МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Західноукраїнський національний університет
Факультет комп'ютерних інформаційних технологій
Кафедра комп’ютерної інженерії

СТРЕЛЬЧУК Владислав Анатолійович

Програмний засіб моніторингу активності підключених пристроїв у безпровідних мережах / Software tool for monitoring the activity of connected devices in wireless networks

спеціальність: 123 – Комп’ютерна інженерія
освітньо-професійна програма – Комп’ютерна інженерія

Кваліфікаційна робота

Виконав: студентка групи КІ-41
СТРЕЛЬЧУК Владислав Анатолійович

Науковий керівник
к.т.н. Мельник Г.М.

ТЕРНОПІЛЬ - 2025

АНОТАЦІЯ

Стрельчук В.А. Програмний засіб моніторингу активності підключених пристроїв у безпровідних мережах. – Рукопис.

Кваліфікаційна робота на здобуття освітнього ступеня «бакалавр» за спеціальністю 123 «Комп'ютерна інженерія», освітньо-професійна програма. Західноукраїнський національний університет, Тернопіль, 2025.

Робота написана обсягом 48 сторінок і містить 7 рисунків, 12 таблиць, 3 додатки та 30 джерел за переліком посилань. Обсяг графічного матеріалу 2 аркуші формату А3.

Метою кваліфікаційної роботи є створення програмного засобу для моніторингу та аналізу активності безпровідних пристроїв. Розроблено алгоритм класифікації пристроїв на основі ключових параметрів активності, таких як інтенсивність трафіку, варіативність, роумінг, тривалість з'єднання та тип підключеної мережі. Запропоновано функції належності для кожного класу пристроїв (персональні, IoT, гостьові), які дозволяють автоматично визначати категорію пристрою за допомогою нормалізованих метрик та вагових коефіцієнтів, що підлягають налаштуванню або навчанню. Розроблено структуру програмного модуля, яка охоплює класи для збору та аналізу параметрів активності пристроїв у Wi-Fi мережі.

Ключові слова: WI-FI, МОНІТОРИНГ, IOT,МАРШРУТИЗАТОР , ROUTEROS.

ANNOTATION

Strelchuk V.A. Software tool for monitoring the activity of connected devices in wireless networks – Manuscript.

Qualification work for the Bachelor degree in specialty 123 “Computer Engineering”, educational and professional program. Western Ukrainian National University, Ternopil, 2025.

The work is written in 48 pages and contains 7 figures, 12 tables, 3 appendices and 30 references. The volume of graphic material is 2 sheets of A3 format.

The purpose of the qualification work is to create a software tool for monitoring and analyzing the activity of wireless devices. An algorithm for classifying devices based on key activity parameters, such as traffic intensity, variability, roaming, connection duration, and type of connected network, has been developed. Membership functions for each class of devices (personal, IoT, guest) have been proposed, which allow automatically determining the device category using normalized metrics and weighting factors that can be configured or trained. A software module structure has been developed that includes classes for collecting and analyzing device activity parameters in a Wi-Fi network.

Keywords: WI-FI, MONITORING, IOT, ROUTER, ROUTEROS.

ЗМІСТ

					КР.КІ. 10660603.00.00.000 ПЗ		
Змн.	Лист	№ докум.	Підпис	Дата			
Розробив		Стрельчук В.А.			Програмний засіб моніторингу активності підключених пристроїв у безпровідних мережах	Літ.	Арк. 7 / Акрушів
Перевір.		Мельник Г.М.					
Консульт.		Савка Н.Я.				ЗУНУ,ФКІТ, КІ-42	
Н. Контр.		Дубчак Л.О.					
Затвердив		Дубчак Л.О.					

ПЕРЕЛІК УМОВНИХ СКОРОЧЕНЬ

ТД	–	Точка доступу
RSSI	–	Received Signal Strength Indicator
SNR	–	Signal-to-Noise Ratio
NMS	–	Network Management Systems

ВСТУП

У період стрімкого розвитку цифрових технологій спостерігається значне зростання кількості пристроїв, які використовують бездротове з'єднання для обміну інформацією. Смартфони, розумні побутові пристрої, камери спостереження, датчики екологічного моніторингу, медичне обладнання та інші елементи сучасного середовища стають активними учасниками трафіку Wi-Fi-мереж. Така різноманітність пристроїв створює складну екосистему, управління якою потребує не лише класичних інструментів адміністрування, а й інтелектуальних засобів спостереження, що здатні адаптуватися до змін і виявляти приховані загрози.

Однією з ключових проблем, що постає перед адміністраторами мереж, є недостатній рівень прозорості стосовно того, які саме пристрої підключаються до мережі, як вони поводяться, наскільки стабільною є їхня присутність і чи не порушують вони політик безпеки. Більше того, навіть у захищених мережах може виникнути потреба ідентифікації невідомих або атипово активних пристроїв — як потенційної ознаки внутрішніх порушень чи зовнішніх атак. Тому моніторинг у реальному часі з аналітичним компонентом стає критично необхідним для забезпечення надійності, цілісності та прогнозованості роботи інфраструктури.

Сфера застосування програмних засобів моніторингу бездротових пристроїв охоплює як побутові, так і корпоративні сегменти. У домашніх мережах користувачі прагнуть контролювати кількість підключень, розподілення трафіку, захист від сторонніх пристроїв. У корпоративних системах ці задачі розширюються: додаються політики доступу, журналювання подій, контроль відповідності пристроїв регламентам і вимогам інформаційної безпеки. Особливу роль такі інструменти відіграють у розгортанні мережевої інфраструктури для інтернету речей (IoT), де кількість підключень перевищує класичні масштаби і часто вимагає автономного прийняття рішень.

Нарешті, моніторинг активності бездротових пристроїв має значний потенціал у сфері досліджень користувацької поведінки, розпізнавання шаблонів трафіку та підвищення ергономіки інтерфейсів доступу до мереж. Завдяки збору даних про

активність пристроїв у часі можна будувати предиктивні моделі навантаження, аналізувати ефективність використання точок доступу, а також формувати адаптивні рекомендації для проектування інфраструктури. Такий підхід відповідає загальній тенденції до побудови прозорих, гнучких і самокерованих мереж нового покоління.

Об’єкт дослідження: бездротова мережа та процеси взаємодії підключених пристроїв із точками доступу. Предмет дослідження**:** алгоритми та показники для моніторингу активності пристроїв.

Метою кваліфікаційної роботи є створення програмного засобу для моніторингу та аналізу активності безпровідних пристроїв. Для досягнення мети потрібно виконати такі завдання:

- проаналізувати існуючі підходи та програмні засоби моніторингу пристроїв у безпровідних мережах;
- обрати технології для ідентифікації та відстеження активності пристроїв;
- розробити алгоритми класифікації пристроїв мережі;
- розробити програмну архітектуру засобу моніторингу активності;
- реалізувати програмний засіб моніторингу активності підключених пристроїв.

Результати дослідження апробовано на ІІ Всеукраїнській науково-практичній конференції студентів, аспірантів та молодих вчених «Інтелектуальні комп’ютерні системи та мережі» [1] (додаток А).

У першому розділі проведено аналітичний огляд бездротових мереж як середовища для передачі даних, з акцентом на властивості, що впливають на моніторинг пристроїв. Розглянуто архітектуру Wi-Fi мереж, особливості обміну на рівні кадрів та ключові параметри взаємодії пристроїв з точками доступу.

У другому розділі створено алгоритм класифікації пристроїв на основі аналізу таких параметрів, як інтенсивність трафіку, тривалість сесії та тип підключення.

У третьому розділі було реалізовано програмний модуль моніторингу активності пристроїв у режимі реального часу із застосуванням мови Python та бібліотек взаємодії з MikroTik RouterOS.

1 АНАЛІЗ ІСНУЮЧИХ ПІДХОДІВ ДО МОНІТОРИНГУ АКТИВНОСТІ У БЕЗПРОВІДНИХ МЕРЕЖАХ

1.1 Основні характеристики бездротових мереж

Wi-Fi мережа є різновидом локальної мережі (LAN), де пристрої обмінюються даними через бездротове середовище, зазвичай у діапазонах частот 2,4 ГГц або 5 ГГц. В основі взаємодії лежить модель клієнт–точка доступу (AP — Access Point).

Основні етапи взаємодії пристроїв у Wi-Fi мережі [1, 3]:

Етап 1. Виявлення мережі (Discovery). Пристрої-клієнти (наприклад, смартфони, ноутбуки) періодично сканують навколишній простір, щоб знайти доступні Wi-Fi мережі. Відбувається обмін спеціальними керуючими фреймами:

- Beacon — повідомлення, яке регулярно надсилає точка доступу для інформування про себе.
- Probe Request/Response — активні запити від клієнта та відповіді від точок доступу.

На цьому етапі пристрій отримує інформацію про назву мережі (SSID), рівень сигналу, типи підтримуваної безпеки та інші параметри.

Етап 2. Підключення (Authentication та Association). Після вибору мережі пристрій починає процес підключення:

- аутентифікація — перевірка прав на підключення. Це може бути відкритий доступ або вимога введення пароля (WPA2/WPA3).
- асоціація — встановлення логічного зв'язку між клієнтом і точкою доступу, створення стійкого сеансу обміну даними.

Пристрій стає повноцінним учасником мережі тільки після завершення обох процедур.

Етап 3. Обмін даними (Data Transfer). Після успішної асоціації відбувається передача користувацьких даних. Дані передаються через кадри типу Data Frame, які інкапсулюють мережеві пакети (IP-пакети, HTTP-запити тощо). Використовується динамічне планування доступу до каналу (наприклад, CSMA/CA — прослуховування перед передачею) для уникнення колізій. Можуть застосовуватися

механізми оптимізації трафіку, як-от агрегація кадрів (A-MPDU) або пріоритезація через QoS.

Етап 4. Переміщення пристрою (Roaming). У великих мережах пристрої можуть переміщатися між різними точками доступу, зберігаючи безперервне з'єднання. Використовується механізм роумінгу, при якому пристрій аналізує рівень сигналу і при його зниженні ініціює перепідключення до сильнішої точки доступу. У сучасних мережах стандарти 802.11r/k/v забезпечують швидке і безшовне перемикання без помітної затримки для користувача [4].

Етап 5. Завершення підключення (Disassociation та Deauthentication)

Пристрій або сама мережа може ініціювати розрив підключення:

– Disassociation — повідомлення про завершення логічного з'єднання без втрати безпеки.

– Deauthentication — повне завершення взаємодії та скасування аутентифікації.

Після цього пристрій повертається у стан пошуку доступних мереж.

Важливі особливості для моніторингу активності:

– Кожна дія супроводжується передачею контрольних кадрів, які можна перехопити і проаналізувати без розшифрування основного трафіку.

– Моніторинг може реєструвати як стабільно підключені пристрої, так і ті, що сканують мережі або переміщуються між точками доступу.

– Поява, зникнення і активність пристрою можна визначити за рівнем сигналу, MAC-адресою та характером переданих кадрів.

Сформуємо UML діаграму діяльності для процесу взаємодії пристроїв у Wi-Fi мережі на рисунку 1.1. На діаграмі представлено основні етапи життєвого циклу пристрою у бездротовій мережі Wi-Fi. Початковим станом є активація бездротового адаптера та перехід у режим сканування навколишнього середовища на наявність доступних мереж.

Після виявлення мереж користувач або система автоматично обирає мережу для підключення. Наступним кроком є процес аутентифікації, під час якого відбувається перевірка права пристрою на доступ до обраної мережі. У випадку

успішної аутентифікації пристрій переходить у стан асоціації, що означає встановлення логічного з’єднання з точкою доступу.

