Міністерство освіти і науки України
Національний технічний університет
«Дніпровська політехніка»

Інститут електроенергетики
Факультет інформаційних технологій
Кафедра безпеки інформації та телекомунікацій

ПОЯСНЮВАЛЬНА ЗАПИСКА
кваліфікаційної роботи ступеню магістра

студента ***Ільмана Микита Віталійовича***

академічної групи ***125м-17-1***

спеціальності ***125 Кібербезпека***

спеціалізації[1] ***Кібербезпека***

за освітньо-професійною програмою ***Кібербезпека***

на тему ***Аналіз рівня інформаційної безпеки в приватних мережах стандарту IEEE 802.11***

Керівники	Прізвище, ініціали	Оцінка за шкалою		Підпис
		рейтинговою	інституційною	
кваліфікаційної роботи	д.т.н., проф. Корнієнко В.І.			
розділів:				
спеціальний	ст.викл. Кручінін О.В.			
економічний	к.е.н., доц. Пілова Д.П.			

Рецензент				

Нормоконтролер	ст. викл. Мєшков В.І.			

Дніпро
2018

ЗАТВЕРДЖЕНО:
завідувач кафедри
безпеки інформації та телекомунікацій

_____ д.т.н., проф. Корнієнко В.І.

«_____»_____20___року

ЗАВДАННЯ
на кваліфікаційну роботу ступеня магістра

студенту ***Ільман М.В.*** **академічної групи** ***125М-17-1***
(прізвище та ініціали) (шифр)

спеціальності ***125 Кібербезпека***

спеціалізації[1] ***Кібербезпека***

за освітньо-професійною програмою ***Кібербезпека***

на тему ***Аналіз рівня інформаційної безпеки в приватних мережах стандарту IEEE 802.11***

1 ПІДСТАВИ ДЛЯ ПРОВЕДЕННЯ РОБОТИ

Наказ ректора НТУ «Дніпровська політехніка» від 29.11.18 № 2025-л_____

2 МЕТА ТА ВИХІДНІ ДАНІ ДЛЯ ПРОВЕДЕННЯ РОБІТ

Об'єкт досліджень ***мережі стандарту 802.11***

Предмет досліджень ***Рівень інформаційної безпеки в мережах стандарту 802.11***

Мета ***підвищення рівня безпеки в мережах стандарту 802.11***

Вихідні дані для проведення роботи ***матеріали науково – дослідної та преддипломної практик***

3 ОЧІКУВАНІ РЕЗУЛЬТАТИ

Наукова новизна ***розробка програми та методики проведення аналізу рівня захищеності мереж стандарту 802.11***

Практична цінність ***зменшення часу та фінансових витрат при проведенні захищеності та експертизи мереж***

4 ВИМОГИ ДО РЕЗУЛЬТАТІВ ВИКОНАННЯ РОБОТИ

Відповідність методичним рекомендаціям до підготовки та захисту дипломної роботи та вимогам нормативним документів з технічного захисту інформації

5 ЕТАПИ ВИКОНАННЯ РОБІТ

Найменування етапів робіт	Строки виконання робіт (початок-кінець)
Огляд джерел за темою та напрям досліджень	03.09.18-06.10.18
Методи досліджень	07.10.18-31.10.18
Результати досліджень	01.11.18-24.11.18
Виконання економічного розділу	25.11.18-04.12.18
Оформлення пояснювальної записки	05.12.18-10.12.18

6 РЕАЛІЗАЦІЯ РЕЗУЛЬТАТІВ ТА ЕФЕКТИВНІСТЬ

Економічний ефект ***запобігання фінансових витрат у разі спроби атаки на мережу***

Соціальний ефект ***захист даних користувачів***

7 ДОДАТКОВІ ВИМОГИ

Завдання видано _____ _Корнієнко В.І._
(підпис керівника) (прізвище, ініціали)

Дата видачі: 03.09.18р.

Дата подання до екзаменаційної комісії: 14.12.18р.

Прийнято до виконання _____ _Ільман М. В._____
(підпис студента) (прізвище, ініціали)

РЕФЕРАТ

Пояснювальна записка: с.__, рис.__, табл.__, джерел__, додатків__.

Об’єкт дослідження: безпровідні мережі стандарту 802.11.

Мета роботи: виявлення вразливостей в безпровідних мережах стандарту 802.11 та підвищення рівня безпеки домашньої мережі.

Методи дослідження: спостереження та експеримент, метод індукції, системний підхід, метод аналізу ієрархій.

Спеціальна частина поділяється на наступні етапи:

- Аналіз вразливостей мережі.

- Аналіз існуючих рішень забезпечення рівню безпеки в мережах 802.11.

- Розробка програми та методики аналізу захищеності мереж.

- Аналіз трьох типових мереж.

- Розробка рекомендацій щодо підвищення безпеки в приватній мережі.

- Вибір «найкращого» роутеру з нижнього цінового сегменту.

В економічному розділі визначено витрати на проектування та експлуатацію системи інформаційної безпеки.

Практичне значення роботи: полягає у розробці рекомендацій, щодо налаштувань елементів приватних мережах стандарту IEEE 802.11.

Наукова новизна: пропонований метод дозволяє більш ефективно виявляти вразливі маршрутизатори в мережі оператора Інтернету.

Напрямки подальших досліджень включають розробку альтернативного програмного забезпечення для маршрутизаторів, розробку систем та механізмів, які дозволять операторам мережі Інтернет підвищити ступінь захисту абонентів від мережевих атак.

ВИЯВЛЕННЯ ВРАЗЛИВОСТЕЙ, ВРАЗЛИВОСТІ, МЕРЕЖЕВІ АТАКИ, ТЕСТУВАННЯ НА ПРОНИКНЕННЯ, МАРШРУТИЗАТОРИ, МЕРЕЖЕВЕ ОБЛАДНЕННЯ, СИСТЕМА МОНІТОРИНГА, ІНФОРМАЦІЙНА БЕЗПЕКА.

РЕФЕРАТ

Пояснительная записка с.__, рис.__, табл.__, приложений__, источников__.

Объект исследования: беспроводные сети стандарта 802.11.

Цель работы: выявление уязвимостей в беспроводных сетях стандарта 802.11 и повышение уровня безопасности домашней сети.

Методы исследования: наблюдение и эксперимент, метод индукции, системный подход, метод анализа иерархий.

Специальная часть делится на следующие этапы:

- анализ уязвимостей сети.

- анализ существующих решений обеспечения уровню безопасности в сетях 802.11.

- разработка программы и методики анализа защищенности сетей.

- анализ трех типовых сетей.

- разработка рекомендаций по повышению безопасности в частной сети.

- Выбор «лучшего» роутеру с нижнего ценового сегмента.

В экономическом разделе определены затраты на проектирование и эксплуатацию системы информационной безопасности.

Практическое значение работы: состоит в разработке рекомендаций относительно настроек элементов частных сетях стандарта IEEE 802.11.

Научная новизна: предлагаемый метод позволяет более эффективно выявлять уязвимые маршрутизаторы в сети оператора Интернета.

Направления дальнейших исследований включают разработку альтернативного программного обеспечения для маршрутизаторов, разработку систем и механизмов, которые позволят операторам сети Интернет повысить степень защиты абонентов от сетевых атак.

ОБНАРУЖЕНИЯ УЯЗВИМОСТЕЙ, УЯЗВИМОСТЕЙ, СЕТЕВЫЕ АТАКИ, ТЕСТИРОВАНИЯ НА ПРОНИКНОВЕНИЕ, МАРШРУТИЗАТОРЫ, СЕТЕВОЕ ОБОРУДОВАНИЕ, СИСТЕМЫ МОНИТОРИНГА, ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ.

ABSTRACT

Explanatory note: p.__, pic.__, tab.__, sources__, applications__.

The object of study: 802.11 wireless networks.

Objective: identify vulnerabilities in 802.11 wireless networks and increase the level of home network security.

Research methods: observation and experiment, induction method, system approach, hierarchy analysis method.

The special part is divided into the following stages:

- analysis of network vulnerabilities.

- analysis of existing solutions to ensure the level of security in 802.11 networks.

- development of the program and methods of network security analysis.

- analysis of three typical networks.

- development of recommendations for improving security in the private network.

- Choosing the "best" router from the lower price segment.

The economic section identifies the costs of designing and operating an information security system.

The practical significance of the work: is to develop recommendations for setting up the elements of private networks of the IEEE 802.11 standard.

Scientific novelty: the proposed method allows you to more effectively identify vulnerable routers in the network of an Internet operator.

Future research areas include the development of alternative software for routers, the development of systems and mechanisms that will allow Internet operators to increase the protection of subscribers against network attacks.

DETECTIONS OF VULNERABILITIES, VULNERABILITIES, NETWORK ATTACKS, PERMITTING TESTS, ROUTERS, NETWORK EQUIPMENT, MONITORING SYSTEMS, INFORMATION SECURITY.

ПЕРЕЛІК УМОВНИХ СКОРОЧЕНЬ

WPA – Wi-Fi Protected Access;

PSK – Pre-Shared Key;

VPN – Virtual Private Network;

KRACK – Key Reinstallation Attack;

QR – Quick Response;

ПЗ – програмне забезпечення;

DoS – Denial-of-service attack

ОС – операційна система.

ЗМІСТ

ВСТУП

У зв'язку з широким розповсюдженням мережі Wi-Fi стає актуальним підтримання високого ступеня її безпеки. У корпоративних мережах задля підтримки високого рівня безпеки створюють цілі спеціалізовані відділи. Але безпровідні технології доступу до глобальної мережі Інтернет використовуються не тільки в великих корпораціях. Так, майже у 85% користувачів, є власна мережа Wi-Fi, яка також потребує належного захисту.

На даний момент постачальники маршрутизаторів гарантують виконання основної функції свого пристрою, але не гарантують, що створена мережа є безпечною. При чому цілі зловмисника можуть бути різними, як проникнення з ціллю виводу пристроїв з ладу, так і перехват особистої інформації.

Метою даної дипломної роботи є розроблення методики ефективного захисту локальних або приватних мереж доступу Wi-Fi. Для вирішення цього питання було розглянуто ступінь захищеності існуючих мереж стандартного користувача. На жаль, стандартні налаштування маршрутизатора майже не дають ніякого захисту створеній мережі. Також були виділенні основні способи налаштувань роутерів.

Для того, щоб зрозуміти, яке ефективно захистити мережу Wi-Fi, були проаналізовані існуючі рішення пошуку атак на мережу Wi-Fi, а також виявлені потенційні види загроз, і структурована класифікація атак.

Результатами даної роботи є оцінка безпеки мереж першого та другого рівня, стандарту IEEE 802.11, був розроблений алгоритм тестування для пошуку та випробування на вразливості апаратних роутерів, створення актуальних рекомендацій, щодо захисту приватної мережі Wi-Fi. Також був проведений аналіз розповсюджених моделей маршрутизаторів по декільком критеріям, важливим для користувача, як наприклад цінова політика, захист інформації в створеній мережі, кількість антен, та ін. Для здійснення остаточного вибору і створення рейтингу була обрана система підтримки прийняття рішень «NooTron», на базі методу аналізу ієрархій.

Таким чином дана дипломна робота має високе теоретичне та практичне значення для захисту приватних мереж більшості користувачів. За результатами даного дослідження користувачі можуть оцінити ступінь безпеки своєї мережі , надати їм більшого рівня захисту, та проаналізувати ринок існуючих маршрутизаторів.

РОЗДІЛ 1. ЗАГАЛЬНІ ВІДОМОСТІ ПРО СТАНДАРТ IEEE 802.11, ЙОГО ВРАЗЛИВОСТІ ТА ЗАСОБИ ЗАХИСТУ

1.1 Загальні відомості про Wi-Fi

Розвиток мережевих технологій призвів до появи набору стандартів IEEE 802.11, більш розповсюджена назва яких – Wi-Fi.

Wi-Fi є бездротовою технологією і як можна побачити з таблиці 1.1 працює у частотних діапазонах від 1 до 60 ГГц.

Таблиця 1.1 – стандарти 802.11

Стандарт	Частоти ГГц	Швидкість максимальна Мбіт/секунду
802.11b	2.4-2.4835	11
802.11a	5	54
802.11g	0.9, 2.4, 3.6, 5, 60	54
802.11n	2.4, 5	150 – 1 антена 600 – використо-вуючи 4 антени
802.11ac	5	6770

У 2018 році бездротові мережі – найбільш зручний спосіб передачі інформації в електронному вигляді.

Переваги бездротових мереж:

- доступність і простота розгортання мережі;
- мобільність користувачів в зоні дії мережі, та їх просте підключення;
- широке поширення мобільних пристроїв.

Технологія Wi-Fi реалізована в більшості пристроїв, крім того, ця технологія має менший вплив на здоров’я людини, та є більш енергоефективною ніж інші стандарти бездротового зв’язку.

Наявність точок доступу Wi-Fi, дозволяє користувачу підключитися до офісної, домашньої або публічної мережі, а також підтримувати з'єднання декількох комп'ютерів між собою.

Площа покриття залежить від: потужності передавача (яка в окремих моделях обладнання регулюються програмно), наявності та характеристики перешкод, типу та кількості антен.

Кожна безпровідна мережа складається з хоча б однієї точки доступу, в більшості випадків, у якості точки доступу використовується мережевий маршрутизатор. Мережеві маршрутизатори поділяються – як за ціною, так і за областю використання Таким чином, для великих корпоративних мереж, та маленьких корпоративних мереж використовується більш дороге, та складне обладнання, а для маленьких офісів та домашнього використання (далі домашні роутери) – призначені маршрутизатори, з істотно нижчою ціною та більш простими налаштуваннями.

Якщо подивитися на статистику продаж маршрутизаторів, то можна зробити висновок, що 85% користувачів мають дома свою мережу Wi-Fi. В той самий час 90% Wi-Fi мереж – домашні, або стоять у не великих офісах і лише 10% належать корпоративним мережам.

За версією найбільшого інтернет-магазину в Україні – Rozetka, найпопулярнішими, серед постачальників домашніх роутерів, є так і фірми: Mercusys, TP-Link, Netis, Keenetic, Xiaomi, Tenda, Asus, Mickotic[1]. А постачальники послуг інтернет (як наприклад Київстар), надають своїм користувачам, на безкоштовній основі, мережеві маршрутизатори таких фірм, як TP-Link, Huawei, D-Link.

Більшість домашніх роутерів, в стандартній комплектації, мають блок живлення та мережевий кабель Ethernet для з’єднання роутеру з ПК, та мають приблизно наступні характеристики:

-Інтерфейс підключення (WAN) 10 / 100BASE-TX Ethernet;

-Мережеві стандарти: 802.11 b / g / n / ac;

-Швидкість: Wi-Fi до 150 Мбіт / с, Lan портів до 100 Мбіт / с;

-Частота: 2,4/5 ГГц;

-LAN порти: 4 шт. для під’єднання за допомогою дротів;

-Static /Dynamic IP за потребою;

-Протоколи безпеки: WEP, WPA / WPA2 Personal, WPA / WPA2 Enterprise;

-Підтримка функції WPS (Wi-Fi Protected Setup) і WMM – функція підключення без пароля;

-Функції захисту роутера;

-Кнопка вимикання/включення Wi-Fi-мережі;

-Антена: внутрішня/зовнішня;

-Підтримка протоколів: PPPoE, IPsec, L2TP, PPTP;

-IPTV(надає змогу налаштувати собі трансляцію інтернет-телебачення, якщо таке надає провайдер);

-Резерв адрес (дозволяє зарезервувати IP – адресу під конкретного користувача);

-DNS (забезпечує більш швидку роботу з інтернетом);

-FTP (функція дозволяє налаштувати свій файловий сервер) [2].

1.1.1 Стандарти безпеки Wi-Fi

WEP (англ. Wired Equivalent Privacy) — найстаріший стандарт захисту бездротового трафіку, заснований на алгоритмі потокового шифрування RC4 (з використанням загального секретного ключа). Існують варіанти з довжиною ключа 64, 128 і 256 бітів [3]. Стандарт WEP не рекомендований для використання, через свою вразливість.

WPA і WPA2 (Wi-Fi Protected Access) – являє собою більш новий стандарт, який вийшов в 2004 році. Технологія WPA прийшла на заміну технології захисту бездротової Wi-Fi мережі WEP. Перевагами WPA є посилений захист. Важливою характеристикою є сумісність між безліччю бездротових пристроїв як на апаратному, так і на програмному рівнях[4].

Також WPA має 2 режими роботи:

-Режим PSK (Pre-Shared Key) – безпровідний доступ, який надає своїм користувача єдиний ключ доступу до своєї мережі. При зміні паролю на маршрутизаторі, доведеться знову авторизуватися з кожного пристрою і вводи-

ти новий ключ доступу. Пароль може мати від 8 до 63 символів. Даний пароль зберігається на безпровідних пристроях. Таким чином, кожен користувач комп'ютера може підключитися до мережі, а також побачити пароль. Схема роботи режиму PSK вказано на рисунку 1.1:

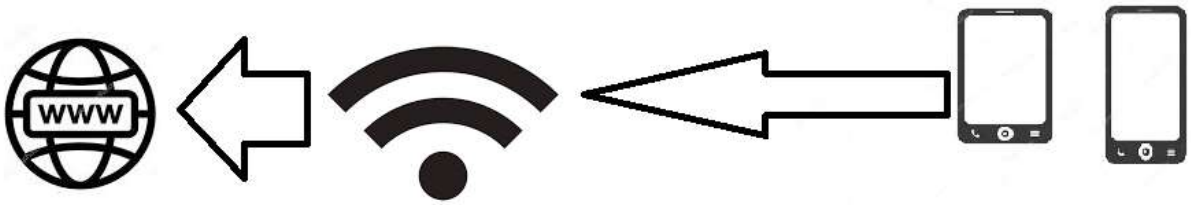

Рисунок 1.1 – Схема режиму PSK

-WPA-Enterprise (WPA-802.1x, RADIUS) – цей режим складніше в налаштуванні і пропонує індивідуальне і централізоване управління доступом до мережі Wi-Fi, та надає необхідний в робочому середовищі захист бездротової мережі. Коли користувачі спробують підключитися до мережі, їм знадобиться надати свої облікові дані для автентифікації.

Даний режим підтримує автентифікацію по протоколу 802.1x через RADIUS-сервер і підходить в тому випадку, якщо встановлено сервер RADIUS. Користувачі фактично не використовують ключі шифрування. Вони створюються захищено та назначаються після початку кожної сесії [5].

