Вінницький національний технічний університет

Факультет інформаційних технологій та комп'ютерної інженерії

Кафедра обчислювальної техніки

Пояснювальна записка

до магістерської кваліфікаційної роботи
магістра

на тему «Система для перевірки та тестування захищеності Wi-Fi мережі»

Виконав: студент 2 курсу, групи 2КІ-20м
спеціальності 123 Комп'ютерна інженерія

_____ Бурак В. В.
Керівник _____к.т.н., проф.
Азарова А. О.
Опонент _к.т.н. доц.. каф. МБІС
_____Карпінець В.В.

Допущено до захисту
Завідувач кафедри ОТ
д.т.н., проф. Азаров О.Д.
«____» _____ 2021 р.

Вінниця 2021

Вінницький національний технічний університет

Факультет інформаційних технологій та комп'ютерної інженерії
Кафедра обчислювальної техніки
Освітньо-кваліфікаційний рівень магістр
Спеціальність 123 Комп'ютерна інженерія

ЗАТВЕРДЖУЮ
Завідувач кафедри
обчислювальної техніки
проф., д.т.н. О. Д. Азаров

_____

«___»_____2021 р.

З А В Д А Н Н Я

НА МАГІСТЕРСЬКУ КВАЛІФІКАЦІЙНУ РОБОТУ СТУДЕНТУ

Бураку Владиславу Вікторовичу

1 Тема роботи «Система для перевірки та тестування захищеності Wi-Fi мережі», керівник роботи Азарова Анжеліка Олексіївна к.т.н., професор, затверджені наказом вищого навчального закладу від 24.09.2021року №227.

2 Строк подання студентом роботи 15.12.2021 р.

3 Вихідні дані до роботи: процесор не гірший за Core i7 5930K, Відеокарта не гірша за Radeon RX 480 G1, ОЗП не менше 32 ГБ із тактовою частотою 3200 МГц і вище, SSD накопичувач.

4 Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити): вступ, безпровідні технології, вразливість безпровідних мереж, система для перевірки та тестування захищеності Wi-Fi мережі, розрахунок економічної доцільності створення системи для перевірки та тестування захищеності Wi-Fi мережі.

5 Перелік графічного матеріалу (з точним зазначенням обов'язкових креслень): зовнішній вигляд одноплатних мікрокомп'ютерів (інтерфейс Waidps, Raspberry Pi 3 model Bi, Intel Edison Kit), швидкість перебору на

одноплатному комп’ютері, швидкість перебору на потужному комп'ютері, схема роботи протоколу 802.1x

6 Консультантів розділів роботи представлено в табл. 1.

Таблиця 1 — Консультанти розділів роботи

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв
1,2,3	Азарова А. О., к.т.н., професор		
4	Лесько О. Й., к.е.н., професор		

7 Дата видачі завдання 07.09.2021 р.

8 Календарний план наведено в табл. 2.

Таблиця 2 — Календарний план

№ з/п	Назва етапів виконання магістерської роботи	Строк виконання етапів роботи	Примітка
1	Постановка задач роботи	07.09.21	
2	Огляд існуючих безпровідних технологій	08.09-09.09.21	
3	Аналіз переваг і недоліків безпровідних мереж	10.09-18.09.21	
4	Виявлення особливостей функціонування безпровідних мереж	19.09-01.10.21	
5	Виявлення вразливостей безпровідних мереж	12.10-22.10.21	
6	Розроблення системи для перевірки та тестування захищеності WI-FI мережі	22.10-31.10.21	
7	Захист мережі за допомогою WPA2-ENTERPRISE	01.11-10.11.21	
8	Підготовка матеріалів та опис системи для перевірки та тестування захищеності WI-FI мережі	11.11-16.11.21	
9	Розрахунок економічної частини роботи	17.11-30.11.21	
10	Оформлення пояснювальної записки та ілюстративного матеріалу	01.12-06.12.21	
11	Аналіз виконання роботи, висновки, додатки	07.12-06.12.21	
12	Перевірка якості виконання магістерської роботи та усунення недоліків	15.12.21	

Студент _____ Бурак В. В.

Керівник роботи _____ Азарова А. О.

АНОТАЦІЯ

Побудова систем для перевірки та тестування захищеності Wi-Fi мережі є актуальною задачею сьогодення.

Розвиток інформаційних технологій та стандартів забезпечення інформаційної безпеки дозволяє захистити мережі на належному рівні, але вплив людського чинника, в особі адміністратора мережі, який залишає поза увагою певні особливості, дозволяє зловмисникам отримати доступ до даних мережі.

У роботі розроблено рекомендації, що уможливлюють закрити доступ до вразливостей, які найчастіше використовують зловмисники і цим забезпечити надійне підключення до бездротової мережі, без побоювань за крадіжку або змінення інформації, що передається.

ANNOTATION

Building systems for checking and testing the security of Wi-Fi network is an urgent task today.

The development of information technology and standards of information security allows to protect networks at the appropriate level, but often the human factor, in the person of the network administrator, misses a number of features that allow attackers to penetrate network data.

The developed recommendations after the analysis will be able to close access to vulnerabilities that are most often used by attackers and thus ensure a secure connection to the wireless network, without fear of theft or alteration of transmitted information.

ЗМІСТ

ПЕРЕЛІК СКОРОЧЕНЬ

БМ — безпровідна мережа,

ЕОМ — електронна обчислювальна машина,

DSSS — Direct Sequence Spread Spectrum,

MIMO — Multiple Input, Multiple Output,

TKIP — Temporal Key Integrity Protocol,

SISO — Single Input, Single Output,

WAVE — Wireless Accessforthe Vehicular Environment,

WEP — Wired Equivalent Privacy

Wi-Fi — Wireless Fidelity,

WiMAX — Worldwide Interoperability for Microwave Access,

WLAN — Wireless Local Area Networks,

WMAN — Wireless Metropolitan Area Networks,

WPAN — Wireless Personal Area Networks,

WPP — Wireless Performance Prediction,

WWAN — Wireless Wide Area Network,

ВСТУП

Бездротові мережі стають все більш важливим ресурсом в умовах розвитку корпоративних та домашніх технологій. Однією з основних потреб їх використання є розширення існуючих провідних мереж з мінімальними витратами в найкоротші терміни.

Зі збільшенням числа мобільних користувачів виникає потреба у найкоротші терміни створення комунікаційних мереж між ними, а саме: для обміну даними, отримання інформації у максимально низькі терміни. Тому природним чином відбувається швидкий розвиток бездротових технологій. Звідси виникла гостра необхідність захисту таких мереж, забезпечення їх інформаційної цілісності та безпеки [1].

Незважаючи на те, що безпека бездротових мереж завжди залишається актуальною, адміністратори таких мереж дуже часто забувають або нехтують найпростішими заходами безпеки, і більшість пристроїв досі надає великі можливості для дій зловмисників.

Зі зростанням обчислювальної потужності обладнання протоколи безпеки, розроблені кілька років тому, втрачають свою актуальність досить швидко [2].

Крім того, питання фізичної безпеки у бездротових технологіях виходить на новий рівень. Через відсутність кабелів неможливо чітко описати периметр мережі, яку потрібно захистити. Отже, складніше організувати розмежування доступу авторизованих та несанкціонованих користувачів.

Зі збільшенням популярності бездротових мереж та ідей розумного будинку для підвищення ступеня комфортності та об'єднання всіх систем у єдину мережу з єдиним центром управління часто використовуються бездротові технології, і одним із перших постає питання забезпечення безпеки таких мереж, адже від цього починає залежати життя та здоров'я людини, а не лише безпека даних [3].

Таким чином, аспекти безпеки є популярними навіть для бездротових мереж, що не мають виходу в Інтернет, але передають особисті дані або інформацію, що становить комерційну таємницю.

Отже, **актуальність** роботи полягає у необхідності створення системи для перевірки та тестування захищеності Wi-Fi мережі.

Мета роботи полягає у побудові системи для перевірки та тестування захищеності Wi-Fi мереж, що дозволяє проаналізувати уразливості, а також шляхи та методи їх усунення.

Завдання роботи:

- виявлення вразливостей бездротових комп'ютерних мереж;
- вироблення засобів захисту вразливих місць Wi-Fi мережі;
- розроблення практичних рекомендацій щодо забезпечення безпеки Wi-Fi мережі;
- побудова автоматизованої системи для перевірки та тестування захищеності Wi-Fi мережі, аналізу її вразливостей та впливу на них.

Об'єктом дослідження є процес створення бездротової технології зв’язку.

Предметом дослідження є алгоритми та протоколи забезпечення безпеки Wi-Fi мереж.

Наукова новизна полягає у новому підході, що стає можливим завдяки використанню сучасних мікроелектронних засобів, які застосовуються для побудови автоматизованої системи для перевірки та тестування захищеності Wi-Fi мережі, система дозволяє перевірити та протестувати захищеність Wi-Fi мережі.

Практичне значення полягає у розробленні рекомендацій щодо створення безпеки Wi-Fi мереж та використанні створеного алгоритму для перевірки та тестування захищеності Wi-Fi мереж.

1 ТЕОРЕТИЧНІ ЗАСАДИ СТВОРЕННЯ БЕЗПРОВІДНИХ МЕРЕЖ

1.1 Роль та значення безпровідних технологій

Бездротові технології – це підклас інформаційних технологій, які слугують для передавання інформації на відстані між двома точками або декількома, не вимагаючи зв'язку за допомогою проводів. Для передавання інформації можуть використовуватися різні середовища та типи випромінювань, найчастіше використовуються радіохвилі, а також інфрачервоне, оптичне або лазерне випромінювання.

Існує багато бездротових технологій, найчастіше відомих за назвами компаній, які просували цей тип технологій, таким як Wi-Fi, WiMAX, Bluetooth. Кожна технологія має певні характеристики, які впливають на область застосування. І тому необхідно класифікувати їх [5].

Існують різні підходи до класифікації бездротових технологій.

За дальністю дії їх класифікують як:

- бездротові персональні мережі (WPAN – Wireless Personal Area Networks), приклади технологій – Bluetooth;
- бездротові локальні мережі (WLAN – Wireless Local Area Networks), приклади технологій – Wi-Fi;
- бездротові мережі масштабу міста (WMAN) – Wireless Metropolitan Area Networks), приклади технологій – WiMAX;
- бездротові глобальні мережі (WWAN – Wireless Wide Area Network), приклади технологій – CSD, GPRS, EDGE, EV-DO, HSPA.

За топологією:

- «Точка-точка»;
- «Точка-багатоточка».

По області застосування:

- корпоративні (відомчі) бездротові мережі – створені компаніями для потреб;

- операторські бездротові мережі – створені операторами зв'язку для надання послуг [1].

Таблиця 1.1 – Порівняння стандартів бездротового зв'язку

Технологія	Стандарт	Використання	Пропускна здатність	Радіус дії	Частоти
Wi-Fi	802.11a	WLAN	до 54 Мбіт/с	до 300 метрів	5,0 ГГц
Wi-Fi	802.11b	WLAN	до 11 Мбіт/с	до 300 метрів	2,4 ГГц
Wi-Fi	802.11g	WLAN	до 54 Мбіт/с	до 300 метрів	2,4 ГГц
Wi-Fi	802.11n	WLAN	до 300 Мбіт/с (у перспективі до 600 Мбіт/с)	до 300 метрів	2,4 – 2,5 або 5,0 ГГц
WiMax	802.16d	WMAN	до 75 Мбіт/с	25-80 км	1,5-11 ГГц
WiMax	802.16e	Mobile WMAN	до 40 Мбіт/с	1-5 км	2,3-13,6 ГГц
WiMax 2	802.16m	WMAN, Mobile WMAN	до 1 Гбіт/с (WMAN), до 100 Мбіт/с (Mobile WMAN)	120-150 км (стандарт у розробленні)	До 11 ГГц
Bluetooth v.1.1	802.15.1	WPAN	до 1 Мбіт/с	до 10 метрів	2,4 ГГц
Bluetooth v.2.0	802.15.3	WPAN	до 2,1 Мбіт/с	до 100 метрів	2,4 ГГц
Bluetooth v.3.0	802.11	WPAN	від 3 Мбіт/с до 24 Мбіт/с	до 100 метрів	2,4 ГГц
ZigBee	802.15.4	WPAN	від 20 до 250 кбіт/с	1-100 м	2,4 ГГц (16 каналів), 915МГц (10 каналів), 868 МГц (один канал)
Інфрачервона лінія зв’язку	IrDa	WPAN	до 15 Мбіт/с	від 5 до 50 сантиметрів, одностороння зв'язок — до 10 метрів	Інфрачервоне випромінювання

На даний момент існує два найбільш застосовувані напрямки:

- робота у замкненому просторі (офіс, виставковий зал тощо);
- з'єднання віддалених один від одного локальних мереж (або віддалених на відстані сегментів локальної мережі).

Розглянемо організацію корпоративних бездротових мережах для роботи в замкненому обсязі, які в наш час дуже активно використовуються для швидкого доступу до локальних та глобальних ресурсів. Найчастіше вони будуються з використанням бездротової технології, більш відомої під назвою Wi-Fi.

Для організації бездротових мереж у замкненому просторі використовуються всеспрямовані антени передавача. Використовуються розроблені стандарти зв'язку для комунікації в бездротовій локальній мережі частотних діапазонів, що не ліцензуються, 0,9, 2,4, 3,6 і 5 ГГц – IEEE 802.11.

Спочатку стандарт IEEE 802.11 передбачав передачу даних по радіоканалу на швидкості близько 1 Мбіт/с і як опцію на швидкості порядку 2 Мбіт/с. Один із перших високошвидкісних стандартів бездротових мереж – IEEE 802.11a – визначає швидкість передавання на швидкості до 54 Мбіт/с. Як робочий діапазон використовується 5 ГГц.

В ідеальних умовах стандарт IEEE 802.11 регламентує швидкість передавання до 54 Мб/с. У менш ідеальних умовах (або при чистому сигналі) пристрої можуть вести зв'язок зі швидкістю<54 Мбіт/с і кратно 6, зазвичай це: 48 Мбіт/с, 36 Мбіт/с, 24 Мбіт/с, 18 Мбіт/с, 12 Мбіт /с та 6 Мбіт/с.

Сумісність стандарту IEEE 802.11a з 802.11b або 802.11g відсутня. Незважаючи на свою назву, стандарт IEEE 802.11b, прийнятий в 1999 році, не є продовженням стандарту 802.11a, оскільки використовуються різні технології: метод прямої послідовності для розширення спектру (DSSS), а якщо бути точніше, то його покращена версія високошвидкісний метод прямої послідовності для розширення спектру (HR-DSSS) 802.11b проти мультиплексування з ортогональним частотним поділом каналів (OFDM) 802.11a. Стандарт 802.11b передбачає використання діапазону частот, що не ліцензується, 2,4 ГГц. Швидкість передавання – до 11 Мбіт / с [2].

У жовтні 2002 року було затверджено проект стандарту IEEE 802.11g, який передбачає використання діапазону частот 2,4 ГГЦ, тим самим забезпечуючи швидкість з'єднання близько 54 Мбіт/с в ідеальних умовах, ніж перевершив стандарт IEEE 802.11b, який дозволяв працювати на швидкостях до 11 Мбіт/с.

Крім того, стандарт 802.11g забезпечує сумісність 802.11b. Сумісність може бути реалізована в режимі модуляції прямої послідовності для розширення спектру, і тоді швидкість з'єднання обмежується в 11 Мбіт/с, а якщо в режимі модуляції мультиплексування з ортогональним частотним поділом каналів, то 54 Мбіт/с. Тому цей стандарт рекомендується і є прийнятним при побудові бездротових комп'ютерних Wi-Fi мереж.

Стандарт 802.11n підвищує швидкість передавання даних практично вчетверо порівняно з пристроями стандартів 802.11g (максимальна швидкість яких дорівнює 54 Мбіт/с) за умови використання в режимі 802.11n з іншими пристроями 802.11n. Теоретично 802.11n здатний забезпечити швидкість передавання даних до 600 Мбіт/с брутто, застосовуючи передавання даних відразу за чотирма антенами. За однією антеною — до 150 Мбіт/с.

Пристрої 802.11n працюють у діапазонах 2,4-2,5 або 5,0 ГГц. Крім того, пристрої 802.11n можуть працювати у трьох режимах:

- успадкованому (Legacy), в якому забезпечується підтримка пристроїв 802.11b/g та 802.11a;
- змішаному (Mixed), у якому підтримуються пристрої 802.11b/g, 802.11a та 802.11n;
- «чистому» режимі – 802.11n (саме в цьому режимі і можна скористатися перевагами підвищеної швидкості та збільшеною дальністю передавання даних, що забезпечуються стандартом 802.11n).

Чорну версію стандарту 802.11n (DRAFT 2.0) підтримують багато сучасних мережевих пристроїв. Підсумкова версія стандарту (DRAFT 11.0), прийнята 11 вересня 2009 року, забезпечує швидкість до 300 Мб/с, Багатоканальний вхід/вихід, відомий як MIMO, та більше покриття [3].

Стандарт 802.11n вводить важливе нововведення – MIMO (Multiple Input, Multiple Output – «багато входів, багато виходів»), за допомогою якого здійснюється просторове мультиплексування: одночасне передавання декількох інформаційних потоків по одному каналу, а також використання для доставки сигналу багатопроменевого поширення, яке мінімізує вплив перешкод та втрат даних, але

вимагає наявності кількох антен. Саме можливість одночасної передачі та прийому даних робить пропускну здатність пристроїв 802.11n більш високою.

На початок 2016 року більшість точок доступу, що пропонуються виробниками, підтримує MIMO 2×2 або 1×1, тобто SISO (однопотокове передавання). Вбудовані в мобільні пристрої Wi-Fi-адаптери зазвичай підтримують режим SISO [4].

Також набір стандартів IEEE 802.11 визначає в основному два режими роботи мережі:

- Ad-hoc, тобто точка-точка – це найпростіша бездротова мережа, де зв'язок між клієнтами (станціями) встановлюється безпосередньо без використання третіх пристроїв, таких як точка доступу;

- клієнт-сервер – бездротова мережа складається, як мінімум, з однієї точки доступу, що є сервером, підключеної до провідної мережі, та деякого набору бездротових клієнтських станцій, які називаються клієнтами.

У зв'язку з тим, що в більшості бездротових мереж необхідно забезпечувати доступ до різних серверів прикладних завдань, принтерів та будь-яких інших пристроїв, підключених за допомогою дротової локальної мережі, зазвичай використовують режим із використанням точки доступу, тобто клієнт-сервер. Без підключення додаткових антен зв'язок для обладнання, що працює в стандарті IEEE 802.11b, досягається приблизно на таких відстанях:

- вільний відкритий простір – близько 500 м;
- кімната, розділена перегородками з матеріалу, що не має у своїй основі великої кількості металу – 100 м;
- офісне приміщення з кількох кімнат – 30 м.

Слід мати на увазі, що через залізобетонні стіни (частіше несучі, тому що в них багато арматури) радіохвилі діапазону 2,4 ГГц можуть взагалі не проходити, тому в розділених такою стіною приміщеннях доведеться ставити свої точки доступу, частіше об'єднані загальною провідною мережею.

Група протоколів IEEE 802.11 регулює й інші сторони мережі та обладнання для їх побудови. Список протоколів з коротким описом їх застосування представлений нижче:

- 802.11 – початковий 1 Мбіт/с та 2 Мбіт/с, 2,4 ГГц та ІЧ стандарт (1997);
- 802.11a – 54 Мбіт/с, 5 ГГц стандарт (1999, вихід продуктів у 2001);
- 802.11b – поліпшення до 802.11 для підтримки 5,5 та 11 Мбіт/с (1999);
- 802.11c – процедури операцій з мостами; включено до стандарту IEEE 802.1D (2001);
- 802.11d – міжнародні роумінгові розширення (2001);
- 802.11e – покращення: QoS, пакетний режим (packetbursting) (2005);
- 802.11F – Inter-Access Point Protocol (2003);
- 802.11g – 54 Мбіт/с, 2,4 ГГц стандарт (зворотна сумісність з b) (2003);
- 802.11h – розподілений за спектром 802.11a (5 GHz) для сумісності у Європі (2004);
- 802.11i – покращена безпека (2004);
- 802.11j – розширення для Японії (2004);
- 802.11k – покращення вимірювання радіоресурсів;
- 802.11l – зарезервований;
- 802.11m – поправки та виправлення для всієї групи стандартів 802.11.
- 802.11n – збільшення швидкості передачі даних (600 Мбіт/с), 2,4-2,5 або 5 ГГц, зворотна сумісність із 802.11a/b/g (вересень 2009);
- 802.11o – зарезервований;
- 802.11p – WAVE – Wireless Accessforthe Vehicular Environment (Бездротовий доступ для середовища транспортного засобу);
- 802.11q – зарезервований, іноді його плутають з 802.1Q;
- 802.11r – швидкий роумінг;
- 802.11s – ESS Wireless mesh network[en] (Extended Service Set – розширений набір служб; Mesh Network – багатозв'язкова мережа);

- 802.11T – Wireless Performance Prediction (WPP, прогноз) продуктивності бездротового обладнання) – методи тестів та вимірювань;
- 802.11u – взаємодія з не-802 мережами (наприклад, стільниковими);
- 802.11v – керування бездротовими мережами;
- 802.11w – Protected Management Frames (захищені керуючі фрейми);
- 802.11x – зарезервований і не використовуватиметься (не треба плутати із стандартом контролю доступу IEEE 802.1X);
- 802.11y – додатковий стандарт зв'язку, що працює на частотах 3,65-3,70 ГГц та забезпечує швидкість до 54 Мбіт/с на відстані до 5000 м на відкритому просторі;
- 802.11ac – новий стандарт IEEE. Швидкість передавання даних – до 6,77 Гбіт/с для пристроїв, що мають 8 антен, затверджено у січні 2014 року;
- 802.11ad – новий стандарт з додатковим діапазоном 60 ГГц (Частота не вимагає ліцензування). Швидкість передавання даних – до 7 Гбіт/с.

Усього у вищезгаданого списку можна виділити два найменування: 802.11F і 802.11T, які є рекомендаціями, а не стандартами, тому і застосовуються великі літери у найменуванні [2].

