Київський столичний університет імені Бориса Грінченка
Факультет інформаційних технологій та математики
Кафедра інформаційної та кібернетичної безпеки
імені професора Володимира Бурячка

«Допущено до захисту»
Завідувач кафедри інформаційної та
кібернетичної безпеки імені
професора Володимира Бурячка
кандидат технічних наук, доцент
Складанний П.М.

_____
(підпис)
« ___ » _____ 20__ р.

КВАЛІФІКАЦІЙНА РОБОТА
на здобуття другого (магістерського)
рівня вищої освіти

Спеціальність 125 Кібербезпека та захист інформації

Тема роботи:
ДОСЛІДЖЕННЯ МЕТОДІВ ЗАХИСТУ ВІД АТАК НА БЕЗДРОТОВІ МЕРЕЖІ ОРГАНІЗАЦІЇ

Виконала
студентка групи БІКСм-1-24-1.4.д
Соболенко Ізабелла Андріївна

_____
(підпис)

Науковий керівник
Кандидат технічних наук, доцент
Платоненко Артем Вадимович

_____
(підпис)

Київ – 2025

Київський столичний університет імені Бориса Грінченка
Факультет інформаційних технологій та математики
Кафедра інформаційної та кібернетичної безпеки
імені професора Володимира Бурячка

Освітньо-кваліфікаційних рівень – магістр
Спеціальність 125 Кібербезпека та захист інформації
Освітня програма 125.00.01 Безпека інформаційних і комунікаційних систем

«Затверджую»
Завідувач кафедри інформаційної та
кібернетичної безпеки імені
професора Володимира Бурячка
кандидат технічних наук, доцент
Складанний П.М.

_____
(підпис)
« ___ » _____ 20__ р.

ЗАВДАННЯ

НА КВАЛІФІКАЦІЙНУ РОБОТУ СТУДЕНТУ

Соболенко Ізабеллі Андріївні

1. Тема роботи: «Дослідження методів захисту від атак на бездротові мережі організації»;
   керівник Платоненко Артем Вадимович, доцент кафедри інформаційної та кібернетичної безпеки імені професора Володимира Бурячка,
   затверджені наказом ректора від «___»_____ 20___ року №__.
2. Термін подання студентом роботи «01» грудня 2025 р.
3. Вихідні дані до роботи:
   3.1 науково-технічна та нормативна література з теми дослідження: наукові праці з кібербезпеки; стандарти ISO/IEC 27001, ISO/IEC 27005:2019; дослідження сучасних методів ML/DL у Wi-Fi; методики побудови IDS;
   3.2 методи: наукові праці з кібербезпеки; стандарти ISO/IEC 27001, ISO/IEC 27005:2019; дослідження сучасних методів ML/DL у Wi-Fi; методики побудови IDS;
   3.3 технології: Kismet; Suricata; PyShark; SIEM; віртуалізація гіпервізора; віртуальні мережі;
   3.4 алгоритми: SVM, Random Forest, XGBoost, CNN/GRU, lightweight cryptography, алгоритми аналізу Wi-Fi фреймів;
   3.5 мова програмування: Python.;

3.6 математичні моделі та методи статистичні моделі, ймовірнісні моделі, метод Монте-Карло, моделі поведінкового аналізу, ризик-орієнтована модель ISO/IEC 27005: .

4. Зміст текстової частини роботи (перелік питань, які потрібно розробити):

4.1Розроблення лабораторного стенду та методики збору телеметрії;

4.2Порівняльна оцінка ефективності систем виявлення атак та формування.

5.Перелік графічного матеріалу:

5.1.Презентація доповіді, виконана в Microsoft PowerPoint.

5.2 Типові схеми включають структурну схему лабораторного стенду віртуалізації із зазначенням гіпервізора та ролей віртуальних машин; схему потоків трафіку та взаємодії компонентів системи виявлення атак (Kismet, Suricata, PyShark, SIEM); схему процесу збору даних, їх кореляції та формування часових вікон у SIEM; схему моделювання атак у середовищі оркестратора із відображенням етапів baseline, запуску атаки та збору артефактів; а також схему формалізації системи захисту Wi-Fi мережі, що охоплює взаємозв’язок активів, загроз, вразливостей, оцінки ризиків та заходів протидії.

6. Дата видачі завдання «14» листопада 2024 р.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів підготовки роботи	Термін виконання	Примітка
1.	Уточнення постановки завдання	14.11.2024	
2.	Аналіз літератури	20.12.2024	
3.	Обґрунтування вибору рішення	15.01.2025	
4.	Збір даних	25.02.2025	
5.	Виконання та оформлення розділу 1.	20.05.2025	
6.	Виконання та оформлення розділу 2.	01.09.2025	
7.	Виконання та оформлення розділу 3.	13.10.2025	
8.	Вступ, висновки, реферат	20.10.2025	
9.	Апробація роботи на науковометодичному семінарі та/або науково-технічній конференції	26.10.2025	
10.	Оформлення та друк текстової частини роботи	10.11.2025	
11.	Оформлення презентацій	12.11.2025	
12.	Отримання рецензій	14.11.2025	
13.	Попередній захист роботи	21.11.2025	
14.	Захист в ЕК	18.12.2025	

Студент _____ Соболенко Ізабелла Андріївна

(підпис) (прізвище, ім’я, по батькові)

Науковий керівник _____ Платоненко Артем Вадимович

(підпис) (прізвище, ім’я, по батькові)

РЕФЕРАТ

Кваліфікаційна робота присвячена технологіям використання методів захисту бездротових мереж в системах кібербезпеки організацій.