Схема роботи режиму WPA-Enterprise вказано на рисунку 1.2:

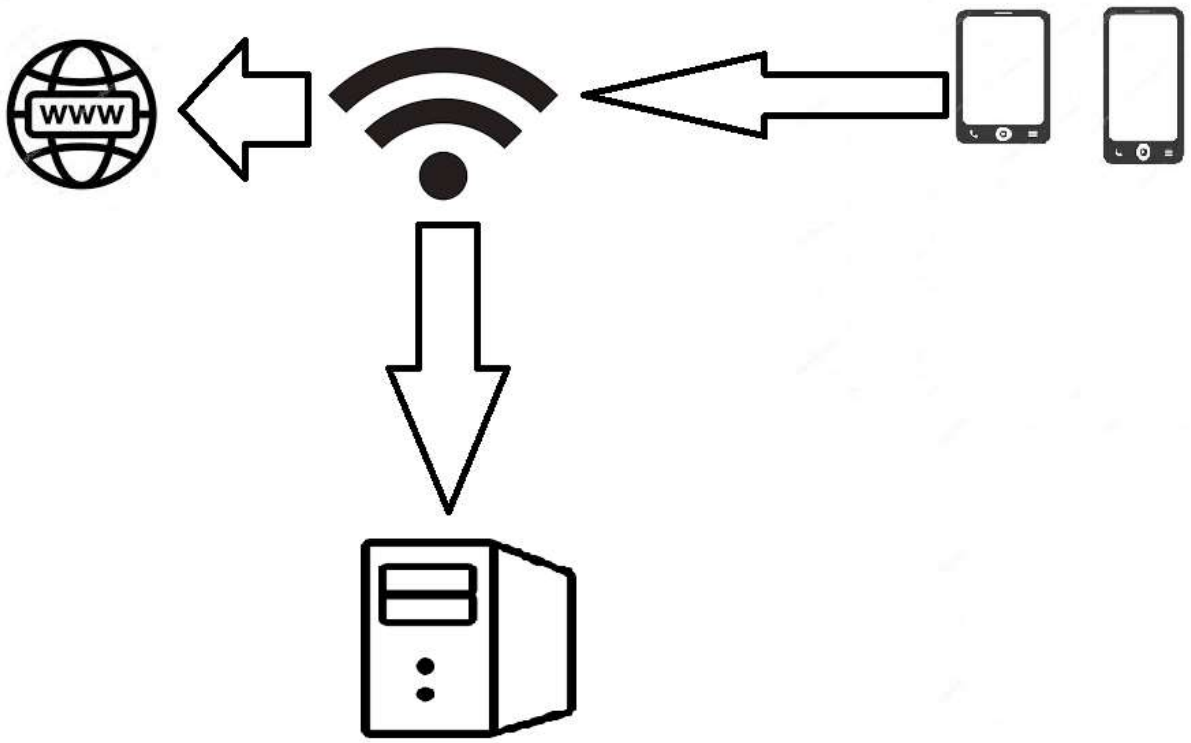

Рисунок 1.2. – Схема режиму Enterprise з радіус сервером

1.1.2 Стандарт WPA3

8 січня 2018 року Wi-Fi Alliance представив оновлену версію стандарту, яка отримала позначення WPA3. Ця версія матиме чотири основні поліпшення. Зокрема, буде посилено безпеку – навіть, якщо користувачі обирають «слабкий» пароль мережі. Також, в цьому стандарті, буде посилено захист приватних даних користувачів у відкритих мережах, шляхом індивідуальних налаштувань алгоритмів шифрування, і з’явиться підтримка набору 192-бітних криптографічних алгоритмів [6].

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

Всі протоколи доступні для впровадження виробниками в їх пристрої. Якщо WPA2 можна вважати показником, то ці протоколи в кінцевому підсумку будуть прийняті повсюдно, але Wi-Fi Alliance не надає ніякого графіка, за яким це повинно буде відбуватися. Швидше за все, з впровадженням но-

вих пристроїв на ринок, поступово WPA3, Enhanced Open і Easy Connect стануть новими опорами безпеки[7].

SAE – новий метод автентифікації пристрою, що намагається підключитися до мережі[8]. SAE – це варіант, так званого «встановлення зв'язку за методом бабки», що використовує криптографію для запобігання вгадування пароля зловмисником. Він говорить про те, як саме новий пристрій, або користувач, має «вітати» мережевий маршрутизатор при обміні криптографічними ключами[9].

SAE йде на заміну методу «попередньо розданого ключа» – PSK, який використовується з моменту презентації WPA2 в 2004-му. PSK також відомий, як встановлення зв'язку в чотири етапи (4-way-handshake), оскільки саме стільки повідомлень, або двосторонніх «рукостискань», необхідно передати між маршрутизатором і пристроями, які можуть бути під'єднані, щоб підтвердити, що вони домовилися з приводу пароля. При тому, що жодна зі сторін не повідомляє його іншій. До 2016 року PSK здавався безпечним, до здійснення відкритої атаки за допомогою перестановку ключа(KRACK)[10].

KRACK (Key Reinstallation Attack) перериває серію рукостискань, прикидаючись, що з'єднання з маршрутизатором тимчасово перервалося. Насправді він використовує повторювані можливості з'єднання, для аналізу рукостискань, поки не зможе здогадатися про те, який був пароль. SAE блокує можливість такої атаки, а також найбільш поширені «оффлайнові» атаки по словнику, коли комп'ютер перебирає мільйони паролів, щоб визначити, який з них підходить до інформації, отриманої під час PSK-з'єднань.

Як випливає з назви, SAE працює на підставі припущення про рівноправність пристроїв, замість того, щоб вважати один пристрій відправляє запити, а друге – встановлює право на підключення (традиційно це були пристрій, що намагається з'єднатися, і маршрутизатор, відповідно). Будь-яка зі сторін може відправити запит на з'єднання, і потім вони починають незалежно відправляти засвідчує їх інформацію, замість того, щоб обмінюватися повідомленнями по черзі, туди-сюди. А без такого обміну у атаки KRACK не буде можливості «вставити ногу між дверима і косяком», і атаки по словнику стануть марними.

SAE пропонує додаткове посилення безпеки, якого не було в PSK – пряму секретність. Припустимо, атакуючий отримує доступ до зашифрованих даних, які маршрутизатор відправляє і отримує з інтернету. Раніше атакуючий міг зберегти ці дані, а потім, в разі успішного підбору пароля, розшифрувати їх. З використанням SAE при кожному новому з'єднанні шифрує новий пароль, тому, навіть якщо атакуючий в якийсь момент і проникне в мережу, він зможе вкрасти тільки пароль від даних, переданих після цього моменту[11].

SAE описаний в стандарті IEEE 802.11-2016, що займає більше 3500 сторінок[12].

1.1.3 192-бітні протоколи безпеки

WPA3-Enterprise, версія WPA3, призначена для роботи в урядових та фінансових установах, а також в корпоративному середовищі, володіє шифруванням в 192 біта. Такий рівень шифрування для домашнього маршрутизатора буде надлишковим, але його має сенс використовувати в мережах, що працюють з особливо важливою інформацією[13].

Зараз Wi-Fi працює з ключом шифрування довжиноюв 128 біт. Ключ шифрування довжиною в 192 біта не буде обов'язковою до використання – це буде варіант налаштувань для тих організацій, мереж, для яких вона буде потрібна. Wi-Fi Alliance також підкреслює, що в промислових мережах необхідно посилювати безпеку по всіх фронтах: стійкість системи визначається стійкістю найслабшої ланки.

Щоб гарантувати належний рівень безпеки всієї мережі, від початку до кінця, WPA3-Enterprise буде використовувати 256-бітний протокол Galois / Counter Mode для шифрування, 384-бітний Hashed Message Authentication Mode режим для створення і підтвердження ключів, і алгоритми Elliptic Curve Diffie-Hellman exchange, Elliptic Curve Digital Signature Algorithm для аутентифікації ключів. Вони мають достатньо складні обчислювальні алгоритми, але їх перевагою є формування 192-бітного ключа на кожному кроці.

Easy Connect – це визнання наявності в світі величезної кількості при-

строїв, приєднаних до мережі. І хоча, можливо, не всі люди захочуть обзавестися розумними будинками, у середньої людини до домашнього маршрутизатора сьогодні, швидше за все, підключено більше пристроїв, ніж в 2004 році. Easy Connect – спроба Wi-Fi альянсу зробити під'єднання всіх цих пристроїв більш інтуїтивним.

Замість того, щоб кожен раз при додаванні пристрою вводити пароль, у пристроїв будуть унікальні QR-коди – і кожен код пристрою буде працювати, як публічний ключ. Для додавання пристрою можна буде просканувати код за допомогою смартфона, вже з'єднаного з мережею.

Після сканування пристрій обмінюється з мережею ключами автентифікації для встановлення подальшої зв'язку. Протокол Easy Connect не пов'язаний з WPA3 – пристрої, сертифіковані для нього, повинні мати сертифікат для WPA2, але не обов'язково сертифікат для WPA3 [14].

Enhanced Open – ще один окремий протокол, розроблений для захисту користувача у відкритій мережі. Відкриті мережі – такі, якими користуються в кафе або аеропорту – несуть в собі цілий комплекс проблем, яких немає при встановленні з'єднання вдома або на роботі[13].

Багато атак, що відбуваються у відкритій мережі, відносяться до пасивних. Коли до мережі підключається велика кількість пристроїв, завдяки фільтрації інформації, можливо зібрати важливі дані багатьох користувачів.

Enhanced Open використовує опортуністичне[15] бездротове шифрування (Opportunistic Wireless Encryption, OWE), певний в стандарті Internet Engineering Task Force RFC 8110[16], щоб захищатися від пасивного підслуховування. Для OWE не потрібен додатковий захист з автентифікації – воно концентрується на поліпшенні шифрування даних, що передаються до публічних мереж, з метою запобігання їх викрадення. Воно також запобігає так звану «просту ін'єкцію пакетів», в якій атакуючий намагається порушити роботу мережі, створюючи і передаючи особливі пакети даних, що виглядають, як частина нормальної роботи мережі.

Enhanced Open не дає захисту з автентифікацією через особливості організації відкритих мереж – вони за визначенням призначені для загального використання. Enhanced Open був розроблений для поліпшення захисту відк-

ритих мереж проти пасивних атак, так, щоб не вимагати від користувачів введення додаткових паролів або проходження додаткових кроків.

1.2 Аналіз загроз інформаційної безпеки в безпровідних мережах стандарту IEEE 802.11

Основні недоліки захисту інформації в бездротових мережах полягають в наступному:

- поширення сигналу за межі контрольованої зони;
- використання вразливих протоколів і методів автентифікації;
- відсутність повного захисту від атак при доповненні стандартів;
- можливі помилки в налаштуванні бездротової мережі.

Цілі, з якими зловмисник намагається проникнути до мережі безпровідного доступу:

-викрадення чи зміна даних в мережі;
-доступ до периферії з мережевим інтерфейсом;
-доступ до каналу інтернет;
-руйнування локальної мережі.

Тобто зловмисник може вплинути на цілісність інформації, її доступність і конфіденційність, чи просто неправомірно користуватися каналом інтернет в своїх цілях.

Основними недоліками безпровідної мережі, які роблять її вразливою до атак є – застаріле обладнання зі старими конфігураціями, та неправильне налаштування наявного обладнання. Чим більше маршрутизатор має функцій, тим вірогідніше, що в ньому можна знайти вразливість, яка ще не усунута:

-WPS;
-віддалений доступ;
-швидке налаштування обладнання.

А деякі функції, що заявляються постачальниками, як ті, що захищають від неправомірного доступу лише ускладнюють користувачам життя. Однією з таких функцій є білий список MAC-адресів: для того, щоб замаскувати свою MAC-адресу під білу зловмиснику – потрібно декілька хвилин, а для звичайного користувача безпровідної мережі, який хоче приєднати новий

пристрій – потрібно кожен раз звертатися до системного адміністратора, або змінювати налаштування точки доступу самостійно.

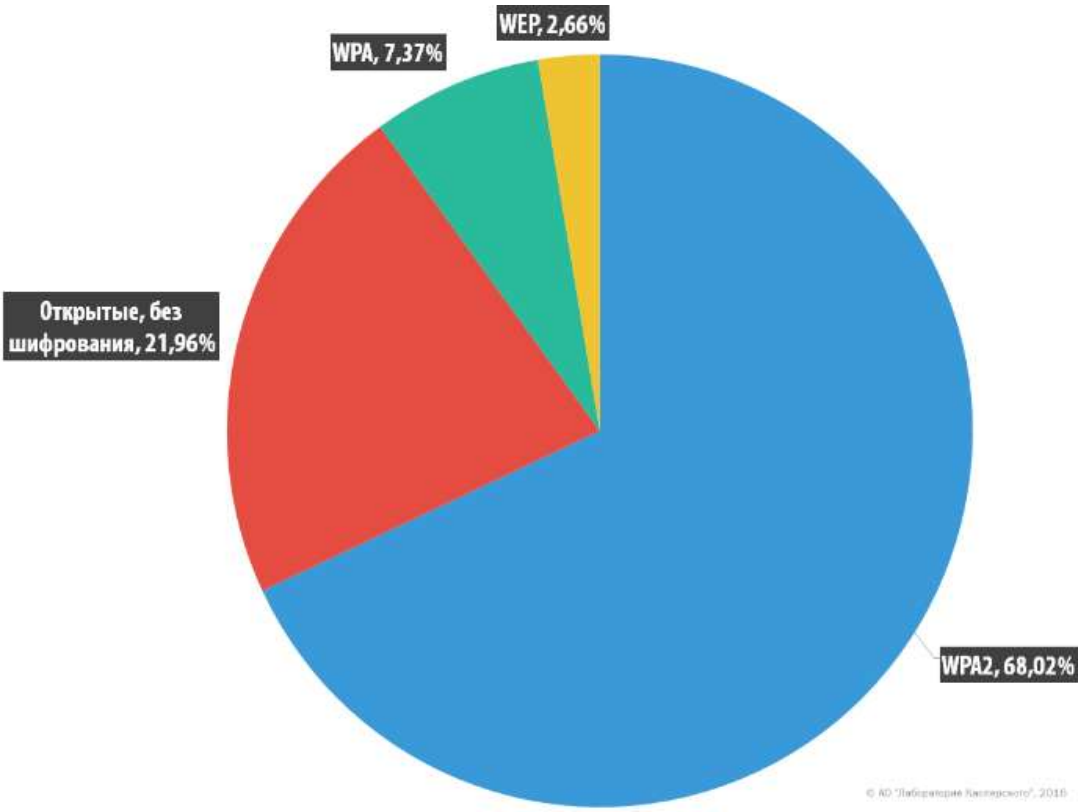

Рисунок 1.3 – світова статистика захищеності точок доступу[17]

Згідно зі звітом компанії Kaspersky близько 24,7% точок доступу Wi-Fi в світі станом на кінець 2016 року не використовували шифрування. При його відсутності зловмисник з пристроєм, що здатний працювати з технологією Wi-Fi та приймачем здатним працювати в режимі моніторингу, може перехопити трафік користувачів, і в режимі «оффлайн» його переглянути чи розшифрувати. На щастя, сучасні системи «онлайн-банкінгу» і «месенджери» – шифрують свої данні. При цьому, залишається велика кількість інформації, яку можна вилучити без зайвих складнощів, а також зростає загроза фішингу.

Близько 10% маршрутизаторів використовують вразливі методи шифрування, такі як WEP та WPA, їх злом займає лічені хвилини, навіть при використанні стійкого пароля.

Але все ж таки більшість пристроїв використовує шифрування стандарту WPA-2, та на жаль, це не дає потрібного рівня інформаційної безпеки в

цих мережах, через слабкі паролі, не коректні налаштування, відсутність оновлень системи чи не закриті вразливості[17].

Більшість користувачів не мають змоги залучити спеціаліста з інформаційної безпеки, або людину, яка має достатню кваліфікацію в цій сфері, до налаштування своєї домашньої мережі. Так ,в інтернет-магазині «Rozetka» така послуга коштує 399 грн. З точки зору інформаційної безпеки, вони можуть: оновити програмне забезпечення, налаштувати гостьовий доступ, вибрати стандарт шифрування та ввести пароль[18].

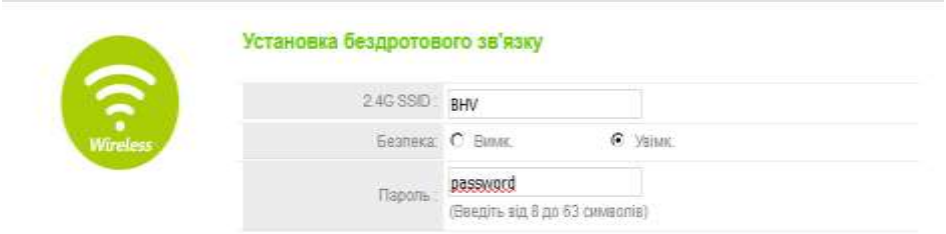

Рисунок 1.4 – небезпечні налаштування Netis WF-2411

1.2.1 Реалізація загроз

Широке поширення Wi-Fi мереж призвело до спроби зробити налаштування бездротової мережі простіше для людей, що не володіють навичками комп'ютерної грамотності. Результатом стала технологія Wi-Fi Protected Setup (WPS). WPS автоматично призначає ім'я мережі і включає шифрування для захисту бездротової мережі від несанкціонованого доступу, при цьому немає необхідності вручну налаштовувати кожен параметр. WPS реалізується на більшості вироблених в даний час бездротових точках доступу, включаючи ASUS, TP-Link, D-Link, Cisco, Linksys, Netis. Крім того, на багатьох пристроях дана функція включена стандартно.

Однак реалізація ідеї використання WPS має недолік, який дозволяє зловмисникові виконати атаку шляхом підбору PIN-коду, за яким відбувається автентифікація користувача. Хоча довжина PIN-код складається із 8 цифр, він розділений на дві половини, причому остання цифра є контрольною сумою коду. Це зменшує максимально можливу кількість спроб автентифікації,

необхідних для вгадування PIN-коду, з 108 (100 000 000) до 104 + 103 (11 000). Відновлення PIN-коду дає атакуючому повний доступ до мережі, причому якщо точка доступу віщає в двох діапазонах частот одночасно (2,4 ГГц і 5 ГГц), то так як радіо-модулі використовують один і той же WPS PIN-код, знання його дозволяє відновити всі ключі WPA.

1.2.2 Класифікація атак

Класифікація атак:

-брутфорс (метод грубого підбору паролей);

-вразливість WPS;

-перехват пакетів;

-інші вразливості.

За статистикою найчастіше мережі Wi-Fi зламують за допомогою дистрибутиву Kali-Linux. Kali-Linux включає в себе великий вибір ПЗ та утиліт, за допомогою яких можна проводити тест на проникнення в тому числі і Wi-Fi мережі.

Для цього він містить таке ПЗ, як:

- Aircrack-ng – це повний набір інструментів для оцінки безпеки мережі WiFi. Він фокусується на різних областях безпеки WiFi:

1) Моніторинг: захоплення пакетів і експорт даних в текстові файли для подальшої обробки сторонніми інструментами;

2) Атака: повторні атаки, деаутентіфікація, підроблені точки доступу та інші за допомогою пакетної ін'єкції;

3) Тестування: перевірка карт WiFi і драйверів (захоплення і уприскування);

4) Крекінг: WEP і WPA PSK (WPA 1 і 2).

Всі інструменти – це командний рядок, яка дозволяє створювати важкі сценарії. Багато графічні інтерфейси скористалися цією функцією. Він працює в основному Linux, але також Windows, OS X, FreeBSD, OpenBSD, NetBSD, а також Solaris і навіть eComStation.

-Airmon-ng – скрипт який переводить мережеве обладнання в режим сканування;

-Wi-Fi Pumpkin – дозволяє реалізувати таку атаку, як «людина посередині». Приклад інтерфейсу Wi-Fi Pumpkin, можна побачити на рисунку 1.4.