1.2 Переваги і недоліки безпровідних мереж

Бездротові локальні мережі Wi-Fi, засновані на протоколах IEEE 802.11, дозволяють підвищувати мобільність співробітників в офісних та виробничих приміщеннях, допомагають позбутися витрат на монтаж та обслуговування провідних мереж, особливо якщо ремонт вже закінчено, а кабелі спочатку не були прокладені.

Бездротові локальні мережі Wi-Fi мають сенс використовуватися на підприємствах з невеликою кількістю робочих місць або коли використовується досить велика кількість бездротових пристроїв (планшетів, ноутбуків, смартфонів, комунікаторів тощо). Найчастіше логічним методом побудови мережі є використання обох типів мереж одночасно: провідних та бездротових мереж Wi-Fi.

Основні переваги полягають у такому:

- простота та швидкість розгортання мережі;
- низька вартість розгортання;
- відсутність проводів на робочому місці або у житловому приміщенні (хоча б частини проводів) [5].

А основні недоліки полягають в тому, що:

- швидкість передавання даних ділиться між пристроями, підключеними до бездротової мережі Wi-Fi у межах однієї й тієї ж точки доступу, що їх обслуговує, це означає, що якщо роутер надає нам швидкість передачі даних близько 220 мбіт/с і до неї буде одночасно підключено, наприклад, 2 планшети, 2 смартфони та ноутбук, то швидкість передачі даних для кожного пристрою складе 220/5 = 44мбіт/с, а насправді буде ще менше, тому що потрібно ще передача службової інформації, яка може займати від 30 до 40 відсотків; в результаті швидкість передачі становить приблизно 26 мбіт/с на один пристрій;
- вплив предметів навколо, таких як дерева, стіни будівель, навіть побутових пристроїв, таких як холодильник;
- досить низька надійність у зв'язку з тим, що все «передається повітрям» і будь-який зловмисник може атакувати цю точку доступу в межах її доступності;
- низька стійкість до злому при неправильному налаштуванні.

Мінуси частково можна перекрити більш якісним та безпечним обладнанням, а також об'єднанням кількох рознесених по приміщеннях точок доступу в одну провідну мережу.

При розгортанні бездротової мережі будинку для підключення пари ноутбуків, комп'ютера та кількох будь-яких гаджетів бездротова мережа Wi-Fi буде ідеальним варіантом за швидкістю розгортання та економічною складовою. Також легко розширює вже створену провідну мережу в приміщенні. Для з'єднання віддалених локальних мереж (або віддалених сегментів локальної мережі) використовується обладнання з спрямованими антенами, що дозволяє збільшити дальність зв'язку до 20 км (а при використанні спеціальних підсилювачів та великій висоті розміщення антен – до 50 км). Причому як подібне обладнання можуть виступати і пристрої Wi-Fi, потрібно лише додати до них спеціальні антени

(звичайно, якщо це допускається конструкцією). Комплекси для об'єднання локальних мереж з топології поділяються на точку-точку і зірку. При топології «точка-точка» (режим Ad-hoc в IEEE 802.11) організується радіомост між двома віддаленими сегментами мережі. При топології «зірка» одна зі станцій є центральною та взаємодіє з іншими віддаленими станціями. При цьому центральна станція має всеспрямовану антену, інші віддалені станції — односпрямовані антени. Застосування всеспрямованої антени на центральній станції обмежує дальність зв'язку дистанцією приблизно 7 км. Тому, якщо потрібно з'єднати між собою сегменти локальної мережі, віддалені один від одного на відстані понад 7 км, доводиться з'єднувати їх за принципом «крапка-крапка». Так організується бездротова мережа з кільцевою чи іншою, складнішою топологією [6].

1.3 Способи зламу WI-Fi мереж

Вищевикладені методи безпеки використовуються для захисту від загроз порушення інформаційної безпеки, ці загрози умовно можна розділити на два класи:

- прямі – загрози інформаційної безпеки, що виникають при інформаційному обміні бездротовою локальною мережею Wi-Fi;
- непрямі – загрози, пов'язані з великою кількістю точок доступу Wi-Fi.

Прямі погрози виникають тоді, коли радіоканал у межах доступності Wi-FI роутера, за допомогою якого здійснюється передавання даних, схильний до легкого втручання з метою отримання несанкціонованого доступу до ресурсів та інформації.

У стандартах, що регламентують роботу Wi-Fi, передбачені як автентифікація, так і шифрування, але ці елементи захисту мають свої вади та слабкі місця.

Шифрування впливає на швидкість передавання даних, і часто воно відключається адміністратором для оптимізації трафіку в бездротовій мережі. Перший стандарт шифрування Wired Equivalent Privacy був дискредитований

знаходженням уразливостей в алгоритмі розподілу ключів RC4. Це трохи загальмувало розвиток ринку бездротових Wi-Fi мереж і викликало створення інститутом інженерів електротехніки та електроніки (IEEE) групи 802.11i для розробки нового стандарту безпеки, що враховує відомі вразливості WEP, що забезпечує 128-бітове шифрування AES та автентифікацію для захисту даних, що передаються.

Альянс Wi-Fi в 2003 р. представив своє бачення цього стандарту, так званий проміжний варіант цього стандарту Wi-Fi Protected Access (WPA). Wi-Fi Protected Access використовує протокол цілісності тимчасових ключів Temporal Key Integrity Protocol (TKIP). Також у ньому почали використовувати метод підрахунку контрольної суми: MIC (Message Integrity Code), яка стала дозволяти перевіряти цілісність пакетів, що передаються. У 2004 альянс Wi-Fi випустили новий, що набрав великої популярності на сьогоднішній день, стандарт WPA2, який є покращенням стандарту WPA. Основна різниця між стандартами WPA і WPA2 полягає в технології шифрування: WPA — TKIP і WPA2 — AES. Стандарт WPA2 дозволяє забезпечити більш високий рівень захисту бездротової мережі, оскільки TKIP дозволяє створювати ключі завдовжки лише до 128 біт, а AES – вже до 256 біт.

Загроза блокування інформації в бездротовому каналі Wi-Fi залишена практично без уваги під час розроблення технології бездротових мереж. Блокування каналу не є небезпечним, тому що зазвичай бездротові Wi-Fi мережі є допоміжними для провідних мереж, незважаючи на те, що блокування може бути підготовчим етапом для проведення атаки «людина посередині», коли між роутером і клієнтським пристроєм впроваджується третій пристрій, що перенаправляє трафік між роутером та клієнтом через себе. Дане використання дозволяє видаляти, по-різному видозмінювати інформацію, а також «підсовувати» неправдиву інформацію.

Слід також звернути увагу на такий тип загроз, як «чужаки». Чужаками (Rogue Devices, Rogues) називають периферійні пристрої та комп'ютери, що надають можливість несанкціонованого доступу до корпоративної мережі,

зазвичай в обхід захисних механізмів, визначених політикою безпеки. Заборона на будь-яке використання пристроїв бездротового зв'язку не зможе захистити від бездротових мережевих атак, якщо в мережі, навмисне або ненавмисне, з'явиться чужинець. У ролі пристрою чужинця може виступати все, що завгодно, у чого є провідний і бездротовий інтерфейси: роутери (включаючи програмні), проектори, сканери, ноутбуки з обома включеними інтерфейсами і т.д.

Під час порушення безпеки безпровідних мереж зловмисники використовують нефіксовану природу зв'язку бездротових пристроїв.

Бездротові Wi-Fi пристрої можуть легко змінювати точки підключення до мережі прямо під час роботи і навіть непомітно для користувача. Наприклад, можуть відбуватися «випадкові асоціації», коли ноутбук з Windows XP (налаштовані на довірчі стосунки до всіх бездротових мереж) або просто неправильно настроєний клієнт бездротової мережі автоматично асоціюється і підключає користувача до найближчої бездротової Wi-Fi мережі.

Таким чином, зловмисник може перемикати на свою підставну точку доступу для подальшого сканування вразливостей, фішингу або атак «людина посередині». А, якщо пристрій при цьому підключено і до провідної локальної мережі, то він стає точкою входу, так званим чужинцем.

На додаток до цього багато користувачів, підключені до внутрішньої локальної мережі, використовуючи Wi-Fi інтерфейс, зазвичай незадоволені якістю та політикою роботи мережі, перемикаються на найближчу доступну точку доступу (або недбало налаштована операційна система робить це автоматично при відмові провідної мережі). При цьому весь побудований захист мережі зазнає краху.

Є ще одна проблема – мережі точка-точка, за допомогою яких зручно передавати файли між колегами або друкувати на принтері, який підтримує Wi-Fi. Але така організація бездротових мереж не підтримує багато методів забезпечення безпеки, що робить їх легко доступною здобиччю для зловмисника. А нові технології Virtual WiFi і Wi-Fi Direct, що прийшли, тільки погіршили ситуацію в плані безпеки.

Уразливості мереж та пристроїв можуть бути викликані некоректно налаштованими мережевими пристроями, пристроями зі слабкими та недостатньо довгими ключами шифрування, що використовують скомпрометовані методи автентифікації – саме ці пристрої зазнають атак у першу чергу. Згідно зі звітами аналітиків, більшість успішних зломів відбувається саме через неправильні налаштування точок доступу та програмного забезпечення клієнта [7].

Ця проблема також може виникати внаслідок некоректно налаштованих точок доступу. Варто підключити некоректно налаштовану точку доступу до мережі для злому останньої. Заводські налаштування, так звані «за замовчуванням», зазвичай не включають шифрування та автентифікацію, або використовують ключі, прописані в посібниках користувача, і тому вони є всіма відомими навіть на офіційних форумах виробника.

Малоймовірно, що користувачі досить серйозно спантеличуються налаштуванням пристроїв, націлених на безпеку. Саме такі точки доступу бездротової мережі і створюють основні загрози захищеним мережам.

Неправильно налаштовані клієнтські пристрої – загроза значно небезпечніша, ніж неправильно настроєні точки доступу. Це клієнтські пристрої, і вони не конфігуруються спеціально для безпеки внутрішньої мережі підприємства. До того ж, зазвичай вони знаходяться за межами периметра контрольованої зони або всередині периметра, що може дозволити зловмиснику проводити всілякі атаки, наприклад, поширювати вірусне програмне забезпечення або просто забезпечувати легкодоступну та зручну точку входу.

Під час злому шифрування захищеність скомпрометованого алгоритму забезпечення безпеки WEP відсутня. Інтернет має у своєму розпорядженні у вільному доступі спеціальним та зручним у використанні програмним забезпеченням для зламування цього стандарту, яке здійснює збір статистики трафіку доти, доки не стане достатньо для відновлення ключа шифрування. Стандарти WPA та WPA2 також мають кілька вразливостей різного ступеня небезпеки, що дозволяють здійснити їх злом, але поки що немає інформації про успішні атаки на WPA2-Enterprise (802.1x).

Якщо мова йде про імперсонацію (Identity Theft), то імперсонація (видача себе за іншу людину) авторизованого користувача – серйозна загроза для будь-якої комп'ютерної мережі, не лише бездротової. Однак, у бездротовій мережі визначення справжності користувача відбувається складніше.

Існують SSID і можна робити спроби фільтрувати за MAC-адресами, але, і те, й інше передається в ефірі у відкритому вигляді. Їх нескладно підробити, а коли підробив, то можна, як мінімум, знизити пропускну здатність мережі, вставляючи неправильні frame, а трохи розібравшись у алгоритмах шифрування, влаштовувати тестування на проникнення в цілу структуру мережі (наприклад, використовувати атаки типу ARP-spoofing).

Імперсонація користувача можлива не тільки у разі заміни MAC-адреси при встановленій MAC-автентифікації або використанні статичних ключів. Схеми побудови мереж на основі 802.1x (WPA2 Enterprise) не є абсолютно безпечними. Деякі механізми (LEAP) мають складність злому, схожу зі зломом WEP. Інші механізми, EAP-FAST або PEAP-MSCHAPv2, хоч і надійніше, але не гарантують стійкості до проведеної зловмисником комплексної атаки.

Відмови в обслуговуванні можуть бути викликані DoS атаками. DoS атаки спрямовані на порушення якості функціонування сервісу бездротової мережі або на абсолютне припинення доступу користувачів та відмови обладнання до перезавантаження. У разі Wi-Fi мережі відстежити джерело, що завалює мережу, специфічним для цього типу атаки, «сміттєвими» пакетами, дуже складно — його розташування обмежується лише зоною покриття. До того ж є апаратний варіант цієї атаки — установка досить сильного джерела перешкод у частотному діапазоні точки доступу, що працюють, так звані «глушилки».

1.4 Особливості функціонування безпровідних мереж

У бездротових мереж є деякі специфічні особливості, які у провідних мережах відсутні. Дані особливості в цілому впливають на загальну продуктивність,

доступність, безпеку та ціну обслуговування бездротової мережі. Їх доводиться враховувати, хоча вони й не приносять будь-якого внеску до шифрування чи автентифікації. Для вирішення таких питань потрібен спеціальний інструментарій та налагоджені механізми адміністрування та моніторингу мережі.

Одним з елементів такого інструментарію є обмеження активності користувачів у неробочий час. Логічним буде рішення обмежити політикою безпеки доступ до мережі поза робочим часом (аж до фізичного відключення електроживлення точки доступу), активність у бездротовій мережі в неробочий час має моніторитися, вважатися як підозріла та піддаватися розслідуванню.

Якість роботи бездротової Wi-Fi мережі як радіоефіру залежить від багатьох чинників. Один із них – інтерференція радіосигналів, яка може дуже знизити пропускну здатність і обмежити кількість користувачів, аж до повної неможливості використання мережі. Як джерело може виступати будь-який пристрій, наприклад, роутер із занадто сильним випромінювачем, не дозволеним у вільному продажу, що випромінює на тій же частоті сигнал достатньої потужності. Це можуть бути як сусідні точки доступу, так і мікрохвильові печі. Цю особливість цілком можуть також використовувати атакуючі як атака відмови в обслуговуванні або для підготовки атаки «людина посередині», заглушаючи безпечні точки доступу і залишаючи свою з таким же SSID (підмінна при атаці людина «посередині»).

Існують інші специфічні особливості бездротових мереж крім інтерференції сигналу. Неправильно налаштований термінал клієнта або антена, що дають збої, можуть значно знижувати якість обслуговування решти користувачів. Або питання стабільності зв'язку, що логічно виникає.

Не тільки сигнал роутера повинен досягти клієнта, але й сигнал клієнта повинен досягти назад роутера. Зазвичай роутери в кілька разів потужніші, і щоб досягти симетрії, можливо, доведеться знизити потужність сигналу на роутері. Для 5 ГГц слід пам'ятати, що надійно працюють лише 4 канали: 36/40/44/48 (для Європи, для США є ще 5). На інших включено режим співіснування з радарами DFS). У результаті, зв'язок роутера та клієнтського пристрою може досить часто пропадати.

1.5 Технології захисту безпровідних Wi-Fi мереж

Для захисту Wi-Fi мереж використовується кілька широко відомих способів, таких, як метод обмеження доступу та метод аутентифікації. Розглянемо методи трохи докладніше.

Метод обмеження доступу фільтруванням MAC-адрес.

До стандарту IEEE 802.11 такий метод не входить. Але є три способи фільтрації:

- роутер дозволяє підключатися клієнтам з будь-якою MAC-адресою;
- роутер дозволяє підключатися клієнтам, чиї MAC знаходяться в білому списку;
- роутер забороняє підключатися клієнтам, чиї MAC перебувають у «чорному списку».

Із точки зору безпеки найнадійнішим може бути другий варіант, але він не розрахований на заміну MAC-адреси, чим легко може скористатися зловмисник.

Режим приховування ідентифікатора точки доступу SSID (Англ. Service Set IDentifier). Для свого виявлення точка доступу періодично здійснює розсилку beaconframes (у перекладі кадрів-маяків). Такий кадр містить певну службову інформацію для підключення, а також містить у собі SSID (ідентифікатор бездротової мережі). У разі режиму приховування SSID – це поле порожнє, тобто стає неможливим виявити вашу бездротову мережу та підключитися до неї, не знаючи значення самого SSID. Але всі клієнти, підключені до мережі, знають SSID і при підключенні, коли розсилають Probe Request (у перекладі спроба на підключення), вказують ідентифікатори цих мереж, збережені в їх профілях підключень. Прослуховуючи робочий трафік даних клієнтів, можна легко отримати значення SSID точки доступу, необхідне для підключення до бажаного роутеру.

Метод аутентифікації (відкрита аутентифікація) – клієнт здійснює запит аутентифікації, в якому присутній тільки свій MAC-адреса. Роутер відповідає відмовою або підтвердженням автентифікації. Рішення приймається на основі

фільтрації за списком MAC-адрес, тобто, по суті – це спосіб захисту бездротової локальної Wi-Fi мережі на основі списку доступу.

Використання для автентифікації шифрів. У SharedKeyAuthentication (аутентифікація із загальним ключем) потрібне налаштування незмінного – статичного ключа шифрування алгоритму WEP (англ. Wired Equivalent Privacy). Клієнт робить запит у точки доступу на автентифікацію, на що отримує підтвердження, яке містить 128 байт випадкової інформації. Станція шифрує отримані дані алгоритмом WEP (проводиться побітове додавання за модулем 2 даних повідомлення з послідовністю ключа) та відправляє зашифрований текст разом із запитом на асоціацію. Точка доступу розшифровує текст та порівнює з вихідними даними. У разі збігу надсилається підтвердження асоціації, і клієнт вважається підключеним до мережі.

Схема автентифікації із загальним ключем уразлива до атак "Man in the middle (людина посередині)". Алгоритм шифрування WEP — це простий XOR ключової послідовності з корисною інформацією, отже, прослухавши трафік між станцією та точкою доступу, можна відновити частину ключа.

Шифри, що використовуються: без шифрування, динамічний WEP, CKIP.

Аутентифікація за MAC-адресою. Цей метод не передбачений у IEEE 802.11, але підтримується більшістю виробників обладнання, наприклад D-Link та Cisco. Відбувається порівняння MAC-адреси клієнта з таблицею дозволених MAC-адрес, що зберігається на точці доступу, або використовується зовнішній сервер аутентифікації. Використовується як додатковий захід захисту.

IEEE розпочав розроблення нового стандарту IEEE 802.11i, але через труднощі затвердження, організація WECA (англ. Wi-Fi Alliance) спільно з IEEE анонсували стандарт WPA (англ. Wi-FiProtectedAccess). У WPA використовується TKIP (англ. Temporal Key Integrity Protocol, протокол перевірки цілісності ключа), який використовує вдосконалений спосіб управління ключами та покадрову зміну ключа [6].

Wi-Fi Protected Access (WPA). Після перших успішних атак на WEP було прийнято розробити новий стандарт 801.11i. Але до нього був випущений

«проміжний» стандарт WPA, який включав нову систему аутентифікації на базі 801.1x і новий метод шифрування TKIP. Існують два варіанти аутентифікації: за допомогою RADIUS сервера (WPA-Enterprise) та за допомогою попередньо встановленого ключа (WPA-PSK)

Використовувані шифри: TKIP (стандарт), AES-CCMP (розширення), WEP (як зворотної сумісності) [8].

WI-FI Protected Access2 (WPA2, 801.11I). WPA2 або стандарт 801.11i — це фінальний варіант стандарту безпеки бездротових мереж. Як основний шифр був обраний стійкий блоковий шифр AES. Система аутентифікації порівняно з WPA зазнала мінімальних змін. Також як і в WPA, WPA2 є два варіанти аутентифікації WPA2-Enterprise з автентифікацією на RADIUS сервері і WPA2-PSK з встановленим ключем.

Використані шифри: AES-CCMP (стандарт), TKIP (як зворотної сумісності) [9].

Cisco Centralized Key Management (CCKM). Варіант аутентифікації від фірми CISCO. Підтримує роумінг між точками доступу. Клієнт один раз проходить автентифікацію на сервері RADIUS, після чого може перемикатися між точками доступу. Використані шифри: WEP, CKIP, TKIP, AES-CCMP» [10].

1.6 Висновки до розділу

Зважаючи на інформацію, яка була проаналізована у розділі, можна зробити висновок про те, що бездротові технології являються одним із підкласів технологій, які безпосередньо сприяють апаратному забезпеченню при передаванні інформації на відстані між кількома точками, які не вимагаючи зв'язку за допомогою провідних мереж.

2 РОЗРОБЛЕННЯ СИСТЕМИ ТЕСТУВАННЯ ВРАЗЛИВОСТЕЙ БЕЗПРОВІДНИХ МЕРЕЖ

2.1 Обґрунтування вибору апаратних засобів для системи тестування захищеності Wi-Fi мереж

Для того, щоб займатися перевіркою та тестуванням захищеності Wi-Fi мережі знадобиться персональний комп'ютер на x86, x64 або ARM архітектурі з встановленою операційною системою Linux з ядром версії не менше 2.6.22. Застосовано ноутбук HPPavilionDV6 3056er із встановленою ОС KaliLinux 2016.2 та встановленими всіма останніми оновленнями.

Wi-Fi адаптер, драйвери якого під операційною підтримують Linux, режими «моніторингу» та «ін'єкцій». Список таких адаптерів можна легко знайти в інтернеті, наприклад, на сайті: https://wikidevi.com/wiki/ Category:Linux_driver/802dot11.

Комплект ПЗ aircrack-ng (версія під Linux), який включає наступні пакети:

— aircrack-ng — зламує ключі WEP та WPA (перебір за словником);

— airdecap-ng — озшифровує перехоплений трафік за відомого ключ;

— airmon-ng — виставляє мережу в режим моніторингу;

— aireplay-ng — пакетний інжектор;

— airodump-ng — аналізатор трафіку: поміщає трафік у файли PCAP або IVS і показує інформацію про мережі;

— airtun-ng — створює віртуальний інтерфейс тунелювання;

— packetforge-ng — створює шифровані пакети для ін'єкції;

— Ivstools — інструменти для злиття та конвертування;

— airbase-ng — надає техніку для атаки клієнта;

— airdecloak-ng — забирає WEP-маскування з файлів pcap;

— airolib-ng — зберігає та керує списками ESSID та паролів, обчислює парні майстер-ключі;

— airserv-ng — відкриває доступ до бездротової мережі з інших комп'ютери;

— 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.

Це програмне забезпечення йде у складі операційної системи.

Бездротова точка доступу, яку будемо налаштовувати під конкретне шифрування і використовувати її як атаковану, використано D-link DIR-615.

Для спрощення та поліпшення якості тестування на проникнення краще використовувати KaliLinux останньої стабільної версії, її можна безкоштовно отримати для некомерційного використання на офіційному сайті розробників: https://www.kali.org/, до неї включені всі пакети для тестування на проникнення.

