ХМЕЛЬНИЦЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ

Факультет інформаційних технологій

Кафедра кібербезпеки

КВАЛІФІКАЦІЙНА РОБОТА

Кузь Михайло Миколайович

на здобуття ступеня вищої освіти магістра

Метод захисту користувачів публічних Wi-Fi-мереж від підроблених точок доступу

Галузь знань	12 – Інформаційні технології
Спеціальність	125 – Кібербезпека та захист інформації
Освітня програма	Кібербезпека та захист інформації

Шифр КРМКБЗІ.240193.24.01.09 ПЗ

Виконав студент 2 курсу група КБЗІм-23-1 _____ Михайло КУЗЬ

Керівник д-р філософії, старший викладач _____ Наталія ПЕТЛЯК

Нормоконтролер д-р філософії, старший викладач _____ Наталія ПЕТЛЯК

До захисту допускаю:

Завідувач кафедри кібербезпеки _____ Юрій КЛЬОЦ

9 12 2025 р.

Хмельницький 2025

ХМЕЛЬНИЦЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ

Факультет Інформаційних технологій

Кафедра Кібербезпеки

Рівень вищої освіти Магістр

Галузь знань 12 – Інформаційні технології

Спеціальність 125 – Кібербезпека та захист інформації

Освітня програма Кібербезпека та захист інформації

ЗАТВЕРДЖУЮ

Завідувач кафедри кібербезпеки

Юрій КЛЬОЦ _____

1 09 2025 р.

З А В Д А Н Н Я
НА КВАЛІФІКАЦІЙНУ РОБОТУ

Кузю Михайлу Миколайовичу

1 Тема Метод захисту користувачів публічних Wi-Fi-мереж від підроблених точок доступу

Керівник роботи доктор філософії, старший викладач Наталія ПЕТЛЯК

Затверджено наказом ректора університету 25 08 2025 № 65

2 Строк подання студентом кваліфікаційної роботи на кафедру 1.12.2025

3 Вихідні дані до роботи Вивчити та проаналізувати існуючі підходи до аналізу трафіку та їх реалізації; розробити структуру аналізатора та варіанти його реалізації; розглянути кілька реалізацій аналізу та обрати найефективнішу; провести тестування розробленого методу; оцінити отримані результати.

4 Зміст пояснювальної записки (перелік питань, які потрібно розробити)
Вступ. Аналіз локальних безпровідних мереж Wi-Fi, атак на безпровідні мережі та механізмів безпеки. Постановка задачі. Розроблення методу захисту безпровідних мереж від підроблених точок доступу. Експериментальна перевірка та оцінка ефективності розробленого методу. Перспективи вдосконалення та інтеграції з іншими системами. Висновки.

5 Перелік графічного матеріалу (із зазначенням обов'язкових креслень)

6 Консультанти розділів кваліфікаційної роботи

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

7 Дата видачі завдання 1 09 2025 р.

КАЛЕНДАРНИЙ ПЛАН

Назва етапів (розділів) кваліфікаційної роботи	Строк виконання етапів роботи	Примітка
Ґрунтовне ознайомлення та дослідження предметної галузі		Виконано
Визначення змісту, структури магістерської роботи		Виконано
Опрацювання першого розділу магістерської роботи		Виконано
Опрацювання статті за результатами дослідження		Виконано
Опрацювання другого розділу магістерської роботи		Виконано
Опрацювання третього розділу магістерської роботи		Виконано
Опрацювання четвертого розділу магістерської роботи		Виконано
Підготовка та опрацювання ілюстративного матеріалу		Виконано
Оформлення магістерської роботи графічної та текстової частини		Виконано
Попередній захист магістерської роботи		Виконано
Захист магістерської роботи на засіданні ЕК		Виконано

Студент _____ Михайло КУЗЬ

Керівник кваліфікаційної роботи _____ Наталія ПЕТЛЯК

АНОТАЦІЯ

Тема кваліфікаційної роботи: Метод захисту користувачів публічних Wi-Fi-мереж від підроблених точок доступу

Автор роботи: студент групи КБЗІм-24-1 Кузь М.М.

Керівник роботи: доктор філософії, старший викладач Петляк Н.С.

Загальний обсяг роботи: 80 сторінок, 7 рисунків, 8 таблиць, 14 формул, 1 додаток, 66 посилань.

Ключові слова: Wi-Fi, інформаційна безпека, підроблені точки доступу, Evil Twin, аномалії, машинне навчання, автокодер.

У роботі розглянуто проблему захисту користувачів публічних Wi-Fi-мереж від підроблених точок доступу та атак типу «злий двійник». Виконано аналіз стандартів IEEE 802.11, сучасних механізмів безпеки та найбільш поширених загроз. Запропоновано метод виявлення підроблених точок доступу на основі поєднання сигнатурного та статистичного аналізу із застосуванням нейронного автокодера для виявлення аномалій у бездротовому трафіку.

Розроблено математичну модель процесу виявлення відхилень та створено програмний прототип аналізатора трафіку мовою Python. Проведені експериментальні дослідження на реальному обладнанні Avaya WLAN 8120/8180 підтвердили ефективність методу: високу точність класифікації, низький рівень хибних спрацьовувань та здатність роботи в режимі реального часу. Метод може бути інтегрований у системи моніторингу корпоративних і публічних Wi-Fi-мереж та підвищує рівень їх інформаційної безпеки.

1.12.2025

ANNOTATION

Theme of qualification work: Method for protecting users of public Wi-Fi networks from rogue access points

Author of the work: student of KBZIm-24-1 Kuz M.M.

Mentor: Doctor of Philosophy Petliak N.S.

Total volume of work: 80 pages, 7 figures, 8 tables, 14 formulas, 1 appendix, 66 references.

Keywords: Wi-Fi, information security, rogue access points, Evil Twin, anomalies, machine learning, autoencoder.

The thesis addresses the problem of protecting users of public Wi-Fi networks from rogue access points and Evil Twin attacks. It includes an analysis of IEEE 802.11 standards, modern security mechanisms, and common wireless threats. A method for detecting rogue access points is proposed, combining signature-based and statistical analysis with a neural-network autoencoder for identifying anomalies in wireless traffic.

A mathematical model of anomaly detection is developed, along with a software prototype of a traffic analyzer implemented in Python. Experimental studies conducted on real Avaya WLAN 8120/8180 equipment confirmed the effectiveness of the method: high detection accuracy, low false-positive rate, and real-time operability. The proposed method can be integrated into monitoring systems of corporate and public Wi-Fi networks and enhances their overall information security.

1.12.2025

ЗМІСТ

ВСТУП

Безпровідні мережі – один із найшвидше зростаючих напрямів телекомунікаційної індустрії [1,2].

Безпровідні системи, зокрема стільникові, супутникові та безпровідні локальні мережі (Wireless Local Area Network), стали невід'ємною частиною повсякденного життя. На сьогодні багато хто володіє більш ніж одним пристроєм, здатним підключатися до безпровідних систем (часто – до кількох одночасно) [2,3].

З вдосконаленням стандартів і зміною офісної та соціальної культури загалом безпровідні мережі стають не просто заміною традиційним дротовим, а й помітним покращенням порівняно з ними.

Використання безпровідної мережі дозволяє не бути прив'язаним до конкретної географічної точки – як у глобальному масштабі при використанні мобільного чи супутникового зв'язку, так і в межах одного приміщення або будівлі при використанні локальної безпровідної мережі. Безпровідні технології передавання даних мають суттєвий вплив на продуктивність і ефективність бізнес-процесів, розширюючи можливості для розвитку та вдосконалення бізнесу шляхом упровадження функцій мобільної передачі голосу, даних, відео та інших застосунків [4-6].

Інфраструктура безпровідних мереж є однією з найдинамічніших у розвитку. Прогнозується, що кількість точок доступу до 2023 року досягне 628 мільйонів, а середня швидкість у локальній безпровідній мережі становитиме 92 МБ/с [1].

Сучасні тенденції у розвитку безпровідних мереж також зумовлені стрімким поширенням Інтернету речей (IoT), що створює нові виклики у забезпеченні безпеки. Зростання кількості підключених пристроїв у побуті та промисловості призводить до значного збільшення мережевого трафіку та розширення поверхні атак. Пристрої IoT часто мають обмежені ресурси для реалізації повноцінних засобів безпеки, що робить їх потенційними вразливими точками в мережі. Це

потребує інтеграції методів контролю та моніторингу у реальному часі для виявлення аномалій у поведінці пристроїв і запобігання несанкціонованому доступу.

Ще однією важливою тенденцією є розвиток мобільних мереж п’ятого покоління (5G), які обіцяють значне підвищення пропускної здатності та зменшення затримок передачі даних. Це відкриває нові можливості для використання безпровідних мереж у критичних сферах, таких як телемедицина, автономний транспорт, розумні міста та промислові автоматизовані системи. Разом із цим зростає потреба у безпечних механізмах автентифікації, шифрування даних і захисту від атак на мережевому та прикладному рівнях.

Особливу увагу зараз приділяють питанням виявлення підроблених точок доступу (Evil Twin Attack) та атак типу Man-in-the-Middle. Такі атаки дозволяють зловмиснику перехоплювати дані користувачів без їх відома, що становить серйозну загрозу для приватності та конфіденційності. Виявлення та нейтралізація таких загроз у реальному часі стає критичною задачею, особливо у відкритих мережах громадського користування – кафе, аеропортах, університетах [3].

З точки зору методології, сучасні підходи до моніторингу безпровідних мереж включають використання аналітичних платформ на базі машинного навчання та штучного інтелекту, що дозволяє автоматично виявляти аномальні шаблони трафіку, підозрілі пристрої та потенційні вразливості. Інтеграція таких рішень у мережеву інфраструктуру забезпечує оперативний захист та зменшує ризики компрометації користувацьких даних.

Загалом, розвиток безпровідних мереж сприяє формуванню нового рівня цифрової взаємодії, де швидкість, мобільність та безпека є ключовими параметрами. Проблеми безпеки стають не тільки технічним, а й соціально-економічним питанням, оскільки від їх вирішення залежить довіра користувачів до технологій та ефективність бізнес-процесів у цифровій економіці. Розробка методів захисту у реальному часі та аналітики трафіку стає необхідною умовою для безпечного і стабільного функціонування сучасних безпровідних мереж [5].

Актуальність даної роботи полягає в тому, що у відкритих джерелах підходи до підвищення безпеки локальних безпровідних мереж описані недостатньо, що поглиблює проблему уразливості користувацьких, а подекуди й корпоративних мереж. Недбале ставлення до безпеки безпровідної мережі дає змогу легко отримати доступ до конфіденційної інформації, тому питання моніторингу таких мереж є одним із найважливіших на сьогодні [7].

Метою цієї роботи є розроблення методу захисту користувачів від підроблених точок доступу у публічній безпровідній мережі в реальному часі, що дасть змогу підвищити безпеку та надійність захищеної мережі.

Для досягнення поставленої мети необхідно вирішити такі завдання:

– вивчити та проаналізувати існуючі підходи до аналізу трафіку та їх реалізації;

– розробити структуру аналізатора та варіанти його реалізації;

– розглянути кілька реалізацій аналізу та обрати найефективнішу;

– провести тестування розробленого методу;

– оцінити отримані результати.

У процесі виконання роботи було використано комплекс теоретичних і практичних методів дослідження, що охоплюють аналітичний, експериментальний та обчислювальний етапи. Проведено огляд наукових джерел, стандартів IEEE 802.11 і сучасних протоколів безпеки (WEP, WPA, WPA2, WPA3) з метою виявлення їхніх уразливостей. Здійснено порівняльний аналіз існуючих методів моніторингу безпровідних мереж (сигнатурних, статистичних, гібридних) і визначено їхні переваги та обмеження. Виконано систематизацію типових атак на Wi-Fi, включно з атаками «злий двійник» (Evil Twin), Man-in-the-Middle та DoS, для подальшого формування набору ознак для аналізу трафіку. Побудовано математичну модель процесу виявлення аномалій, засновану на оцінці похибки реконструкції ознак пакета за допомогою нейронного автокодера. Використано методи статистичного аналізу (обчислення середнього, дисперсії, стандартного відхилення) для визначення порогів виявлення аномальних подій. Застосовано

елементи теорії ймовірностей для оцінки достовірності класифікації «нормальний / аномальний» трафік. Реалізовано навчання нейронної мережі-автокодера на вибірках нормального трафіку з метою формування латентного простору характеристик мережевих пакетів. Проведено виявлення аномалій за відхиленням похибки реконструкції від базового рівня (метод 3σ). Використано бібліотеки Python (TensorFlow, NumPy, Pandas, Scapy) для створення, навчання та тестування моделі. Проведено збір і парсинг реального бездротового трафіку з використанням адаптера в режимі монітора (моніторинг протоколів Radiotap, IEEE 802.11). Виконано тестування розробленого методу на реальних точках доступу Avaya WLAN Access Point 8120 та контролері Avaya WLAN Controller 8180. Здійснено оцінку ефективності за показниками точності виявлення (Precision, Recall, F1-score) і швидкодії в реальному часі. Для реалізації програмної частини застосовано мову програмування Python та бібліотеки Scapy, dpkt, TensorFlow, Keras, Matplotlib. Для обробки трафіку використовувалися формати PCAP, інтерфейси сокетів типу RAW та утиліти iwconfig, ifconfig, tcpdump у середовищі Linux.

Наукова новизна роботи є наступною:

1. У роботі запропоновано новий метод виявлення підроблених точок доступу в безпровідних мережах Wi-Fi, який поєднує сигнатурний та статистичний підходи із застосуванням автокодера нейронної мережі для аналізу аномалій у трафіку.

2. Розроблено математичну модель процесу виявлення аномалій, що базується на оцінці похибки реконструкції вхідних векторів ознак мережевих пакетів (поля протоколів Radiotap, IEEE 802.11, рівень сигналу, частота, MAC-адреси тощо).

3. Вперше для задачі моніторингу безпровідних мереж запропоновано використання контролера Avaya WLAN 8180, яка забезпечує реальний моніторинг та аналіз мережевих подій.

4. Введено уніфіковану схему представлення мережевого пакета як словникової структури, що дає змогу ефективно обробляти великі обсяги даних без надмірності класової моделі Scapy або dpkt.

5. Обґрунтовано підхід до автоматичного визначення порогових значень помилки реконструкції (mean + 3σ), що підвищує точність класифікації «нормальний/аномальний» трафік.

Практична цінність результатів полягає у тому, що:

1. Розроблено прототип програмного комплексу на Python для аналізу бездротового трафіку в режимі реального часу, здатного виявляти підроблені точки доступу, DoS-атаки та аномалії поведінки пристроїв.

2. Запропонований підхід може бути інтегрований у системи моніторингу корпоративних або публічних мереж без модифікації їхньої інфраструктури, лише за рахунок додаткових сенсорів у режимі monitor.

3. Результати дослідження мають прикладну цінність для підвищення кібербезпеки Wi-Fi-мереж у навчальних закладах, державних установах, аеропортах, бізнес-центрах тощо.

4. Реалізований аналізатор може бути використаний як навчальний інструмент у курсах із комп’ютерної безпеки, мережевих технологій і штучного інтелекту.

5. Порівняння ефективності з існуючими рішеннями показало, що запропонований метод забезпечує вищу адаптивність до нових типів атак без необхідності оновлення сигнатурних баз.

1 БЕЗПРОВІДНІ МЕРЕЖІ ТА ІНФОРМАЦІЙНА БЕЗПЕКА

1.1 Локальні безпровідні мережі Wi-Fi

Говорячи про безпровідні мережі, найчастіше мають на увазі локальні безпровідні мережі (WLAN). Цей тип безпровідної мережі описаний Інститутом інженерів електротехніки та електроніки (Institute of Electrical and Electronics Engineers, IEEE) набором стандартів 802.11, більш відомих під торговою маркою Wi-Fi [8].

Особливість такої мережі полягає в її архітектурі. У мережі Wi-Fi завжди є центральна точка доступу та один або кілька клієнтських пристроїв. Передача даних від клієнта можлива лише до точки доступу; клієнти не можуть спілкуватися між собою безпосередньо [9].

Також існують мережі Ad-Hoc, у яких немає централізованої точки доступу, і пристрої передають інформацію безпосередньо один одному. Такі мережі створюються швидко, часто для екстреної передачі даних, тому питання безпеки в них зазвичай має другорядне значення [10]. Мережі типу Ad-Hoc трапляються значно рідше, тому в подальшому розглядатимуться переважно звичайні Wi-Fi-мережі з точкою доступу та клієнтами [11].

Точка доступу в безпровідній мережі у найпростішому варіанті може лише передавати трафік безпровідних клієнтів до дротової мережі, де він маршрутизується. Проте майже всі сучасні точки доступу здатні самостійно виконувати функції маршрутизації трафіку, що дозволяє створити закриту локальну мережу навіть за допомогою єдиного пристрою [11].

Передача даних у мережах Wi-Fi здійснюється в діапазонах частот 2,4 ГГц і 5 ГГц. Для роботи точка доступу налаштовується на певний канал у цьому діапазоні та веде трансляцію виключно в його межах. Ширина каналу може становити від 20 до 160 МГц [12].

Дані в безпровідній мережі передаються у вигляді пакетів, як і в класичній дротовій мережі. На канальному рівні ці пакети інкапсулюються у додатковий заголовок 802.11, який описує параметри передавання та фізичну адресацію

пристроїв, що беруть участь у транзакції.

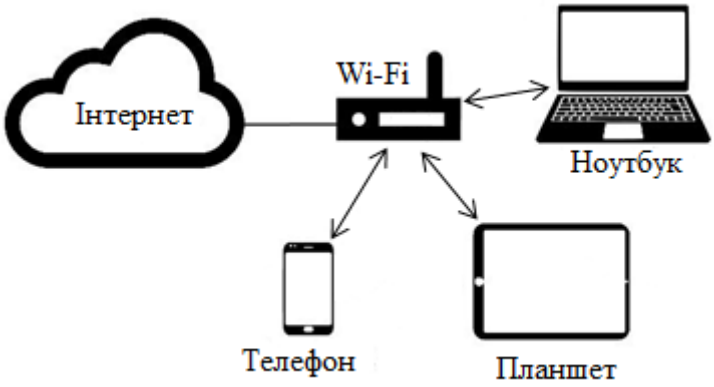

Рисунок 1.1 – Узагальнена схема безпровідної мережі

Передавання даних у безпровідних мережах відбувається у відкритому середовищі. Це значно спрощує перехоплення трафіку та втручання в мережу, тому що зловмиснику достатньо перебувати в зоні дії атакованої мережі. Тому виникає потреба дослідження мережі з метою виявлення шкідливої активності [13, 14].

Існує два основні загальноприйняті підходи до аналізу мережевого трафіку: сигнатурний та статистичний аналізи [15,16].