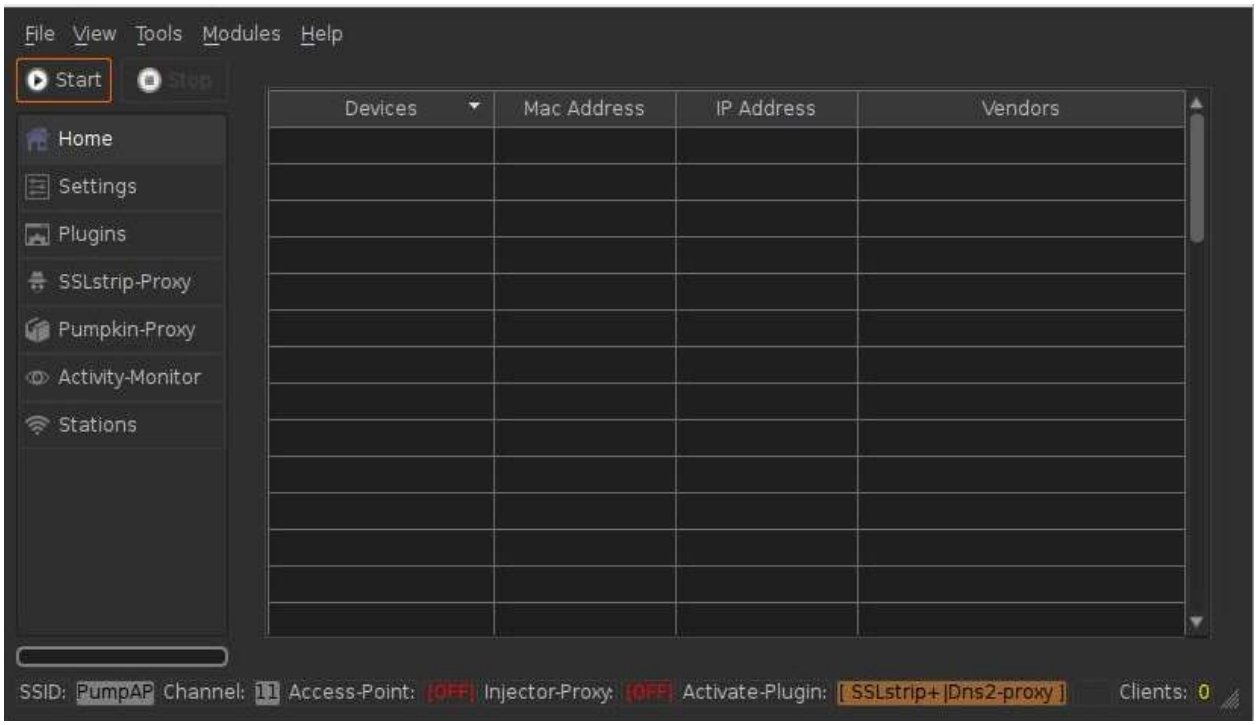

Рисунок 1.4 – інтерфейс Wi-Fi Pumpkin.

Wi-Fi-Pumpkin – це шкідлива інфраструктура АП, яка легко створює ці підроблені мережі, при цьому здійснюється переадресація трафіку користувача, який нічого не подозрює. Він поставляється з функціями, у тому числі з фальсифікованими точками доступу Wi-Fi, деаутинтифікаційними-атаками на клієнтські точки доступу, запитами зонда та облікових даних, прозорим проксі-сервером, атакою поновлення Windows, диспетчером фішингу, отруєнням ARP, DNS-спуфінг, насокним проксі та захватом зображення крім того, WiFi- Pumpkin – дуже повна структура для перевірки безпеки Wi-Fi. Список функцій досить широкий.

- BoopSuite – це набір інструментів, написаних на Python і призначених для безпровідного аудиту та тестування безпеки. Його інтерфейс можна побачити на рисунку 1.5.

Цей набір Wi-Fi інструментів призначений для простого та ефективного використання. Інструменти підтримують частоти 2 ГГц і 5 ГГц. Всі вони написані виключно на Python. Вони мають змогу перехвату «рукостискань», інструмент командного рядка та графічний користувальницький інтерфейс, скрипт для включення режиму монітора та сценарій для деаутентифікації. Все це входить в BoopSuite, а в майбутньому планується додавання нових інструментів, у тому числі:

- BoopMon – для переведення безпровідної карти в режим монітора та в керованому режимі;

- BoopSniff – для показу точок доступу в діапазоні доступності та захоплення рукопожаті;

-BoopStrike – для виконання атак деаутентифікація;

-boopsniff_gui – новий графічний інтерфейс;

-old_boopsniff_gui – старий графічний інтерфейс.

Рисунок 1.5 – інтерфейс Boop

1.3 Існуючі рішення пошуку мережевих атак

Існуючі системи виявлення вторгнень в бездротових мережах орієнтовані на аналіз протоколів бездротового зв'язку сімейства 1EEE 802.11, іден-

тифікацію та аналіз підозрілої активності. Крім того, деякі виробники забезпечують можливість запобігання вторгнень в корпоративну мережу. В цьому випадку бездротові системи здатні здійснювати дії двох типів при виявленні атаки:

- безпровідний вплив – з'єднання між користувачем і точкою доступу обривається за допомогою відправки повідомлення про дисоціації (роз'єднання), після чого точка доступу відмовляє у відновленні з'єднання;

- мережевий вплив – система передає комутатора команду блокувати з'єднання з даним користувачем мережі по порту або MAC-адресою .

Крім того, деякі системи можуть визначити фізичне розташування джерела виявленої загрози за допомогою методу тріангуляції.

1.3.1 Аналіз існуючих засобів пошуку атак на мережу Wi-Fi

1.3.1.1 AirTight Networks

Ця система може бути розгорнута над вже існуючою мережею, та не потребує її змін. AirTight досить проста в використанні спеціалістам класа Junior.

Основні характеристики системи:

- автоматичне виявлення і блокування різних видів бездротових загроз, в тому числі несанкціонованих точок доступу і пасток, DoS-атак, Ad-Hoc мереж і ін .;

- цілодобовий моніторинг продуктивності мережі;

- можливість функціонування сенсорів в режимі «оффлайн»;

- виявлення радіочастотного зашумлення і перешкод;

- розслідування бездротових інцидентів по журналам реєстрації;

-обчислення розташування бездротового пристрою або джерела перешкод;

- захист мобільних пристроїв;

- інтеграція з платформами ArcSight, Checkpoint, McAfee ePO і Qualys, підтримка SNMP і Syslog;

- звіти про відповідність стандартам PCI DSS, SOX, HIPAA, GLBA, DoD Directive 8100.2;

- управління через фізичне підключення, віртуальний сервер або хмара.

В якості сенсорів використовуються власні пристрої AirTight C-75, C-60, C-55, C-50 з підтримкою одного або двох радіоканалів і режимами роботи в ролі точки доступу або виділеного активного сенсора. Найбільш функціональні моделі мають підтримку стандарту 802.11ac і можливість підключення зовнішніх антен[19].

1.3.1.2 AirMagnet Enterprise

Система дозволяє вирішувати наступні завдання:

- визначення несанкціонованих точок доступу і клієнтів;

- контроль політики безпеки використання бездротових мереж;

- виявлення атак в бездротової мережі і протидію їм;

- локалізація зловмисника методом тріангуляції.

Основні характеристики AirMagnet Enterprise:

- підтримка стандарту 802.11ac;

- сигнатурний метод виявлення вторгнень для захисту від загроз;

- наявність аналізатора радіочастот, що дозволяє виявляти перекриття каналів 802.11 і виявляти радіоперешкоди ;

- звіти про відповідність стандартам HIPAA, PCI DSS, GLBA, DoD, ISO 27001, BASEL 2 і CAD3;- запобігання виявлених атак як за допомогою бездротового впливу, так і в кабельній мережі.

Система складається з сенсорів, сервера і консолі управління

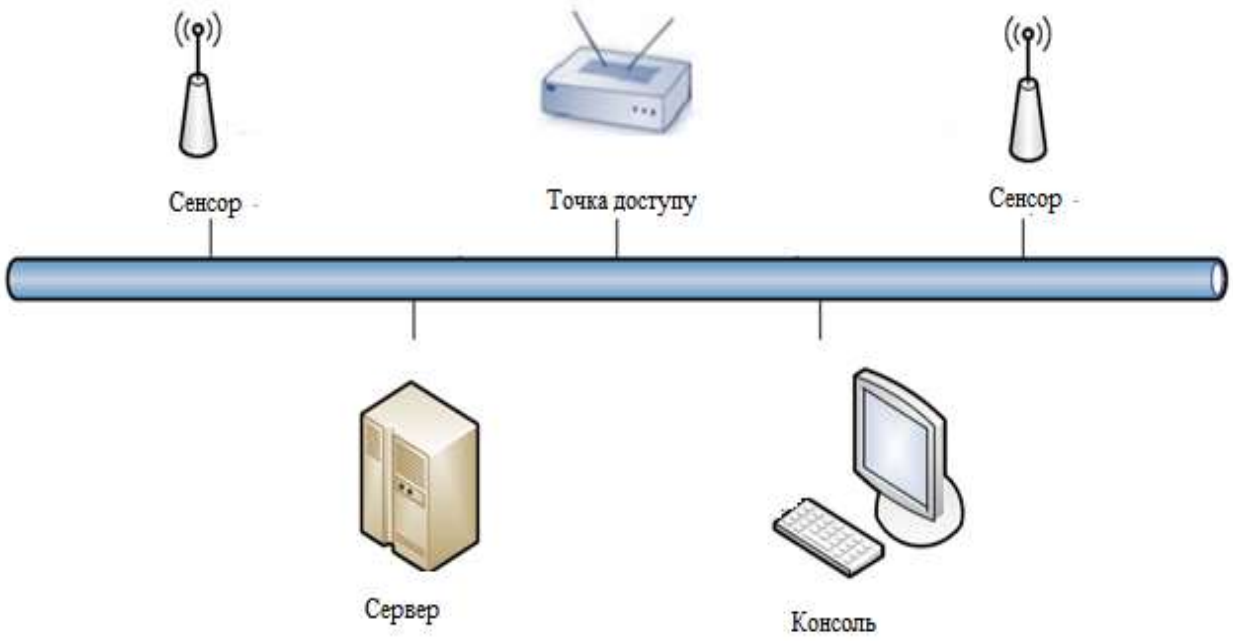

Рисунок 1.6 – приклад архітектури WIDS

Функція тріангуляції дозволяє визначити місцезнаходження бездротового пристрою порушника. Для цього необхідно імпортувати в систему план поверху і вказати розміщення сенсорів і точок доступу на плані. Приблизне розташування пристрою забезпечується в разі виявлення його, як мінімум трьома сенсорами, при цьому великий обсяг генерованої ним трафіку сприяє підвищенню точності визначення місця розташування. Крім того, функція тріангуляції дозволяє заборонити з'єднання з корпоративною мережею, ініційовані з-за меж кордонів захищається периметра організації .

Система дозволяє виявити такі бездротові загрози:

- застосування утиліт взлому;

- атака з повтором перехопленого зашифрованого пакета для прискорення розкриття шифрування;

- атаки по словнику на протокол EAP (велика кількість невдалих спроб встановити сесію);

- помилкові точки доступу, створені за допомогою утиліт і маскуються під корпоративні;

- підміна MAC-адреси з метою обходу фільтрів на основі MAC-адрес;

- спотворені кадри стандарту 802.11;

- пряма передача пакетів між клієнтами, що є порушенням політики;

- атака «людина посередині»;

- помилковий Dynamic Host Configuration Protocol (DHCP) сервер;

- зондування – спроба встановлення з'єднання з будь-якою точкою доступу (Probing)

Система має гнучкий функціонал побудови звітів, які можуть складатися за різними стандартами.

Недоліком системи є складність її налаштування при потребі широкого функціоналу[20].

1.3.1.3 AirDefense Enterprise

Третьою розглянутої WIDS є рішення AirDefense Enterprise компанії Motorola. Дана система дозволяє вирішувати наступні завдання:

- безперервний моніторинг бездротового трафіку 802.11 a / b / g / n і виявлення неавторизованих пристроїв;

- автоматизована захист мережі (безпровідний або традиційної, в якій безпровідні технології заборонені політикою безпеки) від несанкціонованого доступу по бездротових каналах;

- моніторинг відповідності заданої політики безпеки (конфігурації), моніторинг/діагностика бездротової інфраструктури;

- надання інструментарію для розслідування інцидентів безпеки і віддаленого аналізу мережевих проблем;

- координати обчислюються випромінювального пристрою;

- візуалізація покриття мережі в реальному часі;

- аналіз частотного спектра та ін..

Система складається з наступних компонентів :

- центральний сервер у вигляді програмно-апаратного комплексу;

- розподілені сенсори, які збирають інформацію і передають на сервер;

- консоль адміністратора з веб-інтерфейсом на мові Java;

- програмні модулі розширення.

У ролі сенсорів виступають бездротові точки і порти доступу Motorola AP300, AP-5131, AP-7131. При цьому точки, оснащені двома радіомодулями,

здатні паралельно виконувати функції цілодобового моніторингу та надавати безпровідний доступ.

У системі є можливість автоматизованого реагування на бездротові загрози як через бездротову мережу, так і методами, характерними для традиційних мереж.

Для забезпечення ефективного реагування на інциденти в AirDefense реалізована налаштовується схема управління подіями. На центральному сервері зберігається бібліотека подій системи, що містить дані про більш ніж 200 загрози різних типів, таких як активна розвідка, неавторизовані, відкриті і некоректно налаштовані точки доступу, прослуховування, спроби злому протоколів шифрування і атаки по словнику, маскування і фішинг, помилкові точки доступу , ін'єкції трафіку, DoS-атаки і ін.

Дані з сенсорів, проаналізовані різними модулями, далі об'єднуються в одну подію, якій присвоюється певний рівень небезпеки. Кожна подія забезпечується докладною інформацією про її джерела, рекомендовані заходи щодо усунення загрози, даними для аудиту події, що дозволяє інтегрувати систему із зовнішніми системами управління подіями і скоротити час реагування на інциденти.

Система використовує механізми, як традиційного сигнатурного аналізу, аналізу некоректного використання протоколів, пошуку трафіку, який відповідає заданій політиці, так і методики визначення аномального поведінки мережі та контекстно-залежного аналізу,запобігає появі помилкових спрацьовувань.

Система AirDefense Enterprise дозволяє визначати політики безпеки і конфігурації бездротових мереж і контролювати їх застосування, обмежуючи число підтримуваних протоколів автентифікації, стандартів шифрування, швидкостей передачі даних і припиняючи всі спроби з'єднань, що не відповідають заданим політикам. Як тільки система знаходить невідповідне політиці пристрій, вона тут же видає сповіщення адміністратору. Також гнучкий генератор звітів дає можливість створювати звіти як по вбудованим шаблонами про відповідність політикам (PCI DSS, DoD 8100.2, HIPAA, GLBA, SOX), так і власного формату.

Для кожного бездротового пристрою AirDefense Enterprise зберігає значення різних параметрів, таких як стан радіоканалів, характеристики сигналів, активність і потоки трафіку. Система може показати час атаки / злому, точку входу, тривалість атаки, які потоки даних було встановлено та які системи вражені.

Додатковий модуль WEP Cloaking забезпечує захист бездротових мереж, що використовують WEP-шифрування, шляхом наведення сенсорами радіоефіру спеціально сконструйованими неправильними WEP-пакетами, які унеможливлюють відновлення WEP-ключа з зібраного зловмисником трафіку.

Модуль відстежування місцеположення джерел сигналу дозволяє визначити розташування зловмисника, некоректно налаштованого клієнтського пристрою або джерела перешкод методом тріангуляції, а в поєднанні з модулем Advanced Forensics з'являється можливість відстежити переміщення джерел сигналу по контрольованій території. При цьому при визначенні координат об'єкту використовуються імпортовані плани поверхів і приміщень з урахуванням характеристик матеріалів стін, дверей, вікон, міжповерхових перекриттів

AirDefense також виконує роль інструменту системного адміністратора для аналізу і діагностики стану мережі. У поєднанні з додатковим модулем LiveRF система дозволяє в режимі реального часу оцінювати продуктивність мережі, наочно відслідковувати перевантажені канали або точки доступу, виявляти інтерференції, перекриття каналів і мертві зони, визначати основних споживачів смуги пропускання і знаходити неправильно сконфігуровані точки доступу і пристрої, що впливають на працездатність мережі.

Використовуючи додатковий модуль Spectrum Analysis, можна визначати додаткові джерела інтерференції в частотних діапазонах функціонування бездротових мереж, які не використовують протоколи 802.11, наприклад, Bluetooth, бездротові телефони, мікрохвильові печі, бездротові відеокамери та ін..

1.3.1.4 Cisco Wireless Intrusion Prevention System

Ще одна, широко відома система запобігання бездротових атак – Cisco Wireless Intrusion Prevention System (WIPS). Це бездротове рішення, яке дозволяє виявити і локалізувати як провідні, так і бездротові загрози на рівнях моделі OSI з фізичного до мережевого. Система виконує наступні функції:

- виявлення, класифікація і знешкодження помилкових пристроїв і неавторизованих мереж;
- моніторинг і усунення вразливостей;
- аналіз трафіку на предмет наявності слідів відомих утиліт злому і поширених технологій атак;
- моніторинг і автоматична оптимізація продуктивності мережі;
- складання звітів по продуктивності і безпеки, в тому числі на відповідність стандартам.

Основні особливості Cisco WIPS:

- інтегрування функцій бездротового виявлення атак в об'єкти мережевої інфраструктури;
- розподілений аналіз трафіку і аномалій на точках доступу і WLAN-контролерах;
- підтримка до 3000 підключених точок доступу;
- виявлення загроз і мережевих неполадок в реальному часі;
- комбінування бездротового і дротового моніторингу трафіку, аналізу аномалій, перевірки характеристик і конфігурацій бездротових пристроїв;
- захист кадрів управління за допомогою протоколу Cisco MFP .

Рішення включає в себе наступні компоненти :

- точки доступу: локально обробляють бездротової трафік, виконують активну сканування каналів і передають MAC-адреси, рівень сигналу RSSI і інші параметри на WLAN-контролер;
- контролер бездротового локальної мережі (Wireless LAN ControПer, WLC): генерує переривання в системі управління мережею при виявленні атаки або підозрілої активності;

- підсистема мобільних послуг (Mobility Services Engine, MSE): отримує інформацію в режимі реального часу від WLC і виконує її зіставлення з наявними в базі даних;

- підсистема управління мережею (Prime Infrastructure): взаємодіє з MSE, виконує функції моніторингу, налаштування, усунення несправностей, формування звітів і визначення місця розташування об'єктів

Система дозволяє виявити такі події, як:

- неавторизовані точки доступу / клієнти і Ad-Hoc мережі;

- помилкові точки доступу;

- підміна MAC / IP-адрес;

- DHCP-spoiling;

- мережева розвідка: використання утиліт Netstumbler, Wellenreiter, Kismet, помилкові пристрої та ін .;

- обхід автентифікації і злом шифрування: використання утиліт AirSnarf, AirCrack, ASLEAP, Chop-Chop та ін .;

- повтор пакетів, підроблені кадри та ін .;

- атаки на мережеві протоколи 802.11;

- DoS-атаки: використання утиліти AirJack, спотворення протоколів 802.11, радіочастотне зашумлення і ін .;

- радіоперешкоди та зони з недостатнім покриттям (технологія CleanAir). Технологія Cisco Rogue AP Containment дозволяє подавляти сигнал несанкціонованих точок доступу. При цьому знижується якість їх роботи до незадовільного рівня, але можливість підключитися до них все ж залишається. Разом з тим може знижуватися і якість роботи основної мережі – заявлено зниження швидкості до 20%, на практиці зустрічається і 50%

Варто зазначити, що для повноцінної роботи Cisco WIPS необхідний досить великий набір компонентів, що, як наслідок, вимагає значних витрат і відповідного рівня підготовки обслуговуючого персоналу.