2.2 Застосування методу WEP-шифрування для вивчення вразливостей Wi-Fi мереж

Перейдемо до тестування на проникнення в мережу, організовану бездротовою точкою доступу із встановленим на ній для авторизації WEP шифруванням.

Для цього потрібна бездротова точка доступу. Її налаштовано зі зазначенням наступних параметрів:

- назва – mntl;
- пароль – дізнаємось наприкінці;
- тип шифрування – WEP.

Приступимо до дій.

Для початку потрібно залогінитися під обліковим записом root, або будь-який інший, але тоді перед кожною командою потрібно вводити sudo.

Відкриваємо термінал (ctrl + alt + t) та для визначення драйвера вводимо команду: airmon-ng (рис. 2.1).

У результаті виконання програми інтерфейс називається «wlan0», «Chipset» має статус — «Unknown», але драйвер визначився. Якщо подібний вивід або «Chipset» визначився, значить, можемо переходити далі, інакше потрібно налагодити драйвер або використовувати інший Wi-Fi адаптер.

Наступним кроком потрібно перевести карту в режим роботи моніторинг, для цього ввести в терміналі команду: airmon-ngstart wlan0 (рис. 2.2).

Рисунок 2.1 – Виведення результату виконання команди airmon-ng

Рисунок 2.2 – Виконання команди airmon-ngstartwlan0

У результаті виконання команди в передостанньому рядку терміналу бачимо текст: «monitor mode enabled on mon0», що означає, що можемо для моніторингу використовувати включений інтерфейс mon0.

Наступним кроком буде включення режиму прослуховування для визначення доступних Wi-Fi мереж, для цього виконаємо команду airodump-ng mon0 (рис. 2.3).

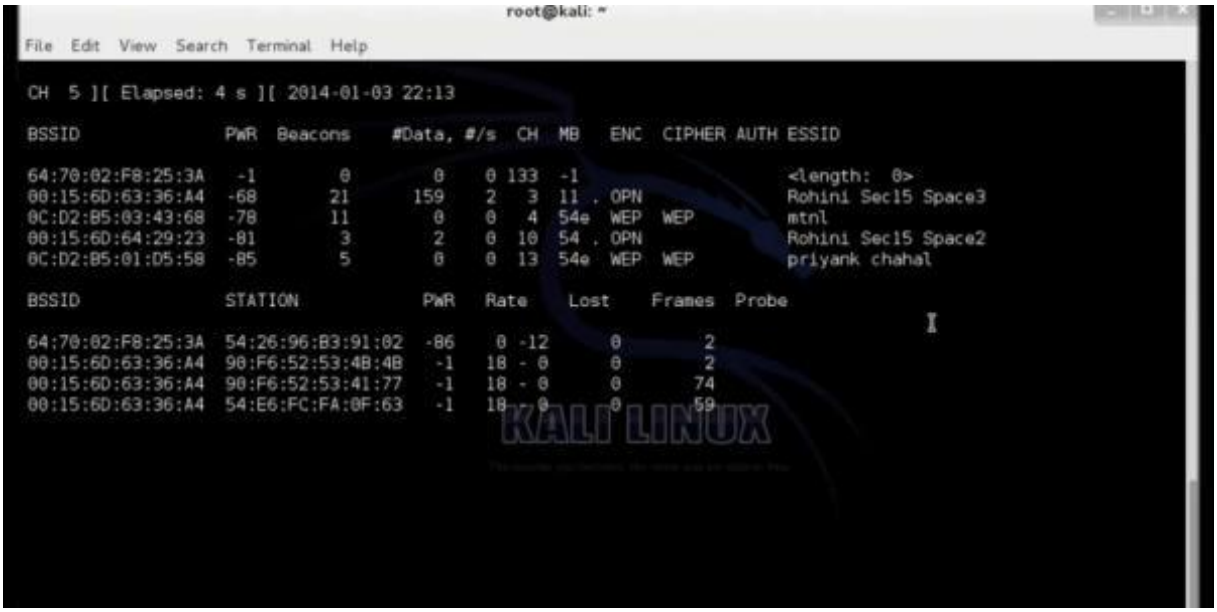

Рисунок 2.3 – Список доступних мереж

У результаті виконання команди можемо спостерігати список бездротових мереж у радіусі дії нашого Wi-Fi адаптера. Можемо спостерігати, що створена спочатку мережа, названа mtnl, має такі важливі для нас характеристики: використовуване шифрування WEP, 4 канал, bssid – фізична адреса точки доступу для відповідної мережі – 0C:D2:B5:03:43:68.

Тепер, знаючи потрібну інформацію, почнемо захоплювати пакети, в яких, можливо, отримаємо зашифрований пароль, зробити це можна ввівши таку команду: airodump-ng–w mtnl-org–c 4 –bssid 0C:D2:B5:03:43:68 mon0 (рис. 2.4).

Технологія wmtnl представлена на рис. 2.4, потрібно записати перехоплені пакети у файл mtnl (файл буде автоматично створено у вигляді: l-org-X.cap, де X номер файлу з перехопленими пакетами змінюватиметься, якщо атака переривалася, і починатиметься заново, не видаляючи старий файл), обрано як і назву мережі, щоби не плутатися; -c 4 —вказівку каналу, на якому працює

бездротова мережа під назвою mtnl; - bssid фізична адреса точки доступу; mon0 — вибір інтерфейсу, у якому виконати захоплення пакетів.

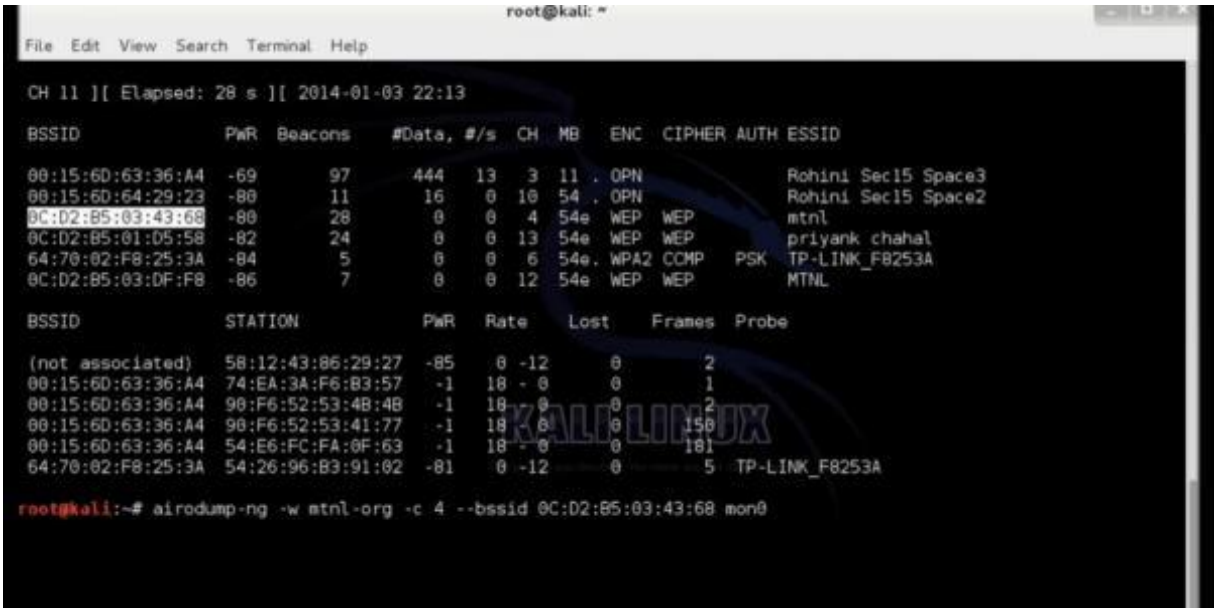

Рисунок 2.4 — Процес захоплення пакетів

Після виконання команди чекаємо орієнтовно 10-15 хвилин, щоб захопити близько 15000 IVS пакетів (пакетів, що містять вектор ініціалізації). Тривалість очікування залежить від активності мережі. Якщо до точки доступу ніхто не підключений, час може затягнутися. Відстань до точки доступу не така важлива, як активність у мережі. Якщо активність маленька, і збір пакетів йде повільно, то спробуємо «розтрусити» точку доступу, для цього відкриваємо ще один термінал — дуже важливо залишити термінал, що використовується раніше, активним, просто згортаємо його в трей і використовуємо команду: aireplay-ng -0 0 -a 0C:D2:B5:03:43:68 mon0, де -0 0 зробити атаку деаутентифікація(-0), доки вона не буде зупинена вручну (0), -a — фізична адреса точки доступу, mon0 — інтерфейс, що використовується для атаки.

Коли закінчили збір приблизно 15000 пакетів, відкриваємо новий термінал, у ньому починаємо розшифровувати пакет, для цього скористаємося командою: aircrack-ng mtnl-org-01.cap (рис. 2.5).

Після закінчення процесу дешифрування побачимо, що пароль 100% розшифровано коректно. Тепер можемо підключитися до точки доступу mtnl, використовуючи пароль: 3937353536.

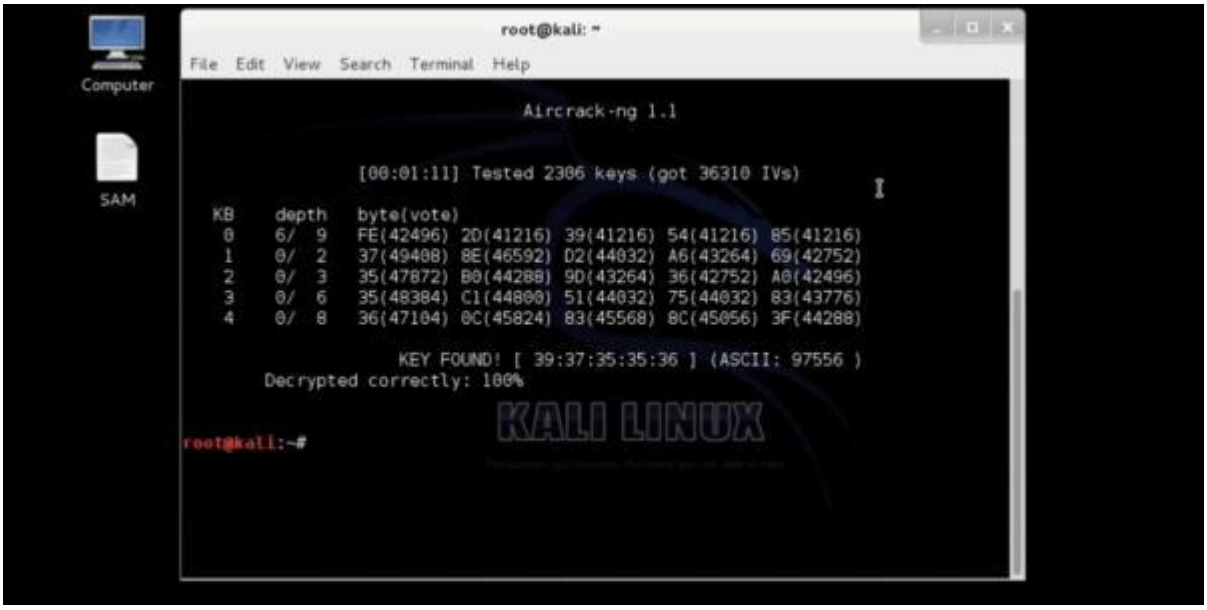

Рисунок 2.5 – Розшифровка пакетів

Якщо цього повідомлення не побачили або побачили, що не на 100%, повторіть захоплення пакетів і зберіть в 2-5 разів більше пакетів. І повторіть процес дешифрування. Кількість пакетів, що захоплюються, може вимагатися більше або менше, залежно від складності і довжини пароля.

2.3 Використання методу WPA/WPA2-шифрування для вивчення вразливостей Wi-Fi мереж

Перейдемо до тестування на проникнення в мережу, організовану бездротовою точкою доступу із встановленим на ній для авторизації WPA/ WPA2 Personal шифруванням.

Для цього потрібна бездротова точка доступу. Налаштовано її із зазначенням наступних параметрів:

- назва – pentest_router;
- пароль – дізнаємося наприкінці тип шифрування – WPA.

Приступимо до дій — для початку потрібно залогінитись під обліковим записом root, або будь-яким іншим, але тоді перед кожною командою потрібно вводити sudo.

Відкриваємо термінал (ctrl + alt + t) та для визначення драйвера вводимо команду: airmon-ng (рис. 2.6).

Рисунок 2.6 – Перегляд драйвера мережевої карти

Виведення команди показує список бездротових карт, які підтримують режим монітора. Якщо жодні карти не вказані, потрібно перепідключити адаптер і переконатися, що він підтримує режим моніторингу. Якщо використовується вбудований адаптер, він не підтримує режим монітора, тоді потрібно використовувати зовнішній за допомогою режиму монітора. У виведенні команди можна переконатися, що карта підтримує моніторинг і називається wlan0.

Далі потрібно перевести карту в режим моніторингу, для цього виконаємо команди airmon-ng start wlan0 (рис. 2.7).

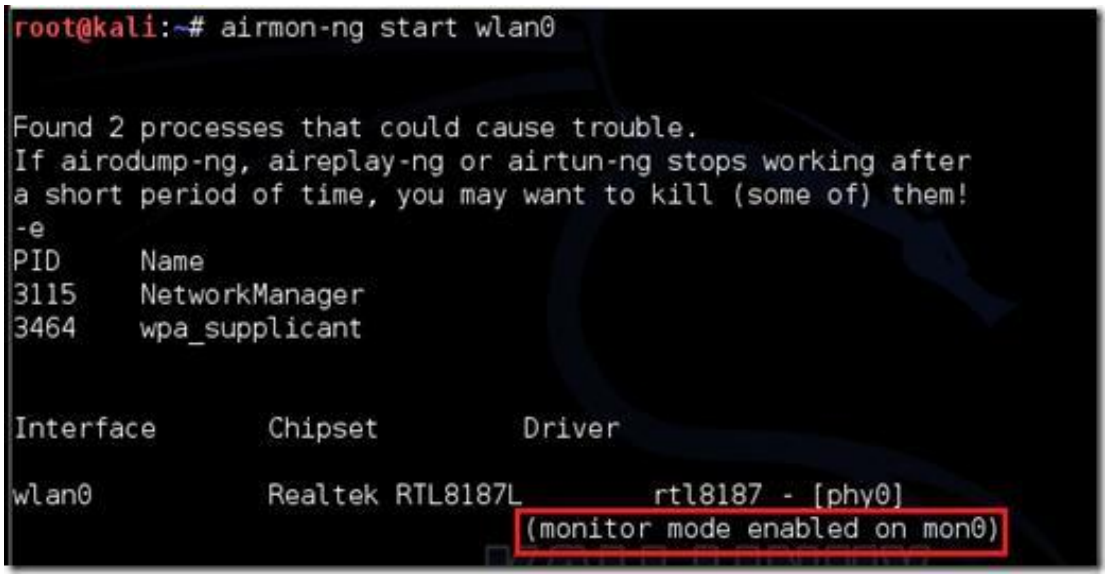

Рисунок 2.7 – Переведення мережевої карти в режим моніторингу

Червоним виділено виведення команди, що означає, що режим моніторингу увімкнено та інтерфейс називається mon0.

Наступним кроком буде включення режиму прослуховування для визначення доступних Wi-Fi мереж, для цього виконаємо команду airodump-ng mon0 (рис. 2.8).

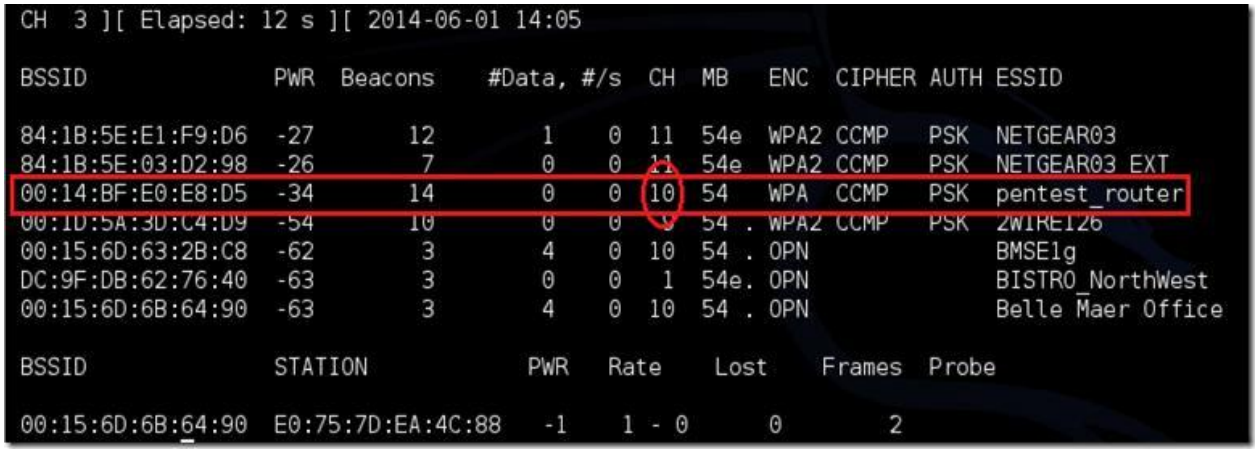

Рисунок 2.8 – Список бездротових мереж

На рис. 2.8 виділено мережу, яку створено та використовуємо для тестування атаки.

Далі потрібно використати команду: airodump-ng -c 10 -bssid 00:14:BF:E0:E8:D5 -w /root/Desktop/ mon0, де: -c – номер каналу, - bssid — фізична адреса точки доступу, -w — шлях, куди записуватимемо перехоплений початковий обмін пакетами, так званий «handshake».

Для того, щоб перехопити handshake потрібно після запуску виконання вищезгаданої команди дочекатися поки хтось підключиться до мережі, або, при наявному вже підключеному клієнті, потрібно зробити деавторизацію підключеного клієнта. Для виконання цього кроку може знадобитися багато часу, якщо активні підключення будуть відсутні. Підключимо будь-який інший пристрій до відомої мережі, емулюючи активність.

На рис. 2.9 відображено підключеного клієнта, де виділення червоним (меншим за розміром) є фізична адреса клієнта.

Рисунок 2.9 – Перегляд підключених клієнтів

Для виконання деавторизації клієнта потрібно, не закриваючи термінал, відкрити другий і виконати команду: aireplay-ng –0 2 –a 00:14:BF:E0:E8:D5 –c 4C:EB:42:59:DE:31 mon0, де -0 – ключ для проведення деавторизації, 2 – кількість пакетів де авторизації, -a – фізична адреса точки доступу, -c – фізична адреса клієнта, mon0 —інтерфейс, який використовується для атаки.

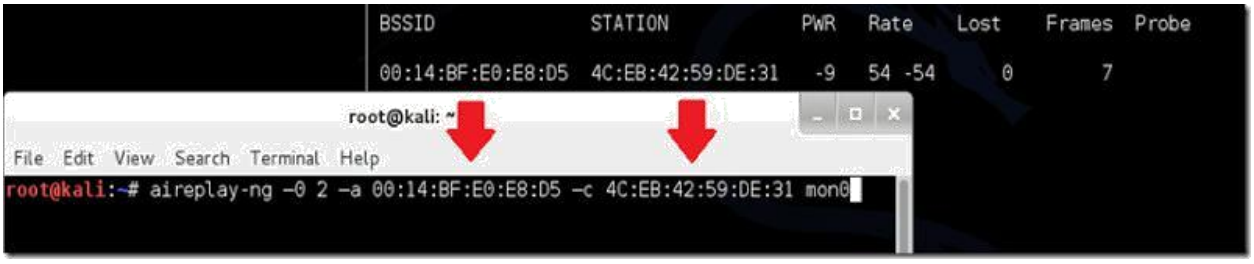

Рисунок 2.10 — Виконання деавторизації клієнта

Якщо все пройшло успішно, побачимо повідомлення в термінал, де виконували попередню команду (рис. 2.11).

Рисунок 2.10 – Перехоплення handshake

Потрібне нам повідомлення зображено на рис. 2.11.

Рисунок 2.11 – Перехоплений handshake

Отримавши це повідомлення, можна переходити до наступного кроку, інакше повторювати попередню команду доти, доки не отримаємо у виведенні повідомлення про отримання handshake'a.

Тепер можемо натиснути клавіші Ctrl+C в терміналі, в якому виконується aireplay. Не варто одразу закривати термінал.

Після цього можемо переходити до злому — використовуватимемо спосіб перебору. Для цього знадобиться словник паролів. Його можна легко знайти на просторах Інтернету або створити свій, дотримуючись лише кількох правил синтаксису: один пароль = один рядок і жодних пробілів перед і після і розширення файлу —.txt.

Приступимо до методу перебору пароля, для цього потрібно виконати команду: aircrack-ng –a2 –b 00:14:BF:E0:E8:D5 –w /root/wpa.txt root/Desktop/*.cap (рис. 2.12), де: -a — це метод атаки з використанням наявного рукостискання (handshake'a), 2 — WPA, -b — фізична адреса атакованої точки доступу, -w — шлях до словника з розширенням — txt, /root/Desktop/*.cap – директорія для збереження cap файлу, що містить пароль.

Рисунок 2.12 – Запуск перебору паролів

На рис. 2.13 після перебору 192 комбінацій у словнику знайшли пароль.

Цей метод не є оптимальним, оскільки, якщо словник місить кілька тисяч комбінацій, перебір виходить дуже довгим і часто трапляється, що пароля, встановленого на роутері, немає у словнику.

