароль протягом 5 хвилин (рисунок 3.25). Найкраще починати розшифровку з відправки на онлайн-сервіс, так як вони мають

більше обчислювальних ресурсів, ніж домашній комп’ютер.

Рисунок 3.26 – Результати злому паролів за допомогою сервісу *passcrack.online*

Ефективність: ефективність цих сервісів залежить від складності пароля та розміру їхньої бази даних. Для простих паролів вони можуть бути досить швидкими, але для складних паролів вони часто неефективні.

Ризики: використання цих сервісів пов'язане з ризиком витоку інформації, оскільки ви завантажуєте хеш пароля на сторонній сервер.

3.10 Різниця між *WPA*2 і *WPA*3

Як було детально описано у попередньому розділі, *WPA*3 є значним покращенням у порівнянні з *WPA*2. Основні відмінності, що впливають на безпеку: - Автентифікація: *WPA*3-*Personal* використовує протокол *SAE* (*Simultaneous Authentication of Equals*) замість *PSK*, що забезпечує кращий захист від атак перебору та відключає їх перехоплення в офлайн-режимі. - Шифрування: *WPA*3-*Enterprise* передбачає використання 192-бітового шифрування, що відповідає найвищим стандартам безпеки.

- Захист у публічних мережах: *WPA*3 забезпечує індивідуальне шифрування трафіку в відкритих мережах за допомогою *OWE* (*Opportunistic Wireless Encryption*).

У контексті злому, *WPA*3 значно ускладнює більшість атак, описаних у цьому розділі, особливо атаки на паролі.

3.11 Висновок до розділу 3

У третьому розділі кваліфікаційної роботи було детально розглянуто ключові техніки та методології, які застосовуються для компрометації бездротових мереж *Wi-Fi*. Аналіз цих способів злому є фундаментальним для розробки ефективних стратегій захисту.

Було висвітлено початковий етап будь-якої атаки – моніторинг мережі, що дозволяє зловмиснику "прослуховувати" радіоефір та збирати інформацію про цільові мережі. Підкреслена важливість перехоплення "рукостискання" (4-*way handshake*) як критичного кроку для подальшого зламу *WPA*/*WPA*2-*PSK* паролів, а також способи прискорення цього процесу за допомогою деаутентифікаційних атак.

Описані основні підходи до отримання паролів після перехоплення "рукостискання": словникові атаки, атаки грубою силою та атаки за маскою. Показано, що ефективність цих атак прямо залежить від складності пароля та

доступності якісних словників або обчислювальних ресурсів. Особливо наголошено на вразливості функції *WPS*, яка, незважаючи на свою зручність, є значною безпековою "дірою", що дозволяє відносно швидко зламати пароль мережі.

Також розглянуто місця зберігання паролів на клієнтських пристроях та маршрутизаторах, а також потенційні ризики, пов'язані з використанням онлайн сервісів дешифрування хешу.

Підкреслена фундаментальна різниця між *WPA*2 та *WPA*3, яка полягає в архітектурних змінах, що роблять *WPA*3 значно стійкішим до більшості розглянутих атак перебору, забезпечуючи "форвардну секретність" та покращений захист навіть у відкритих мережах.

Загалом, цей розділ демонструє, що, хоча бездротові мережі надають значну зручність, їхня відкритість до радіоефіру робить їх постійною мішенню для зловмисників. Розуміння конкретних векторів атак, таких як перехоплення "рукостискання" або експлуатація *WPS*, є необхідним для усвідомленого вибору та правильного налаштування протоколів безпеки. Отримані знання є ключовими для розробки ефективних контрзаходів та підвищення загального рівня кібербезпеки комп'ютерних мереж, що передають дані по радіоканалу.

ВИСНОВКИ

У сучасну епоху інформаційних технологій комп'ютерні мережі є невід'ємною основою функціонування будь-якого підприємства, організації чи домашнього господарства. Їхня зростаюча складність та повсюдне впровадження бездротових технологій, таких як *Wi-Fi* та *Bluetooth*, приносять значні зручності, але водночас породжують нові, комплексні виклики у сфері інформаційної безпеки. Дана кваліфікаційна робота була присвячена аналізу захищених від радіовипромінювання комп’ютерних мереж, досліджуючи як загальні принципи захисту, так і специфічні загрози, пов'язані з передачею даних по радіоефіру.