1.3.1.5 Waidps

Для виявлення аномалій бездротового ефіру в "домашніх" умовах можна використовувати утиліту waidps. Це багатоцільовий інструмент, створений для аудиту (тестування на проникнення) мереж, виявлення бездротового вторгнення (атаки WEP / WPA / WPS) а також запобігання вторгнення (зупинка зв'язку станції з точкою доступу). Крім цього, програма буде збирати всю Wi-Fi інформацію зоні дії і зберігати в базах даних.

Waidps здатна виявляти масові деаутентіфікації, які можуть сигналізувати про можливу атаку на WPA (для перехоплення хендшейка), виявляти атаки з використанням ARP запитів, за допомогою Rogue AP і Evil_Twin, можливих атак перебором WPS та багато іншого.

Програма сама піднімає необхідні їй інтерфейси і начитає моніторити ефір. Цікавою особливістю є, що програму можна використовувати не тільки для виявлення атаки, але так само з її допомогою можна провести безпровідної мережі.

Для роботи програми необхідно додатково встановити пакет aircrack-ng і wireshark.

На рисунку 1.7 зображено приклад інтерфейсу:

Рисунок 1.7 – інтерфейс Waidps

1.3.1.6 Nzyme

Nzyme збирає фрейми 802.11 безпосередньо з ефіру і відправляє їх у систему управління журналом Graylog (з відкритим вихідним кодом), що дозволяє використовувати її в якості IDS WiFi, моніторингу та реагування на інциденти. Для цього потрібно тільки JVM і WiFi-адаптер, що підтримує режим моніторингу.

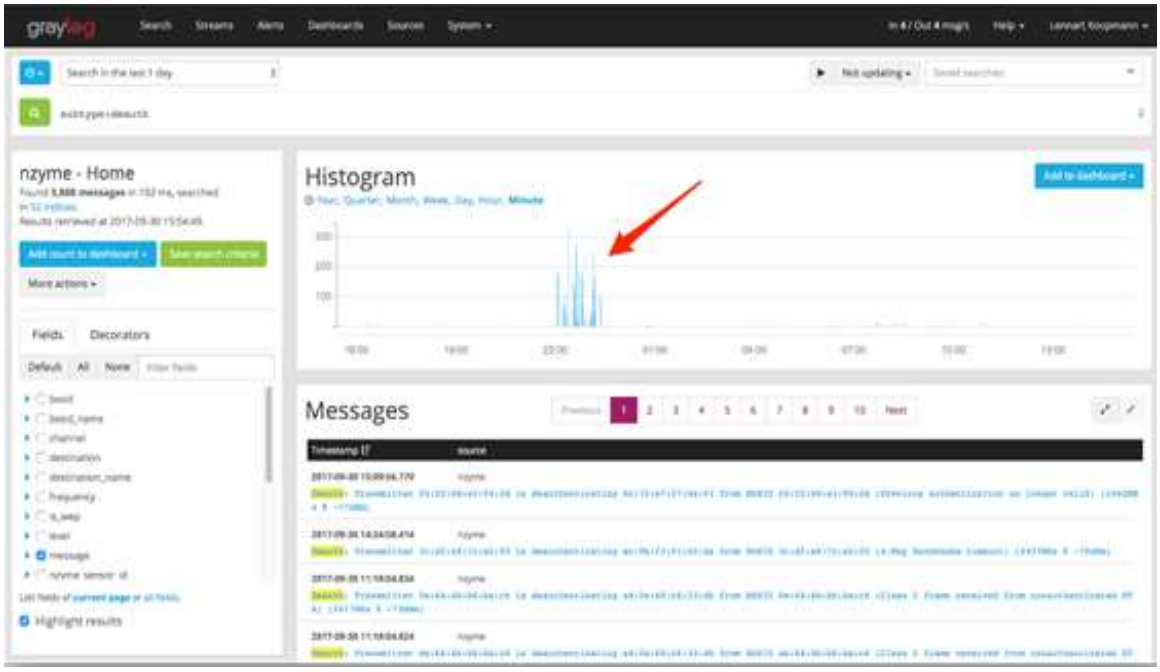

Рисунок 1.8 – інтерфейс Nzyme

Відмінною особливістю даного інструменту є початкова «заточеність» на запуск на слабких машинах, наприклад на Raspberry Pi. Також є можливість запуску nzyme «з коробки» на MacBook.

Для початку необхідно конфігурувати систему для роботи, встановивши deb пакет або скориставшись jar файлом. Також необхідно налаштувати конфігураційний файл для з'єднання з Graylog:

nzyme_id = nzyme

channels = en0:1,2,3,4,5,6,8,9,10,11

channel_hop_command=sudo/System/Library/PrivateFrameworks/Apple80211.framework/Versions/Current/Resources/airport {interface} channel {channel}

channel_hop_interval = 1

graylog_addresses = %graylog IP%:12000

beacon_frame_sampling_rate = 0

Для відображення використовується Graylog (можна використовувати у вигляді віртуальної машини), що дозволяє виводити інформацію в візуальному відображенні [8]:

Рисунок 1.8 – Nzyme з журналом Graylog

1.3.1.7 Avast Free

Компанія Avast надає своїм користувачам доступ до низки функцій свого програмного забезпечення безкоштовно, до цього списку входить «Перевірка Wi-Fi»

Ця функція виявляє наступні вразливості :

-Ненадійні або задані за замовчуванням паролі (для адміністрування маршрутизатора та мережі Wi-Fi)

-Уразливості вбудованого ПЗ (для найбільш відомих постачальників)

-Бездротові мережі без шифрування і захисту

-Взлом DNS (для пристроїв і маршрутизаторів)

-Відкриті порти мережі (для віддаленого доступу, Telnet і так далі)

Результати сканування містять:

-IoT прилади в мережі

-Данні маршрутизатора (IP адреса, MAC адреса, його постачач, модель, SSID та DNS)[9].

За допомогою додатку на ОС Android можна перевіряти не лише безпечність точки доступу, але й прилади які до неї підключені.

Але всі ці функції працюють лише при ручному запуску, в режимі моніторингу вони не працюють навіть в комерційній версії.

1.1.1 Порівняння існуючих засобів пошуку атак

Таблиця 1.2 – порівняння засобів пошуку атак

Комплекси/критерії	Аналіз трафіку	Відповідність стандартам	Ціна продукту	Захист та інші корисні функції	Простота роботи	Сумарно балів (0-35)
Mojo AirTight	5	5	4	5	4	23
AirMagnet Enterprise	4	7	2	6	3	22
AirDefense Enterprise	6	5	3	4	2	20
Cisco WIPS	7	7	1	7	1	23
Waidps	3	0	5	3	6	17
Nzyme	2	0	6	2	5	15
Avast Free	1	0	7	1	7	16

Для порівняння використана шкала балів 0-7

0 – параметр не задовольняє мінімальним вимогам користування

1 – параметр задовольняє мінімальні вимоги для користування

7 – найкращий рівень параметру серед представлених вище програм

1.4 Законність злому точок доступу Wi-Fi

Нажаль, на даний момент в Україні в нормативно-правовій базі не має конкретної відповідальності за взлом та використання чужого безпровідного каналу. Таким чином зловмисник який отримав неправомірний доступ до вашої мережі, згідно закону ще не являється злочинцем, а всі його протиправні дії треба зуміти доказати, перед цим знайшовши зловмисника, тому користувачам домашніх безпровідних мереж потрібно бути пильними.

1.5 Види мереж використовуючих стандарт 802.11

Мережі використовуючи стандарт 802.11 можна поділити за багатьма критеріями, в таблиці 1.3 наведено найважливіші з них.

Таблиця 1.3 – види мереж

Види мереж/ критерії	Швидкість Мбіт/ секунду	Наявність адміністратору	Кількість підключених пристроїв	Кількість користувачів	Рівень мережі
Домашні початкового рівня	До 100	-	До 12-ти	1-5	Перший
Домашні високого рівня	До 1000	+	До 30-ти	1-5	Другий
Відкриті	До 30	+/-	До 100	До 100	Перший
Корпоративні початкового рівня	До 250	+	До 100	До 250	Другий
Корпоративні високого рівня	До 1000	+	-	-	Третій

1.6 Висновки до першого розділу

Пройде, щонайменше, кілька років, до того, як WPA3, Easy Connect і Enhanced Open стануть нормою. Широке поширення WPA3 відбудеться тільки після заміни або поновлення маршрутизаторів. А питання захисту інформації вразливих точок стоїть вже сьогодні, та немає жодної гарантії, що WPA3 не буде мати серйозних вразливостей.

Як можна побачити на таблиці 1.1, жодне з розглянутих рішень не задовольняє потреби користувачів, які не мають змогу розгортати велику та дорогу захисну систему моніторингу, але при цьому мати набор функцій які дозволять відстежити більш-менш серйозні атаки. Також доволі гостро стоїть питання наявності кадрів, які б змогли працювати з цими комплексами, та сумісного обладнання, тому що розгорнути систему захисту від атак при вже розгорнутій бездротовій мережі може бути занадто дорого.[25]

РОЗДІЛ 2 АНАЛІЗ БЕЗПЕКИ МЕРЕЖ ЗА СТАНДАРТОМ

2.1 Загальні умови та вимоги

Оцінити безпеку мереж першого та другого рівня, стандарту IEEE 802.11, якими користується типовий користувач на протязі дня. При наявності недоліків інформаційної безпеки, запропонувати та впровадити рішення, що підвищать показники рівня інформаційної безпеки при користуванні цими мережами.

Основною метою перевірки рівня інформаційної безпеки в домашній безпровідної мережі є виявлення розповсюджених вразливостей та аналіз коректності налаштувань компонентів мережі.

Вимоги для проведення робіт:

— використовувати розповсюджене обладнання нижчого цінового сегменту;

— при проведені дослідів та аналізі їх результатів, враховувати потреби та користувачів та рівень їх кваліфікації.

2.2 Вибір мереж для дослідів, та його обґрунтування

Щоб отримати різноманітні данні і побачити повну картину стану інформаційної захищеності типового користувача, потрібно обрати для досліду мережі, до яких він найчастіше підключається.

Для аналізу безпеки мереж було обрано 3 мережі, різних типів:

- відкрита мережа ВНЗ;
- закрита мережа кафедри;
- домашня мережа.

Безпровідна відкрита мережа ВНЗ є типовою мережею з доволі великою площею покриття, та відкритим доступом, до неї кожного дня під’єднуються сотні користувачів, більшість з яких не має достатнього рівня обізнаності у сфері кібербезпеки.

В мережі кафедри кожен користувач має свій власний набір даних для авторизації в мережі, без яких доступ до неї не буде наданий. Більшість користувачів цієї мережі мають достатній рівень обізнаності у сфері кібербезпеки. У мережі є свій адміністратор, який своєчасно може виправляти помилки в ній.

Домашня мережа була обрана, через велику кількість конференційної інформації, яка через неї проходить, та можливість корегування її налаштувань.

2.2.1 Основні положення та програма випробувань WPA-2 PSK

Об’єктом цих випробувань є домашня мережа з використанням стандарту Wi-Fi за протоколом шифрування WPA-2 з простим паролем, немаюча жодних додаткових налаштувань.

Ціллю цих випробувань є отримання інформації який рівень захищеності має домашня/офісна мережа.

Тест на проникнення має бути націленим на відтворення реальних погроз, тобто без застосування дорогого чи складного устаткування.

Маршуртизатор повинен бути настроєний стандартним набором ПЗ, яке надає постачальник, та без використання складних у використанні для звичайного користувача функцій.

Результатом випробування будуть такі показники:

- Доступність
- Якість сигналу
- Складність отримання неправомірного доступу до мережі
- Кількість часу який потрібно на отримання неправомірного доступу до мережі

Таблиця 2.1 – Критерії оцінки мережі

Критерії оцінки мережі	Шкала вимірювання
Якість сигналу	1-10 умовних одиниць

Стабільність сигналу	1-10 умовних одиниць
Завантаженість ефіру	Кількість точок на тому самому каналі та якість їх сигналу
Вихід сигналу із зони корисної дії	У метрах
Складність отримання доступу до мережі	У хвилинах
Складність отримання прав адміністратору	У хвилинах

Алгоритм аналізу мережі(рисунок 2.1):

1. Зібрати інформацію про мережу:

- Ім’я мережі
- Мак адресу мережі
- Пристрої що до неї підключені
- Зону її дії

2. Просканувати ефір на завантаженість, підрахувати кількість мереж, які використовують той самий канал, або суміжні, та проаналізувати доцільність використовування цього каналу

3. Провести тест на проникнення використовуючи існуючі вразливості, при отриманні доступу до мережі, здійснити спробу отримання прав адміністратору.

4. Проаналізувати налаштування мережі

5. Провести тест на стійкість мережі.

6. З отриманих даних зробити висновок щодо безпеки мережі.

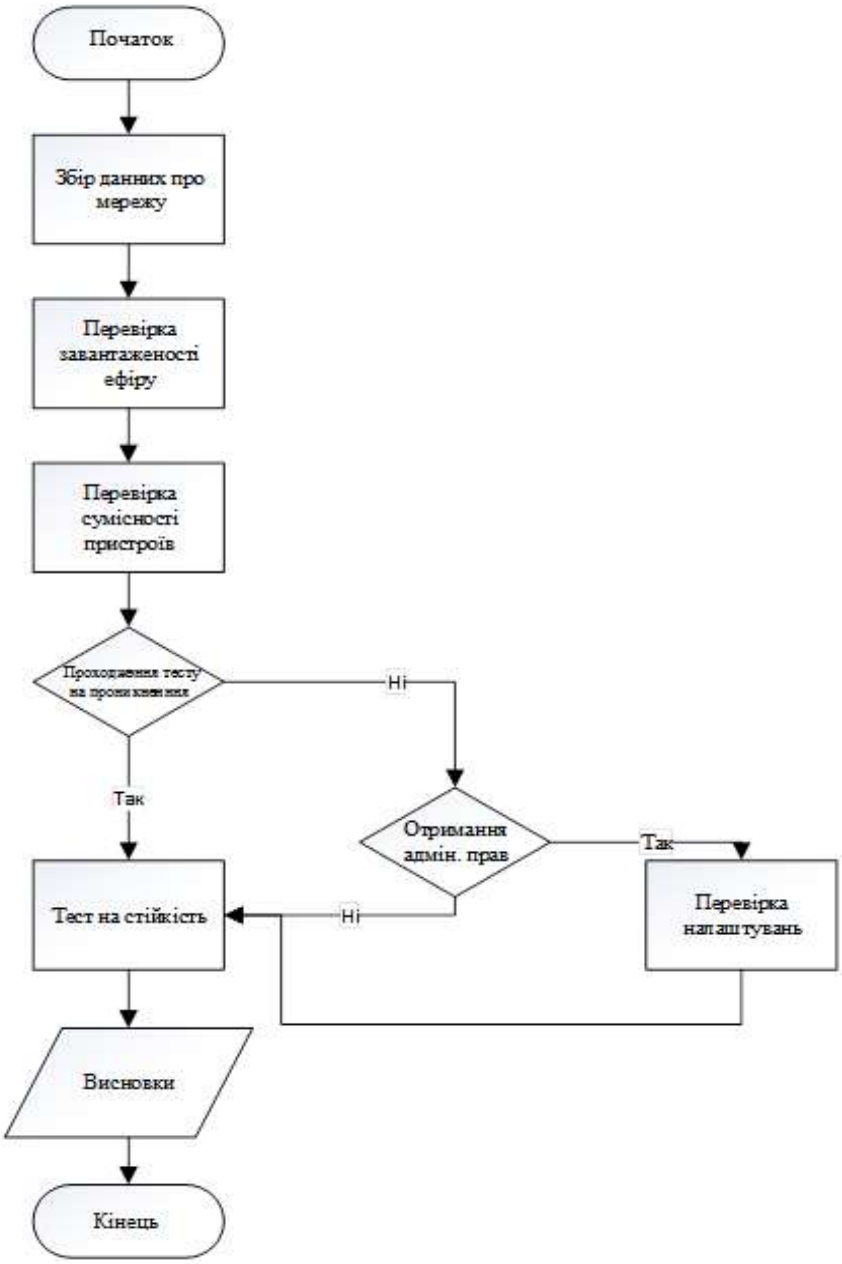

Рисунок 2.1 – Алгоритм аналізу мережі

2.3.1 Визначення обладнання мережі що використовується у досліді

Обладнання, що використовується у досліді:

-Безпровідний-мережевий маршрутизатор netis-WF2411;

-Iphone-5C.

ПЗ, що використовується у досліді:

-netis(WF2411)-V2.1.41694,2017.05.16 13:59 (Прошивка маршрутизатору);

-IOS 10.3.3(Операційна система).

Це технічне та програмне забезпечення було обране як доступне усім користувачам, як за ціною, так і за складністю налаштувань до початку роботи.

2.3.2 Вибір ПЗ та обладнання для аналізу мережі і його обґрунтування

Для аналізу мережі на інформаційну безпеку є доволі велика кількість програмних та програмно апаратних рішень, але нажаль більшість з них має велику ціну та складну структуру і потребує навичок роботи з ними, також існує безкоштовне ПЗ, але стає питання коректності його роботи, тому в цих дослідах доцільно використовувати ПЗ з відкритим кодом, яке слід встановити на ОС Linux, в діструбтиві Kali Linux є велика кількість передвстановаленого ПЗ для проведення аналізу мереж. Після аналізу предвстановленого ПЗ на ОС Kali Linux, за такими критеріями, як функціональність, універсальність та складність використання було вибрано наступне ПЗ:

- Wireshark;
- Ettercap;
- Airmon-ng;
- Airdump-ng.

Для використання цього ПЗ потрібен комп'ютер підтримуючий стандарт 802.11, з мережевим адаптером який підтримує режими моніторингу та ін'єкції, при цьому він має бути мобільним щоб можна було проводити вимірювання в різних точках та не дорогим, щоб не знизити економічну ефективність.

Для аналізу безпеки був обраний ноутбук Aspire ES1—524—5291 з наступними характеристиками:

Таблиця 2.2 – Характеристики ноутбуку

Параметр	Значення
Процесор	AMD E2-9010 RADEON R2, 4 COMPUTE CORES 2C+2G

Оперативна пам’ять	2 GB
Операційна система	Linux
Мережевий адаптер	Intel(R) Dual Band Wireless-AC 3168

2.3 Випробування домашньої мережі

2.3.1 Інформація про мережу

Мережа BHV розташована в багатоповерховому домі зі стінами із залізобетону, та охоплює 7 приміщень точка доступу розташована у кімнаті №1, вікна зроблені з металопластику, двері з деревини. Приміщення № 2,4,5,7 мають спільну стіну з приміщеннями інших власників(рисунок 2.2).