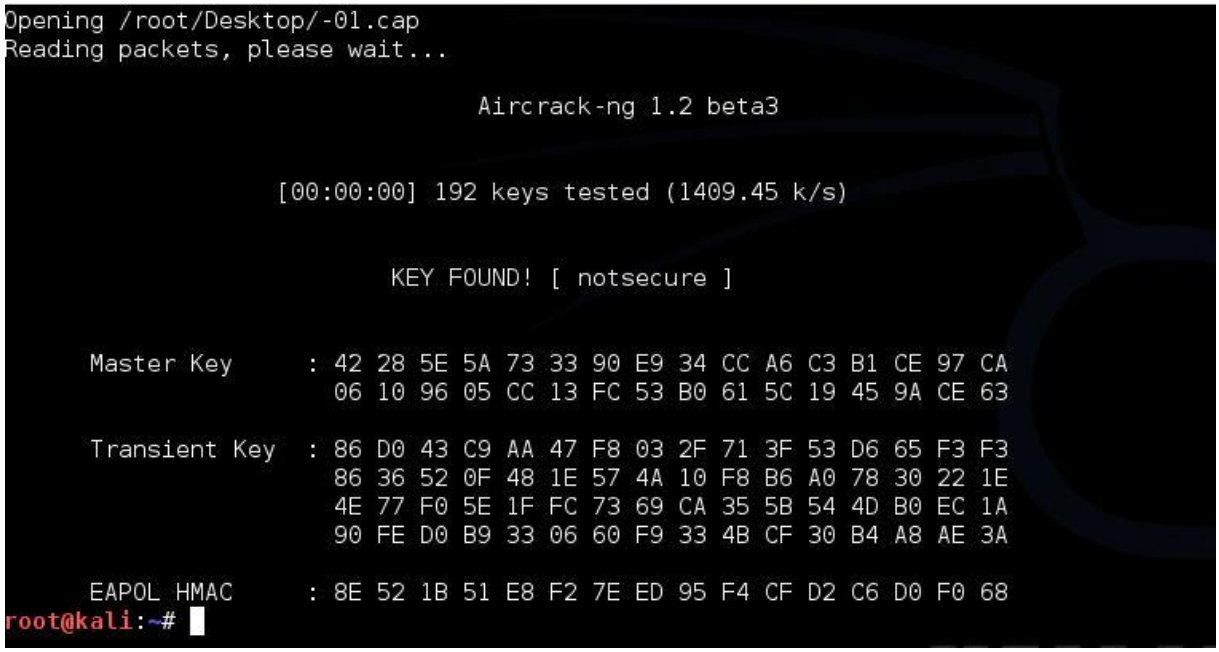

Рисунок 2.13 – Результат перебору паролів

Цей спосіб зручний для перебору найпопулярніших комбінацій, таких, як 12345678, qwertyui і т. п. У разі складних паролів цей спосіб може не мати жодного успіху. Але спробуємо розглянути ще один випадок. Наприклад, точка доступу також налаштована на WPS підключення (підключення за пін-кодом або натисканням клавіші на самому роутері). Для цього виконаємо дії, що і з методом перебору, до кроку визначення точки доступу та її каналу (дії ідентичні). Результат, який потрібен, показано на рис. 2.14.

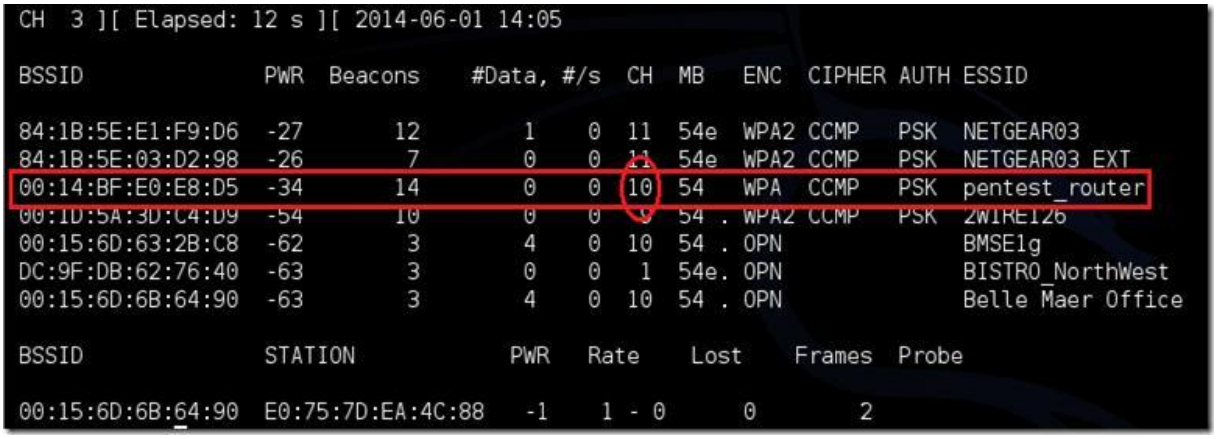

Рисунок 2.14 – Перевірка WPS

Перевіримо, чи WPS на точці доступу командою wash -i mon0. Якщо точки доступу немає у списку, то пробуємо іншу.

Далі починаємо перебір пін-кодів командою reaver -i mon0 -b 1C:BD:B9:B5:C6:B9 -a –vv, де mon0 – інтерфейс, з якого виконуємо атаку, -b – фізична адреса точки доступу, -a – автоматичне визначення параметрів злому, -vv– діагностичні повідомлення. У результаті виконується перебір пін-кодів (рис. 2.15).

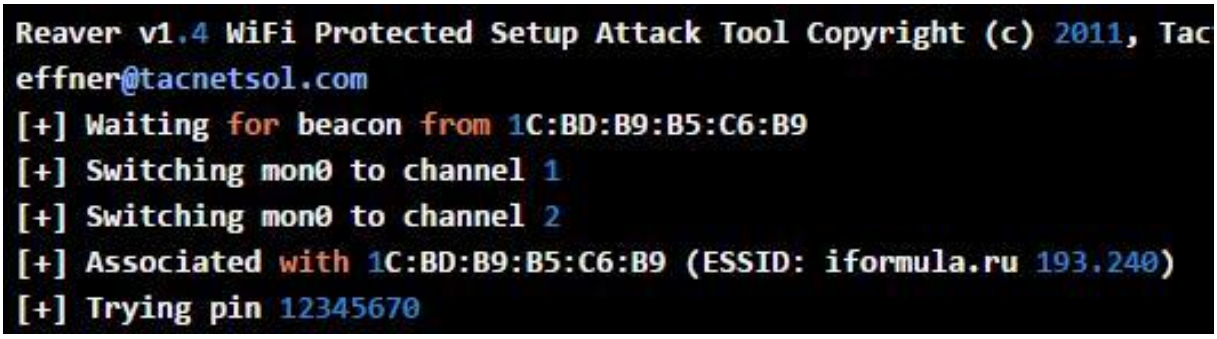

Рисунок 2.15 — Старт перебору пін кодів

Таким само довгим, але більш вірогідним способом можна отримати і WPSпін і WPAkey.

Різними ключами, доступними за командою reaver –h, можна прискорити процес не більше ніж удвічі, або вказати будь-які специфічні параметри для зламування конкретної точки доступу.

Через приблизно 10-12 годин ми отримуємо (рисунок 2.16).

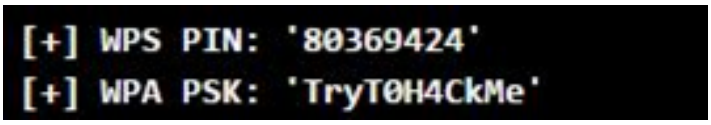

Рисунок 2.16 – Знайдений пін-код

Вищезазначені способи не є оптимальними, адже може статися так, що WPS вимкнено, встановлений пароль є досить великої довжини (встановлювати можна від 8 до 63 символів, і тоді перебір може закінчитися за кілька років, що, зрозуміло, є неактуальним).

Проаналізувавши загальнодоступну інформацію, дізнаємося про райдужні таблиці.

У результаті SQL-ін'єкції на сайті RockYou хакерам вдалося затягнути 32 мільйони паролів відкритим текстом. З того моменту і розпочалася нова епоха. Гігантська база даних дозволила розробникам ПЗ для злому паролів повністю

переробити словники, якими здійснюється брутфорс. Замість «теоретичних» словників вони з'явилися справжні словники з реальними паролями. База RockYou досі залишається унікальним, найкращим ресурсом для злому.

Після кожного нового витоку хешів все більшу частку з них вдавалося підібрати за словником, а ресурси виділялися на аналіз складних паролів, які потім також додавалися до словника. Наприклад, у наш час пароль на зразок Sup3rThinkers вважається легким для злому, тому що він підбирається за словником з кількома замінами, для яких існують відповідні правила. Для прискорення пошуку за словниками з десятків гігабайт застосовуються райдужні таблиці [16].

Тому скористаємося інструментом, що є у вільному доступі, і проведемо атаку на мережу з використанням «райдужних таблиць».

На ноутбуку встановлено відеокарту від AMD. Для проведення атаки потрібно встановити пропрієтарний fglrx драйвер, для цього послідовно виконаємо команди (рис. 2.17):

Оновлення системи:

- apt-get update;
- apt-getdist-upgrade;
- встановлення хедерів Linux та рекомендованих програм apt-get install firmware-linux-nonfree;
- apt-get install amd-opencl-icd apt-get install linux-headers-$(uname -r);
- встановлення драйверів fglrx та контрольної панелі apt-get install fglrx-atieventsdfglrx-driver fglrx-control fglrx-modules-dkms –y.

Тестування установки:

fglrxinfo

fgl_glxgears

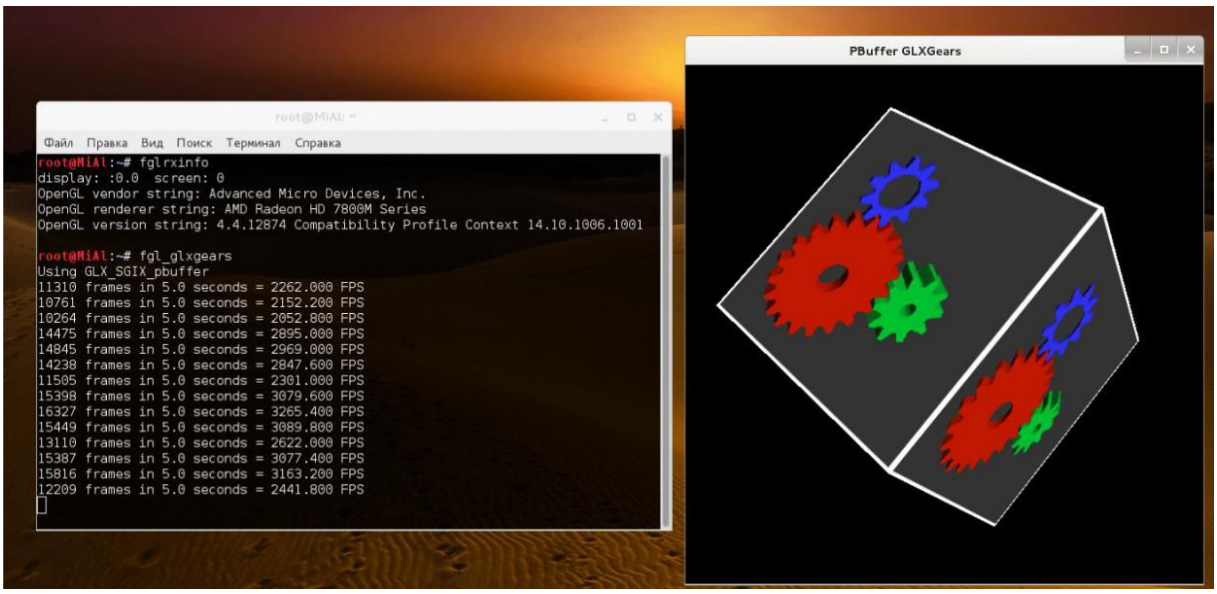

Рисунок 2.17 — Процес підготовки

Тепер потрібно згенерувати xorg.conf.

aticonfig --initial -f

файл xorg.conf буде розміщено у каталозі /etc/X11.

Далі потрібно оновити файл grub.cfg та перезавантажити ноутбук, для цього відкриваємо grub.cfg командою: leafpad /boot/grub/grub.cfg

знаходимо секцію:

```
### BEGIN /etc/grub.d/10_linux ###
menuentry 'Kali GNU/Linux, с Linux 3.18.0-kali3-amd64' --class kali --class gnu-linux --class gnu --class os {
load_video
insmod gzio
insmod part_msdos
insmod ext2
set root='(hd0,msdos1)'
search --no-floppy --fs-uuid --set=root 4b5ccc43-ae6f-4cca-bf7d-0344af8644c6
echo 'Загружается Linux 3.18.0-kali3-amd64 ...'
linux /boot/vmlinuz-3.18.0-kali3-amd64 root=UUID=4b5ccc43-ae6f-4cca-bf7d-0344af8644c6 ro initrd=/install/gtk/initrd.gz quiet
echo 'Загружается начальный ramdisk ...'
initrd /boot/initrd.img-3.18.0-kali3-amd64
}
```

Рисунок 2.18 — Сегмент конфігураційного файлу grub.cfg

І, на кінець наступного рядка (рис. 2.19)

```
linux /boot/vmlinuz-3.18.0-kali3-amd64 root=UUID=4b5ccc43-ae6f-4cca-bf7d-0344af8644c6 ro initrd=/install/gtk/initrd.gz quiet
```

Рисунок 2.19 – Вихідний рядок

Додаємо radeon.modeset = 0, тобто, має вийти такий рядок (рис. 2.20).

```
linux /boot/vmlinuz-3.18.0-kali3-amd64 root=UUID=4b5ccc43-ae6f-4cca-bf7d-0344af8644c6 ro initrd=/install/gtk/initrd.gz quiet r
adeon.modeset=0
```

Рисунок 2.20 – Потрібний рядок

Звернемо увагу на те, що значення UUID, яке в цьому випадку 4b5ccc43-ae6f-4cca-bf7d-0344af8644c6, може бути різним на кожному ПК. Перезаписуйте значення необхідним.

Зберігаємо файл та перезавантажуємо ноутбук командою: Reboot.

Після перезавантаження нам потрібно перевірити, чи встановлено модуль fglrx, командою: lsmod | grepfglrx.

У результаті має бути виведено приблизно таке (рис. 2.21).

```
fglrx 8679112 140
button 12988 1 fglrx
```

Рисунок 2.21 – Перевірка коректності установки модуля fglrx

Далі потрібно встановити AMDAPPSDK 3.0 Beta, для встановлення спочатку скачем зі сторінки завантаження архівів AMD, доступне за посиланням: http://developer.amd.com/tools-and-sdks/opencl-zone/amd-accelerated-parallelprocessing-app-sdk/.

Переходимо до установки SDK, виконаємо такі команди:

- mkdiramdappsdk — створюємо папку;
- mv/root/Downloads/AMD-APP-SDK-v3.0-0.113.50-Beta-linux64.tar.bz2;
- amdappsdk/ – копіюємо завантажений архів у створену папку cdamdappsdk – переходимо до створеної папки;
- tarxvjfAMD-APP-SDK-v3.0-0.113.50-Beta-linux64.tar.bz2 – розпаковуємо архів shAMD-APP-SDK-v3.0-0.113.50-Beta-linux64.sh – запускаємо установник.

Дотримуючись інтерактивної інструкції, проходимо установку до кінця і, найголовніше, коли програма запитає шлях установки, натискаємо Enter, щоб встановити в папку за замовчуванням, а саме /opt - що і потрібно. Далі потрібно

відредагувати файл /root/.bashrc, виконаємо команду leafpad /root/.bashrc і в кінець файлу допишемо, як показано на рис. 2.22.

```
# AMD APP SDK
export AMDAPPSDKROOT=/opt/AMDAPPSDK-3.0-0-Beta/
export AMDAPPSDKSAMPLESROOT=/opt/AMDAPPSDK-3.0-0-Beta/
export LD_LIBRARY_PATH=${AMDAPPSDKROOT}lib/x86_64:${LD_LIBRARY_PATH}
export ATISTREAMSDKROOT=$AMDAPPSDKROOT
```

Рисунок 2.22 – Необхідний конфігураційний файл

Зберігаємо зміни та потім у терміналі виконуємо команду: source ~/.bashrc

Перевірити успішність установки та початкового налаштування можемо командою:env | grep -i amd. Вивід має бути приблизно наступного виду:

```
AMDAPPSDKSAMPLESROOT=/opt/AMDAPPSDK-3.0-0-Beta/
LD_LIBRARY_PATH=/opt/AMDAPPSDK-3.0-0-Beta/lib/x86_64:
ATISTREAMSDKROOT=/opt/AMDAPPSDK-3.0-0-Beta/
AMDAPPSDKROOT=/opt/AMDAPPSDK-3.0-0-Beta/
```

Рисунок 2.23 – Виведення команди env | grep -Iamd

Далі потрібно встановити CAL++. Тепер потрібно підготуватися для наступного кроку, виконаємо команди:

- svn checkout https://github.com/clockfort/amd-app-sdk-fixe s/trunk/include/ CAL $AMDAPPSDKROOT/include/CAL;
- apt-get install cmakelibboost-all-dev.

Завантажуємо сам CAL++ за посиланням:

https://sourceforge.net/projects/calpp/files/calpp-0.90/calpp-0.90.tar.gz/download

Встановлюємо CAL++:

- cd ~/Downloads
- tar-xvfcalpp-0.90.tar.gz
- cd calpp-0.90/

Потрібно відредагувати файл CMakeLists.txt, для цього виконаємо команду:

leafpad CMakeLists.txt.

Знаходимо рядки, що починаються з FIND_LIBRARY та FIND_PATH та поміняємо їх, як показано на рис. 2.24.

```
FIND_LIBRARY( LIB_ATICALCL aticalcl PATHS "$ENV{ATISTREAMSDKROOT}" )
FIND_LIBRARY( LIB_ATICALRT aticalrt PATHS "$ENV{ATISTREAMSDKROOT}" )
FIND_PATH( LIB_ATICAL_INCLUDE NAMES cal.h calcl.h PATHS "$ENV{ATISTREAMSDKROOT}/include/CAL" )
```

Рисунок 2.24 — Результат зміни файлу

Зберігаємо відредагований файл та закриваємо його. Далі для встановлення виконуємо команди:

- cmake. («.» обов'язкова);
- make;
- makeinstall.

Заключним підготовчим етапом буде встановлення Pyrit. Pyrit дозволяє створювати масивні бази даних, попередньо прораховувати частину фази автентифікації IEEE 802.11 WPA/WPA2-PSK з компромісними витратами часу та місця. Використання обчислювальної потужності багатопроцесорних систем та інших платформ, у тому числі ATI-Stream, Nvidia CUDA, OpenCL і VIA Padlock, – це на даний момент найбільш потужний вектор атаки на протоколи безпеки, що найбільш використовуються.

Для встановлення виконаємо наступні команди: apt-getinstalllibpcap-dev – встановлюємо бібліотеку, що бракує, svncheckouthttp://pyrit.googlecode.com/ svn/trunk/ pyrit_svn – завантажуємо pyrit cdpyrit_svn/pyrit/ -переходимо в папку /setup.pybuildinstall – запускаємо установку Установка плагіна CAL++.

Переходимо до папки командою: cd ../cpyrit_calpp/ та редагуємо файл setup.py, для цього введемо команду leafpad setup.py. Знаходимо у файлі рядок: VERSION = '0.4.0-dev' і наводимо його до вигляду:VERSION = '0.4.1-dev'. Знаходимо рядок: CALPP_INC_DIRS.append(os.path.join (CALPP_INC_DIR, 'include')) і наводимо його до вигляду: CALPP_INC_DIRS.append (os.path.join(CALPP_INC_DIR, 'include/CAL')).

Зберігаємо внесені зміни та закриваємо редагування файлу. Далі вводимо команду: ./setup.py buildinstall.

Буде кілька попереджень, але не повинно бути помилок.

Тестуємо Pyrit командою: pyritlist_cores (рис. 2.25).

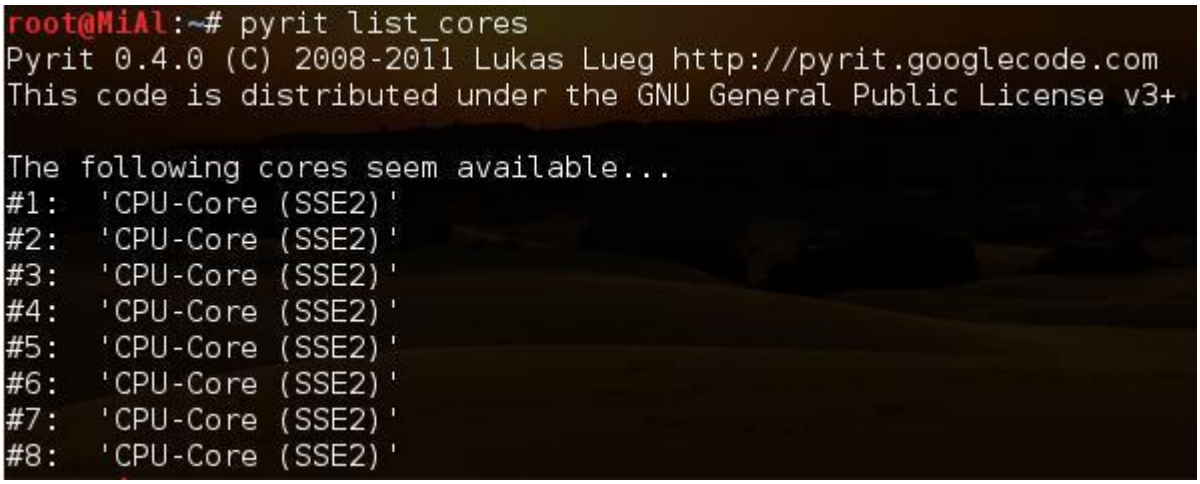

Рисунок 2.25 – Список ядер

Для наочності виконаної роботи наведу два приклади роботи Перший без CAL++ (рис. 2.26). Бачимо 4037,9 PMKs/s. Другий із CAL++ (рис. 2.27). Бачимо 33129,5 PMKs/s.