Сутність сигнатурного аналізу полягає в тому, що існує певна база заздалегідь відомих описів атак (сигнатур), і перевіряючий агент просто порівнює аналізовані пакети з цією базою. Якщо пакет або послідовність пакетів збігається з відомою сигнатурою, вважається, що здійснюється атака, після чого приймається рішення щодо реакції (наприклад, блокування атакуючого пристрою) [15].

Перевагою цього підходу є надійність, передбачуваність і швидкість, проте він не здатний виявляти нові, невідомі атаки, для яких ще не створено сигнатури (оскільки база зазвичай поповнюється вручну розробником).

Статистичний аналіз передбачає визначення “норми” трафіку для мережі за певними показниками, після чого аналізований трафік порівнюється з цією нормою, і при значному відхиленні вважається, що відбувається атака [16].

Перевага цього методу над сигнатурним полягає в тому, що він може виявляти атаки “нульового дня”, тобто атаки, які ще не досліджені та не описані. Водночас статистичний аналіз має низку недоліків: точність виявлення не є ідеальною, деякі складні атаки практично не відрізняються від нормального трафіку, а під час навчання він є дуже чутливим до неякісної або некоректної навчальної вибірки.

У результаті в сучасних рішеннях для аналізу трафіку статистичний аналіз використовується не повною мірою, а лише в спрощеній формі, з наперед заданими параметрами або для визначення якісних характеристик мережі.

Наразі існує безліч програмних і апаратних рішень, що реалізують сигнатурний аналіз мережевого трафіку загалом: Snort, Suricata, Cisco Firepower та інші. Проте відкриті рішення, які б спеціалізувалися саме на аналізі безпровідного трафіку, практично відсутні [17, 18].

У даній магістерській роботі розглядаються етапи розроблення такого рішення, а також загальні питання аналізу мережевого трафіку та захисту користувачів від підроблених точок доступу.

1.2 Стандарти сімейства IEEE 802.11

Сімейство стандартів IEEE 802.11 охоплює низку специфікацій, які описують організацію передавання даних і взаємодію в безпровідних мережах [19]. До мереж Wi-Fi належать стандарти IEEE 802.11a, b, g, n, ac та ax. Вони визначають параметри роботи безпровідних мереж у діапазонах 2,4 ГГц і 5 ГГц [20].

Робочий діапазон стандарту IEEE 802.11b (2,4 ГГц), що базується на методі широкосмугової модуляції з прямим розширенням спектра (Direct Sequence Spread Spectrum, DSSS), поділяється на 14 каналів, які для уникнення взаємних перешкод рознесені на 25 МГц. Передача даних здійснюється через один із 14 каналів. Одночасно можуть бути задіяні лише три непересічні канали. Залежно від

рівня перешкод і відстані між передавачем і приймачем швидкість передавання даних автоматично змінюється [21].

Стандарт IEEE 802.11a, прийнятий у 1999 році, почав застосовуватися на практиці лише через два роки. У ньому описано організацію безпровідної мережі в діапазоні 5 ГГц [22]. Цей стандарт отримав поширення переважно у США та Японії, тоді як у Європі та країнах СНД він не набув значної популярності. У стандарті використовується мультиплексування з ортогональним поділом частот (Orthogonal Frequency Division Multiplexing, OFDM) – схема модуляції сигналу, за якою основний потік даних розділяється на кілька паралельних підпотоків із нижчою швидкістю передавання. Для модуляції кожного підпотоку застосовується окрема несуча частота.

Стандарт визначає такі швидкості передавання даних: 6, 12 та 24 Мбіт/с, як обов'язкові, та 9, 18, 36, 48 і 54 Мбіт/с, як додаткові. Швидкість передавання може збільшуватися за рахунок одночасного використання двох каналів.

Стандарт IEEE 802.11g, ратифікований у 2003 році, є вдосконаленою специфікацією IEEE 802.11b та працює в тому самому частотному діапазоні 2,4 ГГц [20]. Основна перевага полягає у збільшеній пропускній здатності, якщо IEEE 802.11b забезпечував до 11 Мбіт/с, то IEEE 802.11g – до 54 Мбіт/с. У цьому стандарті застосовується схема модуляції OFDM, подібна до IEEE 802.11a, що дозволяє підвищити ефективність передавання.

Стандарт IEEE 802.11g сумісний із IEEE 802.11b: адаптери старого стандарту можуть працювати в мережах 802.11g зі швидкістю до 11 Мбіт/с, а адаптери 802.11g – у мережах 802.11b з аналогічним зниженням швидкості.

Стандарт IEEE 802.11n, ратифікований у 2009 році, визначає мережі, які можуть працювати в обох діапазонах 2,4 ГГц і 5 ГГц [20]. У ньому впроваджено технологію MIMO (Multiple Input Multiple Output), яка дозволяє передавати дані одночасно через кілька антен (до чотирьох). Максимальна теоретична швидкість передавання даних за цим стандартом становить 600 Мбіт/с, що досягається завдяки розширенню ширини каналу з 20 до 40 МГц і застосуванню багатопотокової передачі.

Стандарт IEEE 802.11ac функціонує виключно в діапазоні 5 ГГц і визначає більш широкі радіоканали 80 та 160 МГц [23]. Також запроваджено 256-QAM складнішу схему модуляції, а також підтримку багатокористувацької MIMO (MU-MIMO), що дозволяє передавати дані одночасно кільком користувачам. Максимальна кількість використовуваних антен збільшена до 8.

Стандарт IEEE 802.11ax, опублікований у 2019 році, позиціонується не як «мережа з дуже високою пропускною здатністю», а як «мережа з високою ефективністю» [19]. Збільшення швидкості досягається не за рахунок розширення частотного каналу, а завдяки застосуванню технології OFDMA (Orthogonal Frequency Division Multiple Access) та модуляції 1024-QAM.

Крім того, у стандарті передбачено тимчасове ущільнення передачі, що дозволяє одночасно передавати дані великій кількості клієнтів у межах одного часового інтервалу.

1.3. Механізми безпеки, передбачені стандартами IEEE 802.11

Мережі Wi-Fi забезпечують високу мобільність користувачів і гнучкість розгортання інфраструктури, проте це досягається ціною зниження рівня захищеності [24,25,28]. Механізми безпеки, передбачені стандартами IEEE 802.11, не розв’язують усіх проблем, пов’язаних із захистом інформації в безпровідних мережах [24,34]. Навіть у найновіших стандартах виявляються уразливості, тому питання інформаційної безпеки Wi-Fi-мереж і надалі залишається актуальним [28,31].

Далі розглянуто основні механізми захисту, реалізовані в рамках стандартів IEEE 802.11, а також їх еволюцію від WEP до WPA3 [24-27].

1.3.1 WEP (Wired Equivalent Privacy)

Механізм Wired Equivalent Privacy (WEP) або «еквівалент дротової конфіденційності» був єдиним засобом захисту у першій версії протоколу IEEE

802.11 [24,25,29]. На практиці виявилося, що WEP не забезпечує належного рівня безпеки та є вразливим до численних атак, включно з тими, що дозволяють швидко визначити секретний ключ [29].

Після появи стандарту IEEE 802.11i (2004 р.) WEP офіційно визнано застарілим і не рекомендованим до використання [24,34]. Незважаючи на це, досі існує чимало мереж, у яких WEP допускається як механізм шифрування [32].

WEP підтримує два режими автентифікації: відкриту та загальним ключем [24,29].

При відкритій автентифікації клієнту не потрібно надавати жодних даних для перевірки, найчастіше такі мережі використовують «білий список» дозволених MAC-адрес.

При автентифікації за спільним ключем процедура включає чотири повідомлення: клієнт надсилає запит на автентифікацію; точка доступу надсилає випадкове 128-бітне число; клієнт шифрує його спільним ключем і повертає; точка доступу розшифровує та порівнює результат. Якщо значення збігаються, клієнт вважається автентифікованим.

Цей механізм є одностороннім, тобто клієнт не може автентифікувати точку доступу.

Для шифрування WEP використовує потоковий шифр RC4 (Rivest Cipher 4). Основний ключ (40 або 104 біти залежно від версії) використовується для генерації сеансового ключа, який змінюється для кожного пакета. Цей ключ подається в RC4, а отриманий потік шифрування накладається на пакет за допомогою операції XOR.

1.3.2 Wi-Fi Protected Access (WPA) та WPA2

Протоколи WPA (2003) та WPA2 (2004) були створені для заміни застарілого WEP [26,27,29]. Через те, що його уразливості могли експлуатувати навіть користувачі без спеціальної підготовки, адміністратори мереж почали впроваджувати альтернативні рішення безпеки, зокрема 802.1X і віртуальні приватні мережі (VPN) [26].

WPA використовує Temporal Key Integrity Protocol (TKIP) для шифрування та удосконалену перевірку цілісності даних. Також у WPA вперше впроваджено взаємну автентифікацію через механізми 802.1X та Extensible Authentication Protocol (EAP) [26,27].

Для корпоративних мереж передбачено автентифікацію через RADIUS-сервери, а для домашніх і малих мереж спрощений варіант WPA-PSK (Pre-Shared Key) із фіксованим спільним ключем [26,27].

WPA2, ратифікований у 2004 році та включений до стандарту IEEE 802.11-2007, підтримує як TKIP, так і CCMP, заснований на AES (Advanced Encryption Standard), який вважається найнадійнішим алгоритмом шифрування [27,34].

У WPA2 реалізовано ієрархію ключів.

На верхньому рівні Pre-Shared Key (PSK) або Master Session Key (MSK). Із них генерується Pairwise Master Key (PMK), який використовується для створення Pairwise Transient Key (PTK) та Group Transient Key (GTK) під час встановлення сесії.

PTK далі ділиться на коротші ключі для різних цілей: Temporal Key (TK) – для шифрування уніказтрафіку, Key Confirmation Key (KCK) – для підтвердження ключа, Key Encryption Key (KEK) – для шифрування службових кадрів EAPOL, а GTK – для групового та широкомовного трафіку.

До виявлення атаки KRACK (Key Reinstallation Attack) у 2016 році WPA2 вважався надійним стандартом безпеки [31].

1.3.3 WPA3

Стандарт WPA3, опублікований у 2018 році, усуває низку вразливостей попередньої версії [30,36]. Він замінює традиційну автентифікацію на одночасну автентифікацію рівних (Simultaneous Authentication of Equals, SAE), у процесі якої відбувається “рукостискання стрекози” (dragonfly handshake). Під час цього обміну формується PMK, який далі використовується за тією ж схемою, що і в WPA2 [30].

Крім того, WPA3 підтримує технологію Wi-Fi Enhanced Open, що

забезпечує шифрування трафіку в публічних мережах без автентифікації, запобігаючи його перехопленню.

Також стандарт вводить захищені керуючі кадри (Protected Management Frames, PMF), вони шифруються, що робить неможливим надсилання фальшивих службових повідомлень зловмисниками [30,36].

Для протидії атакам перебору паролів (dictionary attacks) обмежено кількість спроб автентифікації, що підвищує безпечність навіть коротких паролів.

WPA3 став частиною стандарту IEEE 802.11ax, який також передбачає низку технологій підвищення ефективності передачі [36]:

– OFDMA (Orthogonal Frequency Division Multiple Access) – дозволяє передавати дані дев'ятьом клієнтам одночасно у межах одного часово́го інтервалу;

– BSS Coloring (Base Service Set Coloring) – механізм «розфарбовування» базових станцій, який дозволяє пристроям ігнорувати сигнали від сторонніх точок доступу з іншим "кольором".

Поки що лише обмежена кількість пристроїв підтримує WPA3, однак очікується, що він стане основним стандартом безпеки Wi-Fi у найближчі роки.

1.3.4 IEEE 802.11w

Стандарт IEEE 802.11i зосереджувався на конфіденційності та цілісності даних, однак не забезпечував доступності. Через це службові кадри у Wi-Fi-мережах залишалися нешифрованими, що відкривало можливості для DoS-атак [34]. У 2009 році був прийнятий стандарт IEEE 802.11w, який запровадив шифрування службових кадрів і новий груповий ключ для широкомовних повідомлень. Також було реалізовано механізм захищеного запиту асоціації (Security Association Query, SA Query), у разі надходження запиту асоціації точка доступу надсилає SA Query-запит і припиняє асоціацію, якщо не отримує підтвердження відповіді [35]. Попри вимогу Wi-Fi Alliance щодо обов'язкової підтримки цього стандарту, у багатьох реалізаціях він залишається опціональним

або доступним лише в поєднанні з WPA3. Особливо часто це спостерігається у пристроях Інтернету речей (IoT), які можуть не розпізнавати захищені кадри і відмовлятися їх обробляти [36].

1.4 Атаки на безпровідні мережі

1.4.1 Атаки на WEP

Атака PTW названа за прізвищами її авторів Pyshkin, Tews, Weinman і була відкрита в 2007 році. Вона спрямована на злом WEP-ключа більш ефективними, ніж тодішні статистичні методи, підходами [37]. Нині PTW є стандартною атакою в утилітах для злому WEP [38].

Подібно до PTW, атака Hirte орієнтована на отримання секретного WEP-ключа, проте в цьому випадку не потрібна точка доступу, достатньо наявності клієнтського пристрою [39]. Для проведення атаки необхідно, щоб клієнтський пристрій активно шукав мережі, до яких він раніше підключався (сучасні пристрої зазвичай мають увімкнену таку функцію за замовчуванням). Перехопивши пакети, якими клієнт шукає мережі, зловмисник може видавати себе за точку доступу цієї мережі; клієнт автентифікується і асоціюється з підробленою точкою, оскільки в WEP не здійснюється перевірка легітимності точки доступу [37]. Далі зловмиснику потрібно отримати зашифрований ARP- або IP-пакет. Отриманий пакет розбивають на фрагменти і переробляють у ARP-запит; множина таких запитів використовується для збору векторів ініціалізації WEP, необхідних для відомих методів відновлення ключа.

Атаки на злом секретного ключа переважно стосуються WEP, оскільки у цьому протоколі ключ є обчислюваним і для нього існують ефективні методи злому [37,40] Для протоколів WPA, WPA2 і WPA3 подібних атак значно менше: частіше застосовуються атаки перебором словникових фраз, а не безпосереднє обчислення ключа. У подальшому в цій роботі атаки, спрямовані на WEP, не розглядатимуться, оскільки протокол офіційно визнано вразливим і не

рекомендовано до використання. Натомість розроблюваний метод зможе відстежувати наявність WEP у захищуваній мережі і у разі виявлення видавати попередження про необхідність переходу на більш захищені протоколи [41].

1.4.2 Атаки відмови в обслуговуванні

Атаки типу Denial-of-Service (DoS) у безпровідних мережах найчастіше реалізуються через механізми керування та контролю стандартів IEEE 802.11. У мережах, що використовують ранні варіанти стандарту (попередні за 802.11n), такі атаки тривіальні в реалізації, оскільки службові (керуючі) кадри не шифруються [42].

Найнебезпечнішою з таких атак вважається атака кадрами деаутентифікації [43]. У стандартах IEEE 802.11 кадри деаутентифікації трактуються не як запити, а як повідомлення (notification), і будь-який пристрій, який отримав такий кадр, повинен на нього відреагувати. Тому ця атака легко здійснюється і має сильний ефект: при отриманні кадру деаутентифікації від імені точки доступу клієнт повинен негайно відключитися від безпровідної мережі без додаткових дій. Після цього ініціюється процедура повторної автентифікації та асоціації, під час якої клієнт не може передавати трафік. Постійна відправка кадрів деаутентифікації (флуд) унеможливлює користування мережею для жертв атаки. У разі використання широкомовних кадрів ефект поширюється на всі клієнтські пристрої мережі в радіусі дії зловмисника; їх одночасна повторна автентифікація на точці доступу може спричинити пікове навантаження в мережі. Типова схема DoS-атаки наведена на рис. 1.2.

Використання кадрів дисоціації підвищує час повторного підключення клієнта до мережі. Це пояснюється тим, що, всупереч стандарту (який після дисоціації вимагає лише процедури реасоціації для відновлення роботи), багато клієнтських пристроїв після отримання кадру дисоціації розривають з’єднання, надсилаючи потім кадри деаутентифікації і проходячи повні процедури автентифікації та асоціації заново. Флуд кадрами дисоціації виявляється ефективнішим за флуд кадрами деаутентифікації.

У роботах Mayank Agrawal та ін. запропоновано захист від DoS-атак кадрами деаутентифікації та кадрами управління енергозбереження PS-Poll [44]. Проте механізми, описані в цих дослідженнях, не застосовні для захисту від інших видів атак.

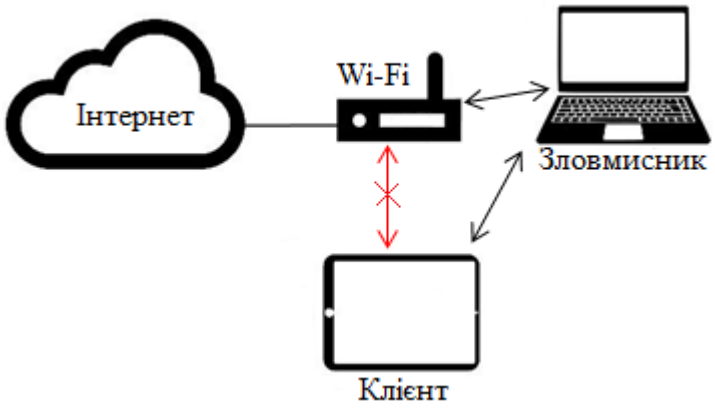

Рисунок 1.2 – Типовий сценарій DoS-атаки

1.4.3 Підроблені (фейкові) мережі

Підроблені мережі створюються зловмисниками з метою приваблення користувачів і проведення проти них різних атак. Зазвичай вони мають привабливі ESSID (назви), наприклад «Free WiFi», «Open» [45].

Підключившись до такої мережі, користувач робить увесь свій трафік доступним для зловмисника, що також відкриває шлях до атак на вищі рівні стеку (наприклад, перехоплення інтернет-сесій). На канальному рівні неможливо надійно визначити, чи є мережа підробленою; вторгнення в трафік користувача можуть виявити лише системи безпеки, що аналізують рівні вище. Користувач повинен підключатися тільки до довірених мереж.

1.4.4 Злий двійник (Evil Twin)

Злий двійник (Evil Twin) – це різновид підробленої мережі, що використовує той самий ESSID, що і легітимна мережа. Точка доступу зловмисника імітує сусідню точку реальної мережі. Ця атака експлуатує механізм,

за яким клієнтські пристрої зазвичай підключаються до точки з найсильнішим сигналом. Найчастіше такі атаки спрямовані проти відкритих мереж (кафе, аеропорти) або мереж, до яких у зловмисника вже є доступ (наприклад, мережа готелю). Після підключення клієнта до підробленої точки зловмисник отримує доступ до його трафіку і може проводити більш складні атаки [46].

1.4.5 Неконтрольована (зловмисна) точка доступу

Неконтрольовані точки доступу (Rogue Access Point) зазвичай організовують особи, що вже мають доступ до корпоративної або домашньої мережі (інсайдери). Такі точки створюються для отримання доступу до трафіку інших користувачів або для обходу частини механізмів безпеки підприємства (наприклад, обходу корпоративної автентифікації). Виявлення і відключення таких точок доступу є складним завданням у межах захищуваної мережі [47].