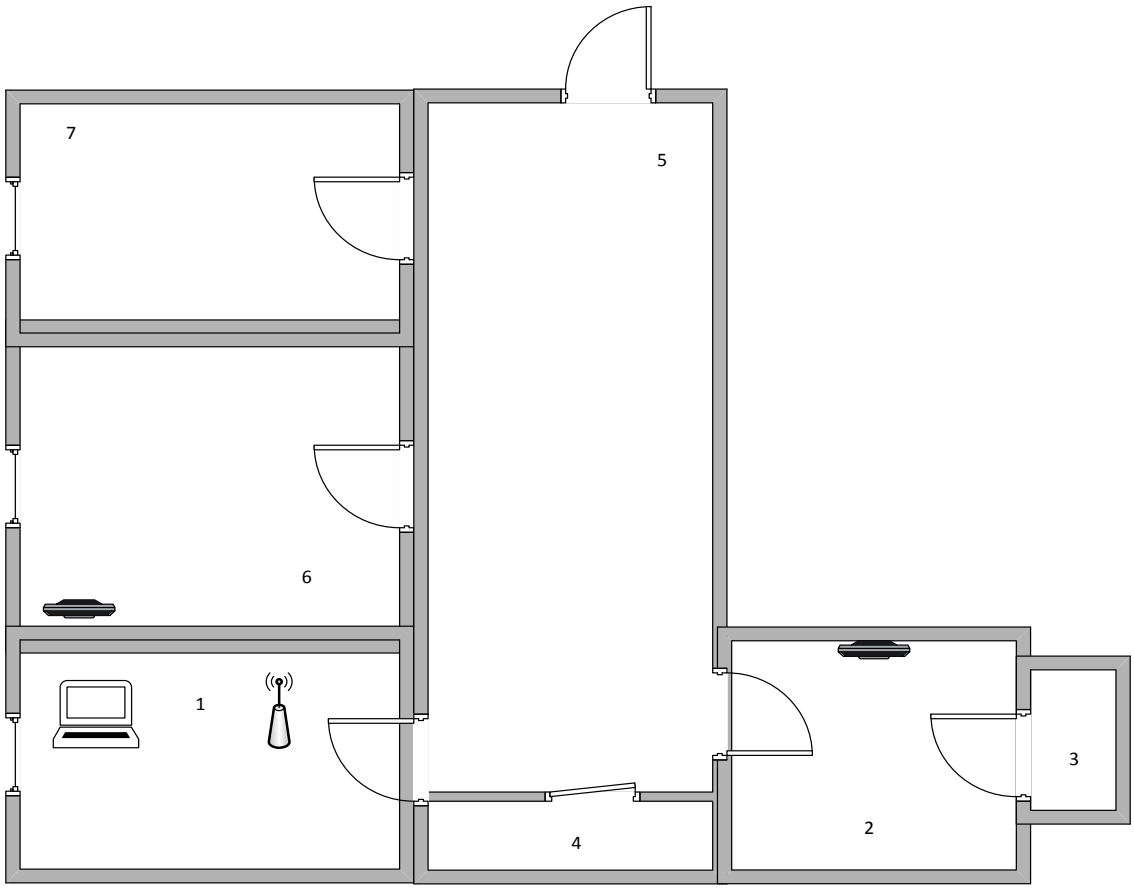

Рисунок 2.2 – Схема приміщення у якому розташована мережа

У таблиці 2.3 вказано характеристики досліджуваної мережі:

Таблиця 2.3 – Характеристики мережі

Параметр	Значення
SSID	BHV
MAC адреса	04:8d:38:84:18:73
Номер каналу	11
Середня відносна потужність сигналу	90%
Вид шифрування мережі	WPA-2 PSK

Вимірювання потужності сигналу проводилось у 7 точках, відображених на Рисунку 2.2.

Таблиця 2.4 – Потужність сигналу у точках виміру

Точка виміру	Відносна потужність сигналу у відсотках
1	100
2	85
3	60
4	80
5	70
6	85
7	70

Згідно з вимірами сигнал мережі виходить за корисну площу, 20 метрів.

В ефірі знайдено 16 точок доступу.

З них лише 5 мають потрібну силу сигналу, щоб негативно заподіяти на цю мережу, але жодна з точок не використовує 11-й канал.

Права адміністратору ні як не захищені, то ж до налаштувань роутера можна зайти просто підключившись до мережі та підключившись до веб інтерфейсу.

Налаштування бездротової мережі які впливають на цілісність доступність та конфіденційність та їх значення відображені у таблиці 2.5

Таблиця 2.5 – Налаштування мережі

Налаштування	Значення	Чи потрібні зміни налаштування
Відключений список фільтрації MAC адрес та резервовані адреси	Вимкнено	Так
Тип автентифікації	WPA/WPA2-PSK	Так
Вид ключа	ASCII	Ні
Складність паролю	Дуже слабкий	Так
WPS налаштування	Вимкнено	Ні
Безпровідний роумінг	Вимкнено	Ні
Ізоляція точки доступу	Ввімкнено	Ні
Короткий Guard Interval	Ввімкнено	Ні
WMM	Ввімкнено	Ні
Потужність передачі	100%	Так
Віддалене управління	Вимкнено	Ні
Складність імені та паролю адміністратору	Відсутнє	Так
FTP сервер	Ввімкнено	Так

У таблиці 2.6 вказані клієнти які знаходяться в досліджуваній мережі.

Таблиця 2.6 – Клієнти мережі

Пристрій	Стандарт	Сумісність із мережею
UE32F5500	IEEE 802.11b/g/n	+
UE43M5572	IEEE 802.11b/g/n	+
Acer	IEEE 802.11ac	+
Iphone7	IEEE 802.11ac с технологией MIMO	+
IphoneSE	IEEE 802.11a/b/g/n	+
Iphone5c	IEEE 802.11b/g/n (802.11n в диапазонах 2,4 ГГц и 5 ГГц)	+

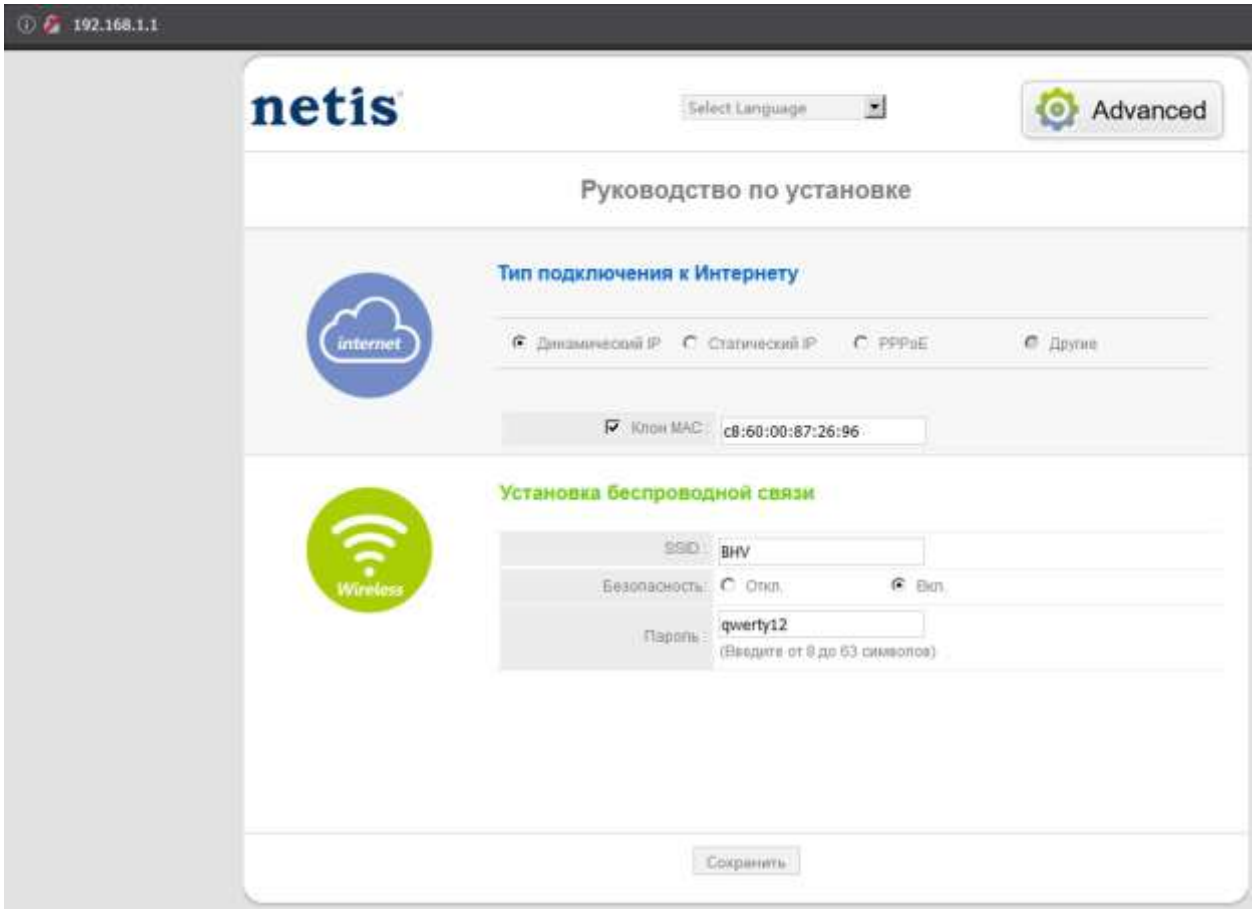

Рисунок 2.3 – Сторінка з налаштуваннями маршрутизатору

На рисунку 1 можна побачити, як постачальник обладнання дає змогу користувачам відключити захист, при цьому немає жодного попередження,

що мережа створена за допомогою цього маршрутизатора може бути небезпечною., тож звичайний користувач може його вважати за безпечне

Смартфон теж ні про що не попереджає користувача рис. 2.4:

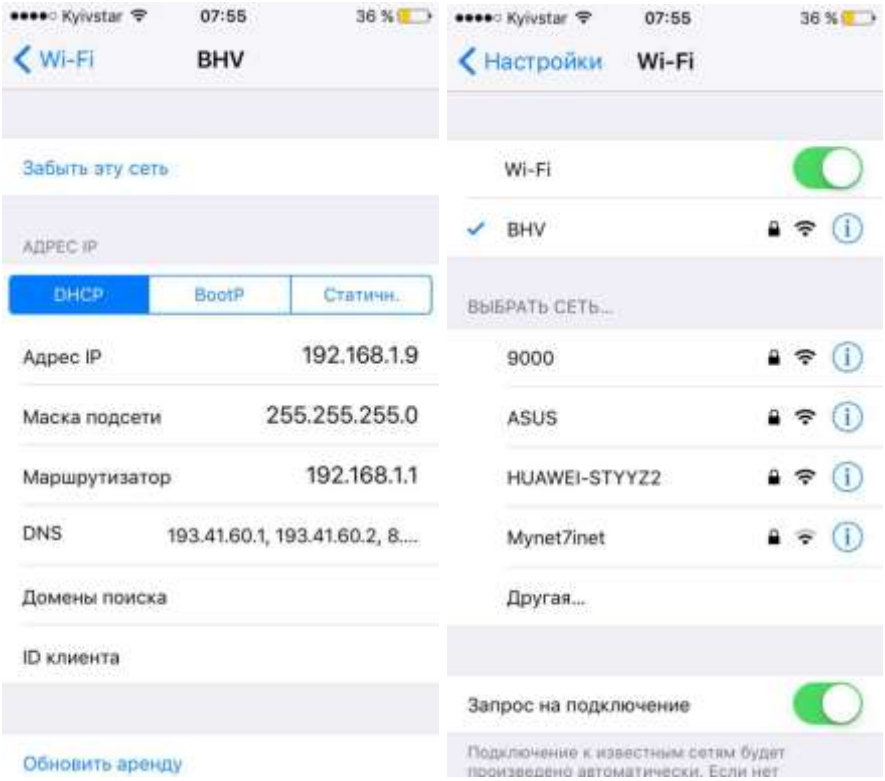

Рисунок 2.4 – Сторінки налаштувань смартфону

В вище описаному випадку, для проведення теста на проникнення якнайкраще підходить дістрибутив Linux – Kali-Linux, тому що він є безкоштовним, та вже містить в собі усе ПЗ, яке потрібно у цих випробуваннях.

2.4 Випробування

1. Підключення маршрутизатору, з стандартними налаштнуваннями
2. Задаємо ім’я точки доступу та 8-ми значного пароль(мінімальна кількість символів)
3. Запускаємо Linux на ноутбуці (На ноубуціна ОС Windows, тому Linux буде запущений з флеш накопичувача)
4. Відкриваємо термінал
5. Запускаємо утиліту airmon-ng Рисунок1.2
6. Переключаємо мережеву карту в режим моніторингу airmon-ng start wlan0 Рисунок1.2
7. Запускаємо моніторинг airodump-ng wlan0mon (рисунок 2.5)

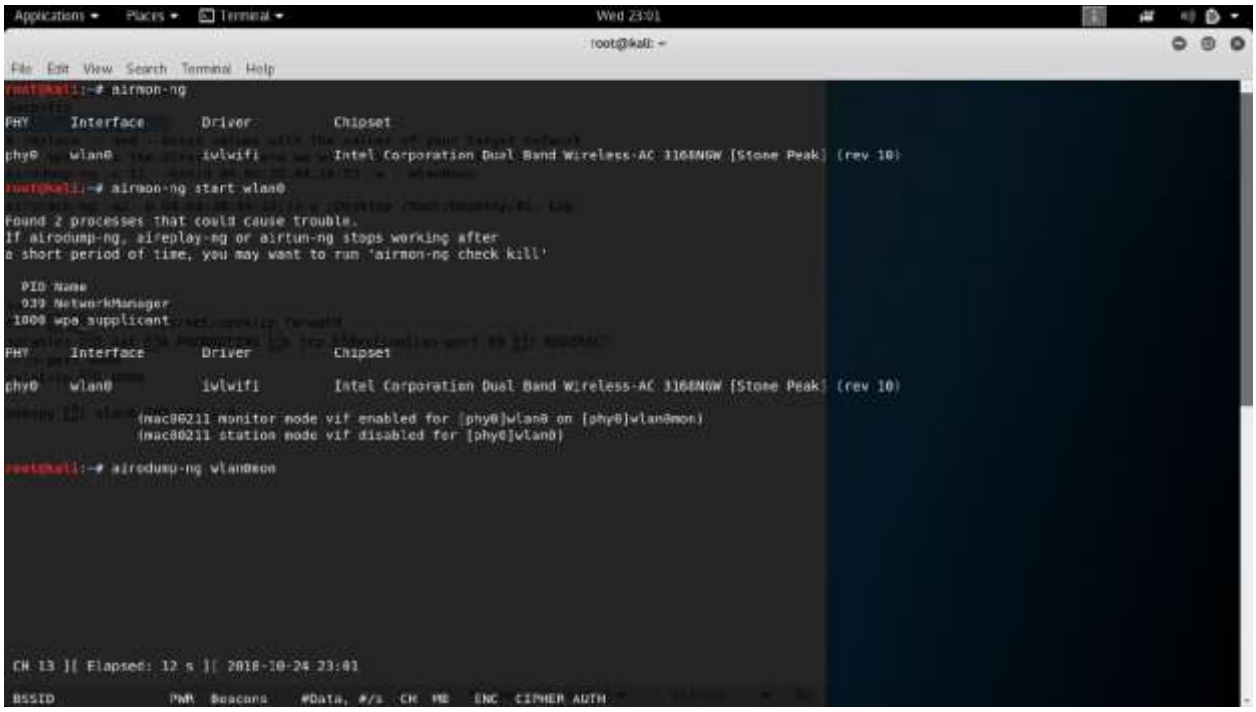

Рисунок 2.5 – Моніторинг airodump-ng wlan0mon

8. Вибираємо потрібну точку доступу airodump-ng -c 11 --bssid 04:8d:38:84:18:73 -w . wlan0mon (рисунок 2.6)

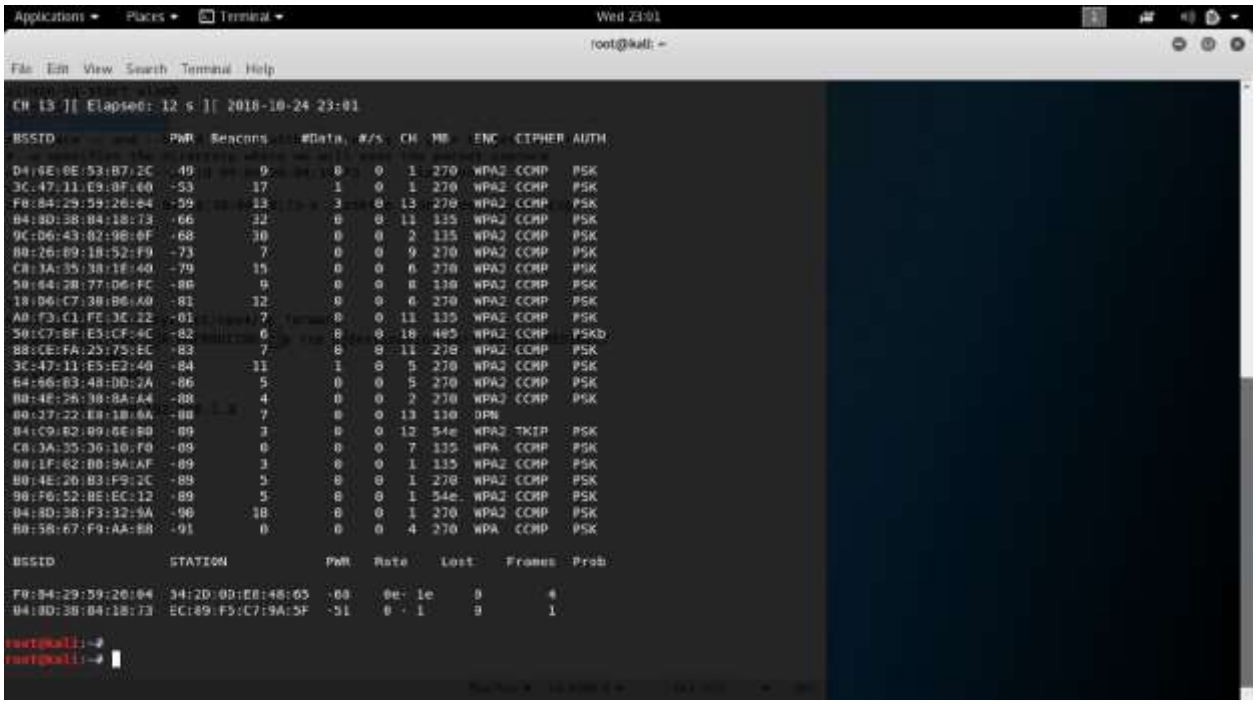

Рисунок 2.6 – Вибір точки доступу

9. Починаємо атаку aircrack-ng -a2 -b 04:8d:38:84:18:73-w /Desktop /Root/Desktop/01. Cap

   Чекаємо, поки жертва під'єднається до мережі та перехоплюємо "handshake" (імітуємо жертву під'єднуючи смартфон до мережі) (рисунок 2.6)