Рисунок 2.26 — Швидкість перебору парольних фраз без CAL++

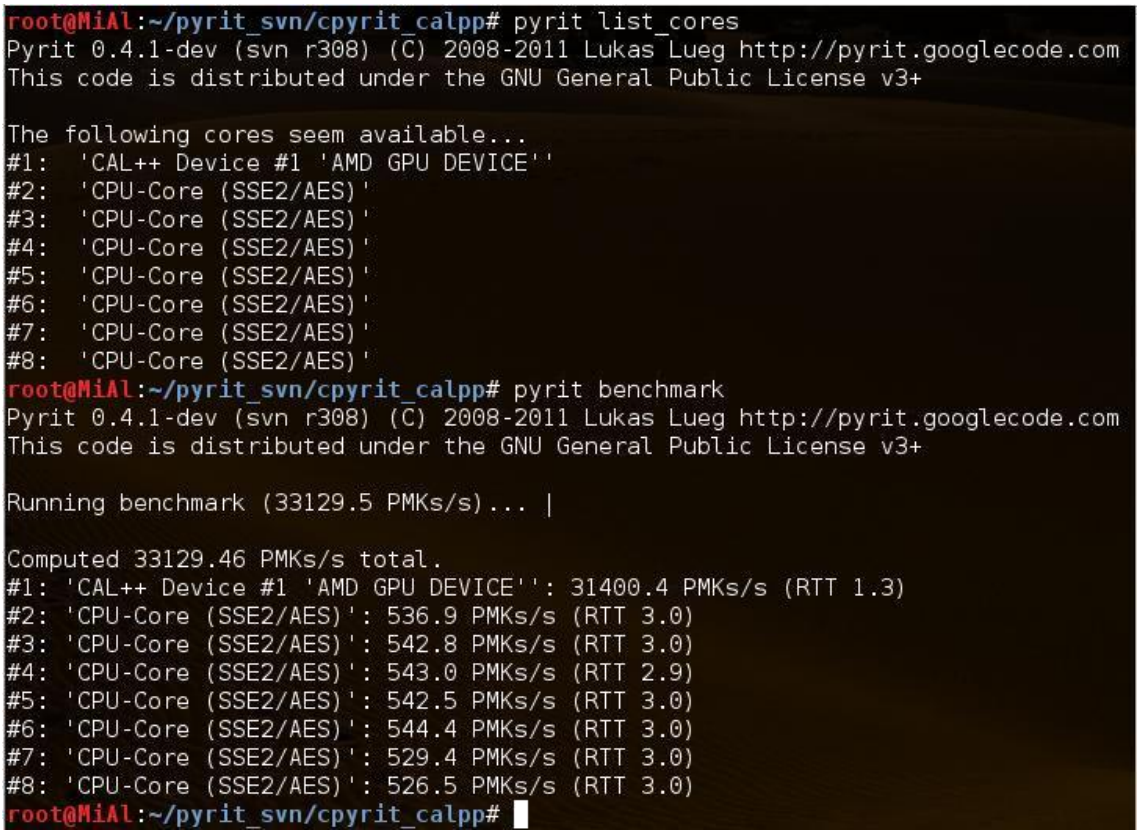

Рисунок 2.27 — Швидкість перебору парольних фраз із CAL++

У PMKs/s вимірюється швидкість, звана SpeedHashcat – швидкість перебору хешів (результату виконання підрахунку хеш функцій).

Тепер ноутбук готовий до атаки з використанням райдужних таблиць. Оскільки використання райдужних таблиць має на увазі такий самий перебір, як і в першому випадку, і підготували ноутбук для прискореного перебору з використанням відеокарти та процесора. Відмінність полягає лише в тому, що перебір буде не безпосередньо кодової комбінації, а хеші з алгоритмом перестановки. Потрібно захопити «рукостискання» – «handshake» Для початку переведемо мережевий адаптер в режим моніторингу.

Для захоплення «handshake» можна, можливо скористатися утилітою, що автоматизує дії, яка називається wifite і йде за замовчуванням в KaliLinux.

Введемо команду Wifite.

Можемо, як ключі вказати тип шифрування (WEP, WPA, WPA2), якщо хочете вивести бездротові мережі з конкретним типом шифрування. Коли програма закінчить роботу, побачимо доступні точки доступу, а також запрошення для

введення точок доступу, з яким хочете отримати handshake. Обрано 1 і 2, для цього введено без лапок "1,2" і натиснуто ENTER, якщо хочете вибрати все відразу, то потрібно замість "1,2" (без лапок) вписати "all" (без лапок). Після того, як натиснуто Enter, звернемо увагу на вивід. Дуже довго на першій точці доступу нічого не відбувалося і щоб не гаяти час натиснуто клавіші ctrl+c. Далі програма запитала, як показано на рис. 2.28.

І тут виявилася зручна функція, так як у реченні було натиснути клавішу «c» для атаки на інші вибрані точки, або «e» для виходу.

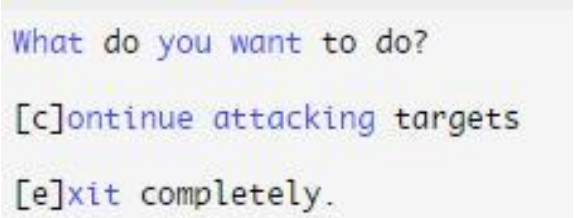

Рисунок 2.28 — Діалогове вікно

Натиснуто «c» і через кілька секунд отримав "handshake", це «рукостискання» було збережено у файлі: /root/hs/BigPond_58-98-35-E9-2B-8D.cap. Після того, як захоплення відбулося, і точок доступу більше немає, програма автоматично завершить своє виконання, і отримаємо командний рядок.

Тепер, коли є файл із захопленим «рукостисканням», можемо піти двома шляхами:

- використовувати атаку за словником;
- використовувати атаку «грубою силою».

У зв'язку з тим, що за статистикою, кожна п'ята точка доступу матиме пароль зі словника rockyou, який поповнюється новими паролями після кожного витоку в Інтернеті, розглянемо спочатку атаку за словником.

Завантажуємо актуальну версію словника за https:// wiki.skullsecurity.org/index.php?title=Passwords Скопіюємо файл словника до каталогу root, виконавши команду: cp /usr/share/ wordlists/rockyou.txt.gz

Розпакуємо архів, виконавши команду:

gunziprockyou.txt.gz.

Відповідно до IEEE 802.11 довжина пароля повинна бути не менше 8 символів і не більше 63, очистимо словник і приберемо всі записи, які не задовольняють умові 7 < кількість символів у записі < 64, виконаємо це такою командою

cat rockyou.txt | sort | uniq | pw-inspector -m 8 -M 63 > newrockyou.txt,

де m 8 –мінімальна довжина символів;

-M 63 – максимальна довжина символів;

sort – відсортувати;

uniq – тільки унікальні записи;

> newrockyou.txt – вихідний файл після сортування.

Тепер визначимо, скільки унікальних комбінацій залишилося, командою wc –lnewrockyou.txt.

Вивід команди видав 9605346 записів = паролів.

Виконавши команду:

wc –lrockyou.txt.

Вивід команди видав 14342346 записів = паролів.

Отже, зробили файл коротшим, що означає, що можемо протестувати словник у більш стислий термін, тепер перейменуємо файл і зробимо його у вигляді: wpa2.lst, командою:

mv newrockyou.txt wpa.lst.

Наступним кроком буде створення ESSID у базі даних Pyrit, для цього виконаємо команду:

pyrit -eBigPondcreate_essid, де BigPond — назва бездротової мережі.

Якщо у назві бездротової мережі є пробіли, то найменування разом із пробілом (як є) пишеться в апострофах.

Наступним кроком потрібно імпортувати відсортований та перейменований словник у базу даних pyrit, для цього виконаємо команду:

pyrit -i /root/wpa.lstimport_passwords.

Створюємо «райдужні таблиці», використовуючи пакетний (batch) процес, для цього виконаємо команду:

Pyritbatch.

Звернемо увагу, що на ноутбуці процесор був задіяний на 100%, і температура на ядрах піднялася до 94 градусів Цельсія. Потрібно бути дуже обережним, і в залежності від того, наскільки великий файл словника та наскільки гарячі процесор та відеокарта. Бажано наскільки можна використовувати додаткове охолодження.

Тепер сам процес злому. Є пара варіантів:

- використовуючи Pyrit;

- використовуючи Cowpatty.

Використовуватимемо атаку на «рукостискання» з бази даних, використовуючи Pyrit, для цього введемо команду:

pyrit -r hs/BigPond_58-98-35-E9-2B-8D.cap attack_db, де hs/ — файл із захопленим handshake'ом, attac_db — використовувана база даних.

Час виконання – кілька хвилин, щоб пройти по всій таблиці бази даних. Швидкість у виведенні команди сягала 159186.00 PMKs/s. І, якщо встановлений пароль був у базі даних, він визначається за кілька хвилин. Очевидно, що це швидше за перші два способи.

Якщо не створювати базу даних, а звертатися безпосередньо до словника (не імпортованого wpa2.lst), то можна скористатися командою pyrit – rhs/BigPond_58-98-35-E9-2B-8D.cap, де -i /root/wpa.lst – шлях до словника, attack_passthrough – атака по проходу (проходитиметься словник, комбінація за комбінацією).

За виконання цієї команди швидкість склала близько 8000 PMKs/s, що значно повільніше і неоптимально.

Продовжимо шукати оптимальний спосіб, для цього спробуємо скористатися cowpatty для проведення нашої атаки, введемо наступну команду:

pyrit -e BigPond -o cow.outexport_cowpatty.

Після запуску процесу перебору, командою:

cowpatty -d cow.out -s BigPond -r hs/BigPond_58-98-35-E9-2B-8D.cap.

Після введення команди буде перевірено великий список паролів на відповідність хеш файлу. Це продовжуватиметься до перебору всіх паролів. Як тільки у файлі словника буде знайдено відповідний пароль, процес злому зупиниться, і вам буде виведено пароль. Швидкість у момент перебору склала 164 823 PMKs/s.

Зробимо висновок, що цей спосіб є найефективнішим і найшвидшим. Дуже зручно за допомогою засобів автоматизації деяких процесів швидко перевіряти безпеку мережі.

2.4 Висновки до розділу 2

Для перевірки і тестування захищеності мережі можна використовувати персональний комп'ютер чи ноутбук з певними параметрами, конфігурацію яких було вказано вище, використовуючи всі встановлені останні оновлення.

3 РОЗРОБЛЕННЯ СИСТЕМИ ДЛЯ ПЕРЕВІРКИ ТА ТЕСТУВАННЯ ЗАХИЩЕНОСТІ WI-FI МЕРЕЖІ

3.1 Тестування захищеності WI-FI мережі з використанням одноплатного комп’ютера

У ході виконання роботи визначено, що потрібний мобільний пристрій на базі ОС Linux, за допомогою якого зможемо робити атаки, в той же час через досить тривалий процес нам потрібна хороша автономність. Крім хорошої автономності необхідний мінімальний розмір пристрою, для того, щоб можна було його сховати в будь-якій сумці, без уваги. Виникає питання: навіщо такі вимоги? Логічним буде висновок, що при зайнятті перевіркою та тестуванням захищеності не потрібно великих габаритів, що цю функцію може виконати будь-яка людина, яка знаходиться в радіусі роботи бездротової точки доступу. Тим самим було демонструючи потенційному замовнику чистоту процесу. Зробивши висновки з вищезгаданих обмежень і провівши аналіз ринку вільно доступних пристроїв, вибір упав на одноплатні комп'ютери на ARM архітектурі.

Переваги перед ноутбуками та нетбуками:

— низьке тепловиділення, що не вимагає активного охолодження і як наслідок безшумності пристрою;

— низьке енергоспоживання, чим досягається достатня автономність;

— відсутність вбудованих пристроїв введення та виведення, таких як клавіатура та монітор, що зменшує розміри пристрою;

— велика кількість програмного забезпечення у вільному доступі.

Недоліки:

— відсутність вбудованих пристроїв введення та виведення, що вимагає додаткових пристроїв для керування;

— низька обчислювальна потужність;

— слабкий контролер живлення.

Дивлячися на переваги та недоліки, виникає усвідомлене розуміння, що одноплатні комп'ютери задовольняють всі вимоги, крім обчислювальної

потужності. Тому що пристроєм введення та виведення може бути будь-який смартфон або планшет. Наявність USB порту та великої кількості вільно доступного ПЗ дозволяє використовувати 3G/4G модем для підключення зовнішнього пристрою управління за протоколами ssh, telnet, VNC та інші.

У ході аналізу ринку одноплатних комп'ютерів було зроблено акцент на двох поширених моделях: Raspberry Pi 3 model B та Intel Edison Kit, які показано на рисунку 3.1, у ході порівняння наведеного в табл. 3.1.

а) Raspberry Pi 3 model Bi

б) Intel Edison Kit

Рисунок 3.1 — Зовнішній вигляд одноплатних мікрокомп’ютерів

Таблиця 3.1 — Порівняння двох популярних одноплатних комп'ютерів

Найменування	Raspberry Pi 3 model B	Intel Edison Kit
Виробник	RaspberryPiFoundation	Intel
Графічний процесор	2-х ядерний videocoreiv	Відсутнє
ОЗУ	1 Гб	1 Гб
Підтримувані ОС	Linux, Windows 10	Linux, Windows embedded
Тип процесора	bcm2387 4-х ядерний cortex-a53	intelatom+intel quark
Встановлені інтерфейси	4 xusb, hdmi, ethernet, micro-sd, audio, dsi, csi, i/o	usb, i/o, wi-fi, bluetooth, Arduino
Частота процесора	1.2 ГГц	500 МГц

Із представленого порівняння за технічними характеристиками Raspberry Pi model B перевершує Intel Edison 3 Kit. У зв'язку з цим для перевірки та тестування захищеності Wi-Fi мережі використовуватимемо RaspberryPi 3 modelB.

3.2 Підготовка одноплатного комп'ютера

Одноплатний комп'ютер у базовій комплектації не дозволяє проводити атаки на бездротові мережі. Щоб з'явилася ця можливість, потрібно:

- оснастити USBWi-Fi адаптером з режимом проведення ін'єкцій;
- карта пам'яті MicroSD16Gb 10Class;
- дистрибутив KaliLinux для RaspberryPi, що включає до свого складу необхідні пакети, такі як airmon, aircrack і т. п.;
- портативний акумулятор з двома USB-портами (2A, 5V, 16000 mAh);
- USB хаб із зовнішнім живленням;
- 3G/4G модем з «білою» IP адресою.

Для керування одноплатним комп'ютером за допомогою стороннього пристрою необхідно встановити та налаштувати SSH сервер. Згодом для керування буде використовуватися SSH підключення із зазначенням наступних параметрів:

- IP-адресою для підключення буде «біла» IP-адреса 3G/4Gмодема;
- логін та пароль будуть використані вказані під час встановлення ОС.

Подальшою дією буде тестування швидкості перебору парольних комбінацій, всі підготовчі дії проведено відповідно до пункту підготовки до проведення атаки на мережу з використанням «райдужних таблиць» (пункт 2.3).

Швидкість перебору 2037,9 парольних комбінацій за секунду, що не є достатнім результатом для швидкого проникнення (рисунок 3.2).

Рисунок 3.2 – Швидкість перебору на одноплатному комп’ютері

Отже, для злому WEP потрібні перехоплені пакети, записані в файл з розширенням .cap; для злому WPA/WPA2 потрібний так зване рукостискання (handshake) та словник парольних фраз; Злом WPA/WPA2 за допомогою райдужних таблиць відрізняється від простого злому лише в методі перебору парольних фраз, де до обчислень залучаються ресурси графічного адаптера. Тому вирішили рознести процеси проведення атаки. За допомогою одноплатного комп'ютера робити захоплення необхідної інформації, а далі для її обробки передавати на віддалену машину, з великими обчислювальними потужностями, порівняно з одноплатним комп'ютером.

3.3 Побудова системи для перевірки та тестування захищеності WI-FI мережі

Для виконання ресурсомістких операцій, таких як пошук по райдужних таблицях, обчислення райдужних таблиць, потрібні великі потужності ЦП і відеокарти. Знаючи про те, що процес захоплення handshake і процес перебору парольних фраз можна рознести, вирішено використовувати стаціонарний персональний комп'ютер, який знаходиться вдома або в офісі, має вихід в Інтернет і має наступні мінімальні характеристики:

— процесор не гірший за Core i7 5930K;

— відеокарта не гірша за Radeon RX 480 G1;

— ОЗП не менше 32 ГБ із тактовою частотою 3200 МГц і вище;

— SSD накопичувач.

Вищевказані мінімальні характеристики комп'ютера дозволяють, зробивши всі підготовчі дії, наведені в пункті підготовки до проведення атаки на мережу з використанням «райдужних таблиць», продемонструвати швидкість перебору в 95218,5 парольних комбінацій (рис. 3.3).

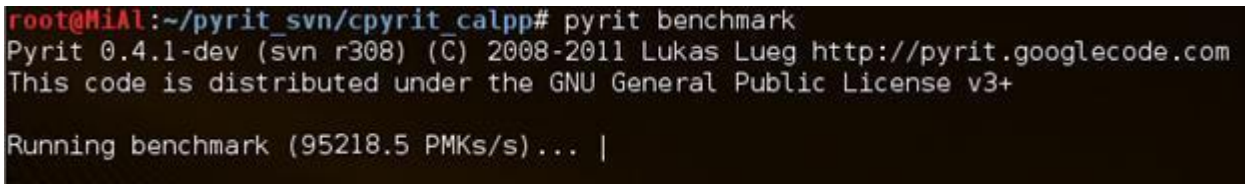

Рисунок 3.3 – Швидкість перебору на потужному комп'ютері

Вказані вище мінімальні характеристики дозволяють отримати пароль SS367JYNbyeEJ285, маючи початкове значення виконання його хешування (8fae34ea751a81a7d41572d38eec54ea) приблизно за 11-12 секунд. Крім виконання операції перебору пароля є ще одна ресурсомістка операція, це операція створення райдужних таблиць, яку потрібно виконувати для кожної точки доступу, що атакується. При перерахованих вище мінімальних характеристиках комп'ютера

створення райдужних таблиць для парольної фрази довжиною від 8 до 63 символів займає близько 15-20 хвилин, що не буде критичним для проведення атаки на проникнення.

Зв'язок двох пристроїв. У ході виконання рознесеного тестування на проникнення з'ясувалося кілька складних нюансів. По-перше, кожна точка доступу, на яку збираємося проводити атаку, має свій унікальний BSSID і в автоматичному режимі складно зробити вибір даної точки доступу, набагато швидше і точніше це робиться при виконанні вручну. По-друге, для отримання handshake потрібно переводити бездротовий інтерфейс в режим моніторингу, при виконанні даної функції скриптом інтерфейс не переводився в 25% випадках з 20 випробувань. По-третє, отримавши handshake і автоматично передаючи його на потужний комп'ютер, є ймовірність неправильної його передачі, для переконання в правильності передачі потрібно додатково передавати контрольну суму з подальшою перевіркою цілісності. Потрібна наявність «білої» IP-адреси на потужному комп'ютері для встановлення сесії передачі від одноплатного на потужний комп'ютер, але це змушує до додатковим затратам. З усього вищесказаного був зроблений висновок, що весь процес рекомендовано відстежувати в реальному часі, і з'являється можливість вносити коригування в алгоритм перевірки та тестування захищеності.

Для керування процесом та передачі файлів між 2 пристроями будемо використовувати третій — керуючий пристрій, в якості якого використовуватиметься планшет або смартфон із підключеним мобільним інтернетом та встановленими:

— TeamViewer;

— SSH клієнт.

TeamViewer буде використовуватися для підключення до потужного комп'ютера та виконання на ньому операцій:

— передача з управителя пристрої на потужний комп'ютер handshake'ів від точок доступу з налаштованим алгоритмом безпеки WPA/WPA2;

— передача з керуючого пристрою на потужний комп'ютер захоплених

пакетів від точки доступу з налаштованим алгоритмом безпеки WEP;

— виконання команд для створення райдужних таблиць;

— управління перебором парольних фраз.

SSH клієнт буде використовуватися для підключення до одноплатного комп'ютера RaspberryPi 3 model B і виконання на ньому операцій:

— переведення бездротового Wi-Fi інтерфейсу в режим моніторингу;

— вибір точки доступу, що атакується;

— захоплення handshake'ів від точок доступу з налаштованим алгоритмом безпеки WPA/WPA2 та передача їх на керуючий пристрій;

— захоплення пакетів від точок доступу з налаштованим алгоритмом безпеки WEP та передача їх одним файлом на керуючий пристрій.

Вищезазначене програмне забезпечення даним функціоналом не обмежується, перераховані лише основні функції, що використовуються в даній роботі.

Покрокова структура виконання перевірки та тестування захищеності. Для перевірки та тестування захищеності необхідно виконати таку послідовність кроків:

— увімкнути потужний комп'ютер із налаштованим авто запуском TeamViewer;

— створити словник, (текстовий файл із парольними фразами), з наявного у вільному доступі rockyou.txt, вибравши всі парольні фрази завдовжки від 8 до 63 символів;

— підготувати одноплатний комп'ютер, підключивши Wi-Fi адаптер та USB 3G/4G модем з «білою» IP-адресою;

— опинитися в радіусі дії точки доступу, що атакується.

— включити одноплатний комп'ютер, вставивши кабель живлення у портативний акумулятор;

— дочекавшись остаточного завантаження одноплатного комп'ютера, (приблизно дві хвилини), підключитися до нього з керуючого пристрою за допомогою SSH клієнта;

— перевести бездротовий Wi-Fi інтерфейс у режим моніторингу;

— вибрати точку доступу, що атакується;

— провести перехоплення handshake'a або пакетів, (залежно від протоколу безпеки встановленого на точці доступу).

— за допомогою команди scp скопіювати handshake або перехоплені пакети, записані у файл під час виконання п. 8;

— завершити SSH сесію;

— скопіювати передані на керуючий пристрій файли в буфер обміну;

— запустити на керуючому пристрої TeamViewer і підключитися до потужного комп'ютера;

— виконати команду вставки (права кнопка миші>вставити) в необхідні директорії на потужному комп'ютері;

— якщо є точка доступу з налаштованим протоколом безпеки WEP, то виконавши команду: aircrack-ng «повний шлях до файлу без лапок», в результаті отримаємо шуканий пароль, який можна використовувати для підключення до бездротової мережі, що атакується. Якщо налаштований алгоритм безпеки WPA/WPA2, слід пропустити даний пункт і перейти до п.16;

— створити ESSID в база даних «pyrit» командою pyrit -e «назва атакованої точки доступу без лапок» create_essid;

— імпортувати до бази даних відсортований словник, отриманий під час виконання п.2 командою pyrit -i «повний шлях до файлу без лапок» import_passwords;

— створюємо «райдужні таблиці», використовуючи пакетний (batch) процес, виконавши команду: pyritbatch;

— активувати cowpatty для швидкого перебору, командою: pyrit-e «назва точки доступу без лапок» -ocow.outexport_cowpatty;

— запускаємо процес перебору парольних фраз командою cowpatty -dcow.out -sBigPond -rhs/"повний шлях до файлу з handshake'ом";

— чекаємо на закінчення виконання процесу перебору парольних фраз та в результаті отримуємо пароль, за допомогою якого можемо підключатися до бездротової мережі.