У випадку атак типу Man-in-the-Middle (MitM) у роботі Zhendong Wu запропоновано зміну методу автентифікації кінцевих пристроїв, але це рішення не завжди реалізовне на практиці.

Типова схема атак, заснованих на підробних мережах, атаках «злий двійник» та атаках із неконтрольованими точками доступу, наведена на рис. 1.3.

1.4.6 Атаки переустановки ключа (KRACK)

Атаки переустановки ключа (Key Reinstallation Attacks, KRACK) – це сукупність атак на WPA2, виявлених у 2016 році Mathy Vanhoef та Frank Piessens. Вони стали одним із головних чинників, що стимулювали розробку більш захищеного стандарту WPA3 [48].

Існує кілька варіантів реалізації цих атак, але суть полягає в тому, що клієнт повторно інсталює (переустановлює) ключі, унаслідок чого скидається вектор ініціалізації (IV). Це дає змогу зловмиснику, який перехопив повідомлення з таким самим IV, прочитати відправлене повідомлення. У випадку WEP і WPA також можливе впровадження (ін’єкція) трафіку зловмисником.

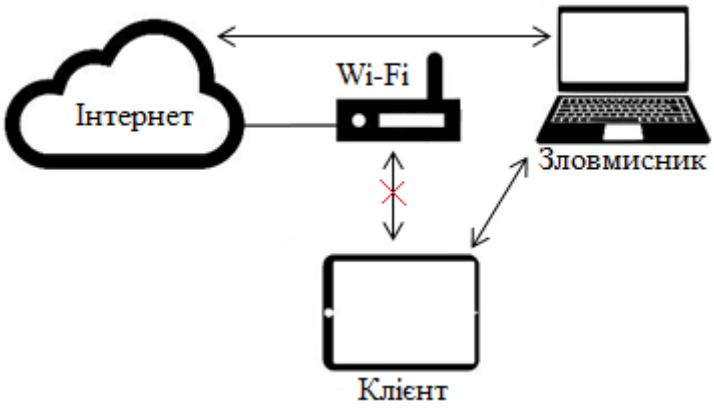

Рисунок 1.3 – Типова схема MitM-атаки

1.5 Постановка задачі

Безпровідні локальні мережі Wi-Fi, що базуються на протоколах IEEE 802.11, забезпечують підвищення мобільності співробітників в офісних і виробничих приміщеннях, сприяють зниженню витрат на монтаж і обслуговування дротових мереж, особливо у випадках, коли ремонтні роботи вже завершено, а кабельна інфраструктура спочатку не була передбачена.

Використання безпровідних локальних мереж Wi-Fi є доцільним на підприємствах із невеликою кількістю робочих місць або у випадках, коли активно застосовується значна кількість бездротових пристроїв – планшетів, ноутбуків, смартфонів, комунікаторів тощо. Найчастіше раціональною стратегією побудови мережі є комбіноване використання дротової та безпровідної інфраструктури, що дозволяє забезпечити гнучкість, масштабованість і зручність користування.

Основні переваги безпровідних мереж Wi-Fi полягають у наступному [15, 16]:

– простота та висока швидкість розгортання мережі;

– низька вартість встановлення;

– відсутність необхідності прокладання кабелів у робочих або житлових

приміщеннях (принаймні частково).

Основні недоліки технології Wi-Fi [15, 16]:

– обмежена пропускна здатність, що розподіляється між усіма пристроями, підключеними до однієї точки доступу. Наприклад, якщо маршрутизатор забезпечує швидкість 220 Мбіт/с, а до нього одночасно підключено два планшети, два смартфони та ноутбук (усього п’ять пристроїв), то середня швидкість для кожного становитиме приблизно 44 Мбіт/с. Насправді цей показник буде нижчим через службовий трафік, який займає 30–40 % каналу, тому реальна швидкість передавання даних може становити близько 26 Мбіт/с на пристрій;

– вплив навколишніх об’єктів, зокрема дерев, стін будівель або побутових приладів (наприклад, холодильників), що можуть погіршувати якість сигналу;

– низька надійність через відкритий характер передавання даних у повітряному середовищі, що створює можливість для атак у межах зони покриття точки доступу;

– низька стійкість до злому у разі неправильної конфігурації мережі.

Частково ці недоліки можна мінімізувати шляхом використання якіснішого та більш захищеного обладнання, а також об’єднанням кількох розташованих у різних приміщеннях точок доступу в єдину дротову мережу.

При розгортанні безпровідної мережі в домашніх умовах для підключення кількох ноутбуків, комп’ютера та мобільних пристроїв Wi-Fi є оптимальним варіантом за швидкістю впровадження та економічною доцільністю. Крім того, така мережа легко інтегрується з уже наявною дротовою інфраструктурою в приміщенні.

Для об’єднання віддалених локальних мереж або сегментів локальної мережі використовується обладнання з направленими антенами, що дозволяє збільшити дальність зв’язку до 20 км, а за використання підсилювачів та розміщення антен на значній висоті – до 50 км. При цьому як передавальні пристрої можуть застосовуватися звичайні Wi-Fi адаптери, оснащені спеціальними антенами (за умови, що це передбачено їх конструкцією).

Комплекси для об’єднання локальних мереж за топологією поділяються на «точка-точка» та «зірка». У топології «точка-точка» (режим Ad-hoc у стандарті IEEE 802.11) створюється радіоміст між двома віддаленими сегментами мережі. У топології «зірка» одна зі станцій виконує роль центрального вузла, який взаємодіє з кількома віддаленими станціями. Центральна станція обладнана всенаправленою антеною, тоді як периферійні станції – односторонніми (направленими) антенами.

Використання всенаправленої антени на центральній станції обмежує дальність зв’язку приблизно 7 км. Тому, якщо потрібно поєднати сегменти локальної мережі, розташовані на більшій відстані, застосовується принцип «точка-точка», що дозволяє побудувати кільцеву або складнішу топологію безпровідного зв’язку. [49-51]

У безпровідних мережах наявні певні специфічні особливості, які відсутні в дротових мережах. Ці особливості загалом впливають на продуктивність, доступність, безпеку та вартість обслуговування безпровідної мережі. Їх необхідно враховувати, навіть попри те, що вони безпосередньо не беруть участі у процесах шифрування чи автентифікації. Для вирішення подібних питань потрібен спеціалізований інструментарій та налагоджені механізми адміністрування й моніторингу мережі.

Доцільним рішенням є обмеження політикою безпеки доступу до мережі поза межами робочого часу (аж до фізичного вимкнення живлення точки доступу). Активність у безпровідній мережі в неробочий час має підлягати моніторингу, розглядатися як підозріла та бути об’єктом розслідування.

Якість функціонування безпровідної мережі Wi-Fi як радіоефірного середовища залежить від багатьох чинників. Одним із ключових є інтерференція радіосигналів, яка може суттєво знизити пропускну здатність і обмежити кількість користувачів, аж до повної неможливості використання мережі. Джерелом інтерференції може бути будь-який пристрій, наприклад маршрутизатор із надмірною потужністю випромінювання, що не допускається до вільного продажу та працює на тій самій частоті з достатньою інтенсивністю

сигналу. До таких джерел можуть належати як сусідні точки доступу, так і побутові прилади – наприклад, мікрохвильові печі. Цю особливість можуть також використовувати зловмисники для здійснення атак відмови в обслуговуванні (DoS) або для підготовки атак типу «людина посередині» (Man-in-the-Middle), блокуючи сигнали легітимних точок доступу й залишаючи лише власну з тим самим SSID (у ролі підробленої точки доступу).

Окрім інтерференції сигналів, безпровідним мережам властиві й інші специфічні особливості. Неправильно налаштований клієнтський термінал або несправна антена можуть істотно знизити якість обслуговування всіх користувачів мережі. Також актуальним є питання стабільності зв'язку: не лише сигнал маршрутизатора має досягати клієнта, але й сигнал клієнта повинен надходити до маршрутизатора. Оскільки потужність передавача маршрутизатора зазвичай у кілька разів вища, для досягнення симетрії може виникнути потреба знизити потужність його сигналу.

Для діапазону 5 ГГц слід враховувати, що стабільну роботу забезпечують лише чотири канали – 36, 40, 44, 48 (для Європи; у США дозволено ще п'ять додаткових каналів). На решті каналів активовано режим співіснування з радарами (DFS), унаслідок чого зв'язок між маршрутизатором і клієнтським пристроєм може періодично перериватися.

Описані вище механізми захисту та той факт, що не всі з них застосовуються в реальних мережах, залишають для зловмисників досить багато можливостей для проведення атак [49]. На сьогодні у відкритому доступі існує велика кількість готових інструментів для здійснення атак різного рівня складності на безпровідні мережі [50,51].

Багато рекомендацій щодо підвищення захищеності безпровідної мережі ґрунтуються на оновленні мікропрограмного забезпечення (прошивки) точок доступу [52]. Однак це не завжди можливо в масштабних мережах, а більшість користувачів не вважають таке оновлення необхідним [53].

Доступність подібних інструментів, недбале ставлення до застосування механізмів безпеки, а також відсутність у багатьох користувачів розуміння

принципів роботи безпровідної мережі створюють значну кількість потенційних загроз інформаційній безпеці [54].

Детальний аналіз атак на Wi-Fi мережі подано у дослідженні Kolias C. та ін. [3]. Автори оцінюють відомі атаки за рівнем їх застосовності та потенційною шкодою. Атаки, що становлять найбільшу загрозу відповідно до цього дослідження, будуть розглянуті у наступному розділі [55].

Окрім вивчення загроз безпровідних мереж, Kolias C. та співавтори наводять опис основних типів атак, достатніх для їх виявлення. Ці дані будуть використані у даній роботі під час розроблення сигнатур для нашого методу [3].

Нині існують рішення, що надають функціонал для аналізу трафіку та захисту безпровідних мереж, зокрема: Cisco Adaptive Wireless IPS, HP Mobility Security IDS/IPS, HP Software RFProtect, Zebra Technologies AirDefense.

Однак майже у всіх випадках їх функціональні можливості обмежуються виявленням менш ніж десяти типів атак. Крім того, відкритих платформних рішень із подібним функціоналом на даний момент не існує [56].

У зв’язку з постійним зростанням кількості користувачів безпровідних мереж та збільшенням обсягів передаваних даних питання забезпечення безпеки таких мереж набуває особливої актуальності. Існуючі рішення з аналізу трафіку та виявлення атак здебільшого мають обмежений функціонал, орієнтований на визначену кількість типових загроз, або є комерційними продуктами з закритим вихідним кодом, що ускладнює їх адаптацію під конкретні потреби.

Тому виникає необхідність власних розробок захисту для безпровідних мереж, яка б забезпечувала аналіз трафіку в реальному часі, виявлення ознак зловмисної активності та підвищення рівня інформаційної безпеки мережі.

Основним завданням роботи є створення методу, здатного здійснювати моніторинг трафіку безпровідної мережі, виявляти потенційні загрози на основі поєднання сигнатурного та статистичного аналізу та, таким чином, захищати від підроблених точок доступу.

2 РОЗРОБЛЕННЯ МЕТОДУ ЗАХИСТУ БЕЗПРОВІДНИХ МЕРЕЖ ВІД ПІДРОБЛЕНИХ ТОЧОК ДОСТУПУ

2.1 Математична модель процесу виявлення підроблених точок доступу

Враховуючи особливості атак в безпровідних мережах, для виявлення аномалій у безпровідному трафіку Wi-Fi було запропоновано застосування нейронної мережі у вигляді автокодера.

Автокодер виконує навчання на нормальних даних, створюючи стислий латентний простір, який дозволяє ефективно реконструювати вхідні пакети та одночасно виявляти відхилення від нормальної поведінки мережі [57,58,59].

Вхідними даними є вектор ознак пакета $x \in R^{20}$, що включає такі характеристики, як розмір пакета, частота, час між пакетами, MAC-адреси в числовому вигляді та протоколи передачі.

$$x = \begin{bmatrix} x_1 \\ x_2 \\ x_3 \\ \vdots \\ x_{20} \end{bmatrix} \in R^{20}, \tag{2.1}$$

де кожна компонента x_i відповідає окремій ознаці пакета.

Архітектура автокодера складається з енкодера та декодера, де кожен шар представлений повнозв’язним (Dense) шаром з функцією активації ReLU [60].

Енкодер:

1. Перший прихований шар: 20 → 16

$$h_1 = \mathrm{Re}\,LU(W_1 x + b_1), W_1 \in R^{16\times 20}, b_1 \in R^{16} \tag{2.2}$$

2. Другий прихований шар: 16 → 8

$$h_2 = \mathrm{Re}\,LU(W_2 h_1 + b_2), W_2 \in R^{8\times 16}, b_2 \in R^8 \tag{2.3}$$

3. Латентний шар: 8 → 4

$$z = h_3 = \mathrm{Re}\,LU(W_3 h_2 + b_3), W_3 \in R^{4\times 8}, b_3 \in R^4 \tag{2.4}$$

Декодер:

1. Перший прихований шар: 4 → 8

$$h_4 = \mathrm{Re}\,LU(W_4 z + b_4), W_4 \in R^{8\times 4}, b_4 \in R^8 \tag{2.5}$$

2. Другий прихований шар: 8 → 16

$$h_5 = \mathrm{Re}\,LU(W_5 h_4 + b_5), W_5 \in R^{16\times 8}, b_5 \in R^{16} \tag{2.6}$$

3. Вихідний шар: 16 → 20

$$\hat{x} = \sigma(W_6 h_5 + b_6), W_6 \in R^{20\times 16}, b_6 \in R^{20}, \tag{2.7}$$

де σ – лінійна функція, значення якої знаходяться в межах [0,1].

Функція втрат автокодера вимірює різницю між вхідним вектором ознак x та його реконструкцією $\hat{x}$. Обчислюється за формулою середньоквадратична помилка (MSE):

$$L = \frac{1}{N}\sum_{i=1}^{N}\left\|x_i - \hat{x}_i\right\|_2^2 \tag{2.8}$$

де N – кількість прикладів у вибірці. Чим менше значення L, тим точніше автокодер відтворює нормальний трафік. Високі значення помилки сигналізують

про аномалії.

Виявлення аномалій за допомогою автокодера базується на порівнянні вхідного пакета з його реконструкцією. Для нового пакету або потоку трафіку x_{new} різниця між початковим пакетом і реконструкцією вимірюється через похибку реконструкції:

$$AnomalyScore(x_{new}) = \left\| x_{new} - \hat{x}_{new} \right\|_2 \quad (2.9)$$

Якщо $AnomalyScore(x_{new}) > \tau$, пакет вважається аномальним. τ визначається, наприклад, як середнє арифметичне + 3 стандартні відхилення помилки реконструкції на нормальних даних.

Схематичне зображення автокодера наведено на рис. 2.1.

x (20) —► Dense(16, ReLU) —► Dense(8, ReLU) —► Dense(4, ReLU) = z

z —► Dense(8, ReLU) —► Dense(16, ReLU) —► Dense(20, Linear/Sigmoid) = x_hat

Вхід: 20 ознак пакета.

Латентний простір: 4 ознаки (стисле представлення нормального трафіку).

Реконструкція: 20 ознак, порівнюється з оригіналом для виявлення аномалій.

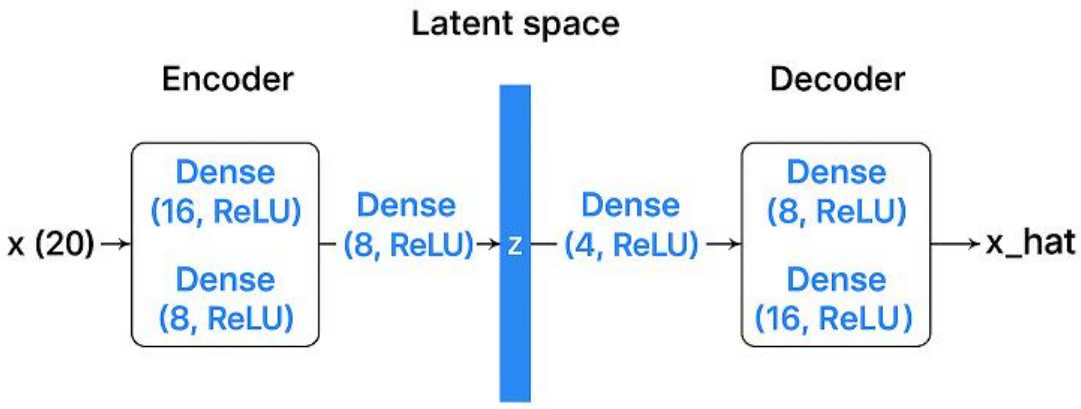

Рисунок 2.1 – Схематичне зображення автокодера

2.2 Вибір джерел даних для процесу виявлення підроблених точок доступу

Для вивчення та тестування атак і мережевих аномалій буде необхідне використання готових або створення нових наборів даних. Ці набори можуть бути представлені у вигляді вибірок певних полів трафіку в будь-якому форматі або у вигляді дампів мережевого трафіку у форматі pcap. Другий варіант є більш доцільним для дослідження, оскільки з часом він може виявити невідомі залежності в мережевому трафіку за різних умов.

Методи створення наборів даних, описані Вілелою, Дугласом В. Ф. Л. та іншими, застосовні у даній роботі [61, 62].

На основі вивчених мов програмування вибір основної мови розробки зупинено на C++ та Python. У таблиці 2.1 наведені основні критерії для порівняння.

У результаті порівняння було прийнято рішення використовувати мову програмування Python. Це інтерпретована, об’єктно-орієнтована мова високого рівня. Динамічна семантика та вбудовані складні структури даних роблять її найбільш придатною для створення прототипу розроблюваного рішення. Окрім того, Python широко використовується для взаємодії з мережею, що може позитивно вплинути на подальшу практичну застосовність розв’язку [63].

Таблиця 2.1 – Порівняння основних властивостей Python та C++

Параметр	Python	C++
Спосіб виконання	Інтерпретований	Компільований
Швидкість виконання	Низька	Висока
Швидкість розробки	Висока	Низька
Кросплатформенність	Так	Ні

Під аномалією в цій роботі розуміється вплив на мережу, здатний призвести до небажаних для користувача наслідків, наприклад до неможливості передати

дані. Оскільки розглядаються аномалії трафіку, під визначення не підпадають перешкоди в каналі та фізичний вплив на елементи мережі. В першу чергу оцінюється позаштатна поведінка безпровідного пристрою (що може вказувати на програмну помилку) та навмисні шкідливі впливи, включно з різними DoS-атаками, атаками типу «людина посередині» (Man-in-the-Middle) та атаками «злий двійник» (Evil Twin).

Для успішного перехоплення безпровідного трафіку повинні виконуватися наступні умови.