У першому розділі було окреслено фундаментальні концепції комп'ютерних мереж та закладено базис розуміння програмно-технічних та програмних методів захисту. Було показано, що антивірусний захист, запобігання несанкціонованому доступу, захист віддаленого доступу та адміністративні заходи формують початковий, але критично важливий рівень безпеки. Однак, було наголошено, що ці заходи не охоплюють всього спектру загроз, зокрема тих, що виникають через побічні електромагнітні випромінювання.

Другий розділ заглибився в аналіз захисту даних під час передачі, зосередившись на бездротових технологіях. Детальне дослідження *Bluetooth* виявило його вразливості, пов'язані з процесами сполучення та шифрування, що потребують уважного налаштування та обізнаності користувачів. Аналіз розвитку стандартів безпеки *Wi-Fi* (від *WEP* до *WPA*3) чітко продемонстрував еволюцію підходів до шифрування та автентифікації. Було підкреслено, що перехід на *WPA*2 і особливо на *WPA*3 є життєво необхідним для забезпечення надійного захисту бездротових мереж від перехоплення даних по радіоканалу.

Третій розділ проілюстрував практичні аспекти злому *Wi-Fi* мереж, демонструючи, як зловмисники експлуатують вразливості радіоефіру та протоколів безпеки. Описані техніки моніторингу мережі, перехоплення "рукостискання" *WPA*/*WPA*2, атаки брутфорс, словникові атаки та атаки на *WPS*

функціонал, а також методи соціальної інженерії, які дозволяють отримати доступ до

мережі та конфіденційних даних. Розуміння цих загроз є ключовим для імплементації ефективних контрзаходів.

На основі проведеного аналізу можна зробити наступні ключові висновки: Універсальність загроз: Сучасні комп'ютерні мережі стикаються з широким спектром загроз, що охоплюють програмні вразливості, людський фактор та, що особливо важливо для цієї роботи, специфічні ризики, пов'язані з радіовипромінюванням.

Важливість багаторівневого захисту: Жоден окремий метод захисту не є достатнім. Ефективна безпека вимагає комплексного, багаторівневого підходу, що поєднує надійні програмні рішення, актуальні криптографічні протоколи та строгі адміністративні заходи.

Критична роль оновлення стандартів: Еволюція стандартів безпеки бездротових мереж (від *WEP* до *WPA*3) є прямою відповіддю на виявлені вразливості. Застосування найновіших протоколів (особливо *WPA*3) є обов'язковою умовою для забезпечення високого рівня захисту даних у радіоефірі.

Усвідомлення ризиків радіовипромінювання: Бездротові мережі за своєю природою передають інформацію через відкритий радіоканал, роблячи її доступною для перехоплення зловмисниками. Це вимагає не лише шифрування на програмному рівні, а й врахування фізичних аспектів захисту від побічних електромагнітних випромінювань, що є подальшим напрямком для поглиблених досліджень та практичних реалізацій.

Людський фактор як слабка ланка: Обізнаність користувачів щодо потенційних загроз та дотримання базових правил кібергігієни (складні паролі, обережність з фішингом, вимкнення невикористовуваних функцій на кшталт *WPS*) є настільки ж важливим, як і технічні засоби захисту.

Таким чином, для забезпечення дійсно захищеної комп'ютерної мережі, особливо тієї, що працює з бездротовим зв'язком, необхідно постійно адаптуватися до нових загроз, впроваджувати найсучасніші технології захисту та пам'ятати, що безпека – це безперервний процес, а не одноразова дія.

Обрано варіант топології комп'юторної мережі типу Зірка. Так як вихід з ладу одного з підконтрольних об'єктів не спричинить критичних пошкоджень всій системі в цілому. Передача даних буде відбуватися за протоколом *TCP / IP* як найбільш розповсюджений.

В залежності від об'єкту мережа буде коливатися від до *WAN.* Наприклад взявши такі об'єкти як побутові комплектуючі з підтримкою технології *IoT*: холодильник, жалюзі, сітильники, магнітофон які можна віднести до системи, адже вони икористовуються в межах будинку чи двору. Чи наприклад машину яка їздить по місту *WAN.* З розвитком технологій навіть літак зможе икористовувати дану технологію, але вона потребує ще дуже великого допрацювання.