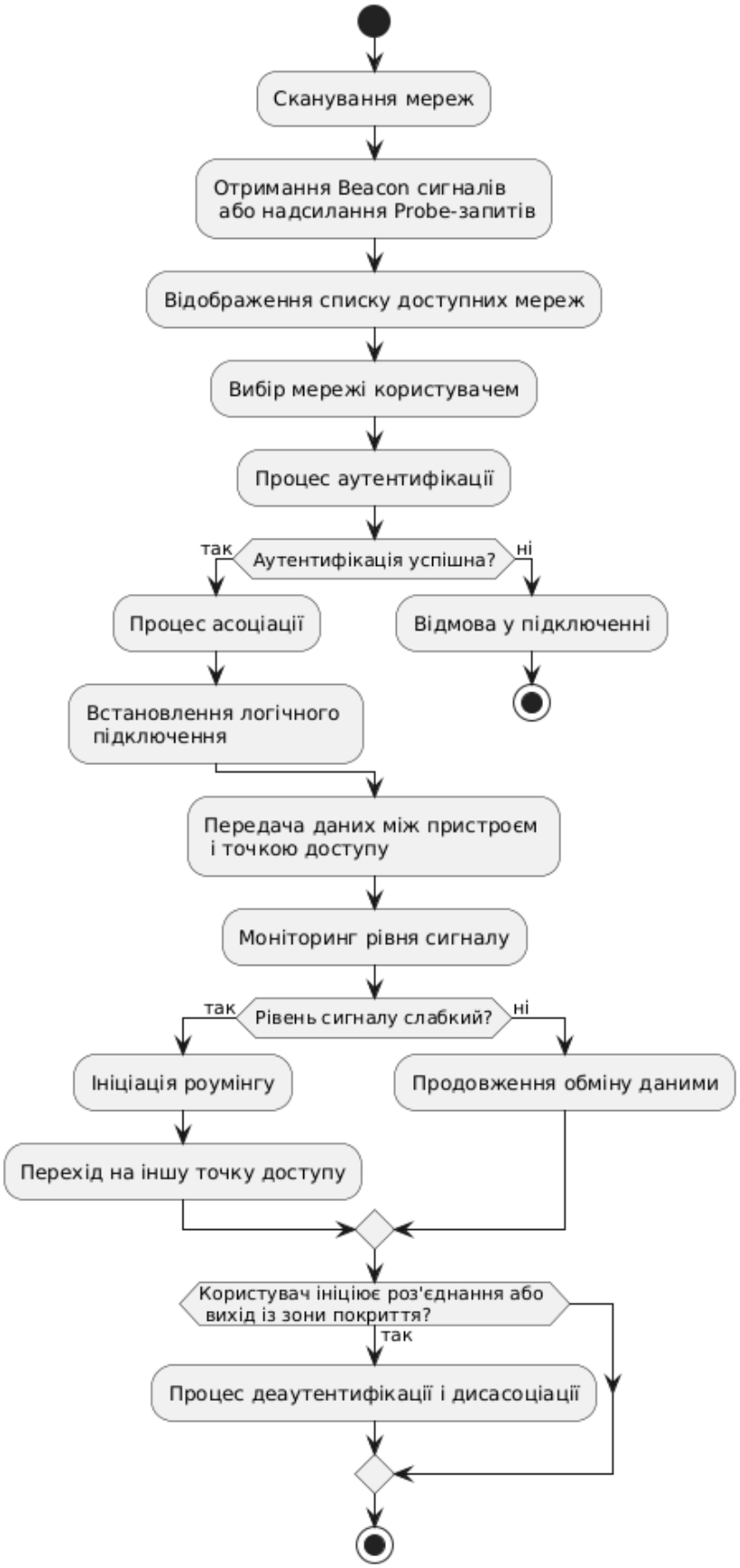


Рисунок 1.1 - Процес взаємодії пристроїв у Wi-Fi мережі

Після асоціації пристрій починає обмін даними у режимі реального часу. Під час пересування користувача або внаслідок змін рівня сигналу може ініціюватися роумінг. Роумінг передбачає пошук іншої точки доступу з кращими умовами з'єднання, що дозволяє забезпечити безперервність сеансу зв'язку. У разі, якщо пристрій або мережа ініціюють розрив підключення, відбувається перехід у стан завершення сесії. Після розриву з'єднання життєвий цикл взаємодії пристрою у Wi-Fi мережі завершується. Діаграма станів на рисунку 1.2 дозволяє наочно відобразити логіку переходів між основними етапами взаємодії пристроїв у безпровідних мережах, що має важливе значення для розробки систем моніторингу активності пристроїв.

Основні характеристики стандартів [5] бездротового зв'язку 802.11a [6], 802.11b, 802.11g, 802.11n, 802.11ac, 802.11ax в таблиці 1.1.

Таблиця 1.1 - Стандарти бездротового зв'язку

Стан-дарт	Частот-ний діапазон	Макси-мальна швидкість	Ширина каналу	Технологічні особливості
802.11a 1999 р	5 ГГц	до 54 Мбіт/с	20 МГц	Більш стійкий до перешкод у міському середовищі завдяки 5 ГГц; коротший радіус дії
802.11b 1999 р	2,4 ГГц	до 11 Мбіт/с	20 МГц	Сумісність із великою кількістю пристроїв; висока зашумленість 2,4 ГГц
802.11g 2003 р	2,4 ГГц	до 54 Мбіт/с	20 МГц	Зворотна сумісність з 802.11b; проблеми через перешкоди
802.11n 2009 р	2,4 ГГц і 5 ГГц	до 600 Мбіт/с	20/40 МГц	Підтримка MIMO; ширша смуга пропускання
802.11ac 2013 р	5 ГГц	до 6,9 Гбіт/с	20/40/80/160 МГц	Підтримка MU-MIMO; висока швидкість для великої кількості пристроїв
802.11ax (Wi-Fi 6) 2019 р	2,4 ГГц і 5 ГГц (частково 6 ГГц)	до 9,6 Гбіт/с	20/40/80/160 МГц	OFDMA, Target Wake Time, підвищена щільність клієнтів

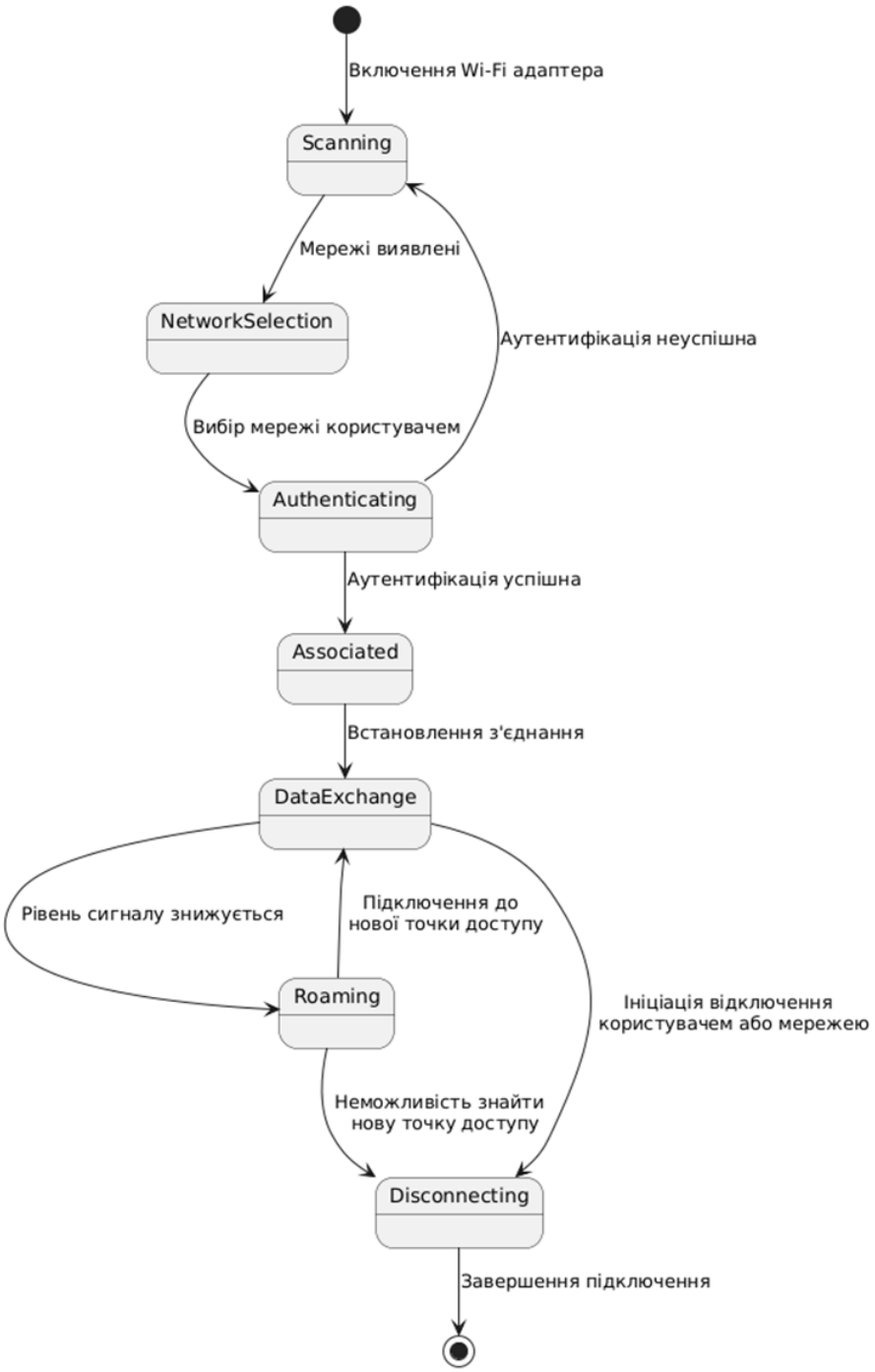


Рисунок 1.2 - Діаграма станів пристрою в Wi-Fi мережі

Вплив особливостей стандартів Wi-Fi на можливості моніторингу активності пристроїв систематизована в таблиці 1.2. У сучасних Wi-Fi мережах одночасно працює велика різноманітність пристроїв, кожен з яких має свої особливості підключення та характерні типи мережевої активності. Розуміння цих особливостей є критичним для ефективного моніторингу та аналізу стану мережі.

Таблиця 1.2 – Моніторинг стандартів

Стандарт	добре для моніторингу	погано для моніторингу
802.11a	Мало перешкод на 5 ГГц, легше відслідковувати пристрої	Маленький радіус покриття, пристрої можуть часто зникати
802.11b	Багато пристроїв підтримують, легко ловити підключення	Дуже багато завад на 2,4 ГГц, важко точно моніторити
802.11g	Швидше передача даних на 2,4 ГГц, краще видно навантаження	Багато перешкод через переповненість частоти
802.11n	Можна працювати і на 2,4, і на 5 ГГц, більше пристроїв підключається	Через багатопотоковість важче точно рахувати активність
802.11ac	Дуже швидка передача, добре видно великі об'єми трафіку	Маленький радіус на 5 ГГц, треба більше точок доступу для спостереження
802.11ax (Wi-Fi 6)	Підходить для великої кількості пристроїв, краще розподіляє трафік	Важко напряму бачити активність, бо дані діляться по слотах

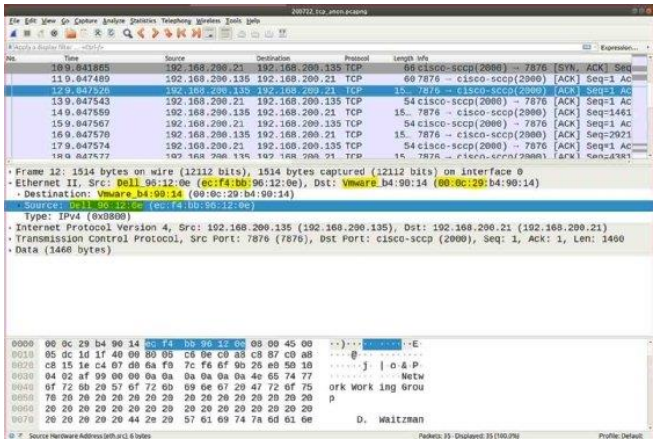
1.2 Огляд сучасних рішень і програмних засобів для моніторингу

Моніторинг Wi-Fi мереж є ключовим для їхньої стабільності, безпеки та продуктивності. Існують як відкриті, так і комерційні програмні рішення, що пропонують різноманітну функціональність. Розглянемо чотири популярні варіанти: Wireshark, Airodump-ng, PRTG Network Monitor та Cisco Prime.