1. Сумісна операційна система. Для захоплення може використовуватися будь-яка UNIX-подібна операційна система. Також можливе використання Windows, однак кількість безпровідних адаптерів з робочими під цю ОС драйверами є суттєво обмеженою.

2. Безпровідний адаптер із підтримкою режиму монітора. Чіпи безпровідних адаптерів можуть працювати в кількох режимах: Infrastructure (бути кінцевою станцією для точки доступу), Ad-hoc (брати участь у одноранговій мережі), Master (виступати точкою доступу), Monitor (пасивно прослуховувати всі пакети у каналі). Для багатьох чіпів типовими є перші два режими, але для перехоплення трафіку необхідно, щоб чіп підтримував перехід у режим монітора. Драйвери, що забезпечують роботу адаптерів у цьому режимі, здебільшого створюються сторонніми розробниками, через що під Linux існує значно більше відповідних драйверів. Проте навіть за наявності робочого драйвера конкретний адаптер іноді може функціонувати в режимі монітора занадто повільно, непередбачувано або нестабільно. Адаптер також має підтримувати той же діапазон частот, що й захищена точка доступу; отже, якщо основна мережа працює в діапазоні 5 ГГц, адаптер повинен підтримувати цей діапазон.

3. Фізична платформа. У нашому арсеналі присутні точки доступу Avaya WLAN Access Point 8120 та контролер Avaya WLAN Controller 8180 [64, 65].

Обладнання може забезпечувати безпеку у кількох режимах:

– Access mode: клієнту надається доступ, при цьому скануються частоти

лише тих каналів, які використовуються в даний момент. У цьому режимі точки працюють за замовчуванням;

– Access-WIDS mode: клієнту надається доступ, одночасно скануються всі частоти в діапазоні 2,4/5 ГГц;

– WIDS Sentry mode: доступ клієнту не надається, скануються всі частоти в діапазоні 2,4/5 ГГц незалежно від регіональної прив'язки;

– WIPS Sentry mode: доступ клієнту не надається, крім повного сканування всіх частот у діапазоні 2,4/5 ГГц незалежно від регіональної прив'язки; виконуються активні дії проти несанкціонованих точок доступу та клієнтів, тобто вони нейтралізуються.

У всіх режимах інформація, отримана під час сканування, надсилається на контролер, який оновлюється з інтервалом 30 секунд.

4. Інформація про захищену точку доступу. Для успішної роботи необхідно знати канал, у якому транслює конкретна точка доступу, і прослуховувати трафік лише в цьому каналі. Якщо в мережі працює кілька точок доступу, для кожної з них потрібно встановлювати окремий виділений адаптер. Якщо відома лише назва мережі (ESSID), можна реалізувати автоматичний пошук точок доступу по кількох каналах і перейти до каналу з сильнішим сигналом. Оскільки на деяких точках (часто домашніх) для вибору каналу встановлений режим «auto», необхідна періодична перевірка наявності точки у поточному прослуховуваному каналі.

Основним об'єктом аналізу будуть мережні кадри (канальний рівень моделі OSI). Також буде досліджено додатковий заголовок Radiotap, у який пакет інкапсулюється приймаючим адаптером. Далі розглядаються основні протоколи, застосовні в методі, що розробляється.

Radiotap – це протокол, який надає додаткову інформацію про прийнятий кадр [66]. Якщо драйвер приймаючого адаптера підтримує цей протокол, кадр буде інкапсульований у нього під час прийому. У полях цього протоколу передається додаткова інформація, наприклад, рівні шуму та сигналу, номер

антени, частота каналу, швидкість передачі, чи фрагментований кадр, чи прикріплена до нього контрольна сума, а також часовий маркер моменту прийому кадру. Крім того, протокол дозволяє розширювати цей заголовок і додатково визначати власні поля.

Приклад заголовку Radiotap

0x00: Version: 0

0x01: Pad: 0

0x02-0x03: Length: 18

0x04-0x07: Present flags: TSFT, Flags, Rate, Channel, dBm Antenna Signal

0x08-0x0F: TSFT: 123456789

0x10: Flags: 0x10

0x11: Rate: 6 Mbps

0x12-0x13: Channel frequency: 2412 MHz

0x14-0x15: Channel type: 0x0080

0x16: Antenna signal: -40 dBm

0x17: Antenna: 1

Пояснення полів:

Version – версія заголовка Radiotap (завжди 0).

Pad – вирівнювання байтів.

Length – довжина заголовка Radiotap у байтах.

Present flags – біти, що вказують, які поля присутні.

TSFT – часовий штамп у мікросекундах.

Flags – флаги пакета (наприклад, чи фрагментовано).

Rate – швидкість передачі.

Channel frequency/type – частота та тип каналу.

Antenna signal – рівень сигналу в дБм.

Antenna – номер антени, яка прийняла пакет.

Заголовок канального рівня в бездротових мережах Wi-Fi визначається стандартами IEEE 802.11. Він визначає тип та підтип переданого кадру, його напрямок, а також чи передається кадр повторно та чи зашифрований він. До цього заголовка включаються MAC-адреси пристроїв, що беруть участь у передачі (в окремих випадках до чотирьох адрес). Це основний заголовок, який необхідно перевіряти при пошуку службових кадрів, наприклад, кадрів деаутентифікації. Оскільки в різних сценаріях у бездротових мережах передаються серії кадрів різних підтипів, відстеження цього поля дозволяє, наприклад, визначити, що новий пристрій підключився до мережі або перейшов до сусідньої точки доступу.

Приклад кадру Wi-Fi:

Frame Control: 0x08 0x01 (Data frame, ToDS=1, FromDS=0)

Duration: 0x013a

Address 1 (DA): 00:11:22:33:44:55

Address 2 (SA): 66:77:88:99:aa:bb

Address 3 (BSSID): 00:11:22:33:44:55

Sequence Control: 0x1001

Data (Payload): [IP packet / TCP segment / HTTP data ...]

FCS: 0x5e4f3a2b

Пояснення полів:

Frame Control – 2 байти, вказує тип кадру, підтип, прапорці.

Duration/ID – 2 байти, час заняття середовища або ідентифікатор.

Address 1 – 6 байт, адреса призначення.

Address 2 – 6 байт, адреса джерела.

Address 3 – 6 байт, адреса BSS, наприклад MAC точки доступу.

Sequence Control – 2 байти, номер послідовності та номер фрагменту.

Address 4 – 6 байт, використовується в режимі WDS.

Data/ Payload – змінний, передані дані, наприклад IP-пакет.

FCS – 4 байти, контрольна сума для перевірки цілісності кадру.

Кадри керування – це окремий тип кадрів 802.11, який визначає такі сценарії, як асоціація та реасоціація з точкою доступу, дисоціація, автентифікація та деаутентифікація, а також операції, що відповідають за інші службові транзакції в бездротовій мережі. Весь заголовок поділяється на дві частини: фіксовані параметри, що містять різну інформацію залежно від підтипу кадру, та теговані параметри. У тегованих параметрах визначаються, наприклад, назва мережі (SSID), яку транслює точка доступу; доступні швидкості передачі; інші можливості пристрою; а також інформація про виробника, яка визначається довільно. Ці кадри визначають взаємодію точки доступу та клієнта в мережі. Наприклад, кадри деаутентифікації відправляються точкою доступу клієнту, коли вона хоче розірвати з'єднання. Також такий кадр може бути відправлений клієнтом точці доступу для повідомлення про припинення з'єднання. Кадри-маяки періодично надсилаються точкою доступу, оголошуючи про її присутність у мережі та можливі параметри підключення. Коли клієнт шукає певну мережу, він відправляє запити зондування (Probe Request). Якщо такі кадри відправляються без конкретної адреси на широкомовлення, клієнт дізнається про всі точки доступу поблизу.

Кадри контролю в бездротових мережах керують доступом пристроїв до середовища передачі. До цього типу належать кадри таких підтипів: Запит на передачу (Request to Send, RTS), Дозвіл на передачу (Clear to Send, CTS), Підтвердження (Acknowledgement, ACK), Контроль енергозбереження (Power-Save Poll, PS-Poll). Наприклад, при увімкненому механізмі RTS/CTS клієнт повинен надіслати кадр RTS і запросити дозвіл на зайняття радіосередовища перед передачею кадру даних. Якщо кінцевий пристрій підтримує механізм PS-Poll, точка доступу зберігатиме кадри, спрямовані цьому пристрою, у буфер поки він неактивний. Як тільки пристрій вийде з режиму енергозбереження, він надішле кадр PS-Poll точці доступу, запитуючи кадри, адресовані йому. Інтервали, протягом яких пристрій відключається та увімкнеться, визначаються

виробником пристрою.

2.3 Алгоритм виявлення підроблених точок доступу в безпровідних мережах

Етапи алгоритму є наступними:

1. Збір даних. Сенсори в режимі monitor пасивно збирають management-фрейми і мережеву телеметрію (beacon, probe, RSSI, канал, BSSID, SSID, прапори шифрування, DHCP/DNS індикації та ін.).

2. Агрегація та попередня обробка. Агрегація подій за BSSID у часовому вікні 30; формування вектору ознак на основі отриманих пакетів (rssi_mean, rssi_std, channel, beacon_interval, num_clients, auth_mode, oui_match, dhcp_flag, dns_redirect_flag тощо).

3. Швидка перевірка. Чи є явна підозра за простими правилами (наприклад, SSID відомий, але BSSID невідомий; відкритий SSID там, де зазвичай WPA2; OUI не співпадає; одночасна поява однакового SSID на нестандартному каналі). Так → позначити запис як ПІДОЗРІЛИЙ і перейти до блоку Інференс автокодера. Ні → перейти до блоку Інференс автокодера.

4. Інференс автокодера. Пропущення нормалізованого вектору через натренований автокодер; отримання реконструкції і обчислення функції втрат.

5. Оцінка порогів. Чи менша помилка за середнє арифметичне + 3 стандартні відхилення помилки реконструкції? Так → позначити трафік, як НОРМАЛЬНИЙ та перейти на етап Логування і збереження для статистики. Ні → позначити трафік, як ВИСОКИЙ РИЗИК та перейти далі.

6. Мітигація. Сповіщення адміністратора з доказами (PCAP, час, RSSI, логи); тимчасове блокування трафіку від підозрілого BSSID на NAC; оновлення правила на контролері Wi-Fi.

7. Логування і збереження для статистики. Створення запису про подію і повернення до етапу Збір даних.

2.4 Структура мережі з модулем виявлення підроблених точок доступу

У провідній мережі фільтрувальний пристрій безпеки зазвичай розташовується перед шлюзом, через який проходить трафік. Таким чином, шкідливий та небажаний трафік не покидає меж локальної мережі.

Однак у бездротовій мережі немає можливості встановити фільтрувальний пристрій між клієнтським пристроєм і маршрутизатором, оскільки вони не з'єднані обмеженим фізичним середовищем. Передані радіохвилі, навіть якщо їх перехопить фільтрувальний пристрій, все одно досягнуть клієнтського пристрою через кілька моментів. Це робить превентивну реакцію на шкідливий трафік у бездротовій мережі неможливою.

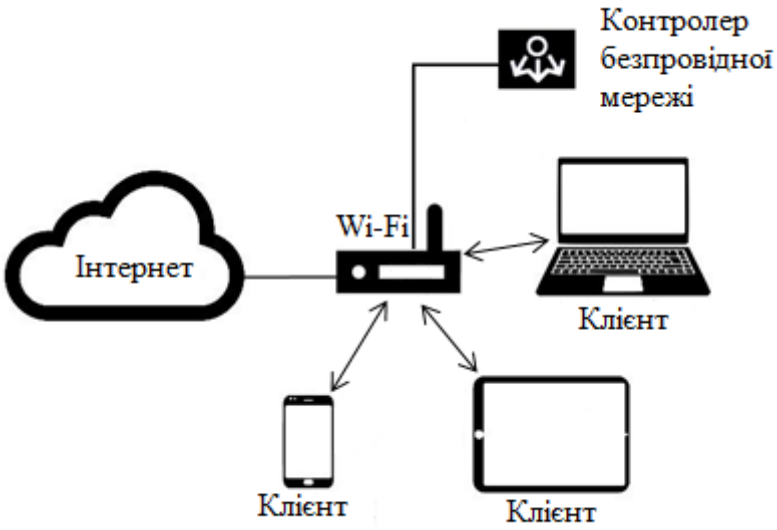

Рисунок 2.2 – Приклад інтеграції контролера в мережу

Для аналізу трафіку в мережі пропонується використовувати контролер Avaya WLAN Controller 8180 для захоплення трафіку, який буде керувати точкою доступу.

Реалізація ділиться на апаратну частину, що включає Avaya WLAN Access

Point 8120, контролер Avaya WLAN Controller 8180, безпровідний адаптер, і програмну частину, що включає операційну систему, драйвери бездротового адаптера та розроблену програму на мові Python. Розглянемо цю програму.

Її можна поділити на кілька логічних компонентів – джерело трафіку, аналізатор трафіку, перевіряючий агент та правила безпеки.

Для захоплення трафіку бездротовий інтерфейс повинен бути переведений у режим моніторингу. Для цього виконуються наступні команди:

ifconfig wlan0 down

iwconfig wlan0 mode monitor

ifconfig wlan0 up

Для успішної конфігурації можуть знадобитися додаткові команди (наприклад, перезапуск мережевого сервісу) залежно від використовуваного адаптера та операційної системи.

Після цього інтерфейс потрібно встановити в той же канал, в якому працює точка, яка захищається. Дізнатися його можна з налаштувань точки, коли він виставлений вручну, або за допомогою цих команд:

netsh wlan show all # в Windows

iwlist wlan0 scanning # в Linux

Виставити інтерфейс у потрібний канал можна командою:

iwconfig wlan0 channel <номер каналу>

Далі в програмі створюється «сирий» сокет, який приймає пакети, не обробляючи їх у мережевому стеку:

s = socket.socket (socket.AF_PACKET, socket.SOCK_RAW, socket.htons (ETH_P_ALL))

s.bind((‘wlan0’, 3))

Тут:

socket.AF_PACKET – сімейство адрес у Linux, що дозволяє відкритому сокету передавати дані безпосередньо в застосунок, минаючи обробку мережевим стеком операційної системи;

socket.SOCK_RAW – тип сокета, дає доступ до даних нижчих рівнів; *socket.htons(ETH_P_ALL))* – тип протоколів, які ми хочемо отримувати. У даному випадку позначає всі вхідні протоколи.

Виклик функції *recv()* надалі на цьому сокеті буде повертати необроблені мережеві пакети, включаючи той канальний рівень, який передбачає використовуваний адаптер. У нашому випадку обробку пакета починатимемо з протоколу Radiotap для отримання додаткової інформації про середовище передачі під час прийому.

2.5 Аналізатор трафіку

Усі мережеві пакети можна розкласти на сукупність протоколів і полів цих протоколів. Крім цього, часто зустрічаються складні поля, наприклад, прапорові. Кожну таку ознаку можна представити у вигляді шляху по пакету – від протоколу до назви поля і його значення. В результаті кожен мережевий пакет можна представити у вигляді набору пар «шлях-значення».

Розкладання бінарних даних, захоплених у мережі, на описані вище або аналогічні логічні структури називається парсингом. Відповідно виникає питання вибору парсера з готових або створення власного.

Насамперед розглядався найпопулярніший модуль Python для роботи з мережевими пакетами, включаючи їх парсинг і створення. Scapy – це програма та бібліотека для маніпуляцій пакетами, яка здатна декодувати велику кількість протоколів, надсилати та захоплювати пакети, а також відстежувати сесії.

Клас пакета в Scapy має складну структуру з численними додатковими полями, включаючи прогнозування вкладеного протоколу, посилання на

вищестоящий протокол, поля за замовчуванням, словник із назвами полів тощо. Весь клас імітує словник, до протоколів якого можна звертатися за назвою протоколу, але до деяких полів вкладених протоколів можна звертатися й безпосередньо, якщо ці поля мають унікальну назву.

Dpkt – модуль для Python, який його творці позиціонують як швидкий і легковаговий інструмент для парсингу та створення пакетів, що підтримує базові протоколи стеку TCP/IP. Класи dpkt справді простіші, ніж у Scapy, і використовують слоти для реєстрації полів, на відміну від словників, як у Scapy.

Слоти – це механізм Python, який замінює динамічну реєстрацію атрибутів класу на основі словників на список заздалегідь визначених атрибутів. Ця технологія дає різний виграш у часі залежно від використовуваної версії Python.

Крім того, у класах dpkt майже немає загальних додаткових полів, окрім поля data, в якому зберігається вкладений протокол або бінарні дані вкладення. Через цю особливість при використанні dpkt немає можливості безпосередньо отримати доступ до вкладених протоколів та їхніх полів.

Тому для роботи з dpkt, за аналогією з класами модуля, був створений шаблонний клас пакета, який розкриває всі присутні в пакеті протоколи в однорівневу структуру, надаючи таким чином прямий доступ до вкладених протоколів.

2.5.1 Власні класи

Після вивчення підходів до парсингу пакетів сторонніх модулів було вирішено написати власний парсер. Перша його версія використовувала прості класи з вкладеними підкласами для складних полів. Після парсингу всі протоколи зберігаються як атрибути основного класу пакета. Звернення до полів відбувається через атрибути класу. Було реалізовано протоколи: Radiotap, IEEE802.11, IEEE802.11 Management, LLC, ARP, IPv4, UDP, DHCP, IEEE802.1x, EAP. Цей набір протоколів використовується й у подальших версіях парсера. Дану реалізацію надалі будемо називати «custom_class».

Надалі створені класи були модернізовані за рахунок використання слотів

для строгого обмеження можливих атрибутів кожного класу. За замовчуванням кожен клас у Python використовує прихований словник для зберігання власних атрибутів, який ініціалізується при створенні екземпляра класу. Однак, якщо для класу оголошені слоти, такого словника створено не буде. Натомість Python виділить ресурси під фіксовану кількість атрибутів, які перераховані в слотах. Дану реалізацію надалі будемо називати «custom_slots».

Реалізовані класи виявилися громіздкими та погано масштабованими, тому було вирішено створити уніфіковані протоколи з більш простим присвоєнням атрибутів. Оскільки розробка здійснюється мовою Python, основним типом даних було обрано словник. Словники в Python дуже оптимізовані, пошук елемента за ключем має складність O(1) і не залежить від розміру словника.

Тому було вирішено створити функції для кожного окремого протоколу, які розкривали б усі поля та їх підполя в однорівневий словник. Те саме відбувається на рівні пакета — усі поля всіх протоколів складаються в один загальний словник, де ключем є повний шлях до поля пакета. З точки зору перевірки полів такий підхід значно простіший за класовий – немає необхідності перевіряти наявність атрибутів-полів у класі перед перевіркою їх значення. У випадку зі словником ми просто перевіряємо наявність поля та можемо одразу отримати значення потрібного поля.