3.4 Створення захисту мережі за допомогою WPA2-ENTERPRISE

Корпоративні мережі з шифруванням WPA2-Enterprise будуються на аутентифікації протоколу 802.1x через RADIUS-сервер. Протокол 802.1x (EAPOL) визначає методи відправлення та прийому запиту даних аутентифікації та зазвичай вбудований в операційні системи та спеціальні програмні пакети.

802.1x передбачає три ролі в мережі:

— клієнт (supplicant) — клієнтський пристрій, якому потрібен доступ у мережу;

— сервер аутентифікації (зазвичай RADIUS);

— аутентифікатор — роутер/комутатор, який з'єднує багато клієнтських пристроїв із сервером аутентифікації та відключає/підключає клієнтські пристрої.

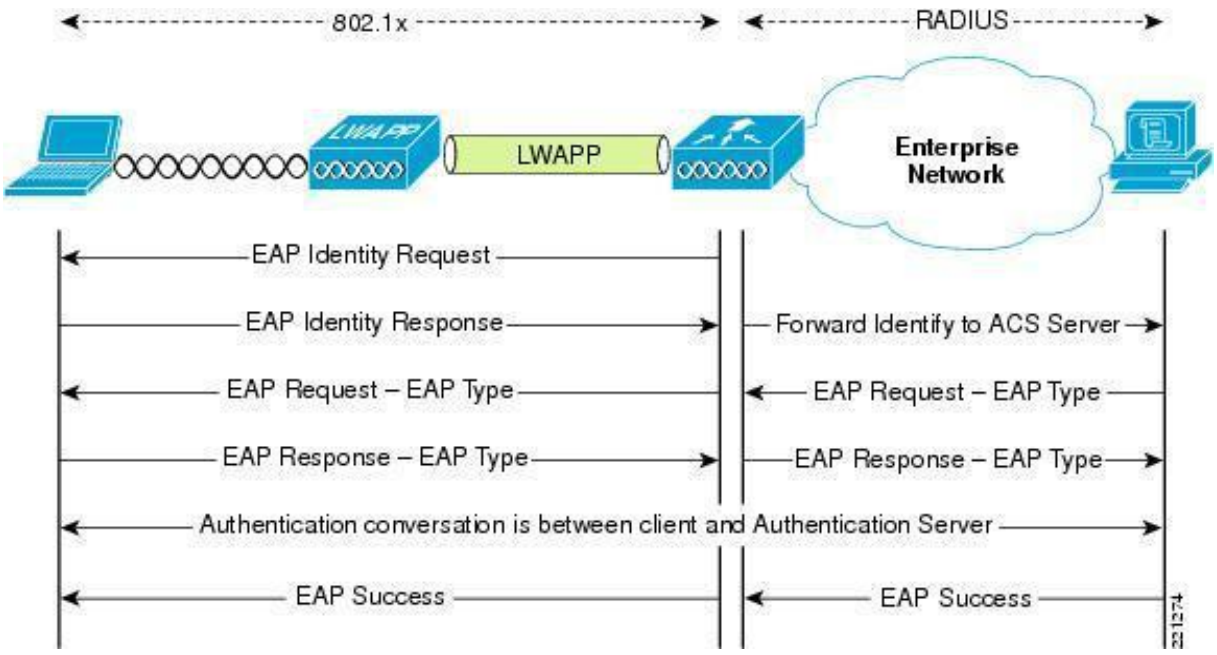

Рисунок 3.4 – Схема роботи протоколу 802.1x

Є кілька режимів роботи 802.1x, але найпоширеніший і найнадійніший наступний.

Аутентифікатор передає EAP-запит на клієнтський пристрій, коли виявляє активне з'єднання. Клієнт відправляє EAP-відповідь — пакет ідентифікації. Аутентифікатор пересилає цей пакет на сервер аутентифікації (RADIUS). RADIUS перевіряє пакет і право доступу клієнтського пристрою за базою даних користувача або іншими ознаками, а потім відправляє на автентифікатор роздільна здатність або заборона підключення. Відповідно, автентифікатор дозволяє або забороняє доступ до мережі.

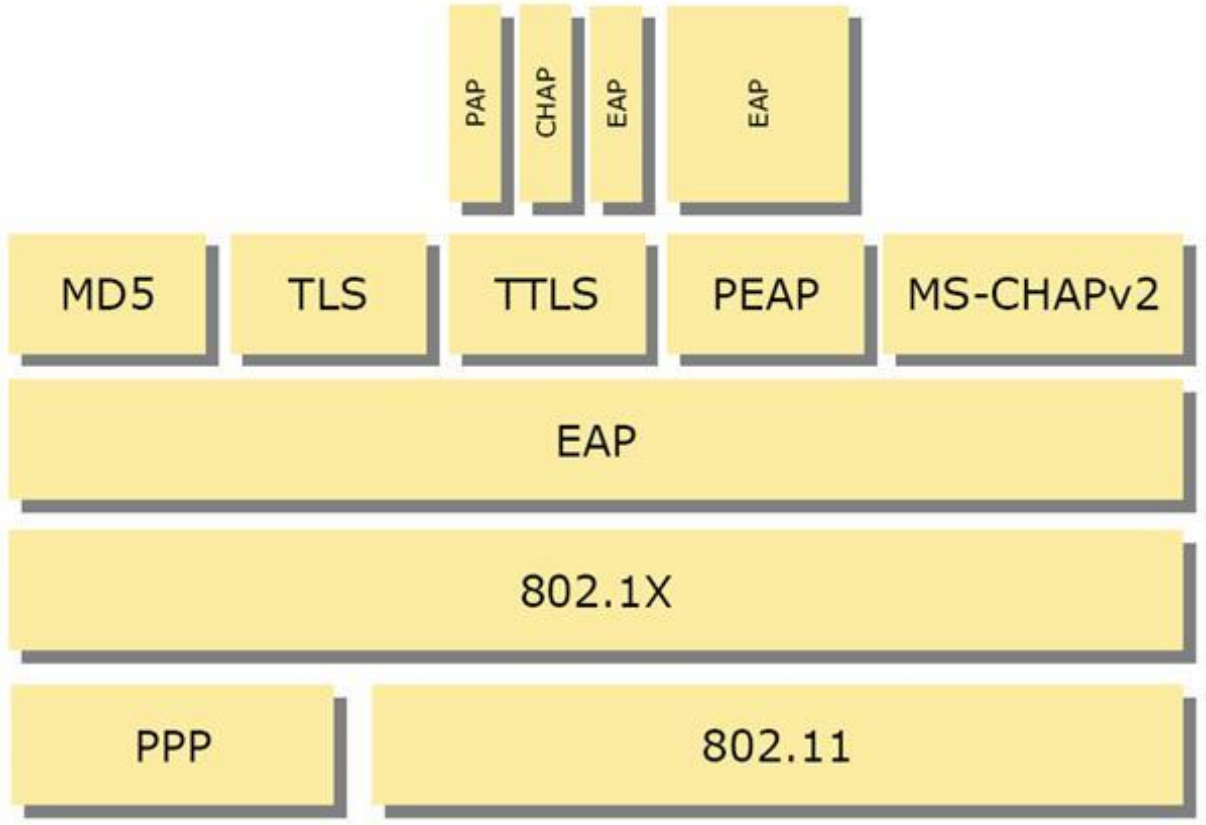

Рисунок 3.5 — Список протоколів, що використовуються

Використання сервера RADIUS дозволяє відмовитись від PSK та генерувати індивідуальні ключі, валідні тільки для конкретної сесії підключення. Простіше кажучи, ключі шифрування неможливо витягти із клієнтського пристрою. Захист від перехоплення пакетів забезпечується за допомогою шифрування по різних внутрішніх протоколах EAP, кожен з яких має свої особливості. Так, протокол EAP-FAST дозволяє авторизуватися за логіном та паролем, а PEAP-GTC — за спеціальним токеном (карта доступу, картки з одноразовими паролями, флешки

тощо). Протоколи PEAP-MSCHAPv2 та EAP-TLS проводять авторизацію за клієнтськими сертифікатами.

Максимальний захист мережі Wi-Fi забезпечує лише WPA2-Enterprise та цифрові сертифікати безпеки у поєднанні з протоколом EAP-TLS або EAP-TTLS. Сертифікат — це заздалегідь згенеровані файли на сервері RADIUS та клієнтському пристрої. Клієнт та сервер аутентифікації взаємно перевіряють ці файли, тим самим гарантується захист від несанкціонованих підключень з чужих пристроїв та помилкових точок доступу. Протоколи EAP-TTL/TTLS входять до стандарту 802.1X та використовують для обміну даними між клієнтом та RADIUS інфраструктуру відкритих ключів (PKI). PKI для авторизації використовує секретний ключ (знає користувач) та відкритий ключ (зберігається у сертифікаті, потенційно відомий усім). Поєднання цих ключів забезпечує надійну аутентифікацію.

Цифрові сертифікати потрібно робити для кожного бездротового пристрою. Це трудомісткий процес, тому сертифікати зазвичай використовуються лише у Wi-Fi-мережах, що потребують максимального захисту. У той же час можна легко відкликати сертифікат та заблокувати клієнта.

Сьогодні WPA2-Enterprise у поєднанні із сертифікатами безпеки забезпечує надійний захист корпоративних Wi-Fi-мереж. При правильному налаштуванні та використанні зламати такий захист практично неможливо «з вулиці», тобто без фізичного доступу до авторизованих клієнтських пристроїв. Тим не менш, адміністратори мереж іноді припускаються помилок, які залишають зловмисниками «лазівки» для проникнення в мережу. Проблема ускладнюється доступністю софту для зламування та покрокових інструкцій, якими можуть скористатися навіть дилетанти.

3.5 Висновки до розділу 3

Під час виконання роботи над попередніми розділами було досліджено, що для реалізації висунутих ідей можна використовувати мобільний пристрій на базі

ОС Linux, за допомогою якого зможемо робити атаки, в той же час, це досить тривалий процес, для чого нам потрібна його відповідна автономність живлення. Крім, іншого, необхідно забезпечити мінімальний розмір пристрою, для того, щоб можна було його заховати будь-де, не привертаючи зайвої уваги.

4 РОЗРАХУНОК ЕКОНОМІЧНОЇ ДОЦІЛЬНОСТІ СТВОРЕННЯ СИСТЕМИ ПЕРЕВІРКИ ТА ТЕСТУВАННЯ ЗАХИЩЕННОСТІ WI-FI МЕРЕЖІ

Результатом виконання даної магістерської кваліфікаційної роботи система перевірки та тестування захищеності Wi-Fi мережі, що відноситься до розряду прикладної науково–технічної роботи та прогнозує виведення науково-технічної розробки на ринок із залученням потенційних інвесторів.

За допомогою економічних розрахунків можна розрахувати ефективність впровадження результатів досліджень у виробництво, тобто комерціалізація наукових досліджень. [11]

4.1 Проведення комерційного та технологічного аудиту науково-технічної розробки

Метою оцінки потенціалу комерційного розвитку є оцінка потенціалу комерційного розвитку, що випливає з науково-технічних досліджень. За результатами оцінки робляться висновки про напрямки (особливості) організації в майбутньому її впровадження з урахуванням встановленої оцінки.

У цілях проведення технологічного аудиту було залучено 3 незалежних експерти. Такими експертами є к.т.н., доц. Колесник Ірина Сергіївна, к.т.н., старший викладач Богомолов Сергій Віталійович та к.т.н., доц. Черняк Олександр Іванович.

Комерційний потенціал інвестицій буде оцінюватись відповідно до дванадцяти критеріїв, наведених у таблиці 4.1.

Таблиця 4.1 — Оцінювання комерційного потенціалу розробки

Критерії оцінювання та бали (за 5-бальною шкалою)					
Критерій	0	1	2	3	4
Технічна здійсненність концепції:					
1	Достовірність концепції не підтверджена	Концепція підтверджена експертними висновками	Концепція підтверджена розрахунками	Концепція перевірена на практиці	Перевірено роботоздатність продукту в реальних умовах

Продовження таблиці 4.1

Ринкові переваги (недоліки):					
2	Багато аналогів на малому ринку	Мало аналогів на малому ринку	Багато аналогів на великому ринку	Один аналог на великому ринку	Продукт не має аналогів на великому ринку
3	Ціна продукту значно вища за ціни аналогів	Ціна продукту дещо вища за ціни аналогів	Ціна продукту приблизно дорівнює цінам аналогів	Ціна продукту дещо нижче за ціни аналогів	Ціна продукту значно нижче за ціни аналогів
4	Технічні та споживчі властивості продукту значно гірші, ніж в аналогів	Технічні та споживчі властивості продукту трохи гірші, ніж в аналогів	Технічні та споживчі властивості продукту на рівні аналогів	Технічні та споживчі властивості продукту трохи кращі, ніж в аналогів	Технічні та споживчі властивості продукту значно кращі, ніж в аналогів
	Експлуатаційні витрати значно вищі, ніж в аналогів	Експлуатаційні витрати дещо вищі, ніж в аналогів	Експлуатаційні витрати на рівні експлуатаційних витрат аналогів	Експлуатаційні витрати трохи нижчі, ніж в аналогів	Експлуатаційні витрати значно нижчі, ніж в аналогів
Ринкові перспективи					
6	Ринок малий і не має позитивної динаміки	Ринок малий, але має позитивну динаміку	Середній ринок з позитивною динамікою	Великий стабільний ринок	Великий ринок з позитивною динамікою
Практична здійсненність					
7	Активна конкуренція великих компаній на ринку	Активна конкуренція	Помірна конкуренція	Незначна конкуренція	Конкурентів немає
8	Відсутні фахівці як з технічної, так і з комерційної реалізації ідеї	Необхідно наймати фахівців або витрачати значні кошти та час на навчання наявних фахівців	Необхідне незначне навчання фахівців та збільшення їх штату	Необхідне незначне навчання фахівців	Є фахівці з питань як з технічної, так і з комерційної реалізації ідеї

Закінчення таблиці 4.1

9	Потрібні значні фінансові ресурси, які відсутні.	Потрібні незначні фінансові ресурси. Джерела фінансування відсутні	Потрібні значні фінансові ресурси.Джерела фінансування є	Потрібні незначніфінансові ресурси. Джерела фінансування є	Не потребує додаткового фінансування
10	Необхідна розробка нових матеріалів	Потрібні матеріали, що використовуються у військово-промисловому комплексі	Потрібні дорогі матеріали	Потрібні досяжні та дешеві матеріали	Всі матеріали для реалізації ідеї відомі та давно використовуються у виробництві
11	Термін реалізації ідеї більший за 10 років	Термін реалізації ідеї більший за 5 років.Термін окупності інвестицій більше 10-ти років	Термін реалізації ідеї від 3-х до 5-ти років.Термін окупності інвестицій більше 5-ти років	Термін реалізації ідеї менше 3-х років. Термін окупності інвестицій від 3-х до 5-ти років	Термін реалізації ідеї менше 3-х років.Термін окупності інвестицій менше 3-х років
12	Необхідно регламентні документи та велика кількість дозвільних документів на виробництво продукту	Необхідно отримання великої кількості дозвільних документів на виробництво та реалізацію продукту	Процедура отримання дозвільних документів для виробництва та реалізації продукту вимагає незначних коштів та часу	Необхідно тільки повідомлення відповідним органам про виробництво та реалізацію продукту	Відсутні будь-які регламентні обмеження на виробництво та реалізацію продукту

На основі таблиці різні експерти, у нашому випадку керівник магістерської роботи та викладачі кафедри ОТ, визначають різні результати. Результати цієї оцінки комерційного потенціалу узагальнено у таблиці 4.2.

Таблиця 4.2 — Результати оцінювання комерційного потенціалу розробки

Критерії	Експерт (ПІБ, посада)		
	1 Колесник І. С., к.т.н., доц. кафедри ОТ	2 Богомолов С.В., к.т.н., ст.викл. кафедри ОТ	3 Черняк О.І., к.т.н., доц. кафедри ОТ
	Бали:		
1.Технічна здійсненність концепції	4	3	3
2.Ринкові переваги (наявність аналогів)	4	4	4
3. Ринкові переваги (ціна продукту)	3	3	3
4.Ринкові переваги (технічні властивості)	3	3	3
5. Ринкові переваги (експлуатаційні витрати)	2	2	3
6. Ринкові перспективи (розмір ринку)	3	3	4
7. Ринкові перспективи (конкуренція)	4	3	3
8. Практична здійсненність (наявність фахівців)	3	3	2
9. Практична здійсненність (наявність фінансів)	2	2	3
10.Практична здійсненність (необхідність нових матеріалів)	2	2	2
11. Практична здійсненність (термін реалізації)	4	3	3
12. Практична здійсненність (розробка документів)	4	3	3
Сума балів	$СБ_1 = 38$	$СБ_1 = 36$	$СБ_1 = 37$
Середньо-арифметична сума балів $СБ_С$	$СБ_С = \frac{\sum_1^3 СБ_i}{3} = \frac{38 + 36 + 37}{3} = 37$		

Відповідно до таблиці 4.2, а також відповідно до рекомендацій, наведених у таблиці 4.3, можна зробити висновок про рівень потенціалу комерційного розвитку.

Таблиця 4.3 — Рівні комерційного потенціалу розробки

Середньоарифметична сума балів $\overline{СБ}$, розрахована на основі висновків експертів	Рівень комерційного потенціалу розробки
0 — 10	Низький
11 — 20	Нижче середнього
21 — 30	Середній
31 — 40	Вище середнього
41 — 48	Високий

З урахуванням середніх арифметичних балів $СБ_С$ = 37, які були визначені експертами, можна зробити висновок, що рівень комерційного потенціалу цієї розробки буде вище середнього.

Система, яка розробляється, повинна буде виконувати такі функції:

— проведення тестування для визначення захищеності безпровідної мережі;

— аналізувати захищеність безпровідної мережі;

— швидко опрацьовувати дані;

— повинна мати функціонал для генерування висновку;

— допомагати приймати рішення системному адміністратору щодо використання засобів захисту.

— орієнтуватися на використання сучасних засобів та способів захисту;

4.2 Розрахунок витрат на здійснення науково-дослідної роботи

4.2.1 Витрати на оплату праці

Основна заробітна плата розробників, що працюють над проектом, визначена у формулі:

$$З_о = \sum_{i=1}^{k} \frac{M_{ni} \cdot t_i}{T_p}, \quad (4.1)$$

де k — кількість посад дослідників, залучених до процесу досліджень;

M_{ni} — місячний посадовий оклад конкретного дослідника, грн;

T_p — середня кількість робочих днів в місяці, *Tp=21…23* дні, обрано 22 дні;

t_i— кількість днів роботи конкретного дослідника, день.

Над створенням розробки працював менеджер проекту та інженер програмного забезпечення, тому ми виконаємо для них усі необхідні розрахунки, і вносимо їх до таблиці 4.5:

$$\text{Зо. к.} = \frac{16000 \cdot 10}{22} = 7272{,}7(\text{грн}).$$

$$\text{Зо. в.} = \frac{11000 \cdot 44}{22} = 22000\ (\text{грн}).$$

Таблиця 4.5 — Витрати на заробітну плату дослідників

Найменування посади	Місячний посадовий оклад, грн.	Оплата за робочий день, грн.	Число днів роботи	Витрати на заробітну плату, грн.
Керівник проекту	16000	727,27	10	7272,7
Старший інженер-програміст	12000	545,45	22	12000
Всього				19272,7

Витрати на основну заробітну плату робітників за відповідними найменуваннями робіт відсутні, тобто $З_p = 0$.

Додаткова винагорода ($З_{\text{дод.}}$) усіх розробників та працівників, які брали участь у цьому етапі роботи, обчислюється як 10 ... 12% від суми основної заробітної плати дослідників та робітників за формулою:

$$З_{\text{дод.}} = (З_{\text{о}} + З_{\text{р}}) \cdot \frac{Н_{\text{дод.}}}{100\%}, \qquad (4.2)$$

де $Н_{\text{дод.}}$ — норма нарахування додаткової заробітної плати.

$$З_{\text{дод.к.}} = \frac{11 \cdot 7272{,}7}{100} = 800 \text{ (грн)},$$

$$З_{\text{дод.в.}} = \frac{11 \cdot 12000}{100} = 1320 \text{ (грн)},$$

$$З_{\text{дод}} = З_{\text{дод.к.}} + З_{\text{дод.в.}} = 2120 \text{ (грн)}.$$

4.2.2 Відрахування на соціальні заходи

Заробітна плата робітників відсутня, тому $З_р = 0$. Нарахування на заробітну плату дослідників та нарахування на заробітну плату працівників, які брали участь у цьому етапі роботи, розраховується як 22% від суми основної та додаткової заробітної плати дослідників і робітників за формулою:

$$З_н = (З_о + З_р + З_{\text{дод}}) \cdot \frac{Н_{\text{зп}}}{100\%} \quad (4.3)$$

де $Н_{\text{зп}}$ — норма нарахування на заробітну плату.

$$З_н = (19272{,}7 + 0 + 2120) \cdot \frac{22\%}{100\%} = 4706{,}39 \text{ (грн.)}$$

4.2.3 Сировина та матеріали

Витрати на матеріали (*М*), у вартісному вираженні розраховуються ок-ремо по кожному виду матеріалів за формулою:

$$М = \sum_{j=1}^{n} Н_j \cdot Ц_j \cdot К_j - \sum_{j=1}^{n} B_j \cdot Ц_{вj}, \quad (4.4)$$

де $Н_j$ — кількість матеріалу *j*-го виду, шт;

n — кількість видів матеріалу;

$Ц_j$ — ціна матеріалу *j*-го виду, грн;

$К_j$ — коефіцієнт транспортних витрат, $К_j$ = (1,1…1,15). Обираємо $К_j$ 1,15;

B_j — маса відходів *j*-го найменування, кг;

$Ц_{вj}$ — вартість відходів j-го найменування, грн/кг.

Результати розрахунків занесено до таблиці 4.6.