Відкриті рішення для моніторингу Wi-Fi забезпечують глибокий контроль та гнучкість, часто використовуються для детального аналізу пакетів, виявлення проблем безпеки та усунення несправностей на низькому рівні. Вони вимагають певних технічних знань.

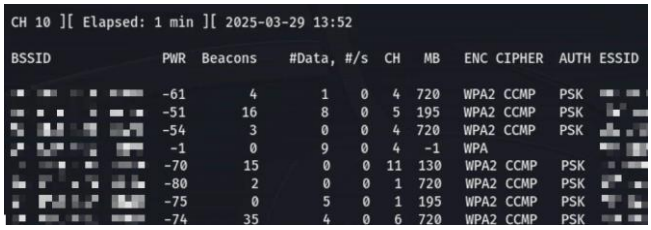
Wireshark [7] – це один з найпопулярніших аналізаторів протоколів мережі, що дозволяє захоплювати та інтерактивно переглядати мережевий трафік, включаючи 802.11. Його переваги – безкоштовність, відкритий вихідний код,

глибокий аналіз пакетів, підтримка тисяч протоколів, кросплатформенність та активна спільнота. Недоліки – не інтуїтивний для новачків, відсутність високорівневого моніторингу, не призначений для великих компаній і може бути ресурсоємним.

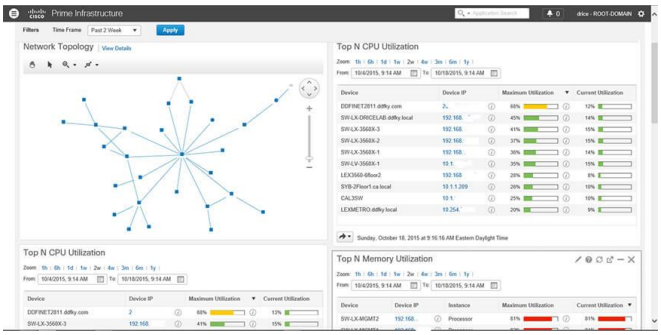


Wireshark

PRTG Network Monitor



Airodump-ng



Cisco Prime Infrastructure

Рисунок 1.3 - Програмні засоби моніторингу

Airodump-ng, частина Aircrack-ng suite, є інструментом для захоплення бездротових пакетів 802.11, що широко використовується для аудиту безпеки Wi-Fi мереж. Він дозволяє збирати інформацію про точки доступу, клієнтів, захоплювати рукостискання для злому паролів WPA/WPA2 [8]. Переваги – спеціалізація на Wi-Fi, виявлення прихованих мереж [9], збір даних для аудиту безпеки, детальна інформація про AP та клієнтів, безкоштовність. Недоліки – вимоги до сумісного бездротового адаптера, високий поріг входу через командний рядок, не є повноцінним інструментом моніторингу продуктивності.

Комерційні рішення пропонують більш інтегровані, автоматизовані та зручні для користувача функції, часто з графічним інтерфейсом, візуалізацією, сповіщеннями та підтримкою. Вони орієнтовані на ширший спектр завдань моніторингу та управління мережею.

PRTG Network Monitor від Paessler [10] – це комплексне рішення для моніторингу мережі [11], включаючи Wi-Fi, що використовує різні сенсори (SNMP, WMI, NetFlow, Packet Sniffing). Переваги – комплексний моніторинг, простий та інтуїтивно зрозумілий інтерфейс, автоматичне виявлення пристроїв, різноманітні сенсори, гнучка система сповіщень, детальні звіти та візуалізація, відмовостійка конфігурація та відсутність вимог до встановлення агентів. Недоліки – платна ліцензія (хоча є безкоштовна версія), може бути ресурсоємним для великих мереж, деякі глибокі аналізи пакетів потребують окремих сенсорів.

Cisco Prime Infrastructure [12] – це інтегрована система управління та моніторингу мережевої інфраструктури від Cisco. Вона призначена для управління дротовими та бездротовими мережами Cisco. Переваги – комплексне управління інфраструктурою Cisco, централізований контроль, детальний моніторинг Wi-Fi, візуалізація та картографія, аналіз Assurance, автоматизація та Plug and Play, інтеграція з іншими сервісами Cisco та пряма підтримка виробника. Недоліки – висока вартість, орієнтований на обладнання Cisco, складність налаштування та експлуатації, висока ресурсоємність.

Для малого та середнього бізнесу, що потребує комплексного моніторингу, ідеальним буде PRTG Network Monitor. Великим корпораціям з інфраструктурою Cisco найкраще підійде Cisco Prime Infrastructure.

Таблиця 1.1 - Порівняльна таблиця програмних засобів

Характеристика	Wireshark	Airodump-ng	PRTG Network Monitor	Cisco Prime Infrastructure
1	2	3	4	5
Основна функція	Захоплення та аналіз мережевих пакетів	Захоплення 802.11 фреймів, аудит безпеки	Моніторинг продуктивності та доступності мережі	Управління, моніторинг та автоматизація мереж Cisco

Продовження таблиці 1.1

1	2	3	4	5
Wi-Fi специфікація	Аналіз 802.11 фреймів, глибокий аналіз	Захоплення фреймів, виявлення AP/клієнтів, захоплення handshakes	Моніторинг AP, контролерів, клієнтів Wi-Fi, пропускна здатність, якість сигналу	Глибоке управління та моніторинг Wi-Fi інфраструктури Cisco
Ціна	Безкоштовно	Безкоштовно	Платна (залежить від сенсорів), є безкоштовна версія	Дуже висока
Масштабованість	Низька (для індивідуального аналізу)	Низька (для точкового аудиту)	Висока (для малих та великих мереж)	Дуже висока (для великих корпоративних мереж Cisco)
Візуалізація	Мінімальна (графіки протоколів)	Відсутня (текстовий вивід)	Висока (графіки, дашборди, карти)	Дуже висока (карти покриття, топології)
Сповіщення	Відсутні	Відсутні	Гнучкі (e-mail, SMS, push)	Гнучкі, інтегровані з системою подій
Призначення	Детальний аналіз трафіку, усунення несправностей	Аудит безпеки Wi-Fi, збір даних для зламу паролів	Загальний моніторинг мережі, продуктивність	Управління та моніторинг великих корпоративних мереж Cisco

1.3 Відстеження активності пристроїв та постановка завдань роботи

Персональні пристрої (смартфони, ноутбуки, планшети) — це найбільш поширена група користувацьких пристроїв у Wi-Fi мережах. Вони зазвичай підключаються через автентифікацію за паролем (WPA2 або WPA3) до основної мережі підприємства або домашньої мережі. Більшість персональних пристроїв підтримують як діапазон 2,4 ГГц, так і 5 ГГц, а новіші моделі також можуть працювати у 6 ГГц (Wi-Fi 6E). Підключення часто відбувається у режимі автоматичного приєднання після першого успішного збереження мережі. Персональні пристрої мають високий рівень варіабельності активності. Вони регулярно обмінюються даними з хмарними сервісами, здійснюють фонові оновлення, перевірку повідомлень та синхронізацію. Смартфони можуть генерувати періодичні короткі сеанси активності навіть у "сплячому" режимі, що створює регулярні, але невеликі піки трафіку. Ноутбуки при активній роботі здатні

генерувати стабільний високий потік даних, особливо під час відеоконференцій, стрімінгу чи передачі файлів.

Моніторинг персональних пристроїв важливий для виявлення надмірного споживання пропускної здатності, підозрілих моделей активності (наприклад, незвичних підключень у неробочий час) або проблем з роумінгом при переміщенні між зонами покриття.

IoT-пристрої (розумні сенсори, камери, побутова техніка) зазвичай підключаються до спеціально виділеної або сегментованої Wi-Fi мережі для пристроїв Інтернету речей. Підключення може бути менш захищеним у порівнянні з персональними пристроями: наприклад, деякі IoT-пристрої не підтримують сучасні протоколи безпеки (WPA3) і працюють лише на 2,4 ГГц. Часто такі пристрої залишаються підключеними тривалий час без відключення. IoT-пристрої мають переважно прогнозовану і регулярну активність. Більшість сенсорів періодично надсилають невеликі об'єми даних (температура, вологість, стан обладнання) за фіксованим графіком. Камери відеоспостереження генерують значно більший потік даних, особливо у режимі постійної трансляції або запису по події (детекція руху). Важливо, що зазвичай активність IoT-пристроїв майже не залежить від часу доби.

Для вирішеннях поставлених в роботі задач важливо контролювати стабільність з'єднання IoT-пристроїв, виявляти аномальні сплески активності (які можуть свідчити про злом або збій) та швидко фіксувати зникнення пристрою з мережі, оскільки це може вказувати на апаратний дефект або втрату живлення.

Третій вид пристроїв можна назвати гостьовими пристроями. Це пристрої відвідувачів, тимчасових користувачів. Гостьові пристрої зазвичай підключаються до окремої гостьової мережі, яка ізольована від основної внутрішньої мережі підприємства або будинку. Часто для доступу використовуються спрощені механізми автентифікації — відкриті мережі з Captive Portal або паролі, які часто змінюються. Гостьові пристрої підтримують лише базові рівні сервісу і мають обмежений доступ до мережевих ресурсів.

Активність гостьових пристроїв є дуже різнорідною. Зазвичай користувачі використовують інтернет для базового серфінгу, електронної пошти або перегляду соціальних мереж. Однак гостьові підключення можуть також супроводжуватися

сплесками трафіку при потоковому відео, оновленні додатків або завантаженні великих файлів. Моніторинг гостьових пристроїв допомагає контролювати використання пропускної здатності, виявляти потенційно шкідливі активності (наприклад, спроби сканування внутрішньої мережі) і запобігати перенавантаженню інфраструктури через неконтрольоване використання ресурсів.

Зведена таблиця порівнює основні категорії пристроїв за підключенням, типовою активністю і важливістю для моніторингу

Таблиця 1.3 - Категорії пристроїв

Категорія пристроїв	Характеристики підключення	Типові шаблони активності	Що важливо моніторити
Персональні пристрої (смартфони, ноутбуки, планшети)	Автоматичне підключення, 2,4 ГГц або 5 ГГц, сучасні протоколи безпеки	Періодичні короткі сеанси, високе навантаження при активному використанні	Споживання трафіку, роумінг між точками доступу, підозріла активність поза робочим часом
IoT-пристрої (сенсори, камери, розумна техніка)	Підключення до 2,4 ГГц мереж, довготривале підключення	Регулярна або постійна передача невеликих обсягів даних; для камер — великий трафік	Стабільність з'єднання, зникнення пристроїв, незвичайні сплески активності
Гостьові пристрої (відвідувачі, тимчасові користувачі)	Окрема гостьова мережа, обмежений доступ, спрощена автентифікація	Короткочасне або непередбачуване використання мережі, іноді великі обсяги трафіку	Перевантаження мережі, спроби сканування або доступу до внутрішніх ресурсів

На практиці моніторинг рідко здійснюється шляхом ручного збору метрик з окремих пристроїв. Використовуються системи управління та моніторингу NMS котрі збирають дані з маршрутизаторів, точок доступу. Системи надають візуалізацію даних (дашборди, графіки) і генерують сповіщення про аномалії або перевищення порогових значень. Різні виробники мережевого обладнання (Cisco, Aruba, Ubiquiti, Ruckus тощо) мають власні NMS зі своїм набором метрик та функціоналом моніторингу.