У даній реалізації в якості загальної точки використовується клас пакета зі слотами, всередині якого окремими атрибутами зберігаються час пакета, список протоколів, номер протоколу канального рівня та основний словник. Це допомагає спростити звернення до складних атрибутів. Однак усі ці елементи можна перенести всередину словника, відмовившись від використання класів. Дану реалізацію надалі будемо називати «custom_dict».

Приклад пакета, розкладеного в словник:

```
for k, v in packet.fields.items():
    print(k, ":", v)
radiotap.version: 0
```

radiotap.pad: 0

radiotap.length: 18

radiotap.present: 18471

radiotap.Flags.short_preamble: 0

radiotap.Flags.bad_fcs: 0

radiotap.Flags.fcs_at_end: 0

radiotap.Flags.fragmentation: 0

radiotap.Flags.wep: 0

radiotap.Flags.preamble: 0

radiotap.data_rate: 2

radiotap.channel.frequency: 2437

Цей клас використовується як загальний для реалізації аналізатора на словниках. У ньому поєднані технології словників для зберігання полів класу та слотів для звернення до загальних атрибутів усіх пакетів.

```
class NetworkPacket:
    __slots__ = 'attributes', 'protocol_list', 'link_type', 'timestamp', 'raw_data'
    def __init__(self, raw_pkt):
        self.timestamp = None
        self.attributes = {}
        self.protocol_list = []
        self.link_type, self.timestamp, self.raw_data = raw_pkt
        payload = (LINK_LAYER_TYPES[self.link_type], self.raw_data)
        while payload:
            proto, data, *extras = payload
            temp_attrs, payload, *extras = PROTOCOL_PARSERS[proto](data, *extras)
            if payload[0] in ('MALFORMED', 'TO_DECRYPT', 'UNKNOWN'):
                payload = None
```

```
            for key, value in temp_attrs:
                self.attributes[f"{proto}.{key}"] = value
            self.protocol_list.append(proto)
        def get_field(self, field_name, default=None):
            return self.attributes.get(field_name, default)
        def get_timestamp(self):
            return datetime.fromtimestamp(float(self.timestamp))
        def summary(self) -> str:
            summary_parts = [f"[{self.get_timestamp()}]"]
            for proto in self.protocol_list:
                if proto_summary := PROTOCOL_SUMMARIES[proto](self.attributes):
                    summary_parts.append(proto_summary)
            return " | ".join(summary_parts)
```

Приклади правил, використаних для аналізу трафіку:

```
[  {
    "rule_name":"DEAUTH_ATTACK",
"triggers":[{"path":"dot11.type","operator":"==","value":0},{"path":"dot11.subtype","
operator":"==","value":12}],
    "responses":[{"action":"print","message":"{{packet_count}} packets at
{{radiotap.dbm_antenna_signal}} dBm"}],
    "limit":100,"check_interval":60,"expire":300  },
  {
    "rule_name":"PSPOLL_ATTACK",
"triggers":[{"path":"dot11.type","operator":"==","value":1},{"path":"dot11.subtype","
operator":"==","value":10}],
    "responses":[{"action":"print","message":"{{packet_count}} packets at
{{radiotap.dbm_antenna_signal}} dBm"}],
    "limit":100,"check_interval":5,"expire":300  },
  {
```

"rule_name":"WEP_ACCESS_POINT",

"triggers":[

{"path":"dot11.type","operator":"==","value":0},

{"path":"dot11.subtype","operator":"==","value":8},

{"path":"dot11mgmt.fixed.capabilities","operator":"==","value":1},

{"path":"dot11mgmt.tagged.rsn_information","operator":"is_none","value":null}

],

"responses":[{"action":"print","message":"AP {{dot11.bssid}} in network {{dot11mgmt.tagged.ssid}}"}],

"limit":5,"check_interval":1,"expire":3600 }]

Порівняння різних властивостей вивчених реалізацій представлено в табл.2.2.

Таблиця 2.2 – Порівняння різних реалізацій аналізатора

Критерій	Scapy	Dpkt	Custom _class	Custom _slots	Custom _dict
Кількість протоколів, які підтримуються	917	68	12	12	12
Додавання нових протоколів	так	ні	так	так	так
Типи значень	Власні типи	int або bytes	int або bytes	int або bytes	int або bytes
Передбачуваність парсинга	Поля залежні від вкладення	Поля залежні від вкладення	Вкладення в полі Payload	Вкладення в полі Payload	Вкладення в явному вигляді
Доступність протоколів	Перевірка наявності	Протоколи вкладені	Окремий список	Окремий список	Окремий список
Доступність полів	Перевірка наявності	Перевірка наявності	Порожнє значення	Порожнє значення	Порожнє значення
Обробка пошкоджених пакетів	До пошкодженого протоколу	Ні	Ні	До пошкодженого протоколу	До пошкодженого протоколу

З розглянутих реалізацій неможливо однозначно обрати одну для подальшої розробки, спираючись лише на основні характеристики. Тому потрібне більш глибоке вивчення та проведення тестування продуктивності представлених реалізацій.

2.6 Висновки до розділу

У другому розділі було розроблено, обґрунтовано та представлено метод захисту безпровідних мереж від підроблених точок доступу, заснований на поєднанні методів аналізу трафіку, машинного навчання та глибокої нейронної мережі типу автокодера.

На основі проведеного аналізу загроз безпеці безпровідних локальних мереж Wi-Fi визначено, що атаки типу Evil Twin, Man-in-the-Middle та інші різновиди створення фальшивих точок доступу залишаються одними з найнебезпечніших, оскільки дають змогу зловмиснику отримати контроль над користувацьким трафіком і доступ до конфіденційних даних. У зв’язку з цим виникла необхідність розроблення методу моніторингу трафіку в реальному часі, здатного своєчасно виявляти такі загрози та мінімізувати ризики компрометації мережевої інфраструктури.

У межах розділу було запропоновано математичну модель процесу виявлення підроблених точок доступу, побудовану на принципі навчання автокодера на вибірці нормального трафіку. Автокодер формує стислий латентний простір ознак і дозволяє визначати аномалії за величиною похибки реконструкції вхідних даних. Такий підхід забезпечує адаптивність до нових типів атак і не потребує попереднього формування бази сигнатур, що є перевагою порівняно з класичними сигнатурними методами виявлення вторгнень.

Було обґрунтовано вибір мови програмування Python як основної для реалізації методу. Python забезпечує високу швидкість розробки, наявність потужних бібліотек для аналізу даних і машинного навчання (Scapy, dpkt,

TensorFlow, NumPy, Keras), а також гнучку інтеграцію з мережевими інтерфейсами та апаратними засобами.

Розроблено алгоритм виявлення підроблених точок доступу, який включає такі основні етапи: збір і агрегація трафіку з бездротового інтерфейсу в режимі монітора; попередня обробка та формування вектора ознак пакета; первинна фільтрація підозрілих подій за простими евристичними правилами (аналіз SSID, BSSID, OUI, режиму шифрування тощо); пропускання векторів через навчений автокодер і розрахунок похибки реконструкції; п отриманої похибки з пороговим значенням (середнє + 3σ); класифікація трафіку як нормального або аномального; реагування – сповіщення адміністратора, ізоляція підозрілої точки доступу, запис журналу подій.

Запропонована структура передбачає поєднання апаратної складової (контролер Avaya WLAN 8180, точки доступу Avaya WLAN 8120, бездротовий адаптер у режимі монітора) та програмного модуля, який виконує парсинг і аналіз трафіку. Така архітектура дозволяє забезпечити моніторинг безпеки мережі на рівні канального протоколу (Radiotap, IEEE 802.11) і створити основу для розгортання розробленого методу в реальному середовищі.

Окрему увагу приділено розробленню власного парсера мережевих пакетів, який формує уніфіковану словникову структуру даних замість громіздких класових ієрархій сторонніх бібліотек. Це рішення спрощує доступ до полів протоколів, підвищує швидкість обробки пакетів і забезпечує гнучкість при масштабуванні.

Таким чином, результати, отримані в другому розділі, свідчать про ефективність запропонованого підходу до виявлення підроблених точок доступу на основі гібридного аналізу мережевого трафіку. Створена математична модель і алгоритм є основою для подальшої програмної реалізації, тестування та оптимізації розробленого методу.

Розроблений метод має потенціал подальшого розвитку – зокрема, для впровадження у вигляді розподіленої системи сенсорів безпеки, інтеграції з корпоративними платформами управління інформаційною безпекою (SIEM), а

також для застосування у середовищах із великою кількістю IoT-пристроїв.

3 ЕКСПЕРИМЕНТАЛЬНА ПЕРЕВІРКА ТА ОЦІНКА ЕФЕКТИВНОСТІ РОЗРОБЛЕНОГО МЕТОДУ

3.1 Тестування парсерів

Для тестування швидкодії парсерів без впливу сторонніх факторів (швидкості радіоінтерфейсу, активності в мережі тощо) експерименти проводилися на дампах трафіку. З цією метою в публічній мережі було зібрано дамп і розділено його на окремі файли розміром від 20 до 50 тисяч кадрів.

Далі п’ятьма різними реалізаціями було здійснено читання кожного з дампів і парсинг пакетів без виконання додаткового аналізу. Для кожного запуску проведено вимірювання часу обробки, обчислено середні значення отриманих результатів та виконано нормування показників.

Середні значення результатів тестування наведено у таблиці 3.1.

Таблиця 3.1 – Середні значення результатів тестування

	Середній час обробки дампа	Середній програш відносно мінімального	Середня кількість пакетів в секунду	Середній виграш відносно мінімального
Scapy	36.05	34.76	1425.76	1.00
Dpkt	3.42	2.34	19062.91	15.41
Custom_class	2.34	1.29	26263.61	16.07
Custom_slots	2.03	1.00	36721.83	31.76
Custom_dict	2.89	1.83	20507.84	16.37

Згідно з отриманими результатами, власний парсер на класах зі слотами виявився найшвидшим (пікова швидкість його обробки досягає 50 000 пакетів за секунду), тоді як парсер Scapy працює майже у 33 рази повільніше.

Такий розрив у швидкодії пояснюється тим, що складна структура Scapy

передбачає широкий спектр застосувань — зокрема, створення пакетів на основі класів і виконання мережевих дій високого рівня. Натомість власний парсер розроблено виключно для розкладання пакета на класові структури, без додаткових функцій формування або відправлення трафіку.

Крім того, кількість підтримуваних протоколів у власному парсері значно менша, ніж у сторонніх бібліотек.

Окрім тестування швидкодії створення класу (або словника) та ініціалізації його атрибутів, необхідно також провести тестування швидкості доступу до значень полів пакета.

3.2 Реалізація структури сигнатур

Для коректної роботи етапу методу, що здійснює сигнатурний аналіз, необхідно мати базу описів атак, які він має виявляти. Такі описи називаються сигнатурами. Залежно від типу атаки сигнатури можуть містити різні дані та відстежувати цілий набір характерних ознак.

Співпадіння однієї або кількох таких ознак із відомим набором правил свідчитиме про наявність атаки.

Розглянемо структуру об’єкта правил. Кожен такий об’єкт включає: найменування для ідентифікації; список умов, які перевіряються у досліджуваному пакеті; список дій, що виконуються у випадку, якщо пакет відповідає всім умовам.

Кожна умова містить три основні складові: шлях, оператор і значення. Шлях визначає поле пакета, значення якого підлягає перевірці, і складається з ієрархічної послідовності: протокол → поле → вкладене поле (за потреби).

Оператор описує тип порівняння, яке необхідно виконати, і може набувати таких значень: == – строго дорівнює; != – не дорівнює; > – більше; >= – більше або дорівнює; < – менше; <= – менше або дорівнює; *y* – наявність поля або протоколу в пакеті; *n* – відсутність поля або протоколу в пакеті.

За потреби перелік операторів може бути розширений.

Значення записується у вільній, але максимально уніфікованій формі. Інтерпретація цього значення перед порівнянням покладається на перевіряючого агента.

Для зберігання сигнатур було обрано мову розмітки JSON, оскільки вона є уніфікованою та зручною для обробки різними системами. Це, однак, накладає певні обмеження на типи даних, які можуть використовуватися як значення, що перевіряються.

Зокрема, без попереднього перетворення неможливо напряму використовувати вбудований тип *bytes* мови Python, у якому зберігаються двійкові дані. У форматі JSON допустимими типами є: цілі та дробові числа, рядки, списки, словники, булеві значення, а також порожній об’єкт *null*.

Кожне співпадіння пакета з набором правил призводитиме до виконання дій, визначених для конкретного правила. У прототипі список дій обмежений підрахунком спрацьовувань та виведенням короткого опису спрацювавшого кадру, проте в реальних системах цей перелік легко можна розширити. Зокрема, пропонується використовувати відправлення інформації на сервер журналів подій, відправлення команд або попереджень контролеру безпровідної мережі та пристрою безпеки, надсилання команд безпосередньо точці доступу (наприклад, занесення певної MAC-адреси до «чорного списку»), а також відправлення кадрів деаутентифікації зловмиснику за наявності вільного радіоінтерфейсу. Окрім того, деякі мережеві пакети можна зберігати для подальшого дослідження.

Після розроблення структури правил було здійснено тестування з різною кількістю активних правил. Для тестування використовувалися прості правила з однією умовою, що перевіряє окреме поле певного протоколу. Перевіряючий агент спроєктовано так, що при першому невідповідності умови перевірка всього правила переривається; отже, у межах тестування більш складні правила дали б менш точні дані. Результати тестування наведено в таблицях 3.2 та 3.3.

На підставі отриманих даних можна зробити висновок, що реалізації з використанням власних класів демонструють найбільше зростання часу при

впровадженні перевірки пакетів. Це свідчить про те, що звертання до атрибутів цих класів є неефективним.

Таблиця 3.2 – Середній час обробки

	При 1 правилі	При 10 правилах	При 100 правилах	При 1000 правилах
Scapy	36.12	40.80	88.07	547.66
Dpkt	3.54	3.88	7.24	40.10
Custom_class	2.42	2.75	6.18	42.30
Custom_slots	2.12	2.46	6.02	43.17
Custom_dict	2.98	3.18	5.04	23.40

Таблиця 3.3 – Середній приріст часу на обробки пакетів

	При 1 правилі	При 10 правилах	При 100 правилах	При 1000 правилах
Scapy	100.80%	113.86%	240.36%	1484.07%
Dpkt	105.89%	120.20%	261.35%	1650.34%
Custom_class	107.18%	132.17%	392.83%	3149.01%
Custom_slots	109.06%	142.56%	491.32%	4146.62%
Custom_dict	105.61%	116.14%	215.63%	1200.03%

Незважаючи на те, що при невеликій кількості правил реалізація на Scapy демонструє найменше зростання часу обробки, а при великій кількості програє лише реалізації на словниках, загальний час обробки для цієї реалізації все одно у десятки разів перевищує показники інших варіантів. Тому дана реалізація не братиме участі в подальшому тестуванні.

Реалізація на Dpkt також показує відносно невелике зростання часу, і в разі неможливості створення власного модуля може бути використана. Проте складність додавання нових протоколів і досить низькі показники продуктивності

роблять її менш придатною, ніж власні реалізації.

За великої кількості правил чітко проявляється перевага безкласової реалізації на словниках — вона демонструє найменше зростання часу обробки. На рисунку 3.1 наведено динаміку зростання часу обробки для різних реалізацій. Видно, що реалізація на словниках стає швидшою за реалізацію на класах зі слотами вже при 50 правилах, а швидшою за реалізацію на звичайних класах – при 36 правилах.

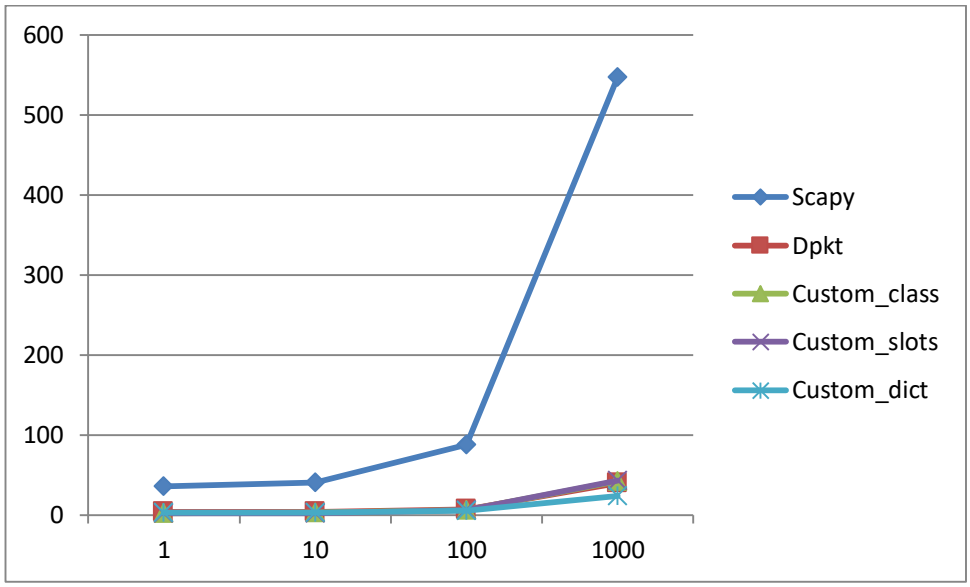

Рисунок 3.1 – Ефективність обробки різних реалізацій

Виходячи з результатів тестування, було прийнято рішення подальшу реалізації методу здійснювати на основі реалізації парсера зі словниками, оскільки зростання затримки під час його використання є повільнішим, ніж у інших варіантів. Це, у перспективі, має суттєвий вплив на масштабованість і практичну придатність розробленого рішення.

Окрім простої перевірки полів пакета, для деяких типів атак необхідно також враховувати статистичні параметри трафіку. У найпростішому випадку можна брати до уваги кількість пакетів за певний проміжок часу. При такому підході межі того, яка кількість пакетів, що відповідають правилу, вважається нормальною, а яка – аномальною, встановлюються вручну на основі попередніх

досліджень і лабораторних експериментів.

Наприклад, виявлення 100 кадрів дисоціації протягом однієї хвилини може свідчити про можливу DoS-атаку.

Крім того, у деяких ситуаціях після спрацювання правила його необхідно тимчасово деактивувати. Для цього вводиться параметр *timeout*. Після спрацювання такого правила воно стає неактивним на кількість секунд, зазначену у цьому параметрі.

Приклад правила з додатковими параметрами:

"name": "EXAMPLE",

"conditions": [...],

"actions": [...],

"target": 3,

"interval": 0.01,

"timeout": 100

Це правило спрацьовує, коли прийнято 3 пакети, що відповідають умові, за 0,01 секунди, після чого воно відключається на 100 секунд.