Підвівши підсумки, для створення максимально безпечної мережі потрібно використовувати протокол *WPA2.* Якщо користувач сам всановлює пароль то потрібно вводити пароль максимально довгим та використвовути спеціальні символи. Пароль не повинен мати якихось простих асоціацій. Найкращим вибором буде ряд випадкових символів. Застосувавши такий метод зловмиснику буде неможливо взламати/підібрати пароль. Так як викиристовуючи такий метод можна в середньому підбирати 5 000 паролів в секунду. На перший погляд це велика цифра. Але взявши вибірку із 80 символів доступних на клавіатурі та взявши пароль із 16 символів. Отримаємо 564 041 196 467 871 540 000 000 000 000

комбінацій паролів. І щоб підібрати пароль знадобиться 3 577 125 802 053 979 832 років. Тобто встановивши с самого початку складний пароль ви вже зможете забезбечити безпеку своєї мережі. Швидкість перебору можна звісно збільшити і до 15 000. Це залежить від способу, що саме взламують, та від самого пристрою. Також можна збільшити кількість пристроїв які будуть виконувати цю операцію. Але все одно час все для підбору залишається таким же захмарним.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Болілий В.О. Комп'ютерні мережі : навчальний посібник / В.О. Болілий,

В.В. Котяк. – Кіровоград : ЦОП Авангард, 2008. – 146 с.

2. *Dixon J. Monitoring with Graphite*: *Tracking Dynamic Host and Application Metrics at Scale* / *Jason Dixon*. – *Sebastopol*, *CA* : *O'Reilly Media*, 2014. – 170 с. 3. Жуков І.А. Основи теорії мереж передачі та розподілу даних : навчальний посібник / І.А. Жуков, М.А. Віноградов, В.І. Дрововозов, Н.Ф. Халімон. – Київ, 2006. – 270 с.

4. *Nagios* : *[*Електронний ресурс*]* – Режим доступу до ресурсу: *https://www.nagios.com/* (Дата звернення: 23.05.2025). – Назва з екрану. 5. *Nagios* : *Solutions* / *Server Monitoring* : *[*Електронний ресурс*]* – Режим доступу до ресурсу: *https://www.nagios.com/solutions/server-monitoring/* (Дата звернення: 24.05.2025). – Назва з екрану.

6. *P2P* архітектура : *[*Електронний ресурс*]* // Вікіпедія. – Режим доступу до ресурсу: *https://uk.wikipedia.org/wiki/Peer-to-peer* (Дата звернення: 27.05.2023). – Назва з екрану.

7. *Parasam S. Kali Linux* 2018: *Assuring Security by Penetration Testing* / *S. Parasam*, *A. Samm*, *T. Heriyanto*, *S. Ali*, *D. Budu*, *D. Johansen*, *L. Allen*. – *Birmingham*, *UK* : *Packt Publishing*, 2018. – 448 с.

8. *PostgreSQL* : *[*Електронний ресурс*]* – Режим доступу до ресурсу: *https://www.postgresql.org/* (Дата звернення: 28.05.2025). – Назва з екрану. 9. *Prometheus* : *[*Електронний ресурс*]* – Режим доступу до ресурсу: *https://prometheus.io/* (Дата звернення: 23.05.2025). – Назва з екрану. 10. *Python* : *[*Електронний ресурс*]* // Вікіпедія. – Режим доступу до ресурсу: *https://uk.wikipedia.org/wiki/Python* (Дата звернення: 25.05.2025). – Назва з екрану. 11. Стандарт *IEEE*: *Bluetooth*, *Zigbee*, *Wi-Fi* : *[*Електронний ресурс*]* // *Finestreet*. – Режим доступу до ресурсу: *http://www.wirelesse.ru/articles/ technologies.php* (Дата звернення: 14.05.2025).

12. *Turnbull J. The Art of Monitoring* / *James Turnbull*. – *Sebastopol*, *CA* : *O'Reilly Media*, 2014. – 250 с.