Метою кваліфікаційної роботи є створення програмного засобу для моніторингу та аналізу активності безпровідних пристроїв. Для досягнення мети потрібно виконати такі завдання:

- проаналізувати існуючі підходи та програмні засоби моніторингу пристроїв у безпровідних мережах;
- обрати технології та алгоритми для ідентифікації та відстеження активності пристроїв;
- розробити алгоритми класифікації пристроїв мережі;
- розробити програмну архітектуру засобу моніторингу активності;
- реалізувати програмний засіб моніторингу активності підключених пристроїв.

2 ПРОЕКТУВАННЯ ПРОГРАМНОГО ЗАСОБУ ДЛЯ МОНІТОРИНГУ АКТИВНОСТІ ПРИСТРОЇВ

2.1 Моделі моніторингу Wi-Fi мережі

Моніторинг активності Wi-Fi мережі є критично важливим для забезпечення її стабільної роботи, оптимальної продуктивності та безпеки. Існує кілька підходів до моніторингу, які різняться за методом збору даних, точкою зняття метрик та типами пристроїв, що відстежуються. Систематизуємо їх за вказаними критеріями.

Пасивний моніторинг передбачає збір та аналіз даних без активного втручання в роботу мережі та без створення штучного трафіку. Він "слухає" існуючий трафік та стан мережі. Характеристики:

- низький вплив на продуктивність мережі.
- дозволяє отримати реальне уявлення про використання мережі та поведінку клієнтів.
- ідеально підходить для аналізу трафіку, виявлення проблем з покриттям, ідентифікації джерел перешкод.

Моніторинг передбачає відповідні метрики:

- RSSI рівень сигналу (Received Signal Strength Indicator) тобто потужність сигналу, який отримує пристрій від точки доступу;
- SNR співвідношення сигнал/шум (Signal-to-Noise Ratio) Показує наскільки сильний корисний сигнал порівняно з фоновим шумом. Вищий SNR означає кращу якість зв'язку;
- завантаженість Wi-Fi каналу може свідчити про перешкоди або надмірне використання каналу;
- загальна кількість клієнтських пристроїв підключених до точки доступу або маршрутизатора;
- статистика трафіку (вхідного та вихідного), що передається через мережу або окремі точки доступу;
- кількість помилок передачі/прийому показує частку пакетів даних, які були втрачені або містили помилки під час передачі;

– фактична швидкість передачі даних (Data Rate) між точкою доступу та пристроєм;

– інформація про сусідні мережі у зоні покриття та їхні канали та рівні сигналу допомагає виявити потенційні джерела інтерференції.

Активний моніторинг передбачає генерацію штучного трафіку або виконання тестів для оцінки продуктивності мережі під певним навантаженням. Характеристики:

– дозволяє оцінити продуктивність мережі в контрольованих умовах;

– ефективний для виявлення проблем з пропускною здатністю, затримками та втратою пакетів;

– вимагає використання спеціалізованого програмного або апаратного забезпечення.

Активний моніторинг має наступні метрики :

– пропускна здатність Throughput;

– затримка Latency або час передачі пакета даних від джерела до отримувача і назад (Round Trip Time) негативно впливають на роботу застосунків, чутливих до часу (наприклад, VoIP, онлайн-ігри);

– втрата пакетів (Packet Loss) тобто відсоток пакетів даних, які не досягли пункту призначення;

– Час підключення необхідний пристрою для успішного підключення до Wi-Fi мережі.

Методи моніторингу також можемо класифікувати за точкою в архітектурі мережі.

Маршрутизатор, як центральний елемент мережі, має уявлення про загальний стан мережі, підключені пристрої та трафік, що проходить через нього. Маршрутизатор надає централізований огляд стану мережі. Дозволяє відстежувати загальний трафік, завантаження каналів WAN (якщо маршрутизатор виконує функції NAT), та стан підключених пристроїв. Є джерелом метрик**:**

– кількість підключених пристроїв;

– загальний обсяг вхідного та вихідного трафіку;

– завантаження процесора та пам'яті маршрутизатора;

- статистика NAT-з'єднань;
- журнали подій (спроби підключення, помилки аутентифікації, тощо);
- стан WAN-з'єднання.

Точка доступу (ТД) відповідає за безпосереднє бездротове підключення пристроїв і має детальну інформацію про стан радіоефіру та взаємодію з клієнтами на своєму сегменті. ТД надає детальну інформацію про стан радіоефіру в конкретній зоні покриття. Моніторинг ТД важливий для виявлення проблем з покриттям, інтерференцією та продуктивністю окремих ТД. Відповідні метрики:

- рівень сигналу RSSI для кожного підключеного пристрою;
- співвідношення сигнал/шум для кожного підключеного пристрою;
- завантаженість конкретного Wi-Fi каналу, який використовує ТД;
- кількість підключених пристроїв до даної ТД;
- статистика трафіку для даної ТД;
- кількість помилок передачі/прийому на даній ТД;
- передаточна швидкість для кожного підключеного пристрою;
- інформація про сусідні точки доступу (як свої, так і чужі);
- кількість спроб підключення (успішних та невдалих) до даної ТД;
- причини невдалих спроб підключення (помилка аутентифікації, DHCP).

Моніторинг спроб підключення, в тому числі невдалих, є важливим для виявлення проблем з аутентифікацією, асоціацією, отриманням IP-адреси та інших причин, які заважають пристроям успішно приєднатися до мережі. Відповідні метрики:

- кількість спроб підключення;
- кількість успішних підключень;
- кількість невдалих підключень;
- причини невдалих підключень (наприклад, неправильний пароль, помилка аутентифікації 802;1X, помилка DHCP, відмова в асоціації, слабкий сигнал);
- MAC-адреса пристрою, що намагався підключитись;
- час спроби підключення.

Пристрої з відкритою архітектурою (наприклад, ноутбуки, деякі смартфони з розширеними можливостями налаштування, спеціалізовані пристрої для

моніторингу) дозволяють встановити додаткове програмне забезпечення для збору детальних метрик з боку клієнта. Можливий збір більш специфічних метрик, що стосуються роботи мережевого адаптера пристрою. Потребує доступу до операційної системи пристрою. Відповідні метрики (додатково до загальних Wi-Fi метрик):

- статистика роботи мережевого адаптера (кількість переданих/прийнятих пакетів, кількість помилок на рівні адаптера).
- інформація про драйвер мережевого адаптера.
- список доступних Wi-Fi мереж, їхній рівень сигналу та канали (з точки зору пристрою).
- результати активних тестів, запущених з пристрою (пінг, тест пропускної здатності).

Більшість споживчих пристроїв (смартфони, планшети, "розумні" пристрої) мають закриту архітектуру, що обмежує або унеможливлює встановлення стороннього програмного забезпечення для детального моніторингу. Моніторинг таких пристроїв здійснюється переважно з боку маршрутизатора або точки доступу. Моніторинг обмежується інформацією, яку надають маршрутизатор або точка доступу про взаємодію з цим пристроєм, а саме:

- всі метрики для підключених пристроїв (рівень сигналу, трафік, помилки з боку ТД, тощо);
- MAC-адреса пристрою;
- IP-адреса пристрою.

Ефективний моніторинг Wi-Fi мережі зазвичай поєднує різні підходи: пасивний для загального огляду та виявлення аномалій, активний для тестування продуктивності під навантаженням, та збір даних як з маршрутизатора, так і з точок доступу для повної картини стану мережі та підключених пристроїв. Розуміння можливостей отримання метрик з різних типів пристроїв також дозволяє обрати найбільш відповідні інструменти та методи моніторингу.

Моніторинг активності Wi-Fi не обмежується лише продуктивністю. Важливо відстежувати властивості безпеки.

– виявлення несанкціонованих (Rogue) точок доступу шляхом моніторингу ефіру на наявність ТД, які не належать вашій мережі, але можуть становити загрозу безпеці або створювати перешкоди.

– Виявлення "злих близнюків", тобто ТД, що імітують легітимні мережі для перехоплення трафіку або облікових даних.

– моніторинг спроб несанкціонованого доступу через відстеження багаторазових невдалих спроб підключення, що може свідчити про спроби підбору пароля.

– виявлення підозрілої активності пристроїв, наприклад, аномально великого обсягу трафіку з одного пристрою, спроб сканування мережі тощо.

– моніторинг стану безпекових налаштувань - перевірка використання сильних методів шифрування (WPA2/WPA3), стану автентифікації 802.1X тощо.

Аналіз протоколів Wi-Fi може надати дуже детальну інформацію про причини проблем, наприклад:

– аналіз кадрів управління та контролю (management and control frames) для виявлення проблем з асоціацією, аутентифікацією, роумінгом;

– аналіз повторної передачі пакетів (retransmissions) на низькому рівні, що вказує на погані умови радіопередачі;

– аналіз затримок між відправленням запитів та отриманням відповідей на різних етапах встановлення з'єднання.

Окрім завантаженості каналу з точки зору Wi-Fi трафіку, важливо моніторити весь радіочастотний спектр для виявлення джерел не-Wi-Fi перешкод (наприклад, мікрохвильові печі, Bluetooth-пристрої, бездротові камери).

2.2 Алгоритми виявлення пасивного прослуховування

Розглянемо алгоритми виявлення пасивного сніфінгу в Wi-Fi мережах розумного будинку на базі пристроїв IoT. Пасивний сніфінг — це тип кібератаки, за якого зловмисник отримує доступ до мережевого трафіку без генерації власних

пакетів. Така атака не створює активної взаємодії з пристроями в мережі й, відповідно, не залишає слідів у журналах чи логах, що робить її вкрай складною для виявлення традиційними методами. Стаття [13] присвячена розробці та валідації методу виявлення пасивного сніфінгу в Wi-Fi мережах розумного дому на базі пристроїв IoT. Основна ідея полягає у використанні мережевої системи моніторингу для збору характеристик пристроїв у поєднанні з ансамблевим навчанням Random Forest для класифікації активності пристроїв як «нормальна» чи «підозріла».

Для IoT-мереж розумного будинку складність може полягати у наступному. Мережа містить велику кількість пристроїв, які часто працюють на легковагових ОС (Contiki, TinyOS), не дозволяє встановити традиційне ПЗ моніторингу. Wi-Fi передає пакети широкомовно, що дає можливість будь-якому пристрою з увімкненим проміскуїтетним режимом прослуховувати весь трафік. Ресурсні обмеження IoT-пристроїв не дозволяють їм виконувати локальний аналіз чи фільтрацію.

Для розв'язання проблем автори запропонували архітектуру, де вся телеметрія про навантаження, використання CPU, пам’яті, диску, затримки RTT тощо передається на мережеву систему моніторингу (NMS). А аналіз здійснюється зовнішнім інструментом — без змін у прошивці чи ПЗ IoT-пристроїв. У системі створюється умисне мережеве навантаження, яке активує фонову роботу сніфінг-програм (Wireshark, Tcpdump), змінюючи метрики роботи системи.

Підхід ґрунтується на класифікації за зібраними характеристиками пристрою, які можуть сигналізувати про приховану активність sniffing-засобів. Зібрані характеристики включають: завантаження CPU, обсяг запису на диск, використання пам’яті, RTT (змінюється при MAC-флудингу [14]), мережевий трафік .