Нижче наведено приклад повного правила для DoS-атаки кадрами дисоціації. Шукаються кадри протоколу 802.11 типу 0 (керування), підтипу 5 (дисоціація). При виявленні 10 таких кадрів протягом 30 секунд правило виведе в консоль інформацію про спрацювання та буде відключене на 10 хвилин:

{"name": " DEATH_FLOOD", "conditions": [

{ "pth": "dot11.type",

"act": "==",

"val": 0},

{"pth": "dot11.subtype",

"act": "==",

"val": 5}],

"target": 10,

"interval": 30,

"timeout": 600,

"actions": [{ "act": "print", "obj": null}],}

3.3 Середовище для тестування

Для захоплення низькорівневого мережевого трафіку необхідні спеціалізовані драйвери. У межах тестового стенда використовується бездротовий адаптер TP-Link Archer T4U. У його останній ревізії застосовується чипсет RTL8822BU.

Як операційну систему тестового стенда обрано Ubuntu. Із додаткового програмного забезпечення, окрім драйверів бездротового адаптера, встановлено Python версії 3.8.

Для тестування був організований стенд зі наступною архітектурою. В якості уразливої точки доступу виступала точка Avaya WLAN Access Point 8120. Для перших двох атак вона працювала в режимі WPA2-PSK без додаткових захисних механізмів, потім для тестування третього правила вона була переведена в режим WEP. MAC-адреса точки 04:95:e6:97:9a:a5.

В якості клієнта виступав ноутбук на базі Ubuntu, MAC-адреса 86:46:04:f5:56:98.

В якості зловмисника виступав ноутбук на базі Kali Linux з безпровідним адаптером. Для здійснення DoS-атаки кадрами деаутентифікації використовувалась утиліта aireplay-ng, вбудована в дистрибутив Kali Linux. Для DoS-атаки кадрами PS-Poll був написаний скрипт на Python, що використовував модуль Scapy для ін’єкції пакетів.

В якості контролера виступав Avaya WLAN Controller 8180.

Почнемо налаштування. Створимо радіопрофіль для режиму Sentry з інтервалом сканування 1 мілісекунда.

WC8180>en

WC8180#conf t

WC8180(config)#wireless

WC8180(config-wireless)#radio-profile 3 wids-wips both

WC8180(config-radio-profile)#rf-scan band both duration 1

WC8180(config-radio-profile)#exit

Тепер прикріпимо цей профіль до обох радіомодулів точки за допомогою профілю точки. До речі, точка 8120 має два радіомодулі, і режим Sentry можна призначити лише одному з них.

WC8180(config-wireless)#ap-profile 7

WC8180(config-ap-profile)#radio 1 profile-id 3

WC8180(config-ap-profile)#radio 2 profile-id 3

WC8180(config-ap-profile)#radio 1 enable

WC8180(config-ap-profile)#radio 2 enable

WC8180(config-ap-profile)#exit

Застосовуємо ці налаштування до конкретної точки:

WC8180(config-wireless)#domain ap CC:F9:54:99:5B:20

WC8180(config-domain-ap)#profile-id 7

WC8180(config-domain-ap)#end

Тепер додаємо дружні точки доступу за таким шаблоном. Для цього потрібно детально вказати їх бездротові параметри:

wids known-ap <mac_address> channel <0 - 216>

wids known-ap <mac_address> security {any | open | wep | wpa}

wids known-ap <mac_address> ssid <ssid_string>

wids known-ap <mac_address> type {known-foreign | localenterprise | other}

wids known-ap <mac_address> wds-mode {any | bridge | normal}

wids known-ap <mac_address> wired-mode {allowed | notallowed}

Налаштовуємо WIDS для ворожих точок.

wids rogue-ap ack {all | rogue_mac_address}

wids rogue-ap trap-interval <60 - 3600>

wids rogue-ap wired-detection-interval <1 - 3600>

3.4 Експериментальна перевірка розробленого методу

Для перевірки було організовано три потоки трафіку, кожен з яких містив 10000 пакетів, з яких 5000 були нормальними, а 5000 мали ознаки того чи іншого класу атаки. Всього було протестовано три атаки: DoS, MITM та EvilTwin.

Загальна вимога до задовільності вирішення задачі, яку виконує розроблюваний метод захисту від підроблених точок доступу, може бути виражена за допомогою відомих і поширених показників якості класифікації:

– TP (True Positive) – кількість випадків, коли метод правильно ідентифікував точку доступу як підроблену;

– FP (False Positive) – кількість випадків, коли метод визначив точку доступу як підроблену, хоча насправді вона є легітимною;

– TN (True Negative) – кількість випадків, коли метод правильно розпізнав легітимну точку доступу як безпечну;

– FN (False Negative) – кількість випадків, коли метод не виявив підроблену точку доступу, помилково класифікувавши її як легітимну.

Класичним синонімом FP є помилки першого роду, а FN – помилки другого роду.

На рисунку 3.2 подано схематичне представлення множин: множина реально наявних підроблених точок доступу позначена червоним колом, множина точок, виявлених алгоритмом – зеленим колом; біла область навколо кіл відповідає легітимним (дозволеним) точкам доступу. Перетин червоного та зеленого кіл відповідає правильно виявленим підробленим точкам (True Positive, TP). Відсутність кіл у відповідній області (біла область) означає коректну

ідентифікацію легітимних точок як безпечних (True Negative, TN). Частина реально підроблених точок, що не потрапила в зелений круг, є пропусками алгоритму (False Negative, FN – помилки другого роду). Частина легітимних точок, що помилково була віднесена алгоритмом до підроблених, утворює помилкові спрацьовування (False Positive, FP – помилки першого роду, «помилкова тривога»).

Рисунок 3.2 – Графічна інтерпретація метрик якості роботи розробленого методу

Результати тестування представлені у таблиці 3.4

Таблиця 3.4 – Порівняння результатів виявлення атак

Тип трафіку	Всього пакетів	TP	TN	FP	FN
Нормальний + DoS	10000	4000	4200	800	1000
Нормальний + MITM	10000	4400	4500	500	600
Нормальний + EvilTwin	10000	4800	4700	300	200

Якість виявлення підроблених точок доступу методом можна оцінити за допомогою інших, більш зрозумілих для інтерпретації показників: повноти, точності, акуратності, помилки та *F*-міри.

Повнота (*r*) характеризує здатність методу виявляти всі підроблені точки доступу, не враховуючи кількість хибних спрацьовувань. Її можна обчислити як частку правильно виявлених підроблених точок серед усіх фактичних підроблених точок доступу:

$$r = \frac{TP}{TP + FN} \times 100\% \tag{3.1}$$

Точність (*p*) показує здатність методу виявляти лише підроблені точки доступу, не помилково класифікуючи легітимні точки як шкідливі. Вона визначається як частка правильно ідентифікованих підроблених точок серед усіх точок, які позначено як підроблені:

$$p = \frac{TP}{TP + FP} \times 100\% \tag{3.2}$$

Акуратність (*a*) характеризує загальну здатність методу приймати правильні рішення під час класифікації точок доступу. Вона визначається як частка правильно класифікованих підроблених і легітимних точок серед усіх перевірених точок:

$$a = \frac{TP + TN}{TP + FP + FN + TN} \times 100\% \tag{3.3}$$

Помилка (*e*), навпаки, характеризує здатність методу приймати неправильні рішення під час класифікації. Її значення дорівнює частці хибно класифікованих точок серед усіх перевірених:

$$e = \frac{FP + FN}{TP + FP + FN + TN} \times 100\% \quad (3.4)$$

F-міра (*f*) зазвичай використовується для узагальненої оцінки якості методу з урахуванням одночасно повноти та точності. Вона визначається як відношення подвоєного добутку повноти та точності до їх суми:

$$f = \frac{2 \times p \times r}{p + r} \times 100\% \quad (3.5)$$

Завдяки наведеним показникам розроблений метод виявлення підроблених точок доступу може бути об’єктивно порівняний як із найближчими аналогами, так і з її власними модифікаціями в процесі подальшого вдосконалення.

Значення показників за кожним типом аналізу трафіку наведено у таблиці 3.5.

Таблиця 3.5 – Результати показників ефективності методу

Тип трафіку	Повнота	Точність	Акуратність	Помилка	*F*-міра
Нормальний + DoS	80%	83.33%	82%	18%	81.67%
Нормальний + MITM	88%	88.79%	89%	11%	88.85%
Нормальний + EvilTwin	96%	94.12%	95%	5%	95.06%

За результатами обчислень видно, що ефективність розробленого методу зростає від першого до третього сценарію, що зумовлено як характером атак, так і особливостями ознак, які аналізує алгоритм.

У випадку DoS-атак метод демонструє достатньо стабільні, але не максимальні показники. Це пояснюється тим, що DoS-атаки створюють велику кількість коротких кадрів управління (наприклад, deauthentication), які частково можуть накладатися на легітимну активність мережі – особливо при великій кількості користувачів. Через це метод має вищий рівень хибних спрацьовувань та пропусків атак. Попри це, результат у понад 80% *F*-міри вважається задовільним для прототипу методу в режимі реального часу.

Під час симуляції атаки Man-in-the-Middle метод показав вищу ефективність, ніж у попередньому сценарії. Це пов’язано з тим, що MITM-атаки мають характерні сигнатурні ознаки – повторення MAC-адрес, дублювання BSSID, нетипові часові мітки та аномалії у структурі кадрів управління. Завдяки поєднанню сигнатурного аналізу з перевіркою статистичних характеристик (кількість сесій, тривалість, частота кадрів), алгоритм зміг точніше відокремити аномальні пакети від звичайного трафіку, зменшивши як кількість хибних спрацьовувань, так і пропусків атак. Отриманий результат *F*-міри ≈ 89% свідчить про високу збалансованість між точністю та повнотою виявлення.

Найвищі показники метод продемонстрував під час виявлення підроблених точок доступу (Evil Twin). Такий результат пояснюється тим, що алгоритм у цьому режимі аналізує комплекс ознак – SSID, BSSID, частоту, тип шифрування, потужність сигналу та послідовність радіоканалів. Ці параметри мають сталі закономірності у легітимній мережі, тому відхилення від нормального профілю легко ідентифікуються. Мінімальні значення хибних спрацьовувань та пропусків атак свідчать про високу точність класифікації та низьку ймовірність помилкових рішень. Це підтверджує ефективність запропонованого поєднання сигнатурного підходу з нейронною мережею-автокодером для аналізу безпровідного трафіку.

3.5 Навантажувальне тестування розробленого методу

Далі було проведено навантажувальне тестування. Воно проходило у два етапи. Перший етап проводився під час захоплення трафіку в реальній мережі з кількома пристроями.

Правила для цих тестів представляють собою структури, близькі до реальних правил, але не спрямовані на виявлення якихось конкретних атак. Вони були згенеровані автоматично з метою коригування завантаження реалізації.

Ми порівняли завантаження центрального процесора при різній кількості активних правил для пошуку. Оскільки реалізоване рішення працює в одному процесі, усе навантаження припадало на одне з чотирьох ядер станції. Максимальне завантаження (25 %) досягалося вже при 1130 активних правилах.

На другому етапі тестування досліджували пропускну спроможність запропонованої реалізації. Для цього з реальних мереж було зібрано 19 дампів різного розміру. Потім для різної кількості правил визначали середню кількість пакетів за секунду та відношення реального часу до часу обробки (таблиця 3.6).

Таблиця 3.6 – Тестування пропускної здатності

Параметр	При 1 правилі	При 10 правилах	При 100 правилах	При 1000 правилах
Середня кількість пакетів за секунду	24313	9498	1244	126
Середнє співвідношення реального часу до часу обробки	5196.73	1881.67	226.23	20.30
Мінімальне співвідношення реального часу до часу обробки	21.94417	7.286031	0.27535	0.016607

Метод також досягає граничного навантаження при великій кількості активних правил, однак успішно справляється з обробкою декількох десятків правил, що робить її практично придатною для використання.

3.6 Висновки до розділу

У третьому розділі проведено експериментальне дослідження функціонування розробленого методу виявлення підроблених точок доступу та інших атак на безпровідні мережі Wi-Fi, а також оцінено її ефективність за основними кількісними показниками точності класифікації.

Було створено тестовий стенд, який моделює реальні умови роботи Wi-Fi-мережі з використанням різних пристроїв і типів атак. У якості апаратної основи використано точку доступу Avaya WLAN Access Point 812, контролер Avaya WLAN Controller 8180, ноутбук зі встановленою Kali Linux для генерації атак і мобільний пристрій на базі Android як легітимного клієнта. Для реалізації атак типу DoS застосовувалася утиліта aireplay-ng, для атаки Man-in-the-Middle та Evil Twin – сценарії, створені з використанням бібліотеки Scapy.

На основі зібраних дампів мережевого трафіку було проведено серію експериментів, спрямованих на визначення повноти (Recall), точності (Precision), акуратності (Accuracy), помилки (Error) та F-міри (F1-score) розробленого методу.

Розрахунки показали:

– для DoS-атак: F-міра ≈ 0,82, точність 83 %, повнота 80 %;

– для Man-in-the-Middle-атак: F-міра ≈ 0,89, точність 90 %, повнота 88 %;

– для “Evil Twin”-атак: F-міра ≈ 0,95, точність 94 %, повнота 96 %.

Отримані результати свідчать, що запропонований метод забезпечує високу ефективність виявлення атак різних типів, причому найкращі показники досягнуто під час визначення підроблених точок доступу. Це пояснюється наявністю у таких атак стійких характеристичних ознак (SSID, BSSID, параметри

шифрування, частота, потужність сигналу), що дає змогу з високою достовірністю виявляти відхилення від нормальної поведінки мережі.

Під час виявлення DoS-атак результати були дещо нижчими через високу динаміку трафіку та можливе перекриття шкідливих кадрів із легітимними, однак навіть у цьому випадку метод продемонстрував стабільну роботу з F-мірою понад 80 %.

Таким чином, проведені експерименти підтвердили, що розроблений метод на основі поєднання сигнатурного аналізу з нейронною мережею-автокодером здатна ефективно виявляти основні типи безпровідних атак, має високу точність (до 95 %), низьку частоту помилкових спрацьовувань, та може бути використана як основа для побудови розподілених WIDS/WIPS-рішень у корпоративних і публічних мережах Wi-Fi.

У результаті експериментальної перевірки підтверджено коректність математичної моделі і практичну придатність запропонованого методу. Отримані дані можуть бути використані для подальшої його оптимізації, адаптації до нових стандартів (Wi-Fi 6/6E) та інтеграції в комплексні засоби моніторингу кібербезпеки.

ВИСНОВКИ

Поставлена в роботі мета розробити метод виявлення підроблених точок доступу та інших аномалій у безпровідному трафіку Wi-Fi у реальному часі підтвердила свою практичну та наукову значущість. Поширення безпровідних технологій, поява великої кількості IoT-пристроїв і розвиток складних сценаріїв атак (Evil Twin, Man-in-the-Middle, DoS) роблять необхідним створення ефективних підходів до автоматичного виявлення аномалій на рівні мережевого трафіку.

Запропонований метод базується на комбінованому застосуванні сигнатурного та статистичного аналізу з використанням нейронної мережі-автокодера для виявлення аномалій за похибкою реконструкції. Такий гібридний підхід дозволяє:

– виявляти відомі типи атак (за допомогою сигнатур) з високою точністю;

– одночасно реагувати на нові або варіативні атаки (за допомогою автокодера, який фіксує відхилення від нормальної поведінки трафіку).

Розроблено математичну модель автокодера з чітко визначеною архітектурою та критерієм виявлення аномалій, заснованим на середньоквадратичній помилці реконструкції. Обґрунтовано вибір порогу детекції як mean + 3σ по розподілу помилок на навчальній (нормальній) вибірці, що забезпечує статистично обґрунтований компроміс між чутливістю та стійкістю моделі до шумів.

Запропоновано уніфіковану схему представлення пакета у вигляді вектору ознак, що включає поля Radiotap і IEEE 802.11 (частота, канал, рівень сигналу, типи кадрів, часові інтервали тощо). Для опису сигнатур розроблено JSON-орієнтовану структуру правил: шлях → оператор → значення, що забезпечує гнучкість і сумісність з різними мовами та інструментами.

Метод був апробований на лабораторному стенді і на дампах реального трафіку. Проведені експерименти з імітацією трьох класичних сценаріїв атак дали наступні результати (за показником *F*-міри):

– DoS (кадри деаутентифікації/дисоціації): F ≈ 0.82;

– Man-in-the-Middle: F ≈ 0.89;

– Evil Twin (підроблені точки доступу): F ≈ 0.95.

Отримані значення вказують на те, що розроблений метод забезпечує високу збалансованість між повнотою та точністю детекції, особливо для завдань ідентифікації підроблених точок доступу.

Експериментально встановлено, що поєднання сигнатурного аналізу (для швидкого виявлення характерних шаблонів) з автокодером (для виявлення нетипових відхилень) дає переваги перед суто сигнатурними або суто статистичними підходами. Метод показав прийнятні показники як для сценаріїв з очевидними сигнатурами (Evil Twin), так і для складніших, динамічних випадків (DoS, MITM), хоча в останніх випадках необхідні додаткові механізми пост-обробки для зниження FP та FN.

Наразі метод має певні обмеження:

– чутливість до якості та репрезентативності навчальної вибірки для автокодера (неправильне або недостатнє навчання може призвести до підвищеної кількості помилок);

– залежність від можливостей апаратури (підтримка режиму монітора, стабільність захоплення трафіку у 2.4/5 ГГц);

– потенційні складнощі при масштабуванні в умовах дуже щільних середовищ із великою кількістю одночасних клієнтів і точок доступу, які потребуватимуть оптимізації продуктивності обробки.

Розроблений метод може бути використаний як складова WIDS/WIPS-рішень: його можна інтегрувати у сенсорні вузли (режим monitor) для попереднього аналізу та передавання тривожних подій до централізованого контролера або SIEM. Метод придатний для застосування в навчальних закладах, на підприємствах і в публічних мережах з метою підвищення безпеки користувацьких сесій.

Пропонований метод має широку перспективу розвитку:

– розширення ознакового простору з урахуванням метаданих вищих рівнів стеку (TCP/HTTP) для покращення детекції MITM-сценаріїв;

– застосування більш складних архітектур автокодерів (згорткові, рекурентні, варіаційні автокодери) для кращого відображення часових та просторових залежностей у трафіку;

– інтеграція з механізмами автоматичного реагування (WIPS) для реалізації політик блокування або ізоляції підозрілих точок доступу;

– адаптація під стандарти Wi-Fi 6/6E та робота в умовах широкого використання OFDMA і MU-MIMO;

– дослідження застосування методів федеративного навчання для збереження приватності при колективному навчанні моделей на даних кількох організацій.

Результати роботи підтвердили припущення про доцільність гібридного підходу: комбінування сигнатурного аналізу з автокодером забезпечує надійний та адаптивний метод виявлення підроблених точок доступу й інших аномалій у безпровідних мережах. Розроблений метод має наукову новизну, апробований експериментально та володіє високою практичною цінністю як основа для подальших розробок у сфері безпеки Wi-Fi.

ПЕРЕЛІК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Cisco Systems. Cisco Annual Internet Report (2018-2023) White Paper. Cisco, 2020. 60 p.