Таблиця 4.6 — Витрати на матеріали

Найменування комплектуючих	Ціна за 1 штуку, грн	Кількість матеріалу, штук	Величина відходів,кг	Ціна відходів, грн/кг	Вартість витраченого матеріалу, грн.
Ручка	20,00	1	0,06	1,70	19,8
Карта пам'яті	450,00	1	0	0,00	450,00
Пачка офісного папіру	95,00	1	0,5	35,50	77,25
Всього (з урахуванням транспортних витрат)					547,05

4.2.4 Амортизація обладнання, програмних засобів та приміщень

В спрощеному вигляді амортизаційні відрахування по кожному виду обладнання, приміщень та програмному забезпеченню тощо можуть бути розраховані з використанням прямолінійного методу амортизації за фор-мулою:

$$А_{обл} = \frac{Ц_б}{Т_в} \cdot \frac{t_{вик}}{12,} \qquad (4.5)$$

де $Цб$ – балансова вартість обладнання, програмних засобів, приміщень тощо, які використовувались для проведення досліджень, грн;

$t_{вик}$ – термін використання обладнання, програмних засобів, приміщень під час досліджень, місяців;

$Тв$ – строк корисного використання обладнання, програмних засобів, приміщень тощо, років.

Таблиця 4.7 — Амортизаційні відрахування по кожному виду обладнання

Найменування обладнання	Балансова вартість, грн.	Строк використання, років	Термін використання, місяців.	Амортизаційні відрахування, грн
ЕОМ	12000	2	1	500
Приміщення	150000	20	1	625
Всього				1125

4.2.5 Паливо та енергія для науково-виробничих цілей

Витрати на силову електроенергію ($В_е$) розраховують за формулою:

$$В_е = \sum_{i=1}^{n} \frac{W_{уі} \cdot t_і \cdot Ц_е \cdot К_{впі}}{\eta_і}, \quad (4.6)$$

де $W_{уі}$ — встановлена потужність обладнання на певному етапі розробки, кВт;

$t_і$ — тривалість роботи обладнання на етапі дослідження, год;

$Ц_е$ — вартість 1 кВт-години електроенергії, грн; (вартість електроенергії визначається за даними енергопостачальної компанії), $Ц_е = 4{,}62$ [];

$К_{впі}$ — коефіцієнт, що враховує використання потужності, $К_{впі} < 1$; обираємо $К_{впі}$ 0,7;

$\eta_і$ — коефіцієнт корисної дії обладнання, $\eta_і < 1$.

$$В_е = \sum_{i=1}^{1} \frac{0{,}07 \cdot 176 \cdot 4{,}62 \cdot 0{,}7}{0{,}8} = 49{,}8 \text{ (грн.)},$$

Проведені розрахунки необхідно звести до таблиці 4.8.

Таблиця 4.8 — Витрати на електроенергію

Найменування обладнання	Встановлена потужність, кВт	Тривалість роботи, год	Сума, грн
ЕОМ	0,07	176	49,8
Всього			49,8

4.2.6 Інші витрати

Витрати за статтею «*Інші витрати*» розраховуються як 50…100% від суми основної заробітної плати дослідників та робітників за формулою:

$$І_в = (З_о + З_р) \cdot \frac{Н_{ів}}{100\%} \quad (4.7)$$

де $Н_{ів}$ — норма нарахування за статтею «*Інші витрати*».

$$І_{в.к.} = 7272{,}7 \cdot \frac{80\%}{100\%} = 5818{,}24 \text{ (грн.)},$$

$$І_{в.в.} = 12000 \cdot \frac{80\%}{100\%} = 9600 \text{ (грн.)},$$

$$I_в = I_{в.к.} + I_{в.в.} = 15418{,}24\ (\text{грн.}).$$

4.2.7 Накладні (загальновиробничі) витрати

Витрати за статтею «*Накладні (загальновиробничі) витрати*» розраховуються як 100…150% від суми основної заробітної плати дослідників та робітників за формулою:

$$В_{нзв} = (З_о + З_р) \cdot \frac{Н_{нзв}}{100\%} \quad (4.8)$$

де $Н_{нзв}$ — норма нарахування за статтею «*Накладні (загальновиробничі) витрати*».

Беремо норму нарахування 100%.

$$В_{нзв.к.} = 7272{,}7 \cdot \frac{120\%}{100\%} = 8727{,}24\ (\text{грн.}),$$

$$В_{нзв.в.} = 12000 \cdot \frac{120\%}{100\%} = 14400\ (\text{грн.}),$$

$$В_{нзв} = В_{нзв.к.} + В_{нзв.в.} = 23127{,}24\ (\text{грн.}).$$

Витрати на проведення науково-дослідної роботи розраховуються як сума всіх попередніх статей витрат за формулою:

$$В_{заг} = З_о + З_р + З_{дод} + З_н + М + К_в + В_{спец} + В_{прг} + А_{обл} + В_е + В_{св} + В_{сп} + I_в + В_{нзв}. \quad (4.9)$$

У нашому випадку:

$З_р = 0, К_в = 0, В_{спец} = 0, В_{прг} = 0, В_{св} = 0, В_{сп} = 0$, тому отримаємо:

$$В_{заг} = З_о + З_{дод} + З_н + М + А_{обл} + В_е + I_в + В_{нзв}$$
$$= 19272{,}7 + 2120 + 4706{,}39 + 547{,}05 + 1125 + 49{,}8 + 15418{,}24 + 23127{,}24 = 66366{,}42\ (\text{грн}).$$

Загальні витрати *ЗВ* на завершення науково-дослідної (науково-технічної) роботи та оформлення її результатів розраховуються за формулою:

$$ЗВ = \frac{В_{заг}}{\eta}, \quad (4.10)$$

де η — коефіцієнт, який характеризує етап (стадію) виконання науково-дослідної роботи. Обираємо його 0,5.

$$ЗВ = \frac{66366,42}{0,5} = 132732,84 \text{ (грн)}.$$

4.3 Розрахунок економічної ефективності науково-технічної розробки за її можливої комерціалізації потенційним інвестором

Розробка чи суттєве вдосконалення програмного засобу (програмного забезпечення, програмного продукту) для використання масовим спо-живачем.

Для всіх наведених випадків можливе збільшення чистого прибутку у потенційного інвестора $\Delta П_i$ для кожного із років, протягом яких очікується отримання позитивних результатів від можливого впровадження та комер-ціалізації науково-технічної розробки, розраховується за формулою:

$$\Delta П_i = (\pm \Delta Ц_o \cdot N \cdot Ц_o \cdot \Delta N)_i \cdot \lambda \cdot \rho \cdot \left(1 - \frac{\vartheta}{100}\right) \qquad (4.11)$$

де $\pm \Delta Ц_o$— зміна основного якісного показника від впровадження результа-тів науково-технічної розробки в аналізованому році;

N — основний кількісний показник, який визначає величину попиту на аналогічні чи подібні розробки у році до впровадження результатів нової науково-технічної розробки;

$Ц_o$ — основний якісний показник, який визначає ціну реалізації нової на-уково-технічної розробки в аналізованому році, $Ц_o = Ц_б \pm \Delta Ц_o$;

$Ц_б$ — основний якісний показник, який визначає ціну реалізації існуючої (базової) науково-технічної розробки у році до впровадження результатів;

ΔN — зміна основного кількісного показника від впровадження результа-тів науково-технічної розробки в аналізованому році;

λ — коефіцієнт, який враховує сплату потенційним інвестором податку на додану вартість. У 2021 році ставка податку на додану вартість становить 20%, а коефіцієнт $\lambda=0,8333$;

ρ — коефіцієнт, який враховує рентабельність інноваційного продукту (

п

ϑ — ставка податку на прибуток, який має сплачувати потенційний інвестор, у 2021 році $\vartheta=18\%$.

с

л

у

В результаті впровадження результатів наукових розробок поліпшується якість програмного забезпечення, що дозволяє збільшити ціну за його впровадження від 1300 грн до 1500 грн.

Ми прогнозуємо щорічний приріст чистого прибутку компанії від впровадження результатів наукових розробок щодо вихідного стану.

Збільшення чистого прибутку підприємства $\Delta П_i$ за перший рік складе:

$$\Delta П_1 = 1300 \cdot 1800 \cdot 0,8333 \cdot 0,3 \cdot \left(1 - \frac{18\%}{100\%}\right) = 713386,1 \text{ (грн).}$$

З

б

і

л

ь

ш

е

н

Н

я

ч

и

с

т

о

г

о

п

р

и

б

у

$$\Delta П_2 = 1400 \cdot 1700 \cdot 0,8333 \cdot 0,3 \cdot \left(1 - \frac{18\%}{100\%}\right) = 489788,48 \text{ (грн).}$$

Збільшення чистого прибутку підприємства $\Delta П_i$ на третій рік складе:

$$\Delta П_3 = 1500 \cdot 1216 \cdot 0,8333 \cdot 0,3 \cdot \left(1 - \frac{18\%}{100\%}\right) = 373905,04 \text{ (грн).}$$

Далі розраховують приведену вартість збільшення всіх чистих прибутків *ПП*, що їх може отримати потенційний інвестор від можливого впровадження та комерціалізації науково-технічної розробки:

$$ПП = \sum_{i=1}^{T} \frac{\Delta П_i}{(1+\tau)^t}, \qquad (4.12)$$

де $\Delta П_i$ — збільшення чистого прибутку у кожному з років, протягом яких виявляються результати впровадження науково-технічної розробки, грн;

T — період часу, протягом якого очікується отримання позитивних результатів від впровадження та комерціалізації науково-технічної розробки, роки;

τ — ставка дисконтування, за яку можна взяти щорічний прогнозований рівень інфляції в країні, *τ = 0,05…0,15*. Обираємо τ 0,1;

t — період часу (в роках) від моменту початку впровадження науково-технічної розробки до моменту отримання потенційним інвестором додат-кових чистих прибутків у цьому році.

$$\text{ПП} = \frac{713386,1}{(1+0,1)^1} + \frac{489788,48}{(1+0,1)^2} + \frac{373905,04}{(1+0,1)^3}$$

$$= 648532,82 + 403207,01 + 280920,39 = 1332660,22 \text{ (грн.)}$$

Далі розраховують величину початкових інвестицій *PV*, які потенцій-ний інвестор має вкласти для впровадження і комерціалізації науково-технічної розробки. Для цього можна використати формулу:

$$PV = k_{\text{інв}} \cdot \text{ЗВ}, \qquad (4.13)$$

де $k_{\text{інв}}$— коефіцієнт, що враховує витрати інвестора на впровадження науко-во-технічної розробки та її комерціалізацію.

Це можуть бути витрати на під-готовку приміщень, розробку технологій, навчання персоналу, маркетингові заходи тощо; зазвичай $k_{\text{інв}}$*=2...5*, але може бути і більшим. Обираємо даний коефіцієнт 2;

ЗВ — загальні витрати на проведення науково-технічної розробки та оформлення її результатів, грн.

$$PV = 2 \cdot 132732,84 = 265465,68 \text{ (грн.)}$$

Тоді абсолютний економічний ефект $E_{\text{абс}}$або чистий приведений дохіддля потенційного інвестора від можливого впрова-дження та комерціалізації науково-технічної розробки становитиме:

$$E_{\text{абс}} = \text{ПП} - PV \qquad (4.14)$$

де *ПП* — приведена вартість зростання всіх чистих прибутків від можливого впровадження та комерціалізації науково-технічної розробки, грн;

PV — теперішня вартість початкових інвестицій, грн.

$$E_{\text{абс}} = 1332660,22 - 265465,68 = 1067194,54 \text{ (грн.)}$$

Внутрішня економічна дохідність інвестицій $\text{Е}_\text{в}$, які можуть бути вкла-дені потенційним інвестором у впровадження та комерціалізацію науково-технічної розробки, розраховується за формулою:

$$\text{Е}_\text{в} = \sqrt[\text{т}_\text{ж}]{1 + \frac{\text{Е}_{\text{абс}}}{PV}} - 1, \qquad (4.15)$$

де $\text{Е}_{\text{абс}}$ — абсолютний економічний ефект вкладених інвестицій, грн;

PV — теперішня вартість початкових інвестицій, грн;

$Т_ж$ — життєвий цикл науково-технічної розробки, тобто час від початку її розробки до закінчення отримування позитивних результатів від її впро-вадження, роки.

$$Е_в = \sqrt[3]{1 + \frac{1067194,54}{265465,68}} - 1 = 0,7$$

Далі визначають бар'єрну ставку дисконтування τ_{min}, тобто мінімальну внутрішню економічну дохідність інвестицій, нижче якої кошти у впрова-дження науково-технічної розробки та її комерціалізацію вкладатися не будуть.

Мінімальна внутрішня економічна дохідність вкладених інвестицій $\tau_{мін}$визначається за формулою:

$$\tau_{мін} = d + f, \qquad (4.16)$$

де d— середньозважена ставка за депозитними операціями в комерційних банках; в 2021 році в Україні d=0,9...0,12. Обираємо d 0,11;

f — показник, що характеризує ризикованість вкладення інвестицій; за-звичай величина f=0,05...0,5, але може бути і значно вищою. Обираємо 0,2;

$$\tau_{мін} = d + f = 0,12 + 0,3 = 0,42\%$$

Величина $Е_в > \tau_{мін}$, отже інвестор може бути зацікавлений у фінансуванні цього дослідження.

Далі розраховуємо період окупності інвестицій $Т_{ок}$, які можуть бути вкладені потенційним інвестором у впровадження та комерціалізацію науково-технічної розробки:

$$Т_{ок} = \frac{1}{Е_в}, \qquad (4.17)$$

де $Е_в$ — внутрішня економічна дохідність вкладених інвестицій.

$$Т_{ок} = \frac{1}{0,7} = 1,4 \text{ року}$$

Оскільки $Т_{ок}$= 1,4 року, тоді розвиток доречний.

ВИСНОВКИ

У магістерській кваліфікаційній роботі було розглянуто популярні технології для створення бездротових мереж, проведено їх порівняльний аналіз, виявлено та представлено вразливості та недоліки алгоритмів забезпечення безпеки бездротових мереж. Різними способами проведено тестування бездротових мереж, щодо перевірки популярних алгоритмів задля забезпечення їх безпеки.

У ході виконання роботи було визначено, що забезпечення безпеки бездротової корпоративної або домашньої мережі останнім часом найчастіше ставиться у пріоритетні завдання адміністраторам даного обладнання.

Виявлення вразливостей бездротових комп'ютерних мереж показало, що алгоритм забезпечення безпеки WEP давно скомпрометований і використання його обмеження доступу сторонніх осіб недоцільно. При використанні алгоритму WEP отримати доступ до мережі можливо за кілька хвилин, за наявності активного клієнта, підключеного до цієї точки доступу. Незважаючи на його слабкий захист, досі у світі кожна 8-10 точка доступу налаштована на використання алгоритму забезпечення безпеки WEP.

Визначено, що від 90 до 92% безпровідних мереж, що залишилися, використовують алгоритм WPA/WPA2, який вважається криптостійким, але розвиток потужних апаратних засобів для особистого користування дозволяє здійснювати дуже швидкий перебір парольних фраз, а якщо для перебору використовуються райдужні таблиці, то на отримання пароля довжиною 63 символи з ймовірністю близько 75% потрібно кілька хвилин.

Під час розгляду алгоритмів створення безпеки було виявлено, що алгоритм WPA2-Enterprise на сьогодні є найстійкішим проти зловмисників. Цей алгоритм підтримує дво- і більш факторну автентифікацію. Крім пароля для підключення до точки доступу є можливість задавати пару логін та пароль для конкретного користувача, які будуть використовуватися при автентифікації на сервері Radius. Крім простої пари логін/пароль, можна налаштувати Radius сервер таким чином, що потрібно підтвердження, отримане в смс або будь-яким іншим способом. Така

аутентифікація дозволяє відкинути більшість зловмисників, оскільки складно відстежити процес аутентифікації. Процес стає практично безглуздим.

Розроблено систему тестування та перевірки захищеності Wi-Fi мережі на основі алгоритмів шифрування **WPA/WPA2 та WPA2-ENTERPRISE.**

В результаті чого виявлено, що бездротові технології є частиною технологій, які сприяють функціонуванню апаратного забезпечення, шо дозволяють співпрацю на відстані між кількома точками, при тому не вимагаючи зв'язку за допомогою провідних мереж.

Під час перевірки і тестування захищеності мережі виявлено можливості використання персонального комп'ютера чи ноутбука з відповідними параметрами та конфігурацічми.

Протягом виконання роботи та використання результатів було досліджено, що для реалізації поставлених задач існує можливість використання мобільних пристрій на базі ОС Linux, за допомогою якого зможемо ініціювати атаки, в той же час, це є тривалий процес, через що виникає проблема забезпечення відповідної автономності живлення.

Під час виконання роботи було розроблено рекомендації щодо конфігурування бездротової мережі.

Також, під час розроблення, було виявлено досить велику кількість проблем, пов'язаних з керуванням одноплатного комп'ютера, для цього знадобився мобільний пристрій, який виступає як дисплей і клавіатура. Варто відзначити, що також за допомогою даного мобільного пристрою здійснювалась передача необхідної інформації між одноплатним і потужним комп'ютерами.

Необхідність передавання даних між комп'ютерами звела нанівець недолік у вигляді відсутності клавіатури та монітора у одноплатного комп'ютера. Крім вищесказаного досягнуто меншої помітності через те, що зараз довге використання мобільного пристрою не привертає уваги в суспільстві.

СПИСОК ЛІТЕРАТУРИ

1. Арістова І. В. Діяльність органів внутрішніх справ щодо реалізації державної інформаційної політики : монографія [Текст] / І. В. Арістова. - Х. : Нац. ун-т внутр. справ, 2006. – 354 с.

2. Почепцов Г. Інформаційна політика : навч. посібник [Текст] / Г. Г. Почепцов – К.: Знання, 2006. – 663 с.

3. Супрун В. М. Інформаційний суверенітет як один з елементів інформаційної безпеки держави: теоретико-правовий аспект [Електронний ресурс]. – Режим доступу : http : // www. nbuv.gov.ua/portal/natural/vkhnu / Pravo / 2009.

4. Ярочкін В. Система безпеки фірми [Електронний ресурс]. – Режим доступу : http : // www. nbuv. gov. ua.

5. Закон України. Про інформацію / [Електронний ресурс] - Режим доступу: http : // zakon. rada.gov.ua/cgi-bin/laws/main.cgi?nreg=2657-12.

6. Боднар І. Р. Сучасні реалії інформаційного суспільства: проблеми становлення та перспективи розвитку: монографія [Текст] / І. Р. Боднар. – Львів: Видавництво Львівської комерційної академії, 2013. – 320 с.

7. Бондаренко В., Литвиненко О. Інформаційна безпека сучасної держави: концептуальні роздуми [Електронний ресурс] / В. Бондаренко, О. Литвиненко - Режим доступу: http://www.crime-research. iatp. org. ua/ library/strateg. htm.

8. Саати Т. Л. Математические модели конфликтных ситуаций. - М. : “Сов. Радио”, 1977. - 304 с.

9. Державна інформаційна політика [Електронний ресурс]. – Режим доступу : http : // merega. org. ua / law / projects / derzh polityka.

10. Боднар І. Р. Роль держави у формуванні інформаційної політики [Текст] / І. Р. Боднар. – Вісник ЛКА. – Львів: Видавництво ЛКА. – Випуск 34. – Серія економічна. – 2011. – С. 291-296.

11. Киричок Р.В. Проблеми забезпечення контролю захищеності корпоративних мереж та шляхи їх вирішення. / Р.В. Киричок, П.М. Складанний, В.Л. Бурячок, Г.М. Гулак, В.А. Козачок / Наукові записки Українського науково-дослідного інституту зв’язку. - 2016. - №3(43). С. 51 -58.

12. Georgia Weidman. Penetration testing A Hands-On Introduction to Hacking / Georgia Weidman // No Starch Press, 2014. С. 179 – 339.

13. Панська А. В. Загрози та вразливості бездротових мереж / А. В. Панська, В. А. Резніченко. // Актуальні задачі та досягнення в галузі кібербезпеки.. – 2017. – №1. – С. 146–147.

14. Конституція України : Закон України від 28.06.96 р. – Режим доступу : http://zakon0. rada.gov.ua/laws/show/254к/96-вр. – Дата звернення 18.02.2018 р.

15. Сащук Г. Інформаційна безпека в системі забезпечення національної безпеки. – Режим доступу : http://journ.univ.kiev.ua/trk/publikacii/satshuk_publ.php. – Дата звернення 18.02.2018 р.

16. Ліпкан В.А. Інформаційна безпека України в умовах євроінтеграції : навчальний посібник / В. Ліпкан, Ю. Максименко, В. Желіховський. – К. : КНТ, 2006. – 280 с.

17. Данильян О.Г. Національна безпека України : структура та напрямки реалізації : навчальний посібник / О. Данильян, О. Дзьобань, М. Панов. – Х. : Фоліо, 2002 – 285 с. 5. Гурковський В.І. Безпека як об’єкт правовідносин в умовах глобального інформаційного суспільства // Правова інформатика. – 2010. – № 2(26). – С. 72-77.

18. Нижник Н. Національна безпека України (методологічні аспекти, стан і тенденції розвитку) : навчальний посібник / Н. Нижник, Г. Ситник, В. Білоус. – Ірпінь : Акад. ДПС України, 2000. – 304 с.

19. Ярочкин В.И. Словарь терминов и определений по безопасности и защите информации / В. Ярочкин, Т. Швецова. – М. : Ось-89, 1996. – 48 с. 8. Питання концепції реформування інформаційного законодавства України / Р. Калюжний та ін. // Правове, нормативне та метрологічне забезпечення системи інформації в Україні : тематичний зб. праць учасників 2-ї науково-технічної конференції. – К., 2000. – С. 17-21. “Інформація і право” № 1(24)/2018 101

20. Бєляков К.І. Деякі питання щодо формування реформи інформаційного законодавства України : мат. міжнародної науково-практичної конференції [“Систематизація законодавства в Україні : проблеми теорії і практики”]. – К. : Інститут законодавства Верховної Ради України, 1999. – С. 253-255.

21. Кормич Б.А. Інформаційна безпека : організаційно-правові основи : навчальний посібник / Б.Кормич. – К. : Кондор, 2004. – 382 с.

22. Ліпкан В.А., Харченко Л.С., Логінов О.В. Інформаційна безпека України : глосарій. – К. : Текст, 2004. – 136 с.

23. Шульга В.І. Сучасні підходи до трактування поняття інформаційна безпека / Ефективна економіка. – 2015. – № 4. – Режим доступу : http:// http://www.economy.nayka.com. ua/ ?op=1&z=5514. – Дата звернення 19.02.2018 р.