13. *Brazil B. Monitoring with Prometheus*: *Effective Monitoring and Alerting Practices for DevOps* / *Brian Brazil*. – *Sebastopol*, *CA* : *O'Reilly Media*, 2018. – 300 с.

КРИВОРІЗЬКИЙ ФАХОВИЙ КОЛЕДЖ
Державного некомерційного підприємства
«Державний університет «Київський авіаційний інститут»

РЕЦЕНЗІЯ
на кваліфікаційну роботу
випускника спеціальності 123 Комп'ютерна інженерія
факультет/відділення «Комп'ютерної і програмна інженерія»
Михайла ЗАЛІЗНЯКА
(Ім`я, ПРІЗВИЩЕ)

Кваліфікаційна робота на тему «Підвищення ефективності та надійності бездротової мережі підприємства шляхом модернізації» присвячена надзвичайно актуальному та комплексному питанню у сфері інформаційної безпеки. В умовах постійного розвитку кіберзагроз та зростаючої складності мережевих інфраструктур, ефективна організація процесу захисту є визначальним фактором для забезпечення стабільності та безпеки будь-якої організації.

Актуальність теми роботи не викликає сумнівів. Сучасні комп'ютерні мережі є критично важливою інфраструктурою, і їхній захист вимагає не лише впровадження окремих технологій, а й чітко організованого, системного підходу, що базується на визначених стандартах та специфікаціях. Робота, що фокусується на саме цій "організації процесу", є вкрай важливою для підготовки фахівців, здатних будувати стійкі та безпечні мережеві рішення.

Змістовність та глибина дослідження:

Робота демонструє системний та всебічний підхід до вивчення поставленої теми. У ній якісно розкрито ключові аспекти, що стосуються організації захисту мереж:

Організаційні засади захисту: Автор розглядає не лише технічні, а й управлінські аспекти безпеки, що є критично важливим для комплексного розуміння процесу захисту. Це включає розробку політик безпеки, процедур реагування на інциденти та управління ризиками.

Огляд технологій захисту: У роботі представлено широкий спектр сучасних технологій, що використовуються для захисту комп'ютерних мереж. Це дозволяє охопити різні рівні мережевої архітектури та забезпечити цілісне розуміння захисних механізмів.

Аналіз стандартів та специфікацій: Особливою перевагою є зосередженість на мережевих стандартах та специфікаціях, які є основою для побудови надійних та сумісних систем безпеки. Це свідчить про глибоку теоретичну підготовку здобувача.

Взаємозв'язок компонентів: Автор успішно демонструє взаємозв'язок між організаційними процесами, технологічними рішеннями та міжнародними

стандартами, підкреслюючи, що лише їхня інтеграція може забезпечити ефективний захист.

Практична цінність роботи є високою. Висновки та рекомендації, викладені в роботі, можуть бути застосовані на практиці при проектуванні, впровадженні та управлінні системами захисту комп'ютерних мереж на підприємствах різного масштабу. Розуміння стандартів та специфікацій є фундаментом для створення безпечних мережевих інфраструктур.

Оформлення та структура роботи відповідають встановленим вимогам до кваліфікаційних робіт. Матеріал викладено логічно, послідовно та зрозуміло. Висновки до розділів та загальний висновок чітко підсумовують основні результати дослідження, а список використаних джерел підтверджує ґрунтовну опрацьованість літературних джерел.

Загальний висновок та рекомендації:

Кваліфікаційна робота здобувача освіти Михайла ЗАЛІЗНЯКА є завершеним науковим дослідженням, яке демонструє глибокі теоретичні знання, системне мислення та практичне розуміння принципів організації процесу захисту комп'ютерних мереж. Робота виконана на високому рівні, відповідає всім вимогам до кваліфікаційних робіт та може бути рекомендована до захисту. Кваліфікаційна робота заслуговує оцінку «ДОБРЕ».

Рецензент Викладач,кти
(науковий ступінь, посада)

«____» _____ 2025 р. _____ Ігор НЕВЛЮДОВ
(підпис) (Ім'я, ПРІЗВИЩЕ)

З рецензією ознайомлений _____ Михайло ЗАЛІЗНЯК
(підпис) (Ім'я, ПРІЗВИЩЕ випускника)

«____» _____ 2025 р.