2. International Telecommunication Union (ITU). The State of Broadband 2021: People-Centred Broadband. Geneva: ITU, 2021. 48 p.

3. Kolias C., Kambourakis G., Gritzalis S. Intrusion detection in 802.11 networks: empirical evaluation of threats and a public dataset // IEEE Communications Surveys & Tutorials. 2016. Vol. 18, No. 1. P. 184-208.

4. PwC. The Economic Value of Wi-Fi: A Global View 2021-2025. PwC, 2021. 36 p.

5. ITWeek. Чому варто інвестувати в бездротову мережу компанії. ITWeek, 2023. URL: https://itweek.com.ua/2023/06/20/chomu-varto-investuvaty-v-bezdrotovu-merezhu-kompaniyi (дата звернення: 06.11.2025).

6. Kyivstar Hub. Ми в онайлн: як і чому інтернет став базовою потребою для бізнесу та життя. Kyivstar, 2025. URL: https://hub.kyivstar.ua/articles/internet-yak-neobhidnist-dlya-biznesu-ta-povsyakdennogo-zhyttya (дата звернення: 06.11.2025).

7. Телекомунікаційні системи та мережі: навчальний посібник/ Укладачі: Микитишин А.Г., Митник М.М., Стухляк П.Д. Тернопіль: Тернопільський національний технічний університет імені Івана Пулюя, 2017. 384 с.

8. Holt A., Huang C.-Y. 802.11 Wireless Networks: Security and Analysis. Springer, 2010. 256 p.

9. Roshan P., Leary J. 802.11 Wireless LAN Fundamentals. Cisco Press, 2009. 320 p.

10. Rao S.S.N., Aruna O., Lakshminadh K. Mobile ad hoc network integrated wireless networks: a survey// International Journal of Engineering and Technology. 2018. Vol. 10, № 4. P. 125-134.

11. Mohammadani K., Kazi H., Channa I., Vasan D. A survey on Integrated Wireless Network Architectures// International Journal of Computer Applications. 2013. Vol. 79, № 4. P. 1-8.

12. Gast M. 802.11® Wireless Networks: The Definitive Guide. O'Reilly Media, 2005. 608 p.

13. Jurdak R. (ed.). Wireless Ad Hoc and Sensor Networks: A Cross-Layer Design Perspective. Springer, 2007. 356 p.

14. Stallings W. Wireless Communications & Networks. Pearson, 2013. 520 p.

15. Scarfone K., Mell P. Guide to Intrusion Detection and Prevention Systems (IDPS). NIST Special Publication 800-94, 2007. 86 p.

16. Northcutt S., Novak J. Network Intrusion Detection. New Riders, 2002. 688 p.

17. Bejtlich R. The Practice of Network Security Monitoring: Understanding Incident Detection and Response. No Starch Press, 2013. 528 p.

18. Hacking for Dummies /Kevin Beaver. 6th ed. Hoboken, NJ: John Wiley & Sons, 2018. 576 p.

19. IEEE Standards Association. The Evolution of Wi-Fi Technology and Standards. IEEE SA, 2023.

20. GeeksforGeeks. Wi-Fi Standards Explained. GeeksforGeeks, 2019.

21. Tektronix. Wi-Fi: Overview of the 802.11 Physical Layer and Transmitter Measurements. Tektronix, 2018.

22. Wikipedia contributors. IEEE 802.11a-1999. Wikipedia, 2024. URL: https://en.wikipedia.org/wiki/IEEE_802.11a-1999 (дата звернення: 06.11.2025).

23. Dell Inc. Wi-Fi Standards: IEEE 802.11ac, 802.11ax, and Wireless Internet Overview. Dell Support, 2023.

24. Безпека WiFi: історія небезпеки WEP, WPA і WPA2 // e-server.com.ua. 29 квіт. 2024. Режим доступу: https://e-server.com.ua/uk/poradi/bezpeka-wifi-istoriia-nebezpeki-wep-wpa-i-wpa2 (дата звернення: 06.11.2025).

25. Типи шифрування Wi-Fi: що використовують сучасні роутери // ipnet.ua. 07 серп. 2025. Режим доступу: https://ipnet.ua/blog/typy-shyfruvannia-wi-fi-shcho-vykorystovuiut-suchasni-routery (дата звернення: 06.11.2025).

26. Lashkari, A. H., Danesh, M. M. S., Samadi, B. A survey on wireless security protocols (WEP, WPA and WPA2/802.11i). University of Malaya / Multimedia

University, Malaysia, 2009. Режим доступу: SciSpace.

27. José Perez. A survey of wireless network security protocols. Texas A&M University Corpus Christi, 2008. Режим доступу: ccsc.org.

28. Mahmoud Khasawneh, Izadeen Kajman, Rashed Alkhudaidy, Anwar Althubyani. A Survey on Wi-Fi Protocols: WPA and WPA2. 2014. Режим доступу: SpringerLink.

29. Lashkari A. H., Danesh M. M. S., Samadi B. A survey on wireless security protocols (WEP, WPA and WPA2/802.11i) / University of Malaya / Multimedia University. Malaysia, 2009. С. 1-15.

30. Perez J. A survey of wireless network security protocols / Texas A&M University Corpus Christi. 2008. С. 1-12.

31. Khasawneh M., Kajman I., Alkhudaidy R., Althubyani A. A Survey on Wi-Fi Protocols: WPA and WPA2. Springer, 2014. С. 45-62.

32. Indira Reddy B., Srikanth V. Review on Wireless Security Protocols (WEP, WPA, WPA2 & WPA3)/ Int. J. Sci. Res. in Computer Science, Eng. & Info. Technology. 2019. Vol. 5, No. 4. С. 112-125.

33. Anita C. Eluwa Trends in Wireless Network Security / Scientific Research Publishing. 2022. С. 23-38.

34. Sari A. Comparative Analysis of Wireless Security Protocols: WEP vs WPA. 2014. С. 7-21.

35. Halbouni A., Ong L.-Y., Leow M.-C. Wireless Security Protocols WPA3: A Systematic Literature Review / IEEE Access. 2023. С. 1005-1020.

36. Wang Z., Feng X., Li Q., Sun K., Yang Y., Li M., Du G., Xu K., Wu J. Off-Path TCP Hijacking in Wi-Fi Networks: A Packet-Size Side Channel Attack / arXiv preprint. 2024. С. 1-15.

37. Vanhoef M., Piessens F. Key Reinstallation Attacks: Forcing Nonce Reuse in WPA2 // ACM CCS. 2017. С. 1315-1328.

38. Vanhoef M. Key Reinstallation Attacks: Breaking the WPA2 Protocol // Black Hat Europe. 2017. С. 1-20.

39. Tews E. Attacks on the WEP protocol (PTW) / Diploma technical report.

2007. С. 1-40.

40. Beck M., Tews E., Weinmann R. Practical attacks against WEP and WPA. 2008. С. 1-18.

41. Aircrack-ng documentation: PTW attack / Aircrack-ng Project. 2024 (оновлення). С. 1-10.

42. Schepers D., et al. On the Robustness of Wi-Fi Deauthentication Countermeasures // WiSec Workshop. 2022. С. 1-14.

43. Caneill M. Attacks against the Wi-Fi protocols WEP and WPA (overview: FMS, KoreK, PTW, fragmentation, replay). 2010. С. 1-28.

44. Sethuraman S. C., et al. Intrusion detection for wireless: Wifiphishing, Evil-Twin and Rogue AP detection // IET Networks. 2019. С. 100-115.

45. Natkaniec M., et al. Wireless Local Area Networks Threat Detection Using 1D-CNN // Sensors. 2023. С. 1-18.

46. Гарист А. В. Аналіз захищеності Wi-Fi мереж // Інформатика, обчислювальна техніка та автоматизація. 2021. № 2 (1). С. 97112. DOI: 10.32838/2663-5941/2021.2-1/16.

47. Агаєв М., Петров І. Виявлення атак деаутентифікації та дисоціації у Wi-Fi мережах // Вісник інформаційної безпеки. 2020. №3. С. 45–58.

48. Alamanni M. What we can learn from attacks on the WEP protocol // Packt Learning How To Tutorials. 2014. С. 1-12.

49. Chatzoglou E., Kambourakis G., Kolias C. How is your Wi-Fi connection today? DoS attacks on WPA3-SAE // Journal of Information Security and Applications. – 2022. Vol. 64. Art. 103058. Режим доступу: https://www.sciencedirect.com/science/article/pii/S221421262100243X

50. Aircrack-ng development team. Aircrack-ng – Wi-Fi security auditing tools suite. Project website, documentation, tools (airmon-ng, aireplay-ng, airbase-ng, aircrack-ng). Режим доступу: https://www.aircrack-ng.org/

51. Kismet Developers. Wireless network detector, sniffer, WIDS. Project website and documentation. Режим доступу: https://www.kismetwireless.net/

52. Wifiphisher/ P0cL4bs et al. Rogue Access Point Framework (phishing,

Evil-Twin automation). GitHub repository. Режим доступу: https://github.com/wifiphisher/wifiphisher

53. P0cL4bs / wifipumpkin3. WiFi-Pumpkin3 framework for rogue AP / MiTM attacks. GitHub repository. Режим доступу: https://github.com/P0cL4bs/wifipumpkin3

54. Chalhoub G., et al. But is it exploitable? Exploring how Router Vendors Implement (or Fail to Implement) Security Updates // Usenix / ACM/NDSS / Preprint (case studies on router firmware updates & user behaviour). 2023. Режим доступу: https://www.georgechalhoub.com/pdf/chalhoub-exploitable2023.pdf

55. Brightwood S. The Importance of Secure Firmware Updates in Maintaining System Integrity. 2024. Режим доступу: https://www.researchgate.net/publication/384687421_The_Importance_of_Secure_Firmware_Updates_in_Maintaining_System_Integrity

56. Pandit P. A Study of Security Tools for Wireless Networks: Kismet, Aircrack-ng, Wifiphisher, WiFi-Pumpkin та ін. Technical Report. Oct. 2021. DOI: 10.13140/RG.2.2.34511.20640.

57. Sakurada M., Yairi T. Anomaly Detection Using Autoencoders with Nonlinear Dimensionality Reduction // Proceedings of the 2014 Workshop on Machine Learning for Cyber Security (MLCS'14). New York: ACM, 2014. P. 4:1-4:7. URL: https://dl.acm.org/doi/10.1145/2685128.2685299 (дата звернення: 06.11.2025).

58. Mirsky Y., Doitshman T., Elovici Y., Shabtai A. Kitsune: An Ensemble of Autoencoders for Online Network Intrusion Detection // Network and Distributed System Security Symposium (NDSS'18). 2018. URL: https://www.ndss-symposium.org/ndss2018/ndss-2018-programme/kitsune-ensemble-autoencoders-online-network-intrusion-detection/ (дата звернення: 06.11.2025).

59. Sethi A., Wang Z., Lin D., Liu Y. Analysis of Autoencoders for Network Intrusion Detection // Applied Sciences. – MDPI, 2021. 11(12): 5678. URL: https://www.mdpi.com/2076-3417/11/12/5678 (дата звернення: 06.11.2025).

60. TensorFlow. Intro to Autoencoders. TensorFlow documentation, 2025. URL: https://www.tensorflow.org/tutorials/generative/autoencoder (дата звернення: 06.11.2025).

61. Vilela D. W. F. L., Lotufo A. D. P., dos Santos Junior C. R. Fuzzy ARTMAP Neural Network IDS Evaluation applied for real IEEE 802.11w database // ResearchGate, 2018. URL: https://www.researchgate.net/publication/328401833_Fuzzy_ARTMAP_Neural_Network_IDS_Evaluation_applied_for_real_IEEE_80211w_data_base (дата звернення: 06.11.2025).

62. Vilela D. W. F. L., et al. A dataset for evaluating intrusion detection systems in IEEE 802.11 wireless networks. KTH Royal Institute of Technology, 2014. URL: https://kth.diva-portal.org/smash/get/diva2%3A1350710/FULLTEXT02.pdf (дата звернення: 06.11.2025).

63. Scapy – packet manipulation program / Philippe Biondi. — Scapy documentation, 2025. URL: https://scapy.readthedocs.io/en/latest/introduction.html (дата звернення: 06.11.2025).

64. Avaya WLAN Access Point 8120. Installation AP 8120. [Електронний ресурс]. Режим доступу: https://fcc.report/FCC-ID/X7CAP8120/1308982.pdf. Назва з екрана.

65. Avaya WLAN Controller 8180. Datasheet. [Електронний ресурс]. Режим доступу: https://cdn-docs.av-iq.com/dataSheet/8180_Datasheet.pdf. Назва з екрана.

66. Wireless Developers Documentation. About Radiotap [Електронний ресурс]. – Режим доступу: (https://wireless.docs.kernel.org/en//developers/documentation/radiotap.html). – Дата звернення: 06.11.2025.

ДОДАТОК А.
СПИСОК ПУБЛІКАЦІЙ

Міністерство освіти і науки України
Хмельницький національний університет

ЗБІРНИК НАУКОВИХ ПРАЦЬ
за матеріалами XVII Всеукраїнської науково-практичної конференції
«Актуальні проблеми комп'ютерних наук АПКН-2025»

14-15 листопада 2025

Хмельницький 2025

УДК 004:37:001:62

Збірник наукових праць за матеріалами XVII Всеукраїнської науково-практичної конференції «Актуальні проблеми комп'ютерних наук АПКН-2025». Хмельницький. 2025. 500с.

У збірнику наукових праць подані перспективні практичні розробки аспірантів, студентів та здобувачів в області сучасних інформаційних технологій. Розглянуто актуальні проблеми комп'ютерних наук, комп'ютерної інженерії, прикладної математики й інженерії програмного забезпечення, приведено ряд робіт по впровадженню інформаційних технологій у виробництво та управління. Висвітлено перспективні розробки сучасних систем пошуку, обробки й захисту інформації, медійних та комунікаційних системи.

УДК 004:37:001:62

Матеріали конференції відтворені з авторських оригіналів, друкуються в авторській редакції та наведені в алфавітному порядку прізвищ авторів. При макетуванні можливі незначні зміни компоновки контенту авторських оригіналів. Відповідальність за якість та зміст публікацій несе автор.

Участь у конференції та складові всіх її етапів (розгляд праць, перевірка на плагіат, макетування, публікація збірника наукових праць та видача сертифікатів) є безкоштовними для всіх учасників. Оргкомітет конференції висловлює подяку учасникам конференції та сподівається на подальшу співпрацю.

З питань проведення конференції та подальшого обміну інформацією звертатись на e-mail конференції: *apkt.khnu@gmail.com*

АКТУАЛЬНІ ПРОБЛЕМИ КОМП'ЮТЕРНИХ НАУК - 2025

XVII Всеукраїнська науково-практична конференція

Метою конференції є висвітлення актуальних проблем комп'ютерних наук, інформатики та інформаційних технологій.

Робочі мови конференції:

українська, англійська

СЕКЦІЇ КОНФЕРЕНЦІЇ:

1. Комп'ютерні науки, штучний інтелект та прикладні інформаційні технології.
2. Комп'ютерна інженерія та системи захисту інформації.
3. Математичне моделювання та інженерія програмного забезпечення
4. Телерадіокомунікації, медійні та комунікаційні системи.
5. Проблеми впровадження інформаційних технологій у виробництво та управління.

СПИСОК ОРГАНІЗАЦІЙ, ПРЕДСТАВНИКИ ЯКИХ БРАЛИ УЧАСТЬ У РОБОТІ КОНФЕРЕНЦІЇ:

Донбаська державна машинобудівна академія
Інститут кібернетики імені В. М. Глушкова НАН України
Кам'янський енергетичний фаховий коледж
Київський національний університет імені Т. Г. Шевченка
Національного аерокосмічного університету імені М. Є. Жуковського «Харківський авіаційний інститут»
Національний технічний університет «Харківський політехнічний інститут»
Сумський державний університет
Харківський національний університет радіоелектроніки
Хмельницький національний університет
Хмельницький фаховий економіко-технологічний коледж УЕП

ОРГКОМІТЕТ КОНФЕРЕНЦІЇ:

СИНЮК О. М. – голова оргкомітету, проректор Хмельницького національного університету з наукової роботи, доктор технічних наук, професор.

ГОВОРУЩЕНКО Т. О. – заступник голови оргкомітету, декан факультету інформаційних технологій Хмельницького національного університету, доктор технічних наук, професор.

БАРМАК О. В. – заступник голови оргкомітету, завідувач кафедри комп'ютерних наук Хмельницького національного університету, доктор технічних наук, професор.

САВЕНКО О. С. – професор кафедри комп'ютерної інженерії та інформаційних систем Хмельницького національного університету, доктор технічних наук, професор.

ВИСОЦЬКА О. В. – завідувач кафедри радіоелектронних та біомедичних комп'ютеризованих засобів і технологій Національного аерокосмічного університету ім. М. Є. Жуковського «Харківський авіаційний інститут», доктор технічних наук, професор.

ЛАВРОВ Є. А. – доктор технічних наук, професор (Сумський державний університет).

ТІМОФЄЄВА Л. В. – відповідальна за студентську науково-дослідну роботу ХНУ.

МАЗУРЕЦЬ О. В. – секретар конференції, доцент кафедри комп'ютерних наук Хмельницького національного університету, кандидат технічних наук, доцент.

МОЛЧАНОВА М. О. – секретар конференції, старший викладач кафедри комп'ютерних наук Хмельницького національного університету, доктор філософії з комп'ютерних наук.

КОНТАКТНА ІНФОРМАЦІЯ:

e-mail для листування: *apkt.khnu@gmail.com*

УДК 004.8

Кузь М.М.

Хмельницький національний університет

АНАЛІЗ ІСНУЮЧИХ РІШЕНЬ ЗАХИСТУ КОРИСТУВАЧІВ WI-FI-МЕРЕЖ ВІД ПІДРОБЛЕНИХ ТОЧОК ДОСТУПУ

У роботі розглянуто проблему безпеки користувачів бездротових Wi-Fi-мереж, зокрема загрозу, пов'язану з підробленими точками доступу. Проведено огляд сучасних підходів до їх виявлення та запобігання атакам. Визначено напрями подальших досліджень, спрямованих на підвищення захищеності користувачів у публічних і корпоративних мережах.

The paper examines the security problem of users of wireless Wi-Fi networks, in particular the threat associated with fake access points. A review of modern approaches to their detection and prevention of attacks is conducted. Directions for further research aimed at increasing user security in public and corporate networks are identified.

У сучасному середовищі бездротові мережі Wi-Fi стали невід'ємною складовою інфраструктури інформаційного обміну як у приватних домогосподарствах, так і в організаціях різного масштабу. Зростання кількості публічних точок доступу в громадських місцях, транспорті та навчальних закладах призвело до істотного підвищення ризиків, пов'язаних із несанкціонованим перехопленням даних користувачів. Однією з найпоширеніших і водночас найбільш небезпечних форм кіберзагроз у Wi-Fi-мережах є підроблені точки доступу, створені зловмисниками з метою перехоплення трафіку, отримання облікових даних або здійснення фішингових атак.