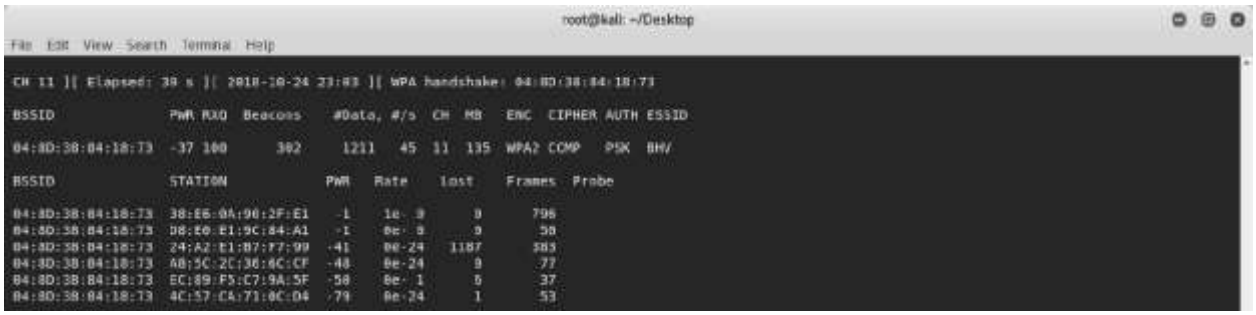

Рисунок 2.6 – Початок атаки

10. Розшифровуємо "handshake" aircrack-ng -a2 -b (bssid маршрутизатора) -w (шлях до словника) /Root/Desktop/*. Cap (рисунок 2.7)

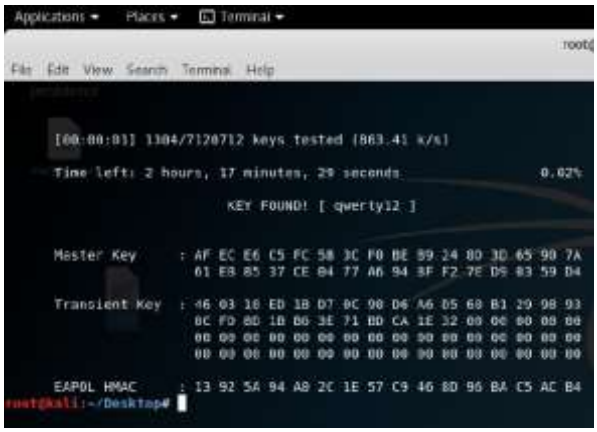

Рисунок 2.7 – Розшифровка

11. Використовуючи логін та пароль під’єднуємося до мережі
12. Перенаправляємо трафік через наш мережевий інтерфейс

sudo -i

echo “I” >/proc/sys/net/upv4/ip_forward

При використанні “жертвою” https протоколу перенапрвляємо йоого на протокол http

iptables –t nat –A PREROUTING –p tcp –destination-port 80 –j REDIRECT

--to-port 8080

sslstrip –l 8080 (рисунок 2.8)

За допомогою Ettercap реалізуємо атаку “Людина посередині”

Рисунок 2.8 – Інтерфейс Ettercap

13. За допомогою Wireshark проводимо моніторинг та фільтрацію трафіку між маршрутизатором та смартфоном (рисунок 2.9)

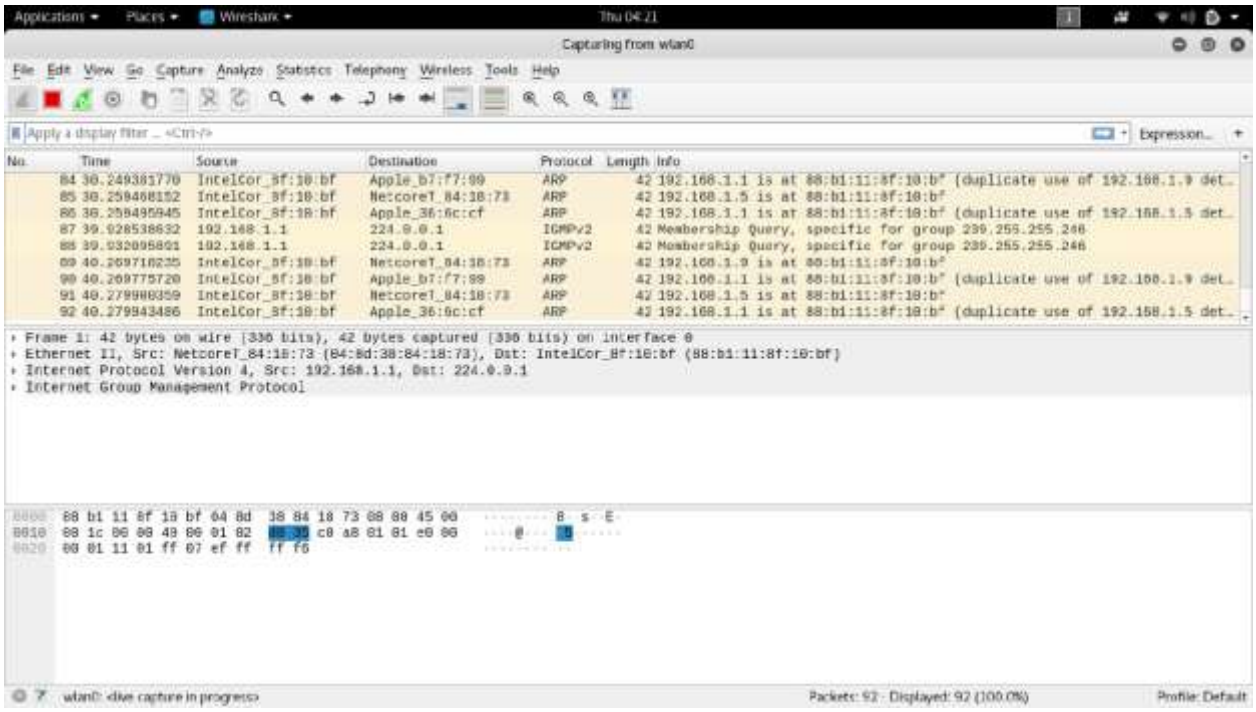

Рисунок 2.9 – Моніторинг трафіку

14. На смартфоні заходимо на сайт dsszi.gov.ua, та вводимо на ньому пошуковий запит “12345678” Рисунок 2.10 в цей час в Wire shark за допомогою фільтрів відстежуємо трафік (рисунок 2.11).

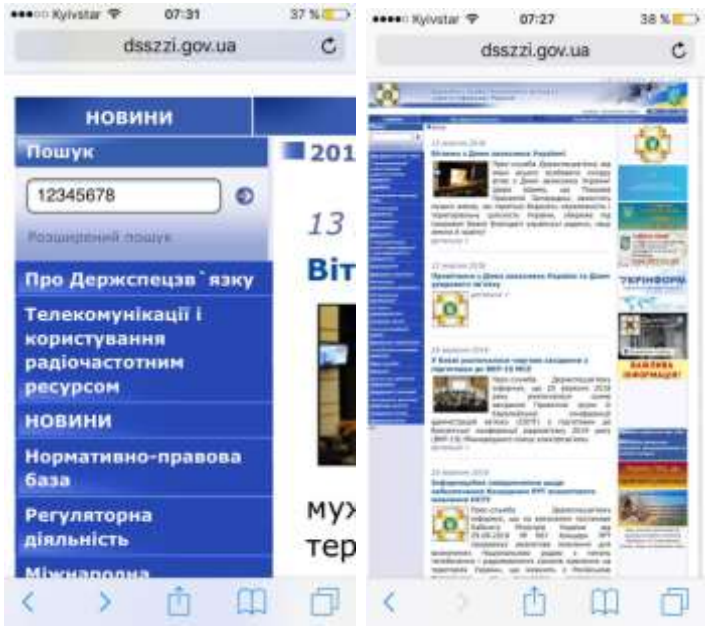

Рисунок 2.10 – Пошук зі смартфона

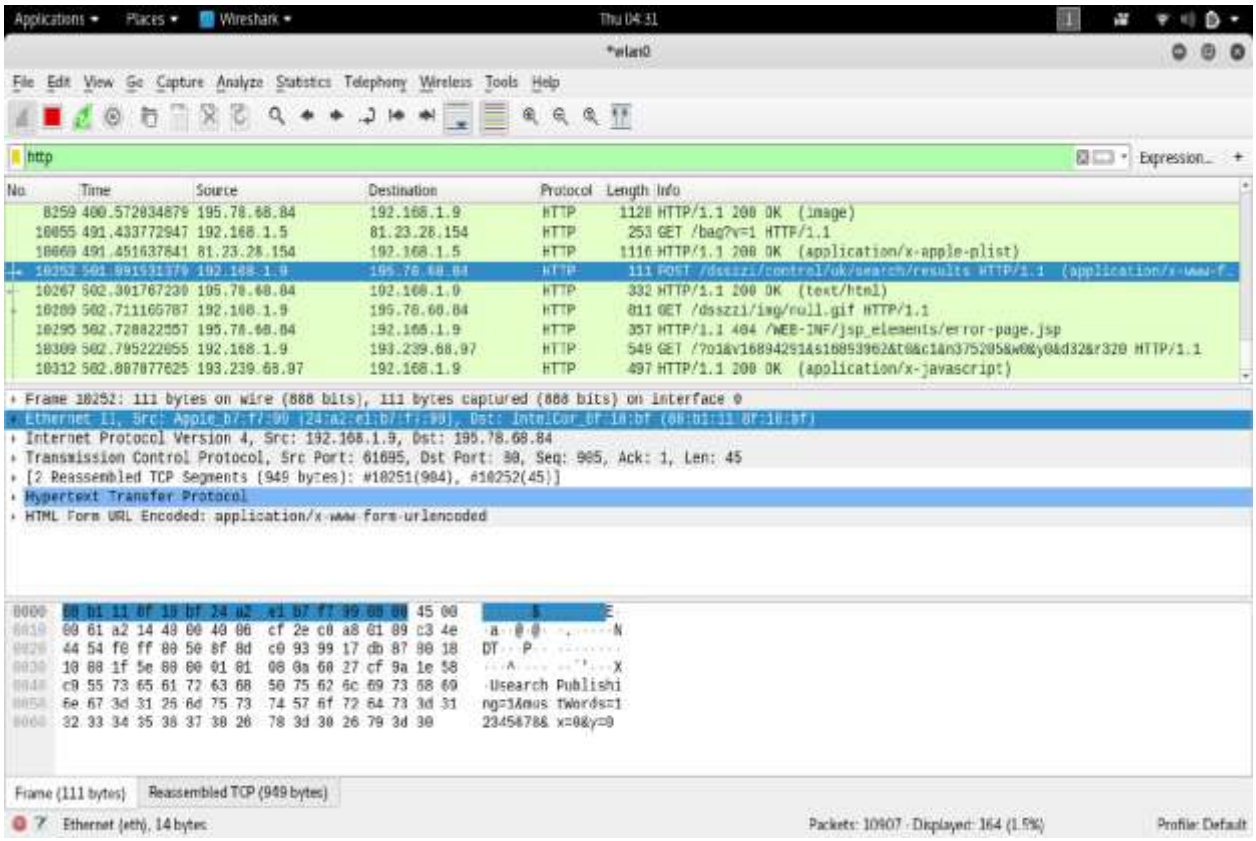

Рисунок 2.11 – Відстеження трафіку

2.5 Висновки з аналізу безпеки домашньої безпровідної мережі

Ця мережа вразлива до перехоплення рукостискання. Wi-Fi мережі при відсутності необхідного захисту можуть бути вразливими до найпростіших атак, які можуть бути реалізовані за лічені хвилини. Налаштування за умовчанням які встановленні постачальником маршрутизатору є не тільки небажаними до використання, але й є потенційною загрозою для конференційної інформації користувачів. Постачальникам обладнання слід вносити більшу ясність в своє ПЗ, видаляти з нього зайві функції та доносити до своїх користувачів усю важливість безпечних налаштувань їх мережі.

В даних випробуваннях було використане устаткування з нижчого цінового сегменту, а ПЗ є безкоштовним, з цього можна зробити висновок, що розглянута мережа не є захищеною навіть від простіших та найрозповсюдженіших атак.

Стійкість мережі знаходиться на більш високому рівні, але ефір є досить згруженими, через це можуть виникнути проблеми з підключенням та швидкістю доступу до мережі.

Мережа потребує додаткових налаштувань, як з точки зору її безпеки, так і з точки зору швидкодії.

2.6 Аналіз безпеки в безпровідних мережах стандарту 802.11 університету та кафедри БІТ

2.6.1 Аналіз безпеки в мережі університету

Мережа університету має наступний SSID: NTUDP, паролю та шифрування на ній зовсім немає, то ж будь який зловмисник за допомогою Wireshark, як це було зроблено після тесту на проникнення при аналізі безпеки домашньої мережі в пункті 3 цієї роботи, виходячи з цього використання цієї мережі є не доцільним, до її повної реструктуризації, чи оновлення до стандарту Enhanced Open. Однак ця мереже досить стійка до перенавантажень, та має сильний і рівномірний сигнал по всій площі її покриття, з оглядом на те, що ця мережа є вузівською, то ж не потребує високих швидкостей та стабільності у роботі.

2.6.2 Аналіз мережі кафедри БІТ

Мережа має наступний SSID: BIT, для доступу в мережу використовується авторизація через сервер, який перевіряє індивідуальні данні для авторизації, мережа адмініструється системним адміністратором, через це має стабільний, потужний сигнал, та гарну стійкість до великих навантажень.

При цьому щоб перехопити логін та пароль не треба витрачати велику кількість ресурсів, за допомогою тієї ж утиліти що і у першому досліді – aircrack-ng. Підбір логіну здійснюються за допомогою бази vstup.info, бо логіном є фамілія і ініціали користувача, а підбір паролю жорстким перебором, чи гібридним підбором. Проаналізувати трафік за допомогою Wireshark. Ця

мережа, є найзахищенішою серед розглянутих, хоч і не дає 100 відсоткових гарантій про захист даних від зловмисника. Покриття мережі покриває всю територію кафедри, сигнал є потужним та стабільним.

2.6.3 Висновки по другій та третій мережі

Відкрита мережа Університету є небезпечною для даних користувачів та небажана для використання в цілому.

Безпровідна мережа кафедри показала найкращі показники з точки зору інформаційної безпеки та стабільності сигналу.

2.7 Рекомендації зі зміни налаштувань, їх обґрунтування

Список зарезервованих адрес, дає гарантію того, що всім пристроям що потребують першочергового доступу до мережі.

Тип автентифікації треба налаштовувати згідно з сумісністю пристроїв. В розглянутій мережі всі пристрої підтримують WPA-2, тому не доцільно використовувати режим автентифікації, який є менш стійким до атак.

Таблиця 2.4 – Налаштування мережі

Налаштування	Встановлені значення	Чи потрібні зміни налаштування
Відключений список фільтрації MAC адрес та резервовані адреси	Додати пристрої, які використовуються найчастіше у мережі в список зарезервованих адрес	Так
Тип автентифікації	WPA2-PSK	Так
Вид ключа	ASCII	Ні
Складність паролю	Пароль потрібен складатися щонайменше з десяти символів, хоча б 2 з них мають бути спеціальними	Так
WPS налаштування	Вимкнено	Ні
Безпровідний роумінг	Вимкнено	Ні
Ізоляція точки доступу	Ввімкнено	Ні
Короткий Guard Interval	Ввімкнено	Ні
WMM	Ввімкнено	Ні
Потужність передачі	80%	Так
Віддалене управління	Вимкнено	Ні
Складність імені та паролю адміністратору	Данні авторизації мають відрізнятися від стандартних та мати значний рівень складності	Так
FTP сервер	Вимкнути	Так

2.8 Рекомендація до установки програмного забезпечення та дій для зменшення ймовірності атаки.

Встановити Wireshark на ПК підключений до мережевого маршрутизатору через Ethernet

При неможливості підключення через Ethernet, чи неможливості встановлення програмного забезпечення користувач має заходити та перевіряти список підключених пристроїв власноруч. При вияві несанкційовано підключених пристроїв додати їх адресу до чорного списку MAC адрес, та змінити пароль доступу до мережі.

2.9 Вибірка актуальних безпечних маршрутизаторів

2.9.1 Таблиця порівняння маршрутизаторів

Згідно з даними інтернет-магазину Rozetka було обрани 6 альтернатив маршрутизаторів для їх подальшого порівняння, за важливими для користувача критеріями.

Таблиця 2.5 – Порівняння маршрутизаторів

Модель маршрутизатору	Швидкість мережі	Підтримання стандартів	Кількість антен	Ціна у грн	Захисту мережі від перенавантаження	Наявність захисту мережі	Підтримка VPN
TP-LINK TL-WR841N	300	8021.11 b,g,n	2	530	+	+	+

Продовження табл. 2.1 – Порівняння маршрутизаторів

Netis WF2411E	150	8021.11 b,g,n	1	300	-	-	-
Asus RT-N12E	300	8021.11 b,g,n	2	530	+	+	+
Mercusys	300	8021.11 b,g,n	2	300	+	-	-

MW301R							
D-Link DIR-615S	300	8021.11 b,g,n	2	500	-	-	+
Tenda F300	300	8021.11 b,g,n	2	400	-	-	-

2.9.2 Вибір найкращої альтернативи

За допомогою системи підтримки прийняття рішень(СППР) NooTron[25], було обрано найкращу альтернативу із даної вибірки, яка найбільше задовольняє критерії. Для здійснення вибірки був обраний метод аналізу ієрархій, який найбільш підходить для даної задачі. На рисунку 2.12 зображено початок роботи з СППР NooTron:

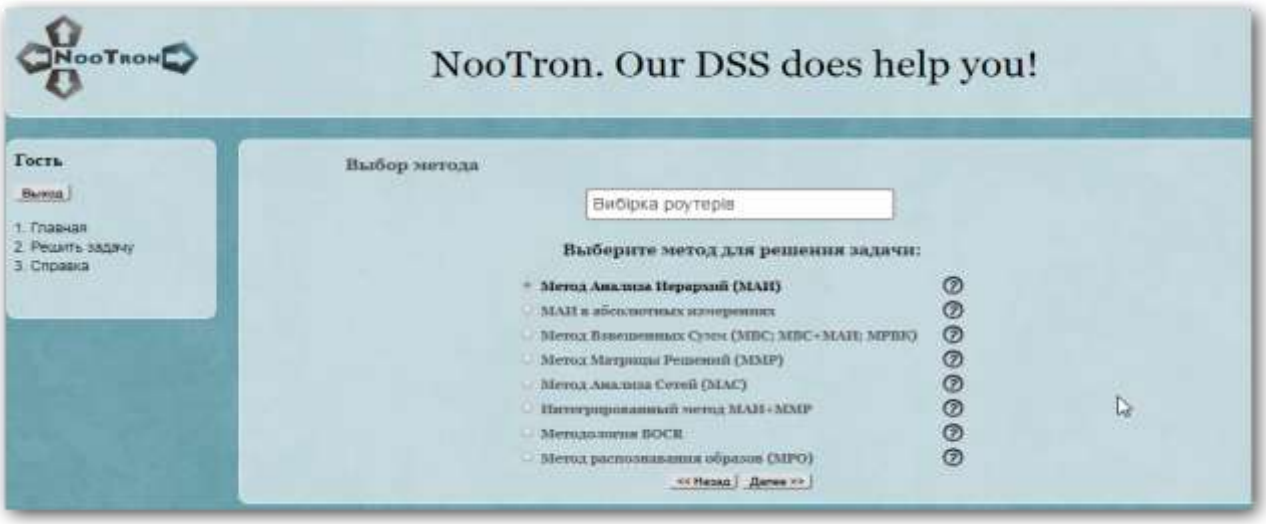

Рисунок 2.12 – Форма вибору методу

Потім були занесені основні дані з таблиці (рисунок 2.13), для здійснення рішення щодо найкращої альтернативи. Критерій підтримання стандартів не враховувався, так як всі альтернативи мають однакове значення.