Система класифікує пристрій за ознаками як: not to sniffing; Tcpdump Verbose Mode; Tcpdump Write Mode; Wireshark; Tshark.

Усі ці режими використовуються як класи для задачі багатокласової класифікації.

Оскільки пасивний сніфінг не створює трафік, він майже не помітний без стороннього впливу. Автори пропонують створити штучне навантаження, яке запускається спеціально для викриття такого типу атак. Це може бути:

– флуд ARP-пакетів через macof.py [15];

– імітація сесій у мережі через підроблені TCP-з'єднання;

– створення великого обсягу випадкового трафіку, що провокує sniffer-засіб до зберігання або обробки.

У цей час NMS збирає метрики:

– завантаженість CPU - чи зростає споживання при збільшенні трафіку;

– чи з'являється запис на диск у відповідь на навантаження;

– чи фіксується ріст використання RAM у програмах аналізу трафіку;

– чи зростає час RTT відповіді ICMP-запитів (як побічний ефект навантаження на систему);

– трафік: чи зростає обсяг вхідних/вихідних пакетів.

Після порівняння цих метрик у стані без навантаження і при навантаженні, система:

– створює профіль типових реакцій;

– обчислює похідні характеристики (середнє, дисперсію, стандартне відхилення);

– використовує z-статистику для виявлення значущих відхилень;

– передає ці метрики у моделі машинного навчання для класифікації.

Модель виявлення sniffing-активності базується на порівнянні метрик роботи системи в умовах навантаження і без навантаження. Для аналізу використовуються статистичні характеристики, такі як:

– Середнє значення часу відгуку (RTT);

– Стандартне відхилення;

– Коефіцієнт зміни.

Модель Z-статистики Z, яка визначає ступінь відхилення для різних умов

$$Z = \frac{\bar{X}_1 - \bar{X}_2}{\sqrt{\frac{S_1^2}{n_1} + \frac{S_2^2}{n_2}}},$$

де μ_1, μ_2 математичні сподівання RTT для різних умов

$\bar{X}_1, \bar{X}_2$ середні RTT для вибірок розміру n_1 і n_2

S_1, S_2 стандартні відхилення

Якщо $Z > 2.36$, гіпотеза про однаковість умов відхиляється, що може свідчити про наявність сніфінгу.

Авторами побудовано датасет з такими параметрами:

- 31 ознака (CPU, Memory, Disk, RTT, Traffic)
- 10 класів активності (нормальна, різні режими сніфінгу Tcpdump, Wireshark)
- 12000 зразків, зібраних у домашній Wi-Fi мережі
- штучне навантаження генератором трафіку macof.py для посилення ефекту

Автори встановили що найважливіші ознаки це: використання пам'яті, обсяг запису на диск, вхідний/вихідний трафік. Практичне значення має те, що штучне навантаження підсилює ефект і дозволяє виявити навіть приховані атаки. Обмеження:

- модель потребує попереднього навчання на пристроях у мережі;
- точність знижується для нових/небачених пристроїв;
- RTT в умовах Wi-Fi дуже нестабільний.

Метрики (CPU, пам'ять, диск, трафік, пінг, RTT) беруться з пристрою, який підозрюється у сніфінгу. У дослідженні цей пристрій — Raspberry Pi, на якому навмисно запускаються сніфінг-програми (tcpdump, wireshark), щоб симулювати роботу зловмисника.

Для зчитування даних використовують NMS-систему (Network Monitoring System) — у дослідженні це Paessler PRTG, яка отримує дані через SNMP-протокол. Це означає, що до пристрою потрібно мати підключення. Пристрій має бути керований (тобто мати агент або SNMP-службу). Дані збираються легально і централізовано — для цілей контролю і навчання моделей.

На корпоративних/керованих IoT-платформах [16] ці пристрої зазвичай централізовано адмініструються, тож доступ до SNMP, телеметрії, тощо — цілком можливий. У таких умовах система могла б виявляти приховану/несанкціоновану активність, наприклад:

– Wi-Fi камера почала сильно писати на диск або передавати великі обсяги трафіку;

– сенсор без потреби використовує пам’ять або мережу;

– пристрій, що мав бути пасивним, почав відповідати на ARP/DNS.

2.3 Алгоритми класифікації пристроїв на основі активності

За активністю пристрою у мережі ми можемо визначати, до якої категорії він належить (див 1.1):

– персональний пристрій,

– IoT-пристрій,

– гостьовий пристрій.

Кожен пристрій спостерігається за певними характеристиками активності. Ми обираємо основні параметри, які можемо вимірювати або розраховувати. Позначимо:

– A — середня інтенсивність трафіку пристрою (кількість переданих байтів на одиницю часу, наприклад, за хвилину)

– V — варіація активності протягом дня (розкид обсягу трафіку, коефіцієнт варіації)

– S — частота зміни точок доступу (кількість роумінг-подій за певний час)

– T — середня тривалість підключення (середній час безперервного перебування пристрою у мережі)

– P — тип мережі підключення (основна мережа або гостьова, бінарна ознака)

Згідно з поведінкою пристроїв можемо сформувати базові закономірності:

– для персональних пристроїв високе A, середня V, високе S, тривалі T, підключення до основної мережі (P=0).

– для IoT-пристроїв низьке A, низька V, майже нульове S, дуже велике T, підключення до окремої IoT-мережі або основної (P=0).

– для гостьових пристроїв різне A, високе V, низьке S, коротке T, підключення до гостьової мережі (P=1).

Введемо прості функції належності для кожного класу пристроїв:

Формула для ймовірності персонального пристрою):

$$C_{\text{personal}} = w_1 \cdot \text{norm}(A) + w_2 \cdot \big(1 - \text{norm}(V)\big) + \\ + w_3 \cdot \text{norm}(S) + w_4 \cdot \text{norm}(T) + w_5 \cdot (1 - P).$$

Формула для обчислення ймовірності IoT-пристрою

$$C_{\text{IoT}} = w_1' \cdot \big(1 - \text{norm}(A)\big) + w_2' \cdot \big(1 - \text{norm}(V)\big) + \\ + w_3' \cdot \big(1 - \text{norm}(S)\big) + w_4' \cdot \text{norm}(T) + w_5' \cdot (1 - P).$$

Формула для обчислення ймовірності гостьового пристрою

$$C_{\text{guest}} = w_1'' \cdot \text{norm}(V) + w_2'' \cdot \big(1 - \text{norm}(T)\big) + w_3'' \cdot P,$$

де: norm(X) — нормалізація показника X у діапазоні [0,1],

w_i — вагові коефіцієнти для відповідних ознак.

Класифікаційне рішення. Після обчислення значень C_{personal}, C_{IoT}, C_{guest} пристрій відноситься до тієї категорії, для якої функція має найбільше значення:

$$\text{Class} = \arg\max\big(C_{\text{personal}}, C_{\text{IoT}}, C_{\text{guest}}\big).$$

Для нормалізації параметрів потрібно знати типові мінімальні та максимальні значення для кожної метрики в мережі.

Вагові коефіцієнти w можна налаштовувати емпірично або за допомогою навчання на основі зібраних даних (наприклад, за допомогою простого машинного навчання). У реальній системі доцільно використовувати ще додаткові параметри: тип використовуваного протоколу, патерни запитів до серверів тощо. Схему алгоритму наведено на кресленні КР.КІ.10660603.00.00.001.С1

3. РОЗРОБКА І ТЕСТУВАННЯ ПРОГРАМНОГО ЗАСОБУ МОНІТОРИНГУ АКТИВНОСТІ

3.1. Реалізація програмного модуля моніторингу у реальному часі

Розробка програмного модуля для моніторингу активності пристроїв у Wi-Fi мережі вимагає комплексного підходу до вибору мов програмування та відповідних середовищ. Цей вибір зумовлюється низкою критеріїв: доступ до мережевого рівня, можливість інтеграції з обладнанням MikroTik, обробка великої кількості подій у реальному часі, а також потреба у зручному відображенні даних та масштабованості системи.

Python було обрано як основну мову розробки з огляду на такі переваги:

– багата екосистема бібліотек для мережевого аналізу, зокрема scapy [17], socket, pyshark [18], librouteros [19], які забезпечують доступ до Wi-Fi трафіку, sniffer-режиму, та API MikroTik RouterOS.

– зручність у роботі з базами даних (SQLite, PostgreSQL) через ORM-фреймворки (SQLAlchemy, peewee) або безпосередньо.

Як супутню мову обрано Bash для автоматизації запуску скриптів, збору логів, cron-задач. Для роботи над проєктом використовуються такі середовища:

– Visual Studio Code [20] легке, розширюване середовище, з інтеграцією терміналу, git, підтримкою Python та Docker.

– офіційні інтерфейси взаємодії з маршрутизаторами MikroTik RouterOS Terminal/API [21], зокрема для отримання даних із /interface wireless registration-table, /ip dhcp-server lease, /tool sniffer.

Для реалізації програмного модуля моніторингу активності в бездротовій мережі доцільно провести огляд бібліотек і фреймворків, які забезпечують доступ до необхідної інформації як на рівні мережевих кадрів, так і через взаємодію з мережевим обладнанням. Одним з базових інструментів у цій сфері є бібліотека Scapy, що дозволяє працювати з мережевими пакетами на низькому рівні. Вона надає можливість перехоплення й аналізу Wi-Fi кадрів у monitor mode, включаючи пакети типу beacon, probe, authentication і association. Scapy особливо цінна для

реалізації пасивного аналізу оточення без необхідності з'єднання з мережею, хоча її використання вимагає наявності підтримуваного обладнання та прав адміністратора в системі.

У випадках, коли необхідно отримати інформацію безпосередньо від маршрутизатора, ефективними є бібліотеки, орієнтовані на взаємодію з MikroTik RouterOS. Зокрема, бібліотека RouterOS-API дозволяє надсилати команди через TCP API до маршрутизатора та отримувати структуровані відповіді з реєстраційної таблиці бездротових інтерфейсів, DHCP-сервера, firewall та інших модулів. Вона забезпечує доступ до актуальної інформації про підключені пристрої: MAC-адреси, рівень сигналу, використовуваний протокол, тривалість з’єднання тощо. Також передбачена можливість програмного керування параметрами маршрутизатора, що відкриває перспективи для автоматизованого реагування на мережеві події.

Альтернативним і зручнішим з точки зору структури бібліотечним рішенням є librouteros. Ця бібліотека також реалізує клієнт для RouterOS API, але забезпечує більш зрозумілий і лаконічний синтаксис у порівнянні з RouterOS-api, а також кращу інтеграцію з асинхронними механізмами в Python. Вона особливо зручна при створенні регулярних запитів у фоновому режимі або під час побудови веб-сервісів, які відображають дані з маршрутизатора в реальному часі. Простота використання та читабельність коду роблять librouteros придатною для створення студентських проєктів, орієнтованих на розгортання в локальному середовищі.

Завдання кваліфікаційної роботи полягає у створенні програмного засобу, який дозволяє автоматично моніторити та аналізувати активність пристроїв у Wi-Fi мережі, підключених через маршрутизатор. Модель повинна забезпечити збір мережевих та інтервальних метрик (MAC-адреси, трафік, частота ARP і DNS-запитів, broadcast-активність, рівень сигналу, використання протоколів), а також динамічно визначати аномальну або підозрілу поведінку пристроїв. Додатково модель передбачає автоматичне сповіщення адміністратора у разі виявлення підозрілої активності.