24. Лукашов А.И. Информационная безопасность как объект уголовно-правовой охраны в законодательстве Республики Беларусь : мат. научной конференции [“Концептуальные проблемы информационной безопасности в союзе России и Беларуси”]. – СПб., 2000. – Режим доступу : http://jurfak.spb.ru/conference/2001.htm. – Дата звернення 19.02.2018 р.

25. Брижко В.М. е-боротьба в інформаційних війнах та інформаційне право : монографія / В.М. Брижко, М.Я. Швець. – К. : НДЦПІ АПрН України, 2007. – 239 с.

26. Фисун Ю.А. Вопросы информационной безопасности личности, общества и государства накануне 21 века : мат. международной конференции [“Информатизация правоохранительных систем”], (м. Москва, 7 – 8 июня 2000 г.). – М., 2000, – С. 86-92.

27. Панарин И. Технология информационной войны : монографія / И. Панарин. – М. : “КСП+”, 2003. – 320 с.

28. Бондар І.Р. Інформаційна безпека як основа національної безпеки / Mechanism of Economic Regulation. – 2014. – № 1. – С. 68-75.

29. Громико І., Саханчук Т. Державна домінантність визначення інформаційної безпеки України в умовах протидії загрозам // Право України. − 2008. − № 8. – С. 130-134.

30. Баранов А.А. Концептуальные вопросы информационной безопасности Украины : сб. материалов [“Нормативно-правовая база защиты информации”]. – К., 1997. – С. 53-58. 20. Остроухов В., Петрик В. До проблеми забезпечення інформаційної безпеки України // Політичний менеджмент. – 2008. – № 4. – С. 135-141.

31. Про Основні засади розвитку інформаційного суспільства в Україні на 2007 – 2015 роки : Закон України від 09.01.07 р. – Режим доступу : zakon5.rada.gov.ua/laws/show/537-16. – Дата звернення 13.02.2018 р.

32. Про телекомунікації : Закон України від 18.11.03 р. – Режим доступу : zakon2.rada.gov. ua/laws/show/1280-15. – Дата звернення 13.02.2018 р.

33. Апанасевич Е. Что такое тестирование методом «белого ящика»? [Електронний ресурс] / Е. Апанасевич // Stormnet. – 2017. – Режим доступу до ресурсу: https://www.it-courses.by/white-box-testing/. Промышленные компании: векторы атак [Електронний ресурс] / ф // Positive Technologies. – 2018. – Режим доступу до ресурсу: https://www.ptsecurity.com/ru-ru/research/analytics/ics-attacks-2018/

34. Бездротові системи безпеки: як збільшити радіус дії Wi-Fi? [Електронний ресурс] // worldwision. – 2018. – Режим доступу до ресурсу: https://worldvision.com.ua/ua/besprovodnye-sistemy-bezopasnosti-kak-uvelichit-radius-deystviya-wi-fi/.

35. Информационная безопасность в системах охранного видеонаблюдения [Електронний ресурс] // Videomax. – 2019. – Режим доступу до ресурсу: https://www.videomax-server.ru/support/articles/informatsionnaya-bezopasnost-v-sistemakh-okhrannogo-videonablyudeniya/.

36. Практичні аспекти проведення тесту на проникнення (Електрон. ресурс) / Спосіб доступу: URL: http://www.osp.ru/text/233652/5908864/

37. Тест на проникнення (Електрон. ресурс) / Спосіб доступу: URL: http://www.dsec.ru/about/articles/st/

38. Уязвимости корпоративных информационных систем, 2019 [Електронний ресурс]// Positive Technologies. – 2019. – Режим доступу до ресурсу: https://www.ptsecurity.com/ru-ru/research/analytics/corporate-vulnerabilities-2019/.

39. Web Application Firewall [Електронний ресурс] // Allta. – 2020. – Режим доступу до ресурсу: http://allta.com.ua/nashi-resheniya/informacionnaya-bezopasnost/waf.

40. Методичні вказівки до виконання економічної частини магістерських кваліфікаційних робіт / Уклад.: В. О. Козловський, О. Й. Лесько, В. В. Кавецький.

— Вінниця : ВНТУ, 2021. — 42 с. Безпека периметра корпоративної мережі [Електронний ресурс] // Системний інтегратор інженерних рішень "Goobkas - ONE CONTRACTOR".. – 2020. – Режим доступу до ресурсу: https://goobkas.com/g80295191-bezpeka-perimetra-korporativnoyi.

ДОДАТОК А

Міністерство освіти та науки України

Вінницький національний технічний університет

Факультет інформаційних технологій та комп'ютерної інженерії

Кафедра обчислювальної техніки

ЗАТВЕРДЖУЮ

Завідувач кафедри ОТ

_____проф., д.т.н. О. Д. Азаров

«___» _____ 2021 р.

ТЕХНІЧНЕ ЗАВДАННЯ

на виконання магістерської кваліфікаційної роботи

«Система для перевірки та тестування захищеності Wi-Fi мережі»
08-23.МКР.017.00.000 ТЗ

Науковий керівник: к. т. н., доц. каф ОТ

_____ Азарова А.О.

Магістрант групи 2КІ-20м

_____ Бурак В.В.

Опонент _к.т.н. доц.. каф. МБІС
_____Карпінець В.В.

Вінниця 2021

1 Підстава для виконання магістерської кваліфікаційної роботи (МКР)

1.1 Актуальність дослідження пов’язана зі збільшенням популярності бездротових мереж та ідей для використання урізних установах для підвищення ступеня комфортності та об'єднання всіх систем у єдину мережу з єдиним центром управління. Через ситуацію, що виникла часто використовуються бездротові технології, і одним із перших постає питання забезпечення безпеки таких мереж, адже від цього починає залежати функціонування установи вцілому, а не лише безпека даних які циркулюють в інформаційній системі даної організації [3].

Таким чином, аспекти безпеки є популярними навіть для бездротових мереж, що не мають виходу в Інтернет, але передають особисті дані або інформацію, що становить комерційну таємницю.

1.2 Наказ про затвердження теми магістерської кваліфікаційної роботи.

2 Мета і призначення МКР

2.1 Мета роботи полягає у побудові системи для перевірки та тестування захищеності Wi-Fi мереж, що дозволяє проаналізувати уразливостей, а також шляхи та методи їх усунення.

2.2 Призначення розробки — виконання магістерської кваліфікаційної роботи.

3 Вихідні дані для виконання МКР

Створити систему для перевірки та тестування захищеності Wi-Fi мережі

4 Вимоги до виконання МКР

МКР повинна задовольняти такі вимоги:

— виявляти вразливості бездротових комп'ютерних мереж.
— виробляти засоби захисту вразливих місць Wi-Fi мережі.
— розробляти практичні рекомендації щодо забезпечення безпеки Wi-Fi

мережі;

— розробляти автоматизовані системи для перевірки та тестування захищеності Wi-Fi мережі, аналізу її вразливостей та впливу на них.

5 Етапи МКР та очікувані результати в таблиці А.1

Таблиця А.1 — Етапи виконання роботи

№ з/п	Назва етапів виконання магістерської роботи	Строк виконання етапів роботи	Примітка
1	Постановка задачі роботи	07.09.21	
2	Огляд існуючих безпровідних технологій	08.09-09.09.21	
3	Аналіз переваг і недоліків безпровідних мереж	10.09-18.09.21	
4	Виявлення особливостей функціонування безпровідних мереж	19.09-01.10.21	
5	Виявлення вразливосей безпровідних мереж	12.10-22.10.21	
6	Розробка системи для перевірки та тестування захищеності WI-FI мережі	22.10-31.10.21	
7	Захист мережі за допомогою WPA2-ENTERPRISE	01.11-10.11.21	
8	Підготовка матеріалів та опис системи для перевірки та тестування захищеності WI-FI мережі	11.11-16.11.21	
9	Розрахунок економічної частини роботи	17.11-30.11.21	
10	Оформлення пояснювальної записки та ілюстративного матеріалу	01.12-06.12.21	
11	Аналіз виконання роботи, висновки, додатки	07.12-06.12.21	
12	Перевірка якості виконання магістерської роботи та усунення недоліків	15.12.21	

6 Матеріали, що подаються до захисту МКР

До захисту МКР подаються: пояснювальна записка МКР, ілюстративні та графічні матеріали, протокол попереднього захисту МКР на кафедрі, відзив наукового керівника, відзив рецензента, протоколи складання державних екзаменів, анотації до МКР українською та іноземною мовами, довідка про відповідність оформлення МКР діючим вимогам.

7 Порядок контролю виконання та захисту МКР

Виконання етапів розрахункової та графічної документації МКР контролюється науковим керівником згідно зі встановленими термінами. Захист МКР відбувається на засіданні Державної екзаменаційної комісії, затвердженою наказом ректора.

8 Вимоги до оформлення МКР

Вимоги викладені в «Положенні про кфаліфікаційну роботу у Вінницькому національному технічному університеті» з урахуванням змін, що подані у бюлетені ВАК України № 9-10, 2011р., а також в МЕТОДИЧНИХ ВКАЗІВКАХ до дипломного проектування, ДСТУ 3008-2015, ДСТУ 3974-2000 «Правила виконання дослідно-конструкторських робіт. Загальні положення» та діючого ГОСТ 2.114-95 ЄСКД.

9 Вимоги щодо технічного захисту інформації в МКР з обмеженим доступом відсутні.

Технічне завдання до виконання отримав _____ Бурак В.В.

ДОДАТОК Б

Порівняння стандартів бездротового зв'язку

Таблиця Б.1 — Порівняння стандартів бездротового зв'язку

Технологія	Стандарт	Використання	Пропускна здатність	Радіус дії	Частоти
Wi-Fi	802.11a	WLAN	до 54 Мбіт/с	до 300 метрів	5,0 ГГц
Wi-Fi	802.11b	WLAN	до 11 Мбіт/с	до 300 метрів	2,4 ГГц
Wi-Fi	802.11g	WLAN	до 54 Мбіт/с	до 300 метрів	2,4 ГГц
Wi-Fi	802.11n	WLAN	до 300 Мбіт/с (у перспективі до 600 Мбіт/с)	до 300 метрів	2,4 - 2,5 або 5,0 ГГц
WiMax	802.16d	WMAN	до 75 Мбіт/с	25-80 км	1,5-11 ГГц
WiMax	802.16e	Mobile WMAN	до 40 Мбіт/с	1-5 км	2,3-13,6 ГГц
WiMax 2	802.16m	WMAN, Mobile WMAN	до 1 Гбіт/с (WMAN), до 100 Мбіт/с (Mobile WMAN)	120-150 км (стандарт у розробці)	До 11 ГГц
Bluetooth v.1.1	802.15.1	WPAN	до 1 Мбіт/с	до 10 метрів	2,4 ГГц
Bluetooth v. 2.0	802.15.3	WPAN	до 2,1 Мбіт/с	до 100 метрів	2,4 ГГц
Bluetooth v. 3.0	802.11	WPAN	від 3 Мбіт/с до 24 Мбіт/с	до 100 метрів	2,4 ГГц
ZigBee	802.15.4	WPAN	від 20 до 250 кбіт/с	1-100 м	2,4 ГГц (16 каналів), 915МГц (10 каналів), 868 МГц (один канал)
Інфрачервона лінія зв’язку	IrDa	WPAN	до 15 Мбіт/с	від 5 до 50 сантиметрів, одностороння зв'язок — до 10 метрів	Інфрачервоне випромінювання

ДОДАТОК В

Виведення результату виконання команди airmon-ng. Виконання команди airmon-ngstartwlan0

Рисунок В.1 — Виведення результату виконання команди airmon-ng

Рисунок В.2 — Виконання команди airmon-ngstartwlan0

ДОДАТОК Д

Результат перебору паролів

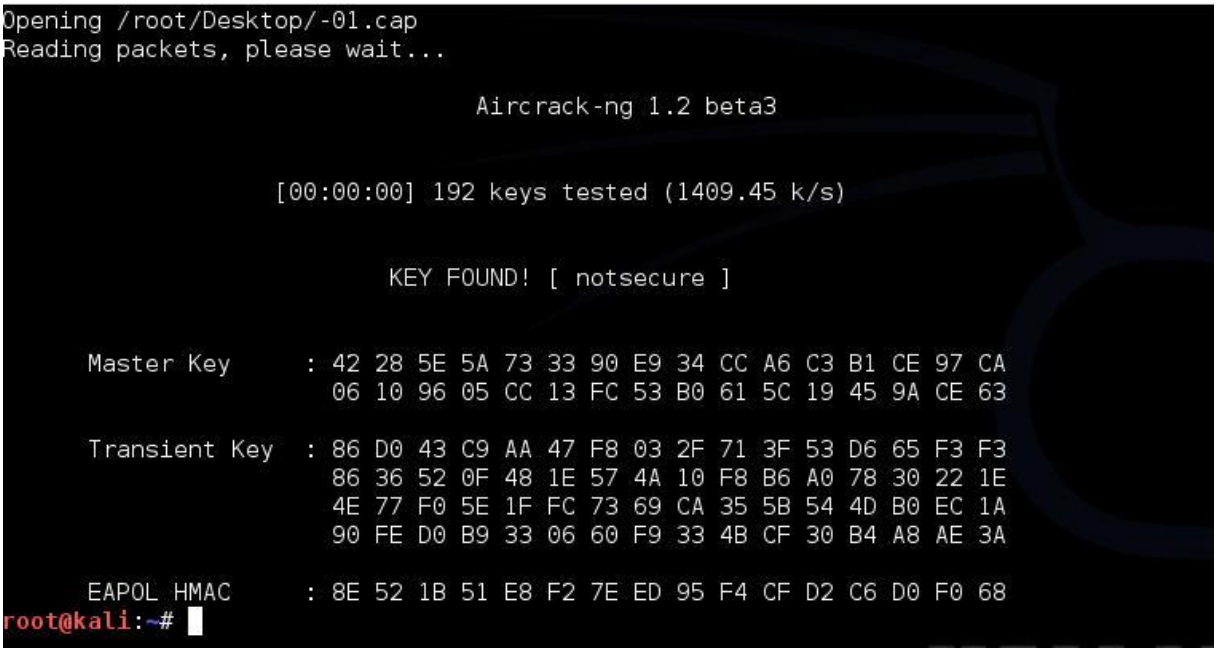

Рисунок Д1 — Результат перебору паролів

ДОДАТОК Є

Зовнішній вигляд одноплатних мікрокомп’ютерів

а) Raspberry Pi 3 model Bi

б) Intel Edison Kit

Рисунок Ж.1 — Зовнішній вигляд одноплатних мікрокомп’ютерів

ДОДАТОК Ж

Схема роботи протоколу 802.1x

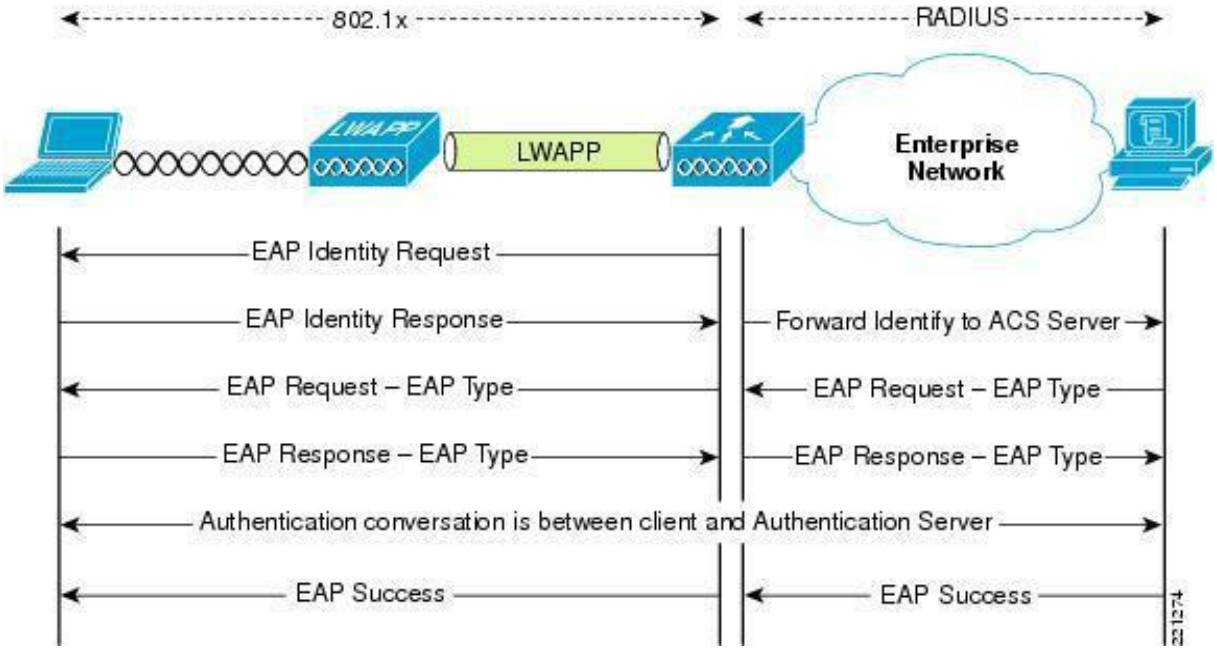

Рисунок И.1 — Схема роботи протоколу 802.1x

ДОДАТОК И

Список протоколів, що використовуються

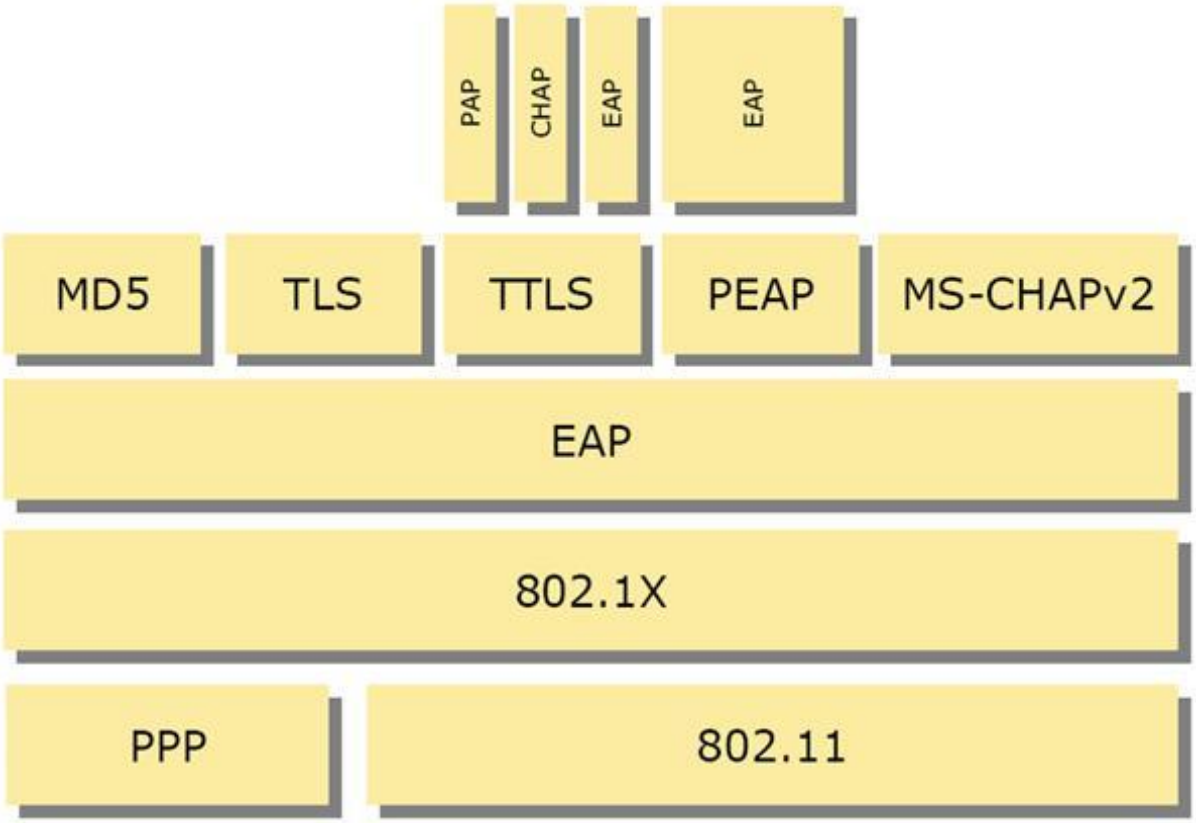

Рисунок К1 — Список протоколів, що використовуються

ДОДАТОК К

ПРОТОКОЛ ПЕРЕВІРКИ НАВЧАЛЬНОЇ (КВАЛІФІКАЦІЙНОЇ) РОБОТИ

Назва роботи: Система для перевірки та тестування захищеності Wi-Fi мережі

Тип роботи: магістерська кваліфікаційна робота

(кваліфікаційна робота, курсовий проект (робота), реферат, аналітичний огляд, інше (зазначити))

Підрозділ кафедра обчислювальної техніки

(кафедра, факультет (інститут), навчальна група)

Науковий керівник Азарова А.О.к.т.н., проф.каф.ОТ

(прізвище, ініціали, посада)

Показники звіту подібності

Plagiat.pl (StrikePlagiarism)		Unicheck	
КП1			
КП2		Оригінальність	89,3%
Тривога/Білі знаки	/	Схожість	10,7%

Аналіз звіту подібності (відмінити подібне)

- ✓ Запозичення, виявлення у роботі, оформлені коректно і не містять ознак плагіату.
- ☐ Виявлені у роботі запозичення не мають ознак плагіату, але їх надмірна кількість викликає сумніви щодо цінності і відсутності самостійності її автора. Робот направити на доопрацювання.
- ☐ Виявлені у роботі запозичення є недобросовісними і мають ознаки плагіату та/або в ній містяться навмисні спотворення тексту, що вказують на спроби приховування недобросовісних запозичень.

Заявляю, що ознайомлений(-на) з повним звітом подібності, який був згенерований Системою щодо роботи (додається)

Автор _____ Бурак В.В.

(підпис) (прізвище, ініціали)

Опис прийнятого рішення

Ступінь оригінальності роботи відповідає вимогам, що висуваються до МКР

Особа, відповідальна за перевірку _____ Захарченко С.М.

(підпис) (прізвище, ініціали)

Експерт _____ _____

(за потреби) (підпис) (прізвище, ініціали)