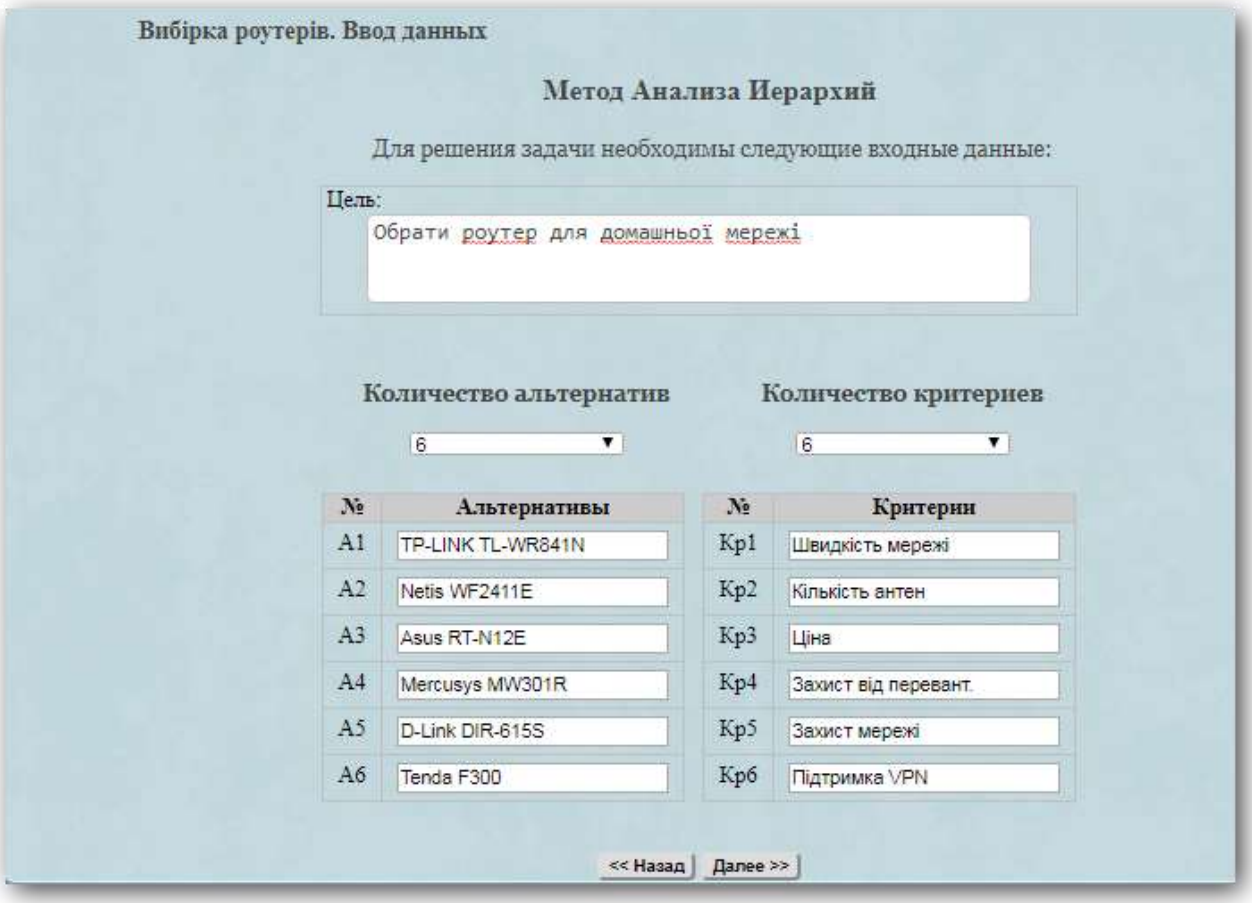

Рисунок 2.13 – Введення даних для аналізу

Наступним етапом роботи з СППР NooTron – оцінюванню важливості критеріїв(рисунок 2.14). Для цього було обрано шкалу Сааті, де 1 – немає переваги(альтернативи рівні), а 9 – велика перевага альтернативи. Найбільш важливими для даної цілі є критерії ціни та захисту мережі.

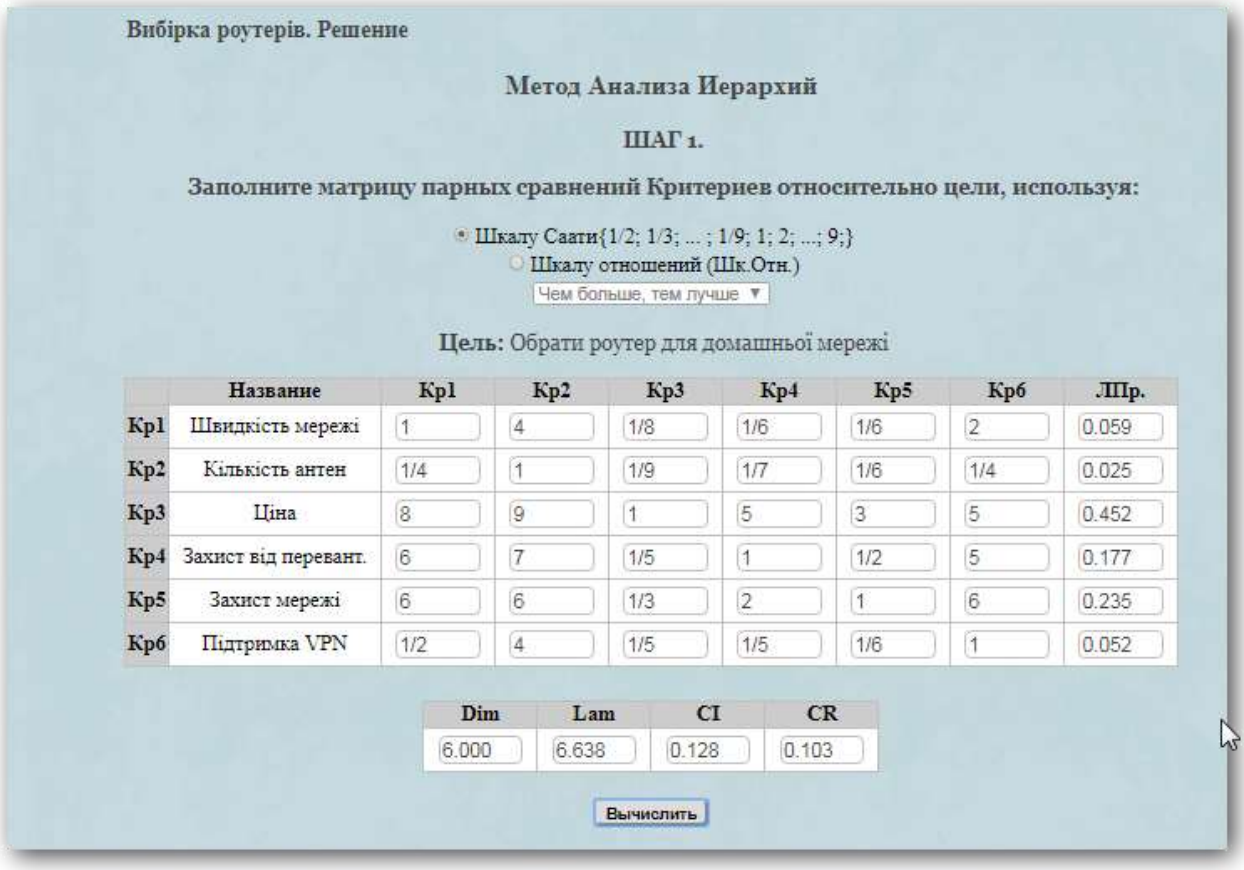

Рисунок 2.14 – Оцінювання переваг критеріїв

Після оцінки важливості кожного критерію, був проведен аналіз альтернатив по кожному з них(рисунки 2.15 – 2.20). Для критеріїв «Швидкість мережі», «Кількість антен», та «Ціна» була використана «шкала відношень, а для останніх – «шкала Сааті).

Вибірка роутерів. Решение

Метод Анализа Иерархий

ШАГ 2.

Сравните альтернативы попарно по отношению к каждому Критерию в шкале Саати или в шкале отношений, заполнив матрицы парных сравнений.

2.1 По отношению к критерию "Швидкість мережі", используя:

Шкалу Саати{1/2; 1/3; ... ; 1/9; 1; 2; ...; 9;}
Шкалу отношений (Шк.Отн.)
Чем больше, тем лучше

	Название	A1	A2	A3	A4	A5	A6	ЛПр.
A1	TP-LINK TL-WR841N	1	300/150	300/300	300/300	300/300	300/300	0.182
A2	Netis WF2411E	150/300	1	150/300	150/300	150/300	150/300	0.090
A3	Asus RT-N12E	300/300	300/150	1	300/300	300/300	300/300	0.182
A4	Mercusys MW301R	300/300	300/150	300/300	1	300/300	300/300	0.182
A5	D-Link DIR-615S	300/300	300/150	300/300	300/300	1	300/300	0.182
A6	Tenda F300	300/300	300/150	300/300	300/300	300/300	1	0.182
Шк.Отн.	Швидкість мережі	300	150	300	300	300	300	

Dim	Lam	CI	CR
6.000	6.000	0.000	0.000

Вычислить

Рисунок 2.15 – Оцінка альтернатив згідно с критерієм «Швидкість мережі»

Вибірка роутерів. Решение

Метод Анализа Иерархий

ШАГ 2.

Сравните альтернативы попарно по отношению к каждому Критерию в шкале Саати или в шкале отношений, заполнив матрицы парных сравнений.

2.2 По отношению к критерию "Кількість антен", используя:

Шкалу Саати{1/2; 1/3; ... ; 1/9; 1; 2; ...; 9;}
Шкалу отношений (Шк.Отн.)
Чем больше, тем лучше

	Название	A1	A2	A3	A4	A5	A6	ЛПр.
A1	TP-LINK TL-WR841N	1	2/1	2/2	2/2	2/2	2/2	0.182
A2	Netis WF2411E	1/2	1	1/2	1/2	1/2	1/2	0.090
A3	Asus RT-N12E	2/2	2/1	1	2/2	2/2	2/2	0.182
A4	Mercusys MW301R	2/2	2/1	2/2	1	2/2	2/2	0.182
A5	D-Link DIR-615S	2/2	2/1	2/2	2/2	1	2/2	0.182
A6	Tenda F300	2/2	2/1	2/2	2/2	2/2	1	0.182
Шк.Отн.	Кількість антен	2	1	2	2	2	2	

Dim	Lam	CI	CR
6.000	6.000	0.000	0.000

Вычислить

Рисунок 2.16 – Оцінка альтернатив критерієм «Кількість антен»

Вибірка роутерів. Решение

Метод Анализа Иерархий

ШАГ 2.

Сравните альтернативы попарно по отношению к каждому Критерию в шкале Саати или в шкале отношений, заполнив матрицы парных сравнений.

2.3 По отношению к критерию "Ціна", используя:

○ Шкалу Саати{1/2; 1/3; ... ; 1/9; 1; 2; ...; 9;}
◉ Шкалу отношений (Шк.Отн.)

Чем меньше, тем лучше

	Название	A1	A2	A3	A4	A5	A6	ЛПр.
A1	TP-LINK TL-WR841N	1	300/530	530/530	300/530	500/530	400/530	0.126
A2	Netis WF2411E	530/300	1	530/300	300/300	500/300	400/300	0.223
A3	Asus RT-N12E	530/530	300/530	1	300/530	500/530	400/530	0.126
A4	Mercusys MW301R	530/300	300/300	530/300	1	500/300	400/300	0.223
A5	D-Link DIR-615S	530/500	300/500	530/500	300/500	1	400/500	0.135
A6	Tenda F300	530/400	300/400	530/400	300/400	500/400	1	0.167
Шк.Отн.	Ціна	530	300	530	300	500	400	

Dim	Lam	CI	CR
6.000	6.000	0.000	0.000

Вычислить

Рисунок 2.17 – Оцінка альтернатив згідно с критерієм «Ціна»

Вибірка роутерів. Решение

Метод Анализа Иерархий

ШАГ 2.

Сравните альтернативы попарно по отношению к каждому Критерию в шкале Саати или в шкале отношений, заполнив матрицы парных сравнений.

2.4 По отношению к критерию "Захист від перевант.", используя:

◉ Шкалу Саати(1/2; 1/3; ... ; 1/9; 1; 2; ...; 9;)
○ Шкалу отношений (Шк.Отн.)

Чем больше, тем лучше

	Название	A1	A2	A3	A4	A5	A6	ЛПр.
A1	TP-LINK TL-WR841N	1	5	1	1	5	5	0.277
A2	Netis WF2411E	1/5	1	1/5	1/5	1	1	0.056
A3	Asus RT-N12E	1	5	1	1	5	5	0.278
A4	Mercusys MW301R	1	5	1	1	5	5	0.278
A5	D-Link DIR-615S	1/5	1	1/5	1/5	1	1	0.056
A6	Tenda F300	1/5	1	1/5	1/5	1	1	0.056

Dim	Lam	CI	CR
6.000	6.000	0.000	0.000

Рисунок 2.18 – Оцінка альтернатив згідно с критерієм «Захист від перевантажень»

Вибірка роутерів. Решение

Метод Анализа Иерархий

ШАГ 2.

Сравните альтернативы попарно по отношению к каждому Критерию в шкале Саати или в шкале отношений, заполнив матрицы парных сравнений.

2.5 По отношению к критерию "Захист мережі", используя:

Шкалу Саати{1/2; 1/3; ... ; 1/9; 1; 2; ...; 9;}
Шкалу отношений (Шк.Отн.)
Чем больше, тем лучше

	Название	A1	A2	A3	A4	A5	A6	ЛПр.
A1	TP-LINK TL-WR841N	1	5	1	5	5	5	0.357
A2	Netis WF2411E	1/5	1	1/5	1	1	1	0.072
A3	Asus RT-N12E	1	5	1	5	5	5	0.357
A4	Mercusys MW301R	1/5	1	1/5	1	1	1	0.071
A5	D-Link DIR-615S	1/5	1	1/5	1	1	1	0.071
A6	Tenda F300	1/5	1	1/5	1	1	1	0.071

Dim	Lam	CI	CR
6.000	6.000	0.000	0.000

Рисунок 2.19 – Оцінка альтернатив згідно с критерієм «Захист мережі»

Вибірка роутерів. Решение

Метод Анализа Иерархий

ШАГ 2.

Сравните альтернативы попарно по отношению к каждому Критерию в шкале Саати или в шкале отношений, заполнив матрицы парных сравнений.

2.6 По отношению к критерию "Підтримка VPN", используя:

Шкалу Саати{1/2; 1/3; ... ; 1/9; 1; 2; ...; 9;}
Шкалу отношений (Шк.Отн.)
Чем больше, тем лучше

	Название	A1	A2	A3	A4	A5	A6	ЛПр.
A1	TP-LINK TL-WR841N	1	5	1	5	1	5	0.277
A2	Netis WF2411E	1/5	1	1/5	1	1/5	1	0.056
A3	Asus RT-N12E	1	5	1	5	1	5	0.278
A4	Mercusys MW301R	1/5	1	1/5	1	1/5	1	0.056
A5	D-Link DIR-615S	1	5	1	5	1	5	0.278
A6	Tenda F300	1/5	1	1/5	1	1/5	1	0.056

Dim	Lam	CI	CR
6.000	6.000	0.000	0.000

Рисунок 2.20 – Оцінка альтернатив згідно с критерієм «Підтримка VPN»

2.9.3 Оптимальний вибір

Отримані результати даного дослідження вказані на рисунках 2.9.10-2.9.11. Отже найкращим вибором серед даних альтернатив є TP-LINK TL-

WR841N і Asus RT-N12E, які мають однаковий пріоритет і ціну в 530 грн, на другому місці маршрутизатор Mercusys MW301R, за ціною 300 гривень.

Вибірка роутерів. Результат

Метод Анализа Иерархий

Цель: *Обрати роутер для домашньої мережі*

1. Матрица приоритетов Критериев относительно цели и Альтернатив относительно каждого из критериев:

	Пр.Кр.	TP-LINK TL-WR841N	Netis WF2411E	Asus RT-N12E	Mercusys MW301R	D-Link DIR-615S	Tenda F300
Швидкість мережі	0.059	0.182	0.090	0.182	0.182	0.182	0.182
Кількість антен	0.025	0.182	0.090	0.182	0.182	0.182	0.182
Ціна	0.452	0.126	0.223	0.126	0.223	0.135	0.167
Захист від перевант.	0.177	0.277	0.056	0.278	0.278	0.056	0.056
Захист мережі	0.235	0.357	0.072	0.357	0.071	0.071	0.071
Підтримка VPN	0.052	0.277	0.056	0.278	0.056	0.278	0.056

Рисунок 2.21 – Результат

2.Глобальные приоритеты Альтернатив:

№	Альтернативы	Гл. Пр.
I	TP-LINK TL-WR841N	0.220
II	Asus RT-N12E	0.220
III	Mercusys MW301R	0.185
IV	Netis WF2411E	0.138
V	Tenda F300	0.120
VI	D-Link DIR-615S	0.117

3.Диаграмма глобальных приоритетов альтернатив:

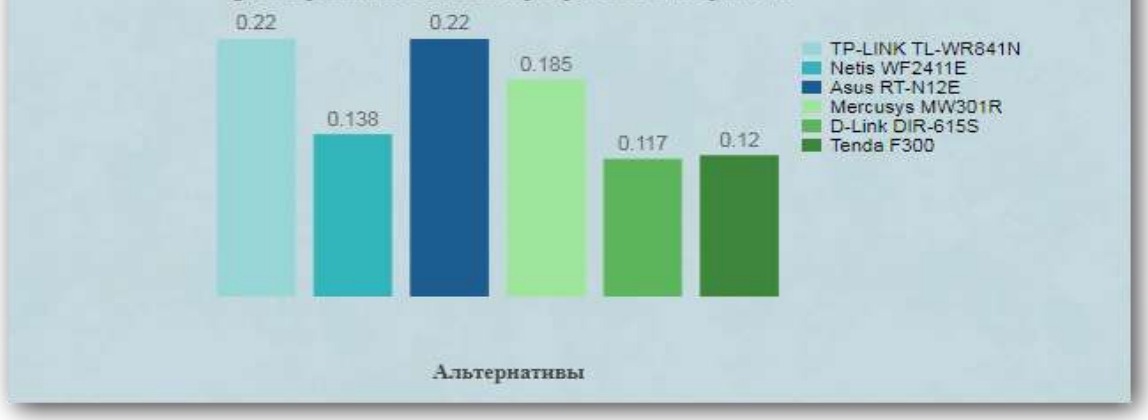

Рисунок 2.22 – Графічний вид результату

2.9 Висновок до другого розділу

В цьому розділі була розроблені програма та методика аналізу безпеки мереж за стандартом IEEE 802.11, були проаналізовані 3 типових мережі, з результатів аналізу видно, що розглянуті мережі потребують налаштувань та захисту, а мережа відкрита мережа ВНЗ зовсім не бажана в використанні до її модернізації.