На рисунку 3.1 зображено діаграму класів програмного засобу. Опис методів класів наведено в таблиці 3.1. Діаграму класів наведено на кресленні КР.КІ.10660603.00.00.002.С1

Клас RouterClient відповідальний за моніторинг мережевої активності окремого клієнтського пристрою в локальній Wi-Fi мережі. Цей клас виконує роль об'єкта-інтерфейсу до даних про трафік, що генерується конкретним MAC-адресованим пристроєм, і дозволяє проводити як кількісну, так і якісну оцінку його поведінки.

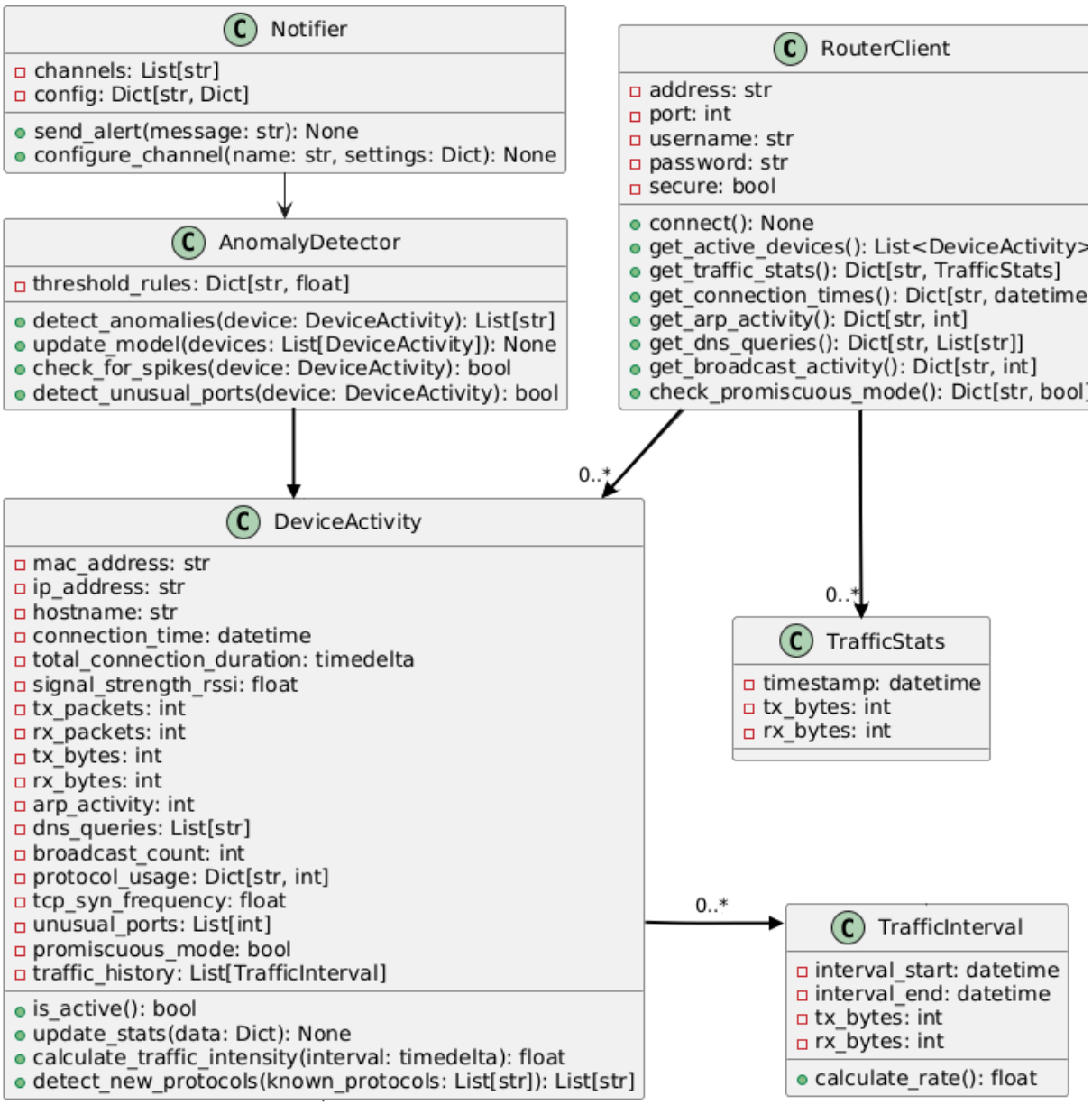


Рисунок 3.1- Діаграма класів

Метод get_arp_activity() призначений для аналізу кількості ARP-запитів, що надходять від пристрою за певний інтервал часу. Підвищена частота таких запитів може вказувати на аномальну активність або спроби сканування мережі. Аналогічно, метод get_dns_queries() дозволяє отримати перелік або кількість DNS-запитів, ініційованих пристроєм. Це дає змогу виявити спроби підключення до

зовнішніх доменів, що не характерні для типових користувачів, або визначити тип пристрою за шаблонами доменів.

Метод get_broadcast_activity() фіксує частоту розсилки широкомовних пакетів (broadcast), що є важливим показником активності пристрою на канальному рівні. Його застосування дозволяє оцінити, чи є пристрій джерелом надмірного фону, який може впливати на загальну пропускну здатність мережі. Останній метод, check_promiscuous_mode(), виконує спеціальну перевірку: чи відповідає пристрій на мережеві запити, які не адресовані безпосередньо йому. Така поведінка є типовою ознакою активного проміскуїтетного режиму, який використовується для перехоплення трафіку і є критичним з точки зору безпеки.

Клас RouterClient відіграє ключову роль у системі моніторингу, забезпечуючи доступ до діагностичних показників поведінки окремих пристроїв у мережі, що дозволяє класифікувати їхню активність, виявляти потенційні загрози та забезпечувати підтримку політик доступу на основі поведінкових критеріїв.

Клас DeviceActivity є центральною структурою для збереження та аналізу характеристик мережевої активності окремого пристрою в бездротовій мережі. Його основне призначення полягає у фіксації поведінкових і технічних параметрів, які дозволяють оцінити тип, роль і потенційні ризики, пов’язані з підключенням пристрою до мережі. Клас структурує дані в розрізі як окремих подій, так і часових інтервалів, що робить його придатним для аналітики реального часу, трендового аналізу та машинного навчання.

Метод signal_strength_rssi зберігає або обчислює рівень сигналу між пристроєм і точкою доступу (RSSI), що є критичним для оцінки фізичної віддаленості або мобільності пристрою. Цей показник також допомагає у виявленні далеких чи зовнішніх спостережуваних пристроїв, які не є частиною домашньої або корпоративної мережі. Параметр arp_activity дозволяє оцінити інтенсивність ARP-запитів — як індикатор активності пристрою на канальному рівні, потенційного сканування або конфліктів адрес. Аналогічно, dns_queries є індикатором комунікаційної активності пристрою в контексті доступу до зовнішніх або внутрішніх ресурсів. Аналіз списку доменів може бути використаний для класифікації пристроїв за призначенням (побутовий, офісний, IoT).

Таблиця 3.1 - Опис класів та методів

Клас	Методи
RouterClient	get_arp_activity() – отримує частоту ARP-запитів. get_dns_queries() – отримує DNS-запити пристроїв. get_broadcast_activity() – частота broadcast-пакетів пристрою. check_promiscuous_mode() – визначає, чи відповідає пристрій на ARP/DNS-запити, що вказує на проміскуїтетний режим.
DeviceActivity	signal_strength_rssi – сигнал пристрою для визначення віддаленості. arp_activity – кількість ARP-запитів. dns_queries – перелік DNS-запитів пристрою. broadcast_count – кількість broadcast-запитів. protocol_usage – використання мережевих протоколів. tcp_syn_frequency – частота відкриття TCP-з'єднань. unusual_ports – список незвичайних портів, які використовуються. promiscuous_mode – чи працює пристрій в проміскуїтетному режимі. traffic_history – історія трафіку по інтервалах для розрахунку інтенсивності.
TrafficStats і TrafficInterval:	Для збереження історичних даних трафіку, з яких можна розрахувати інтенсивність та виявити аномалії
AnomalyDetector	check_for_spikes() – визначає різкі зміни інтенсивності трафіку. detect_unusual_ports() – виявляє підозріле використання незвичайних портів

Метод broadcast_count дозволяє фіксувати кількість широкомовних повідомлень, які генерує пристрій, що важливо для оцінки його впливу на завантаження сегменту мережі. Параметр protocol_usage визначає, які мережеві протоколи активно використовуються (наприклад, HTTP, HTTPS, MQTT, SMB), що дозволяє ідентифікувати профіль поведінки пристрою. Метод tcp_syn_frequency відстежує кількість SYN-пакетів, які ініціюють нові TCP-з'єднання, що є ключовим індикатором клієнтської чи серверної активності, а також може вказувати на потенційні сканування портів.

Метод unusual_ports зберігає список нестандартних або нетипових портів, які використовуються пристроєм. Це може бути ознакою специфічного програмного забезпечення або потенційно небажаного трафіку. Параметр promiscuous_mode

фіксує, чи працює пристрій у проміскуїтетному режимі, що важливо для виявлення пасивного аналізу трафіку. Нарешті, traffic_history відображає змінну активність пристрою у часі й використовується для побудови динамічних профілів, оцінки навантаження та виявлення аномалій.

Клас AnomalyDetector призначений для виявлення відхилень у поведінці пристроїв у бездротовій мережі на основі аналізу мережевої активності. Його функціональне призначення полягає в ідентифікації нетипових патернів, які можуть свідчити про потенційні загрози, зловмисну активність або порушення звичайного режиму роботи пристрою.

Метод check_for_spikes() реалізує механізм виявлення різких змін інтенсивності мережевого трафіку за допомогою аналізу часових рядів. Його основне завдання — ідентифікувати стрибкоподібні відхилення від базової лінії трафіку пристрою, що можуть бути зумовлені несанкціонованим використанням пропускної здатності, DoS-атаками або активацією прихованих сервісів. Для цього зазвичай використовуються методи скользячого середнього, зваженого згладжування або статистичні критерії, що порівнюють поточну активність з попередніми інтервалами.

Метод detect_unusual_ports() спрямований на виявлення нетипового використання мережевих портів, які не відповідають очікуваному шаблону для даного типу пристрою. Наприклад, використання нестандартних портів на IoT-пристрої або раптова поява відкритих портів, характерних для сервісів віддаленого керування, може вказувати на порушення політики безпеки чи компрометацію. Методика порівнює активні порти з попередньо зібраним профілем типових портів і відмічає ті, що не належать до цього списку.

3.2. Розгортання модуля в інфраструктурі бездротової мережі

Розгортання засобу моніторингу активності в бездротовій мережі передбачає кілька послідовних етапів, які охоплюють як технічну, так і аналітичну частину процесу. На першому етапі виконується підготовка інфраструктури, зокрема

налаштування точок доступу з підтримкою збору статистики, активація API на маршрутизаторі (наприклад, MikroTik), а також забезпечення доступу до журналів DHCP, ARP, DNS та інших протоколів. Наступним кроком є розробка або налаштування програмного модуля, який виконує збір, обробку та збереження параметрів активності пристроїв. Тут використовуються бібліотеки для взаємодії з маршрутизатором, аналізу трафіку й нормалізації метрик.

Можна створити узагальнену схему архітектури мережі та позначити на ній ключові точки збору інформації та типи моніторингу, пов'язані з описаними в 2.1 варіантами (рисунок 3.2).