Проблема полягає в тому, що користувач, підключаючись до знайомої або нібито легітимної мережі, не має технічної можливості швидко перевірити автентичність точки доступу. Такі атаки ускладнюються тим, що підроблені точки можуть мати ті самі SSID, MAC-адреси та параметри шифрування, що й справжні мережі. З огляду на це, питання виявлення та нейтралізації фальшивих точок доступу є одним із напрямів інформаційної безпеки бездротових технологій. Практичне значення проблеми визначається необхідністю забезпечення конфіденційності, цілісності та доступності даних користувачів.

За останні роки було опубліковано значну кількість робіт, присвячених проблематиці виявлення підроблених точок доступу. У працях міжнародних дослідників розглянуто методи аналізу поведінкових характеристик точок доступу, зокрема часових затримок, інтенсивності пакетів і відмінностей у рівнях сигналу. Українські науковці досліджували питання побудови систем моніторингу Wi-Fi-простору для виявлення аномалій та розробки засобів активного захисту на основі аналізу радіочастотних параметрів.

Існуючі рішення можна умовно поділити на три групи: програмні методи, апаратні системи виявлення та гібридні підходи. Програмні методи передбачають використання клієнтських або серверних додатків, які здійснюють перевірку параметрів з'єднання, сертифікатів або відбитків точок доступу. Апаратні системи базуються на аналізі радіочастотних сигналів і можуть ідентифікувати джерела передавання за унікальними фізичними характеристиками, що дозволяє точніше визначати підроблені пристрої. Гібридні рішення поєднують переваги обох підходів, інтегруючи аналіз на рівні сигналу з програмними перевірками автентичності.

Попри значний прогрес у цій сфері, більшість рішень мають обмеження щодо масштабованості, вартості реалізації або рівня автоматизації. Зокрема, системи моніторингу Wi-Fi середовища у великих корпоративних мережах потребують значних ресурсів для оброблення даних, тоді як користувацькі додатки часто не мають доступу до низькорівневих параметрів адаптерів і не забезпечують повноцінний захист. Таким чином, залишаються невирішеними питання оптимізації точності виявлення при збереженні продуктивності системи, а також підвищення рівня адаптивності алгоритмів до нових типів атак.

Метою даної роботи є проведення системного аналізу сучасних методів виявлення та запобігання підробленим точкам доступу у Wi-Fi-мережах, визначення їхніх переваг і недоліків, а також обґрунтування напрямів подальшого вдосконалення механізмів захисту користувачів. Завдання дослідження полягає в узагальненні існуючих підходів, оцінці ефективності наявних алгоритмів і визначенні вимог до перспективних систем захисту, здатних функціонувати в умовах динамічного радіочастотного середовища.

У процесі дослідження було встановлено, що основні методи виявлення підроблених точок доступу поділяються за принципом дії на три групи: сигнатурні, поведінкові та контекстно-аналітичні. Сигнатурні методи базуються на порівнянні характеристик точки доступу з базою даних відомих легітимних пристроїв. Цей підхід ефективний у стабільних середовищах, проте вразливий до нових або змінених фальшивих точок. Поведінкові методи аналізують особливості обміну пакетами, рівень сигналу, швидкість автентифікації та інші динамічні параметри, що дозволяє виявляти аномалії, але вимагає значних обчислювальних ресурсів. Контекстно-аналітичні системи поєднують дані з різних джерел — зокрема GPS-координати, інформацію про довірені мережі та часові шаблони підключення — створюючи профіль користувацької поведінки.

Сучасні дослідження показують, що використання методів машинного навчання дозволяє підвищити точність і адаптивність таких систем. Наприклад, моделі на основі класифікації дерев рішень або нейронних мереж можуть автоматично визначати фальшиві точки за статистичними ознаками, навіть якщо ті змінюють свої параметри. Водночас необхідність великої кількості навчальних даних і обмеження мобільних пристроїв знижують ефективність практичної реалізації цих підходів.

Особливу увагу привертає концепція побудови довірених мереж (Trusted Wi-Fi Frameworks), у яких автентифікація здійснюється не лише за SSID і паролем,

а й за цифровими сертифікатами або криптографічними ключами, пов'язаними з конкретним пристроєм. Така модель дозволяє значно зменшити ризик перехоплення сесії, однак її впровадження потребує централізованого управління й підтримки інфраструктури публічних ключів.

Водночас у контексті публічних мереж перспективними є методи колективного моніторингу, коли пристрої користувачів спільно формують базу довірених точок доступу, обмінюючись даними про спостережувані аномалії. Це дозволяє створювати децентралізовані системи виявлення, які не залежать від одного адміністратора.

Результати проведеного аналізу свідчать, що жодне з існуючих рішень не забезпечує універсального захисту в усіх сценаріях використання Wi-Fi. Тому доцільним є поєднання декількох методів — наприклад, сигнатурного аналізу для попереднього фільтрування і поведінкового моніторингу для глибокої перевірки. Перспективним напрямом є впровадження інтегрованих систем, які використовують машинне навчання в поєднанні з апаратними засобами вимірювання параметрів сигналу.

Проведений аналіз показав, що проблема захисту користувачів Wi-Fi-мереж від підроблених точок доступу залишається надзвичайно актуальною через стрімкий розвиток технологій бездротового зв'язку та зростання кількості мобільних користувачів. Існуючі рішення забезпечують частковий рівень захисту, але потребують подальшої адаптації до умов реального середовища. Основними напрямами вдосконалення є інтеграція методів штучного інтелекту для автоматизованого виявлення аномалій, створення гібридних архітектур безпеки, що поєднують програмні та апаратні підходи, а також розробка стандартів обміну даними між системами моніторингу різних постачальників.

Подальші дослідження мають бути спрямовані на створення уніфікованої системи оцінювання довіри до точок доступу, яка могла б функціонувати як у корпоративному, так і у відкритому середовищі. Важливим завданням є підвищення рівня обізнаності користувачів щодо ризиків підключення до невідомих мереж та впровадження освітніх програм із кібергігієни. Отже, розвиток технологій захисту Wi-Fi не може розглядатися лише з технічного боку — він має супроводжуватися соціально-освітніми заходами, спрямованими на формування культури безпечного користування цифровими ресурсами.

Перелік посилань

1. Наталія Лукова-Чуйко, Тетяна Лаптєва. Удосконалення методу впявлення та локалізації нелегальних точок доступу до бездротової мережі об'єктів інформаційної діяльності. Безпека інформаційних систем і технологій. Вип. 1, с. 21-27. DOI:10.17721/ISTS.2023.1.21-27.

2. Яровий, Р. О., Подвиженко, А. В., Переверзєв, А. М., Левченко, С. В. Публічні WI-FI мережі: захист особистої інформації. Науковий вісник Таврійського державного агротехнологічного університету. 2025. Вип. 15, с. 245-250. DOI: 10.32782/2220-8674-2025-25-1-29

АКТУАЛЬНІ ПРОБЛЕМИ КОМП'ЮТЕРНИХ НАУК 2025

ЗБІРНИК НАУКОВИХ ПРАЦЬ

Комп'ютерна верстка: **Мазурець О. В.**

Підписано до друку 15.11.2025.
Версія друку «APKN2025_CorpusPaper v5mod93 Final».

E-mail: *apkt.khnu@gmail.com*
ХНУ. м. Хмельницький, вул. Інститутська,11.

500

Завідувачу кафедри кібербезпеки
к.т.н., доц. Кльоцу Ю.П.
здобувача вищої освіти
Кузя Михайла Миколайовича
студента ФІТ, 2 курсу, групи КБЗІм-24-1

ЗАЯВА

З правилами чинного Положення про систему забезпечення академічної доброчесності у Хмельницькому національному університеті, згідно з яким виявлення академічного плагіату є підставою для відмови в допуску кваліфікаційної роботи до захисту і застосування заходів академічної відповідальності, ознайомлений. Про використання спеціалізованих програмних засобів (СПЗ) StrikePlagiarism та Anti-Plagiarism для перевірки кваліфікаційних робіт здобувачів вищої освіти на наявність академічного плагіату оповіщений. Надаю університету право на передачу моєї роботи для обробки та збереження в базах даних СПЗ і використання роботи для виявлення академічного плагіату в інших роботах, які перевіряються СПЗ.

Також надаю свою згоду на обробку й збереження університетом моєї роботи в Інституційному репозитарії Хмельницького національного університету.

Робота надається для перевірки в електронному варіанті. Електронна версія моєї роботи збігається (ідентична) з друкованою.

01.12.2025
дата

підпис

Anti-Plagiarism (UA) v-15.281 Educational

The maximum coincidence with one document 2.0%

Dictionaries check: en_US, ru_RU, ua_UA. **Errors in the documents: 11%**

	Document		Sum coincidence on the DB	
ID: 251494 Title: Метод захисту користувачів публічних Wi-Fi-мереж від підроблених точок доступу Added in a DB: 2025-12-03 Authors: Кузь Михайло Миколайович Heads: Петляк Н.С, Consultants: Opponents:	Symbols	Lexemes	Symbols	Lexemes
	92455	764	2516 (3%)	34 (4%)

Plagiarism sources

ID	Description	Plagiarism presence in the document	
		Symbols	Lexemes

Протокол аналізу звіту подібності науковим керівником

Заявляю, що я ознайомився (-лась) з Повним звітом подібності, який був згенерований Системою виявлення і запобігання плагіату щодо роботи:

Автор: Кузь Михайло Миколайович

Співавтор:

Назва: Метод захисту користувачів публічних Wi-Fi-мереж від підроблених точок доступу

Науковий керівник: Петляк Наталя Сергіївна

Підрозділ: Кафедра кібербезпеки

Коефіцієнт подібності 1:4%

Коефіцієнт подібності 2:1.5%

Мікропробіли: 0

Заміна букв: 0

Інтервали: 0

Білі знаки: 0

Дата створення звіту: 2025-12-03 22:22:28.0

Після аналізу Звіту подібності констатую наступне:

☐ **Запозичення, виявлені в роботі є законними і не є плагіатом. Рівень подібності не перевищує допустимої межі. Таким чином робота незалежна і приймається.**

☐ **Запозичення не є плагіатом, але перевищено граничне значення рівня подібностей. Таким чином робота повертається на доопрацювання.**

☐ **Виявлено запозичення і плагіат або навмисні текстові спотворення (маніпуляції), як передбачувані спроби укриття плагіату, які роблять роботу невідповідною вимогам законодавства (Ст. 32. ЗУ Про вищу освіту, пункт 3.1, Ст. 42. ЗУ Про освіту) та вимог НАЗЯВО (Критерій 5), а також кодексу етики і процедурам. Таким чином робота не приймається.**

Обгрунтування:

Дата експерт

РІШЕННЯ ЕКСПЕРТНОЇ КОМІСІЇ

КАФЕДРИ КІБЕРБЕЗПЕКИ

ПРО ДОПУСК КВАЛІФІКАЦІЙНОЇ РОБОТИ ДО ЗАХИСТУ

Назва: Метод захисту користувачів публічних Wi-Fi-мереж від підроблених точок доступу

Автор: Кузь Михайло Миколайович

Освітня програма: освітньо-професійна

Рівень вищої освіти магістр

Спеціальність: 125 – Кібербезпека та захист інформації

Науковий керівник: Петляк Наталія Сергіївна, PhD, старший викладач

На основі аналізу кваліфікаційної роботи на дотримання вимог академічної доброчесності (у т.ч. відсутності ознак академічного плагіату) з урахуванням результатів перевірки роботи спеціалізованим програмним засобом(ами) комісія зробила такий висновок:

№	Висновок	Позначка про відповідність
1	Ознаки академічного плагіату	
1.1	Запозичення, виявлені в роботі, є законними і не є академічним плагіатом (далі – зазначаються підстави віднесення запозичень до правомірних, якщо потрібно). Робота приймається до захисту.	відповідає
1.2	Виявлені запозичення не є академічним плагіатом, розміщені в розділах, які не описують безпосередньо авторське дослідження, але кількість цитат перевищує обсяг, виправданий поставленою метою роботи (далі – зазначаються детальні та аргументовані підстави віднесення запозичень до правомірних). Робота приймається до захисту, але має бути відкоригована.	
1.3	Виявлені запозичення не є академічним плагіатом, але частково розміщені в розділах, які описують безпосередньо авторське дослідження, а кількість цитат перевищує обсяг, виправданий поставленою метою роботи. Робота може бути допущена до захисту після того як буде відкоригована та доопрацьована і успішно пройде повторну перевірку на академічний плагіат.	
1.4	Робота містить навмисні текстові спотворення, передбачувані спроби укриття текстових запозичень або інші прояви академічного плагіату. Робота містить фабрикацію або фальсифікацію даних. Робота не допускається до захисту.	
2	Інші види порушень академічної доброчесності	

Підтвердження:

Оригінальність тексту роботи за результатами перевірки системою StrikePlagiarism складає 96,02%, оригінальність тексту роботи за результатами перевірки системою Anti-Plagiarism v-15.257 складає 98%.

Згідно з Положенням про систему забезпечення академічної доброчесності у ХНУ (https://khmnu.edu.ua/wp-content/uploads/normatyvni-dokumenty/polozhennya/pro-systemu-zabezpechennya-akademichnoyi-dobrochesnosti.pdf, Додаток В) кваліфікаційна робота, виконана за освітньо-професійною програмою, кількісні показники рівня унікальності тексту у відсотках до загального обсягу матеріалу в якій складає 75-100 %, визнається роботою з високим рівнем унікальності тексту: «Текст вважається унікальним і не потребує додаткових дій щодо запобігання неправомірним запозиченням».

Дата: 3.12.2025

Завідувач кафедри кібербезпеки _____ Юрій КЛЬОЦ

Гарант освітньої програми _____ Віра ТІТОВА

Керівник кваліфікаційної роботи _____ Наталія ПЕТЛЯК

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ХМЕЛЬНИЦЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ

РЕЦЕНЗІЯ НА КВАЛІФІКАЦІЙНУ РОБОТУ

освітньо-кваліфікаційного рівня «магістр»

Студент Кузь Михайло Миколайович
Тема: «Метод захисту користувачів публічних Wi-Fi-мереж від підроблених точок доступу»
Галузь знань 12 «*Інформаційні технології*» Спеціальність 125 «*Кібербезпека та захист інформації*» Освітня програма «Кібербезпека та захист інформації»

Обсяг дипломної роботи освітньо-кваліфікаційного рівня «магістр»:
кількість листів креслень ____; кількість сторінок записки 75;
1. Короткий зміст КР та прийнятих рішень У роботі проведено огляд наукових джерел, стандартів IEEE 802.11 і сучасних протоколів безпеки (WEP, WPA, WPA2, WPA3) з метою виявлення їхніх уразливостей. Здійснено порівняльний аналіз існуючих методів моніторингу безпровідних мереж (сигнатурних, статистичних, гібридних) і визначено їхні переваги та обмеження. Виконано систематизацію типових атак на Wi-Fi, включно з атаками «злий двійник» (Evil Twin), Man-in-the-Middle та DoS, для подальшого формування набору ознак для аналізу трафіку. Побудовано математичну модель процесу виявлення аномалій, засновану на оцінці похибки реконструкції ознак пакета за допомогою нейронного автокодера. Використано методи статистичного аналізу (обчислення середнього, дисперсії, стандартного відхилення) для визначення порогів виявлення аномальних подій. Застосовано елементи теорії ймовірностей для оцінки достовірності класифікації «нормальний / аномальний» трафік. Реалізовано навчання нейронної мережі-автокодера на вибірках нормального трафіку з метою формування латентного простору характеристик мережевих пакетів. Здійснено оцінку ефективності за показниками точності виявлення (Precision, Recall, F1-score) і швидкодії в реальному часі.
2. Висновок про відповідність КР завданню Кваліфікаційна робота у повній мірі відповідає поставленому завданню як в теоретичній так і у практичній частині роботи.
3. Характеристика виконання кожного розділу роботи, ступінь використання останніх досягнень науки і техніки і передових методів роботи: У вступі обґрунтовується актуальність теми роботи, її зв'язок з галуззю знань «Інформаційні технології» та спеціальністю «Кібербезпека та захист інформації», формулюється мета та основні завдання кваліфікаційної роботи. У першому розділі було проведено аналіз атак на існуючих безпровідних мереж Wi-Fi та механізмів безпеки, передбачених стандартами IEEE 802.11. У другому розділі розроблено метод захисту безпровідних мереж від підроблених точок доступу. У третьому розділі проведено експериментальну перевірку та оцінку ефективності розробленого методу.
4. Позитивні сторони кваліфікаційної роботи робота демонструє достатній рівень опрацювання теми та містить послідовний виклад основних етапів дослідження, включно з оглядом існуючих методів аналізу трафіку та спробою застосування нейронного автокодера для виявлення аномалій у Wi-Fi мережах. Позитивним є залучення реальних даних трафіку та використання практичних інструментів для тестування, що свідчить про прагнення автора поєднати теорію з практикою. Запропонований підхід має базовий рівень новизни та може слугувати відправною точкою для подальших, глибших досліджень і вдосконалення моделей виявлення аномалій у безпровідних мережах.

5. Негативні сторони кваліфікаційної роботи: робота, попри досягнуті результати, має низку помітних недоліків. Частина теоретичного матеріалу подана надмірно об'ємно. Практична частина не завжди містить достатньо детального обґрунтування вибору окремих рішень – зокрема, структури моделі, набору ознак та порогових значень, що робить результати менш переконливими. Обмеженим є порівняння з існуючими підходами: аналіз конкурентних методів виконано стисло, без кількісного співставлення. Крім того, експериментальна база є доволі вузькою, оскільки тестування проведене фактично на одному типі обладнання та невеликих вибірках трафіку, що не дає можливості однозначно оцінити універсальність запропонованого рішення.

6. Оцінка графічного оформлення та пояснювальної записки роботи. офомлення відповідає вимогам

7. Відгук про роботу в цілому кваліфікаційна робота справляє позитивне враження та демонструє достатній рівень опанування тематики. Матеріал подано послідовно та логічно, структура роботи витримана, а основні розділи змістовно пов'язані між собою, що дозволяє читачу без труднощів відстежувати хід дослідження. Пояснювальна записка містить достатню кількість прикладів та ілюстрацій, які сприяють кращому розумінню запропонованого методу та підтверджують його практичну спрямованість. Попри означені недоліки, дослідження має завершений характер і може бути оцінене як таке, що відповідає встановленим вимогам до кваліфікаційних робіт.

8. Інші зауваження -

9. Оцінка дипломної роботи Розглянувши позитивні та негативні сторони представленої кваліфікаційної роботи, можна зробити висновок, що робота заслуговує оцінки «задовільно» (65/E).

РЕЦЕНЗЕНТ (прізвище, ім'я, по батькові, посада, місце роботи) декан факультету інформаційних технологій, доктор технічних наук, професор Говорущенко Тетяна Олександрівна

« 3 » грудня 2025 . (підпис)