Більшість користувачів безпровідних мереж є недостатньо освіченими у інформаційній безпеці, це наражає всю інфраструктуру та інших користувачів на небезпеку. Неосвічені користувачі можуть «віддавати» зловмисникам паролі від мереж та заражати їх.

Постачальники послуг та обладнання повинні попереджати людей, про те що вони можуть втратити свою конференційну інформацію, та доносити до них важливість правильних налаштувань мережі та використання додаткового ПЗ для підвищення інформаційної безпеки.

Згідно з характеристиками та ціною маршрутизаторів кращими маршрутизаторами в нижньому ціновому сегменті були визнані TP-LINK TL-WR841N і Asus RT-N12E, що є показником того, що на безпеці своєї мережі економити не можна.

РОЗДІЛ 3. ЕКОНОМІЧНА ЧАСТИНА

Метою розділу є обґрунтування економічної доцільності проведення аналізу рівня інформаційної безпеки в домашній мережі

3.1 Визначення капітальних витрат на аналіз рівня безпеки в домашній мережі побудованій за допомогою бездротового зв'язку

3.1.1 Визначення трудомісткості розробки та опрацювання системи аналізу

Трудомісткість аналізу рівня безпеки визначається за формулою (3.1) та враховує тривалість кожної робочої операції, починаючи з складання технічного завдання і закінчуючи оформленням документації (за умови роботи одного спеціалісту):

$$t = t_{тз} + t_{в} + t_{а} + t_{опр} + t_{д}, \text{ годин}, \quad (3.1)$$

де $t_{тз}$ – тривалість складання технічного завдання на розробку ПЗ;

$t_{в}$ – тривалість вивчення ТЗ, літературних джерел за темою тощо;

$t_{а}$ – тривалість розробки блок-схеми алгоритму;

$t_{опр}$ – тривалість опрацювання (складання програми та методики);

$t_{д}$ – тривалість підготовки технічної документації на ПЗ.

$$t = 50 + 3 + 70 + 10 = 123, \text{ години}.$$

3.1.2 Розрахунок витрат на створення системи

Витрати на створення системи Ксс складаються з витрат на заробітну плату виконавця Ззп і вартості витрат машинного часу, що необхідний для опрацювання програми на ПК Змч:

$$Ксс = Ззп + Зм, \text{ грн,} \quad (3.2)$$

$$Ксс = 7953.18 + 213 = 8166.18, \text{ грн.}$$

Заробітна плата виконавця враховує основну і додаткову заробітну плату, а також відрахування на соціальне потреби (пенсійне страхування, страхування на випадок безробіття, соціальне страхування тощо) и визначається за формулою:

$$З_{зп} = (t \cdot З_{пр}) + Сп, \text{ грн,} \quad (3.3)$$

де t – загальна тривалість створення ПЗ, годин,

Зпр – средньогодинна заробітна плата з нарахуваннями, грн/годину.

Сп – відрахування на соціальні потреби

$$З_{зп} = 123 \cdot 53 + 22\% = 7953.18, \text{ грн.}$$

Вартість машинного часу для налагодження програми на ПК визначається за формулою:

$$З_{мч} = t_{опр} \cdot С_{мч} + t_{д}, \text{ грн,} \quad (3.4)$$

де $t_{опр}$ – трудомісткість налагодження, годин,

$t_д$ – трудомісткість підготовки документації на ПК, годин,

$С_{мч}$ – вартість 1 години машинного часу ПК, грн./година.

Вартість 1 години машинного часу ПК визначається за формулою:

$$С_{мч} = Р \cdot t_{нал} \cdot С_е + \frac{Ф_{зал} \cdot Н_а}{F_р}, \text{ грн} \qquad (3.5)$$

де Р – встановлена потужність ПК, кВт;

$С_е$ – тариф на електричну енергію, грн/кВт · година;

$Ф_{зал}$ – залишкова вартість ПК на поточний рік, грн.;

$Н_а$ – річна норма амортизації на ПК, частки одиниці;

$F_р$ – річний фонд робочого часу (за 40-годинного робочого тижня $F_р$ = 1920.

Залишкова вартість ПК визначається виходячи з фактичного терміну його експлуатації як різниця між первісною вартістю та зносом за час використання.

$$С_{мч} = 0.3 \cdot 3 \cdot 2 + \frac{6300 \cdot \frac{1}{3}}{1920} = 2.9, \text{ грн,}$$

$$З_{мч} = 70 \cdot 2.9 + 10 = 213 \text{ , грн.}$$

Визначена таким чином вартість створення програмного забезпечення Кпз є частиною одноразових капітальних витрат разом з витратами на придбання і налагодження апаратури системи інформаційної безпеки.

складають:

$$К = Каз + Кн, \text{ грн} \qquad (3.6)$$

де: $К_{аз}$ – вартість закупівлі апаратного забезпечення та допоміжних матеріалів, тис. грн;

$К_н$ – витрати на проведення досліджень та налагодження роботи системи.

$$К = 8166 + 6152 = 14318, \text{грн}$$

3.1.2 Розрахунок поточних (експлуатаційних) витрат

Експлуатаційні витрати – це поточні витрати на експлуатацію та обслуговування об'єкта проектування за визначений період (наприклад, рік), що виражені у грошовій формі. Через особливості проекту експлуатаційні витрати складаються лише за амортизації обладнання, що було куплене для аналізу мережі.

Річний фонд амортизаційних відрахувань ($С_а$) визначається у відсотках від суми капітальних інвестицій за видами основних фондів і нематеріальних активів (ПЗ)

У випадку нашого проекту, амортизаційні відрахування нараховуються лише за ноутбук, та розподілені лінійно на 3 роки, тому

$$Са = 2722, \text{грн/рік}$$

Та складають 33,4 %/рік.

3.2 Оцінка можливого збитку від атаки

Кінцевим результатом впровадження й проведення заходів щодо забезпечення інформаційної безпеки є величина відвернених втрат, що розраховується, виходячи з імовірності виникнення інциденту інформаційної безпеки й можливих економічних втрат від нього.

3.2.1 Оцінка величини збитку

$$В = (Зс + Пзч) \cdot 20, \quad (3.7)$$

де:

$З_с$ –збереження середньостатистичної сім'ї;

$П_{зч}$ – вартість поновлення даних.

Середня вартість поновлення жосткого диску на 500 Гігабайт = 2800 грн

$$В = (30000 + 2800) \cdot 20 = 656\,000 \text{ грн}$$

3.2.2 Загальний ефект від впровадження системи інформаційної безпеки

Загальний ефект від впровадження системи інформаційної безпеки визначається з урахуванням ризиків порушення інформаційної безпеки і становить:

$$Е = В \cdot R, \quad (3.8)$$

$$Е = 65.600 \cdot 0.1 = 6.56$$

де:

В – загальний збиток від атаки, тис. грн;

R – очікувана імовірність атаки, частки одиниці.

3.3 Визначення та аналіз показників економічної ефективності системи інформаційної безпеки

Оцінка економічної ефективності системи захисту інформації, розглянутої у спеціальній частині дипломного проекту, здійснюється на основі визначення та аналізу наступних показників:

Коефіцієнт повернення інвестицій ROSI показує, скільки гривень додаткового прибутку приносить одна гривня капітальних інвестицій на впровадження системи інформаційної безпеки.

$$ROSI = \frac{E}{K} \cdot N, \text{ частки одиниці,} \qquad (3.9)$$

$$ROSI = \frac{0.656}{14318} \cdot 1000 = 22$$

де E – загальний ефект від впровадження системи інформаційної безпеки (розділ 3.2 методичних вказівок, формула 3.8), тис. грн;

К – капітальні інвестиції за варіантами, що забезпечили цей ефект, тис. грн.

N – мінімальна кількість мереж до застосування

Проект системи інформаційної безпеки визнається доцільним за умови

$$ROSI > E_н . \qquad (3.10)$$

При $ROSI < E_н$ варіант є збитковим і більш економічним визнається відмова від його реалізації.

Нормативне значення коефіцієнта повернення інвестицій визначається з наступних міркувань.

1. Якщо організація здійснює фінансування капітальних інвестицій у систему інформаційної безпеки за рахунок позикових коштів, тобто за рахунок банківського кредиту, то в якості бажаного значення $E_н$ варто приймати величину плати за кредит (кредитної ставки) $N_{кр}$.

Проект визнається економічно доцільним, якщо розрахункове значення коефіцієнта повернення інвестицій перевищує величину банківської кредитної ставки з урахуванням інфляції:

$$ROSI > (N_{кр} + N_{інф})*0.01 , \quad (3.11)$$

де $N_{кр}$ – банківська кредитна ставка, %;

$N_{інф}$ – річний рівень інфляції, %.

Для вибраного варіанта визначається розрахунковий строк окупності капітальних інвестицій $T_р$.

$$E_н = 0.2+0.1=0.3$$

Термін окупності капітальних інвестицій $T_о$ показує, за скільки років капітальні інвестиції окупляться за рахунок загального ефекту від впровадження системи інформаційної безпеки:

$$T_O = \frac{K}{E} = \frac{1}{ROSI}, \text{ років}, \quad (3.12)$$

$$T_O = \frac{1}{22} = 0.045 , \text{ року}.$$

3.4. Висновки до економічного розділу

Проаналізувавши результати економічного розділу, капітальні витрати, можливу величину збитку, індекс економічної доцільності та строки окупності капітальних інвестицій, можна вважати, що при застосуванні результатів цієї роботи в одиничному випадку цей проект є економічно недоцільним, але якщо використовувати програми та методики при аналізі інших подібних мереж, то аналіз кожної послідуючої мережі та впровадження заходів з ціллю підвищення безпеки в них буде збільшувати економічну доцільність цього

проекту, при потребі налаштувань 1000 мереж, інвестування будуть вважатися доцільними.

4. ВИСНОВКИ

Ця робота показала навявність вразливості до загроз у безпровідних мережах стандарту 802.11. Проаналізувавши типові мережі можна зробити висновок, що в більшості з них не приділялася увага інформаційній безпеці, або мережа була створена людиною, яка не має потрібного рівня обізнаності в безпеці інформації.

Результатами даної роботи є оцінка безпеки мереж першого та другого рівня, стандарту IEEE 802.11, був розроблений алгоритм тестування для пошуку та випробування на вразливості апаратних роутерів, створення актуальних рекомендацій, щодо захисту приватної мережі Wi-Fi. Також був проведений аналіз розповсюджених моделей маршрутизаторів по декільком критеріям, важливим для користувача, як наприклад цінова політика, захист інформації в створеній мережі, кількість антен, та ін. Для здійснення остаточного вибору і створення рейтингу була обрана система підтримки прийняття рішень «NooTron», на базі методу аналізу ієрархій.

З економічною точки зору проект є доцільним, а підвищення кількості опрацьованих мереж буде підіймати економічну вигоду.

ПЕРЕЛІК ПОСИЛАНЬ

1. Ціна на маршрутизатори [Електронний ресурс] // Rozetka. – 2018. – Режим доступу до ресурсу: https://rozetka.com.ua/routers/c80193/price=299-1000;sort=popularity/
2. Замовляйте послугу «Роутер» і отримаєте знижку на абонплату [Електронний ресурс] // Kyivstar – Режим доступу до ресурсу: https://kyivstar.ua/ru/home-kyivstar/service/wifi.
3. WEP [Електронний ресурс] // Wikipedia – Режим доступу до ресурсу: https://uk.wikipedia.org/wiki/WEP.
4. WPA [Електронний ресурс] // Wikipedia – Режим доступу до ресурсу: https://ru.wikipedia.org/wiki/WPA.
5. В чем разница между режимами WPA-Personal и WPA-Enterprise [Електронний ресурс] // Tp-link. – 2013. – Режим доступу до ресурсу: https://www.tp-link.com/ru/faq-500.html.
6. Wi-Fi Alliance® introduces security enhancements [Електронний ресурс] // Wi-Fi Alliance. – 2018. – Режим доступу до ресурсу: https://www.wi-fi.org/news-events/newsroom/wi-fi-alliance-introduces-security-enhancements.
7. Wi-Fi становится безопаснее: всё, что вам нужно знать про WPA3 [Електронний ресурс] // Вячеслав Голованов. – 2018. – Режим доступу до ресурсу: https://habr.com/post/424925/.
8. Simultaneous Authentication of Equals: A Secure, Password-Based Key Exchange for Mesh Networks [Електронний ресурс] // IEEE. – 2008. – Режим доступу до ресурсу: https://ieeexplore.ieee.org/document/4622764/.
9. D. Harkins, Ed. Dragonfly Key Exchange [Електронний ресурс] / D. Harkins, Ed. // IETF. – 2015. – Режим доступу до ресурсу: https://tools.ietf.org/html/rfc7664.
10. Атака с переустановкой ключа [Електронний ресурс] // Wikipedia – Режим доступу до ресурсу: https://ru.wikipedia.org/wiki/Атака_с_переустановкой_ключа.

11. Perfect forward secrecy [Електронний ресурс] // Wikipedia – Режим доступу до ресурсу: https://ru.wikipedia.org/wiki/Perfect_forward_secrecy.

12. IEEE Standard for Information technology--Telecommunications and information exchange between systems Local and metropolitan area networks--Specific requirements – Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications [Електронний ресурс] // IEEE. – 2016. – Режим доступу до ресурсу: https://ieeexplore.ieee.org/document/7786995/.

13. Security [Електронний ресурс] // wi-fi.org – Режим доступу до ресурсу: https://www.wi-fi.org/discover-wi-fi/security.

14. Wi-Fi Easy Connect [Електронний ресурс] // wi-fi.org – Режим доступу до ресурсу: https://www.wi-fi.org/discover-wi-fi/wi-fi-easy-connect.

15. Оппортунистическое шифрование [Електронний ресурс] // Wikipedia – Режим доступу до ресурсу: https://ru.wikipedia.org/wiki/Оппортунистическое_шифрование.

16. D. Harkins, Ed. Opportunistic Wireless Encryption [Електронний ресурс] / D. Harkins, Ed. // IETF. – 2017. – Режим доступу до ресурсу: https://tools.ietf.org/html/rfc8110.

17. Легезо Д. Исследование: незащищенные Wi-Fi-сети по всему мир [Електронний ресурс] / Денис Легезо // KaspeskyLab. – 2016. – Режим доступу до ресурсу: https://securelist.ru/research-on-unsecured-wi-fi-networks-across-the-world/29731/.

18. Аналіз засобів захисту при використанні обладнання стандарту IEEE 802.11. // Дніпровська Політехніка. – 2018. – №10. – С. 41.

19. Mojo AirTight [Електронний ресурс] // Mojonetworks – Режим доступу до ресурсу: https://www.mojonetworks.com/mojo-airtight.

20. Installation and test [Електронний ресурс] // Flukenetworks – Режим доступу до ресурсу: https://www.flukenetworks.com/installation-and-test.

21. AirMagnet [Електронний ресурс] // Flukenetworks – Режим доступу до ресурсу: https://airmagnet.flukenetworks.com/assets/datasheets

22. Сафонов Л. Wi-Fi is over: вычисляем нарушителей беспроводного эфира [Електронний ресурс] / Лука Сафонов // Pabr. – 2017. – Режим доступу до ресурсу: https://habr.com/post/339270/.

23. Avast Free Antivirus [Електронний ресурс] // Avast – Режим доступу до ресурсу: https://www.avast.ru/free-antivirus-download.

24. Методичні рекомендації до виконання дипломних робіт (проектів) бакалаврів та магістрів спеціальностей 125 Кібербезпека, 172 Телекомунікації та радіотехніка / Упоряд.: О.Ю. Гусєв, О.В. Герасіна, О.М. Алексєєв,О.В. Кручінін. – Дніпро: НГУ, 2018. – 50 с.

25. NooTron [Електронний ресурс] – Режим доступу до ресурсу: https://nootron.net.ua/.

ДОДАТОК А. ВІДОМІСТЬ МАТЕРІАЛІВ ДИПЛОМНОГО ПРОЕКТУ

№	Формат	Найменування	Кількість листів	Примітка
1	А4	Реферат		
2	А4	Список умовних скорочень		
3	А4	Зміст		
4	А4	Вступ		
5	А4	1 Розділ		
6	А4	2 Розділ		
7	А4	3 Розділ		
8	А4	Висновки		
9	А4	Перелік посилань		
10	А4	Додаток А		
11	А4	Додаток Б		
12	А4	Додаток В		
13	А4	Додаток Г		

ДОДАТОК Б. ПЕРЕЛІК ФАЙЛІВ НА ЕЛЕТРОННОМУ НОСІЇ

1. Магістерська робота Ільман М_О_125м-17-1.docx – Пояснювальна записка
2. Ільман М_В.pptx – Презентація

ДОДАТОК В. ВІДГУК КЕРІВНИКА КВАЛІФІКАЦІЙНОЇ РОБОТИ

ВІДГУК

на дипломну роботу магістра на тему:

«Аналіз рівня інформаційної безпеки в приватних мережах стандарту IEEE 802.11»

студента групи 125м–17–2 *Ільмана Микити Віталійовича*

Мета дипломної роботи – забезпечення безпеки інформації в приватних мережах стандарту IEEE 802.11.

Тема дипломної роботи безпосередньо пов’язана з об’єктом діяльності фахівця за спеціальністю 125 Кібербезпека – розвиток методик тестування інформаційних систем.

Задачі дипломної роботи (аналіз особливостей функціонування та вразливостей мережах стандарту IEEE 802.11, аналіз існуючих методів та засобів захисту, розробка програми та методики тестування систем, проведення тестування та обробка отриманих результатів) віднесені в освітньо-кваліфікаційній характеристиці магістра до класу евристичних, вирішення яких основане на знаково-розумових уміннях фахівця.

Практичне значення результатів проектування полягає у розробці рекомендацій, щодо налаштувань елементів приватних мережах стандарту IEEE 802.11.

До недоліків дипломної роботи відносяться:

– деякі пункти методики вимагають додаткових експериментальних перевірок;
– відділення від графіка роботи;
– структура викладення програми та методики відрізняється від рекомендованої.

Оформлення пояснювальної записки до дипломного проекту виконано з деякими відхиленнями від стандартів.

Ступінь самостійності виконання дипломної роботи висока.

За час дипломування Ільман М.В. виявив себе фахівцем, здатним самостійно, на високому рівні вирішувати поставлені задачі.

В цілому дипломна робота виконана у відповідності до вимог, що пред'являються до дипломної роботи магістра, заслуговує оцінки "добре", а Ільман М.В. присвоєння йому кваліфікації професіонала із організації інформаційної безпеки.

Керівник спеціальної частини
дипломної роботи магістра,
старший викладач _____ О.В. Кручінін

Керівник дипломної
роботи магістра,
д.т.н, проф. _____ В.І. Корнієнко

ДОДАТОК Г. Відгук керівника економічного розділу

Керівник розділу _____ _____
(підпис) (ініціали, прізвище)