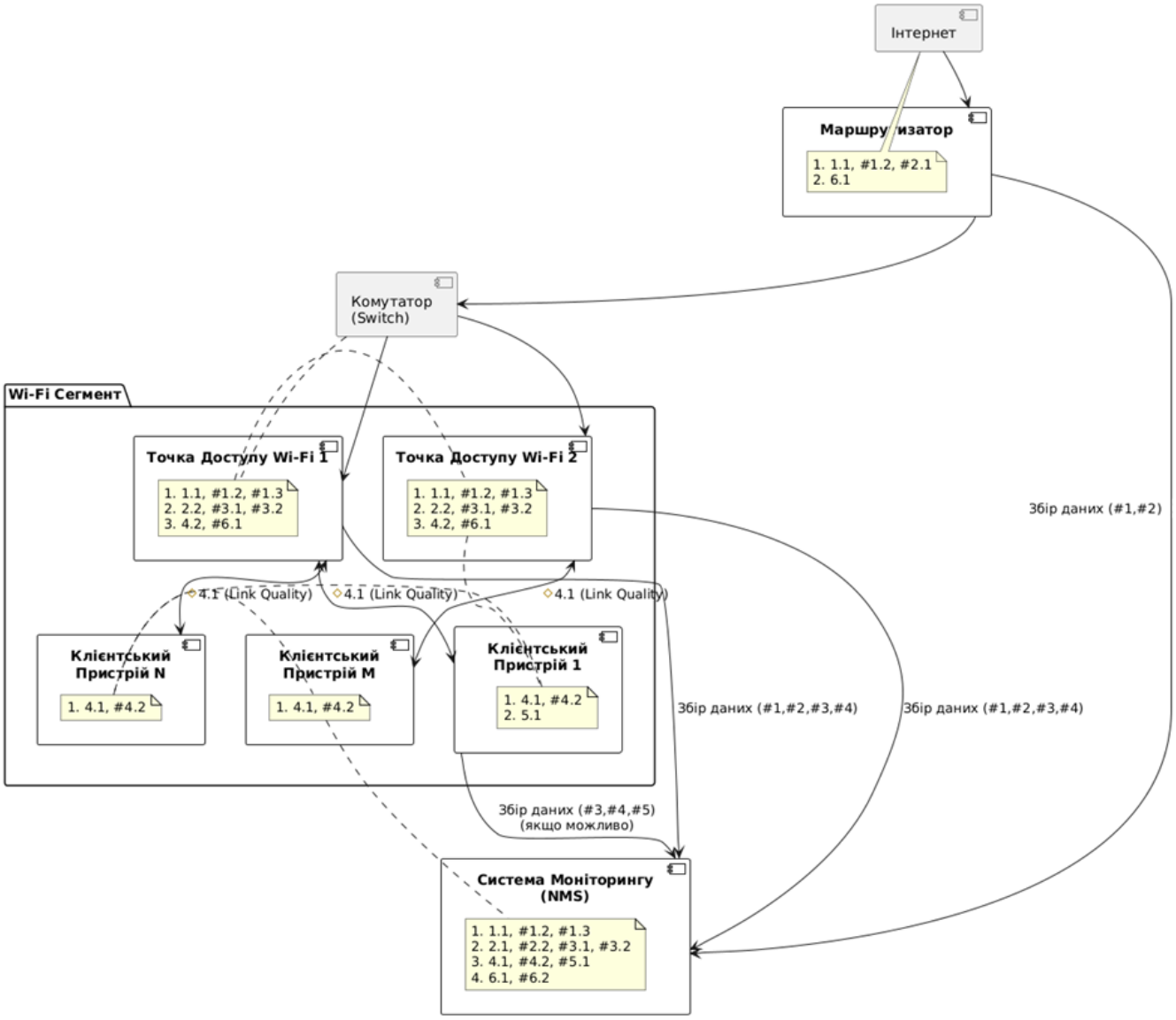


Рисунок 3.2 -Точки збору інформації та типи моніторингу мережі

Схема зображує типову архітектуру локальної мережі з доступом до

Інтернету, яка включає маршрутизатор, комутатор (необов'язково, але типово для багатьох ТД) та точки доступу, до яких підключаються клієнтські пристрої. Система Моніторингу (NMS) збирає дані з різних компонентів мережі.

Номери на рисунку позначають зони збору метрик або типи моніторингу, пов'язані з відповідними компонентами (таблиця 3.1).

Таблиця 3.1 – Підписи до рисунку

Зони збору метрик	Тип інформації
#1. Моніторинг за методом	#1.1 Пасивний моніторинг: збір даних про існуючий трафік та стан мережі без активного втручання. #1.2 Активний моніторинг: генерація штучного трафіку для тестування продуктивності під навантаженням. #1.3 Моніторинг спектру: виявлення джерел радіочастотних перешкод .
#2. Моніторинг за точкою зняття метрики	#2.1 З Маршрутизатора: метрики, що стосуються загального стану мережі, WAN-з'єднання, загального трафіку, стану маршрутизатора. #2.2 З ТД: метрики, що стосуються безпосередньо бездротового сегменту, стану радіоефіру, взаємодії з клієнтами на рівні ТД.
#3. Моніторинг за статусом пристроїв	#3.1 Для успішно підключених пристроїв: метрики якості з'єднання та активності пристроїв, що наразі працюють у мережі. #3.2 Для пристроїв, що намагались підключитись: метрики, пов'язані зі спробами підключення, включаючи успішні та невдалі спроби та їхні причини.
#4. Моніторинг каналу/з'єднання	#4.1 Якість бездротового з'єднання (Link Quality): метрики, що описують якість зв'язку між конкретною ТД та конкретним клієнтським пристроєм (RSSI, SNR, Data Rate). #4.2 Статистика радіоінтерфейсу на ТД або клієнті: кількість помилок, ретрансляцій, колізій на фізичному та канальному рівнях.
#5. Моніторинг з пристрою	#5.1 Метрики з клієнтського пристрою: Детальна інформація про роботу мережевого адаптера клієнта, результати тестів, запущених з пристрою, досвід користувача.
#6. Додатковий моніторинг	#6.1 Безпековий моніторинг: Виявлення загроз, несанкціонованих пристроїв, моніторинг безпекових подій. #6.2 Історичні Дані та Трендінги: Збір, зберігання та аналіз метрик за тривалий період для виявлення закономірностей, планування та аналізу ефективності змін.

Отже, з маршрутизаторів (RouterOS, OpenWRT, UniFi тощо) можна зібрати наступні метрики.

Таблиця 3.2 – Систематизація метрик

Тип	Зібрані дані
Мережеві параметри	MAC-адреса / IP-адреса — для ідентифікації пристрою. Час останнього підключення / загальний час в мережі. Рівень сигналу (RSSI) — для фіксації місця/віддаленості. Кількість вхідних/вихідних пакетів (Tx/Rx). Обсяг вхідного/вихідного трафіку (в байтах). Частота ARP-запитів/відповідей — ARP-активність. DNS-запити, їх кількість та типи. Частота broadcast-пакетів, які ініціює пристрій. Типи протоколів, які використовує пристрій (HTTP, TLS, ICMP тощо). Частота відкриття нових з’єднань (TCP SYN). Присутність в unusual ports (нехарактерні порти). Використання проміскуїтетного режиму — можливо лише через ARP/DNS-challenge.
Інтервальні метрики (динаміка)	Зміна інтенсивності трафіку за хвилину/10 хв/годину. Раптовий стрибок у запитах або передачі даних. Поява нових протоколів або напрямків трафіку.

Джерела метрик для обладнання MikroTik /ip accounting, /interface monitor-traffic, /ip firewall connection, /tool sniffer, SNMP, DHCP/ARP таблиці, syslog, torch.

3.3 Тестування програмного засобу моніторингу

Приклад отримання інформації про активні та відомі Wi-Fi пристрої (рисунок 3.3) містить такі параметри:

- Тип протоколу (Wi-Fi mode / protocol) 802.11n, 802.11ac, 802.11ax.
- Статус з'єднання: associated, authenticated, unauthenticated, disconnected.

Wi-Fi Device Activity Report – MikroTik Router
Generated on: 2025-05-04 09:30:00
SSID: HomeNetwork_2.4GHz

Connected Devices:

#	MAC Address	Device Name	Signal (dBm)	Protocol	Wi-Fi Status	Connection State
1	[redacted]	Samsung_Galaxy_S9	-53	802.11ac	associated	connected
2	[redacted]	Laptop_HP_Office	-62	802.11n	associated	connected
3	[redacted]	ESP32_Sensor_1	-71	802.11b	authenticated	connected
4	[redacted]	Desktop_PC_LAN	-48	802.11ac	associated	connected

Recently Known but Disconnected Devices:

#	MAC Address	Device Name	Last Signal (dBm)	Protocol	Wi-Fi Status	Connection State
1	[redacted]	iPhone_Maria	-68	802.11n	unauthenticated	disconnected
2	[redacted]	Kindle_Paperwhite	-80	802.11g	unauthenticated	disconnected
3	[redacted]	SmartTV_LG_Living	-75	802.11n	deauthenticated	disconnected

Рисунок 3.3 - Інформація про активні та відомі пристрої

Приклад типізації пристроїв на основі історичних даних. Виділяються типи пристроїв за поведінкою підключення:

- Frequent – пристрій регулярно з'являється в мережі;
- Intermittent – пристрій періодично зникає і з’являється (нестабільна активність);
- New – пристрій виявлено вперше;
- One-time – пристрій був підключений лише один раз.

SSID: SmartHome_AP_5GHz

Connected Devices:

#	MAC Address	Device Name	Signal(dBm)	Protocol	Device Type	Connection Frequency
1	[redacted]	Desktop_PC_Office	-48	802.11ac	frequent	Connected daily
2	[redacted]	Samsung_Galaxy_S9	-52	802.11ax	intermittent	Connected 10 of last 30 days
3	[redacted]	ESP32_Sensor_Balcon	-75	802.11n	frequent	Uptime >90%
4	[redacted]	Laptop_Visitor_Jane	-66	802.11ac	new	First seen today

Previously Connected Devices (Currently Offline):

#	MAC Address	Device Name	Last Seen	Last Sign	Protocol	Device Type	Connection Freq
1	[redacted]	Kindle_Guest	2025-04-31	-78	802.11g	one-time	once
2	[redacted]	iPhone_Maria	2025-05-02	-63	802.11n	intermittent	3 of last 30 days
3	[redacted]	SmartTV_LivingRoom	2025-05-03	-71	802.11n	frequent	Online 6+ hours daily

Summary:
• Total known devices: 7
• Actively connected: 4
• Recently offline: 3
• Device classification source: Historical Wi-Fi connection logs over 30 days

Classification Criteria:
- **Frequent**: ≥20 connections/30 days або uptime ≥70%
- **Intermittent**: 2–19 connections/30 days або uptime між 10% і 70%
- **New**: перше з’єднання сьогодні
- **One-time**: лише одне з’єднання за весь період спостереження

Рисунок 3.4 – Класифікація пристроїв за поведінкою підключення

Класифікація пристроїв у мережі на основі заданих параметрів активності (див. 2.3) наведена на рисунку 3.5

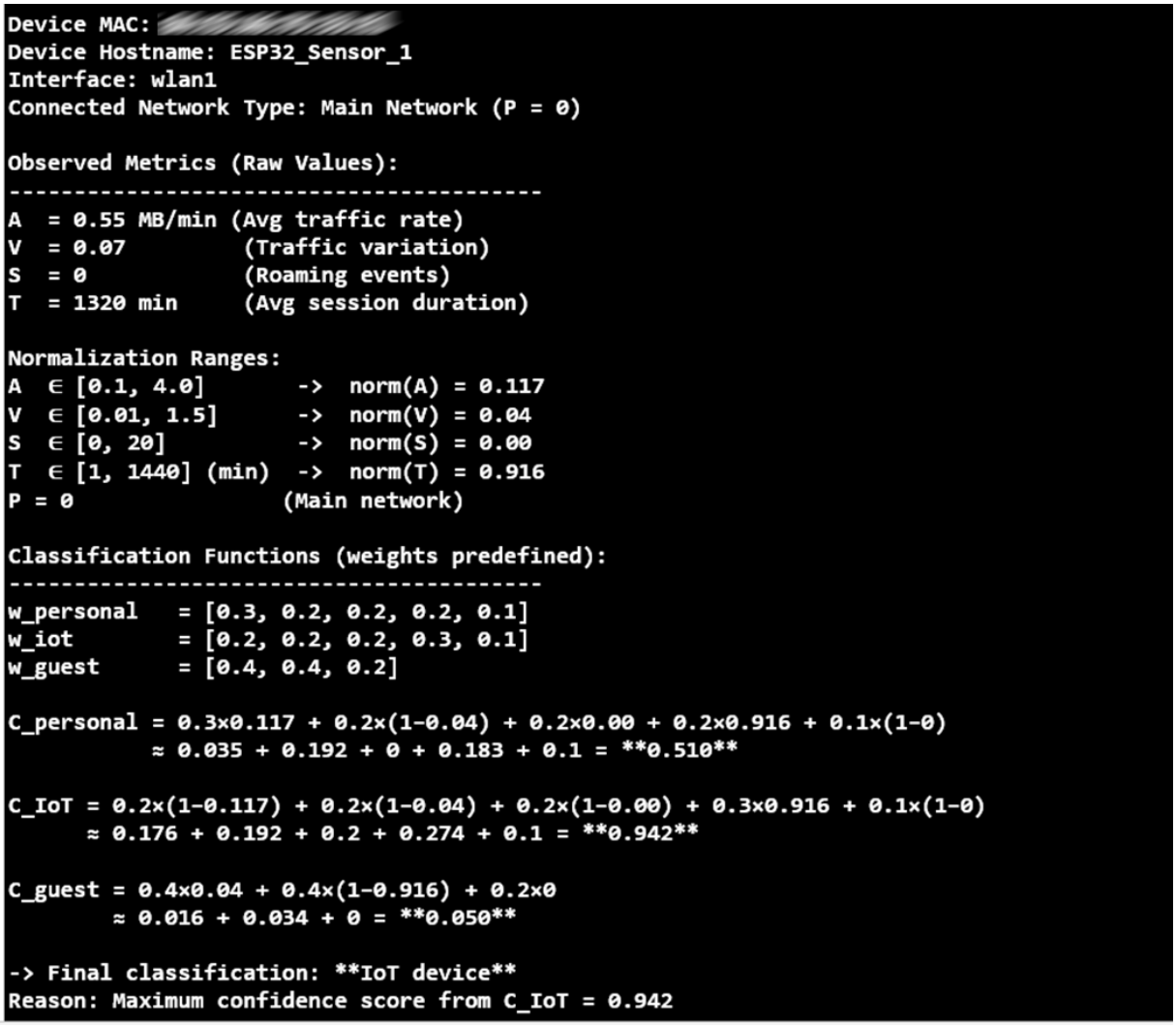


Рисунок 3.5 - Класифікація пристроїв у мережі на основі активності

У процесі тестування програмного модуля було перевірено коректність збору даних, обчислення параметрів активності та класифікації пристроїв у режимі реального часу. Наведені скріншоти з консолі підтверджують, що система успішно ідентифікує пристрої в мережі, фіксує їхній MAC-адрес, рівень сигналу, тип підключення та обчислює ймовірність належності до однієї з трьох категорій: персональний, IoT або гостьовий. Для кожного пристрою розраховано значення класифікаційних функцій, і система приймає рішення на основі максимальної оцінки. Результати виводяться у стислому форматі та зберігаються в лог-файлі, що підтверджує працездатність модуля та коректність реалізованого алгоритму.

ВИСНОВКИ

В результаті виконання кваліфікаційної роботи отримано наступні висновки

1. Проаналізовано принципи функціонування бездротових мереж, сучасні програмні засоби моніторингу Wi-Fi і характерні шаблони поведінки персональних, IoT та гостьових пристроїв. На основі цього сформульовано вимоги до системи моніторингу та визначено ключові параметри активності, що використовуватимуться для подальшої класифікації пристроїв у мережі.

2. Обґрунтовано вибір технологій моніторингу, що поєднують пасивний і активний підходи до збору даних із маршрутизаторів, точок доступу та клієнтських пристроїв. Ураховано, що маршрутизатори забезпечують глобальний огляд мережі, тоді як точки доступу дозволяють деталізовано аналізувати параметри зв’язку та ефірного середовища, зокрема рівень сигналу, кількість помилок, швидкість передачі та спроби підключення.

3. Розроблено алгоритм класифікації пристроїв на основі ключових параметрів активності, таких як інтенсивність трафіку, варіативність, роумінг, тривалість з'єднання та тип підключеної мережі. Запропоновано функції належності для кожного класу пристроїв (персональні, IoT, гостьові), які дозволяють автоматично визначати категорію пристрою за допомогою нормалізованих метрик та вагових коефіцієнтів, що підлягають налаштуванню або навчанню.

4. Розроблено структуру програмного модуля, яка охоплює класи для збору та аналізу параметрів активності пристроїв у Wi-Fi мережі. Архітектура базується на використанні Python з інтеграцією бібліотек Scapy, RouterOS-API та librouteros і підтримки як пасивного, так і активного моніторингу.

5 Реалізовано засіб який здійснює збір, обробку та виведення інформації про підключення, активність і протоколи пристроїв на основі метрик, отриманих із маршрутизаторів MikroTik. Система також підтримує виявлення аномалій, класифікацію пристроїв за поведінкою, та формування попереджень для адміністратора у разі виявлення підозрілої активності.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Стрельчук В. А., Гладій А. І. Модель програмного забезпечення для моніторингу пристроїв у wi-fi мережах. *ІІ Всеукраїнська науково-практична конференція студентів, аспірантів та молодих вчених «Інтелектуальні комп'ютерні системи та мережі» (ІКСМ весна 2025)*. (м. Тернопіль, . м. Тернопіль, С. 92–93.

2. Baker J. Exploring Audio Sensing in Detecting Social Interactions Using Smartphone Devices. 2020. DOI:10.13140/RG.2.2.18190.59201.

3. 802.11 Association process – wifi-bond. URL: https://wifibond.com/2017/04/08/802-11-association-process/ (accessed 20/05/2025).

4. ISO/IEC/IEEE International Standard - Information technology–Telecommunications and information exchange between systems Local and metropolitan area networks–Specific requirements Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications. *ISO/IEC/IEEE 8802-11:2012(E) (Revison of ISO/IEC/IEEE 8802-11-2005 and Amendments)*. 2012. P. 1–2798. DOI:10.1109/IEEESTD.2012.6361248.

5. IEEE SA - The Evolution of Wi-Fi Technology and Standards. URL: https://standards.ieee.org/beyond-standards/the-evolution-of-wi-fi-technology-and-standards/ (accessed 04/06/2025).

6. IEEE Standard for Telecommunications and Information Exchange Between Systems - LAN/MAN Specific Requirements - Part 11: Wireless Medium Access Control (MAC) and physical layer (PHY) specifications: High Speed Physical Layer in the 5 GHz band. *IEEE Std 802.11a-1999*. 1999. P. 1–102. DOI:10.1109/IEEESTD.1999.90606.

7. Wireshark. The world's leading network protocol analyzer. *Wireshark*. URL: https://www.wireshark.org/ (дата звернення: 04.06.2025).

8. Марченко В. В., Крючкова Л. П. Радіомоніторинг частотних каналів мережі Wi-Fi. *Сучасний захист інформації*. 2(38), 2019. URL: https://journals.dut.edu.ua/index.php/dataprotect/article/download/2312/2211/

9. Як зламати Wi-Fi: стартуємо з хакерської утиліти Aircrack-Ng - iSearch - ефективний пошук в Інтернеті. URL:

http://isearch.kiev.ua/uk/searchpractice/internetsecurity/1726-how-to-crack-wi-fi-start-with-hacking-tools-aircrack-ng (дата звернення: 20.05.2025).

10. PRTG Network Monitor: All-in-One Network Monitoring Software. *Paessler - The Monitoring Experts*. 2025. URL: https://www.paessler.com/prtg (дата звернення: 20.05.2025).

11. published D. M. Hands on: I tested the Paessler PRTG Network Monitor - see what I thought of it. *TechRadar*. 17.03.2025. URL: https://www.techradar.com/pro/paessler-prtg-network-monitor-23-4-review (дата звернення: 20.05.2025).

12. Cisco Prime Infrastructure - Cisco. URL: https://www.cisco.com/c/en/us/support/cloud-systems-management/prime-infrastructure/series.html (accessed 20/05/2025).

13. Jung Jin H., Rahimi Ghashghaei F., Elmrabit N. et al. Enhancing Sniffing Detection in IoT Home Wi-Fi Networks: An Ensemble Learning Approach With Network Monitoring System (NMS). *IEEE Access*. Vol. 12, 2024. P. 86840–86853. DOI:10.1109/ACCESS.2024.3416095.

14. MAC Flooding Program Project Overview | Cybercademy. URL: https://cybercademy.org/mac-flooding-program-project-overview/ (accessed 04/06/2025).

15. WhiteWinterWolf macof.py, a MAC address table overflow utility. URL: https://github.com/WhiteWinterWolf/macof.py (accessed 04/06/2025).

16. Українські компанії IoT та розумного будинку | DOU. URL: https://dou.ua/forums/topic/51818/ (дата звернення: 04.06.2025).

17. Scapy is a powerful interactive packet manipulation library written in Python. URL: https://scapy.net/ (accessed 04/05/2025).

18. pyshark: Python wrapper for tshark, allowing python packet parsing using wireshark dissectors. URL: https://github.com/KimiNewt/pyshark (accessed 04/06/2025).

19. Kostka Ł. luqasz/librouteros. Python implementation of MikroTik RouterOS API. URL: https://github.com/luqasz/librouteros (accessed 18/05/2025).2025.

20. Visual Studio Code - Code Editing. Redefined. URL: https://code.visualstudio.com/ (accessed 04/06/2025).

21. socialwifi/RouterOS-api. Python API to RouterBoard devices produced by MikroTik. Social WiFi, 2025. URL: https://github.com/socialwifi/RouterOS-api (accessed 18/05/2025).2025.

22. Гапак О. М., Балога С. І. Захист інформації в комп'ютерних системах: підручник. Ужгород : ПП «АУТДОР-ШАРК», 2021. 184 с.

23. Жураковський Б. Ю., Зенів І. О. Комп'ютерні мережі Частина 1: навчальний посібник. Київ : КПІ ім. Ігоря Сікорського, 2020. 336 с.

24. Голь В. Д., Ірха М. С. Телекомунікаційні та інформаційні мережі: навчальний посібник. Київ : ІСЗЗІ КПІ ім. Ігоря Сікорського, 2021. 250 с.

25. Bonaventure O. Computer Networking: Principles, Protocols and Practice. Saylor, 2022. 278 p.

26. Camisso J. Making Servers Work: A Practical Guide to Linux System Administration. DigitalOcean, 2020. 281 p.

27. The Cisco Learning Network. 2024. URL: https://learningnetwork.cisco.com

28. Eksim A. Wireless Communications and Networks - Recent Advances. InTech, 2012. 596 p.

29. pytest documentation. URL: https://docs.pytest.org/en/stable/ (accessed 03/05/2025).

30. Березький О. М., Мельник Г. М., Дубчак Л. О. та ін. Методичні вказівки до випускних кваліфікаційних робіт освітнього рівня "Бакалавр" спеціальності "Комп'ютерна інженерія". ред. О. М. Березький. Тернопіль : ЗУНУ, 2024. 52 с.