Робота складається зі вступу, трьох основних розділів, що містять 11 рисунків та 13 таблиць, висновків та списку використаних джерел.

Об'єктом дослідження в роботі є процес організації та забезпечення кіберзахисту бездротових мереж у сучасних інформаційних системах. *Предметом дослідження* є методи виявлення та протидії атакам, спрямованим на порушення цілісності, конфіденційності та доступності бездротового трафіку.

Мета роботи — підвищення рівня інформаційної безпеки організацій за рахунок удосконалення методів захисту бездротових мереж, зокрема через практичне моделювання типових атак і аналіз трафіку.

Для того щоб досягнути поставлену мету у роботі:

- проведено аналіз сучасних підходів до побудови систем захисту бездротових мереж;
- досліджено особливості реалізації типових атак (деаутентифікація, Evil Twin, перехоплення WPA-handshake);
- обґрунтовано ефективність засобів виявлення атак (Kismet, Suricata) та розроблено власний скрипт на Python з використанням Pyshark Для аналізу трафіку.

Науковою новизною отриманих результатів є те, що в роботі розроблено метод автоматизованого виявлення підозрілих подій у трафіку та отримано журнали атак, скріншоти та підсумкові таблиці, що демонструють ефективність методів захисту.

Практичним значенням і галуззю застосування результатів є те, що запропоновані підходи можуть бути використані для створення безпечних бездротових мереж в організаціях, що працюють з конфіденційною інформацією, а також у державних установах, фінансових структурах та IT-компаніях.

Ключові слова: КІБЕРБЕЗПЕКА, БЕЗДРОТОВА МЕРЕЖА, ІНФОРМАЦІЙНО — АНАЛІТИЧНА СИСТЕМА, WPA3, VPN, IDS, KALI LINUX, PYSHARK, ВІРТУАЛЬНА МАШИНА.

ЗМІСТ

СПИСОК УМОВНИХ ПОЗНАЧЕНЬ, СИМВОЛІВ, ОДИНИЦЬ, СКОРОЧЕНЬ І ТЕРМІНІВ

Evil Twin	–	Тип атаки, при якій створюється фальшива точка доступу
Wi -Fi	–	Технологія бездротового зв’язку на основі стандартів IEEE 802.11
SSID	–	Service Set Identifier — ідентифікатор бездротової мережі
AP	–	Access Point — точка доступу
DoS	–	Denial of Service — атака на відмову в обслуговуванні
MITM	–	Man -in - the -Middle — атака «людина посередині»
WLAN	–	Бездротова локальна мережа
WPA/WPA2/WPA3	–	Протоколи захисту бездротових мереж
VPN	–	Віртуальна приватна мережа
IDS/IPS	–	Системи виявлення та запобігання вторгненням
Kismet	–	Інструмент для моніторингу бездротових мереж
Suricata	–	Система виявлення вторгнень з підтримкою аналізу трафіку
Pyshark	–	Python-бібліотека для аналізу мережевого трафіку
Kali Linux	–	Дистрибутив Linux для тестування на проникнення
Aircrack — ng	–	Набір інструментів для аудиту бездротових мереж
mdk4	–	Утиліта для генерації атак на Wi-Fi
MAC — адреса	–	Унікальний ідентифікатор мережевого інтерфейсу
Handshake	–	Процес встановлення з’єднання між клієнтом і точкою доступу
Трафік	–	Потік даних у мережі
Пакет	–	Одиниця передавання даних у мережі
Сканування	–	Процес виявлення активних пристроїв у мережі
Віртуальна машина (VM)	–	Програмна емуляція комп’ютера

ВСТУП

Актуальність дослідження. Розвиток цифрових технологій зробив бездротові мережі одним із основних компонентів сучасної корпоративної інфраструктури. Їх використання забезпечує мобільність, гнучкість та зручність доступу до інформаційних ресурсів, але водночас створює нові вектори атак. За даними Verizon DBIR, понад 80% кіберінцидентів пов’язані з зовнішніми атаками, а найбільш поширеними методами проникнення є викрадення облікових даних та фішинг [1]. В свою чергу, це свідчить про зростання ризиків, пов’язаних із бездротовими технологіями, особливо в умовах віддаленої роботи, яка стала нормою останні роки.

Бездротові мережі, зокрема Wi-Fi, є вразливими до атак типу Evil Twin, деаутентифікації, перехоплення WPA-handshake, що дозволяє зловмисникам отримати доступ до конфіденційної інформації або порушити роботу систем. У багатьох організаціях, особливо малого та середнього бізнесу, відсутні спеціалізовані засоби захисту, а відповідальність за інформаційну безпеку часто покладена на одну особу, що ускладнює впровадження комплексних рішень.

У таких умовах особливої актуальності набуває ризик-орієнтований підхід до захисту інформації, який базується на системному аналізі загроз, оцінці ризиків та управлінні ними. Відповідно до ДСТУ ISO/IEC 27005:2019, управління ризиками інформаційної безпеки включає процеси ідентифікації, аналізу, оцінювання та обробки ризиків.

Для підприємств, які не мають ресурсів на впровадження дорогих міжнародних методик, доцільним є використання простих і доступних інструментів, що дозволяють здійснювати базовий моніторинг та аналіз ризиків. Одним із таких інструментів є SWOT-аналіз, який дозволяє ідентифікувати внутрішні слабкі сторони організації, зовнішні загрози та можливості, що можуть бути використані для підвищення рівня захисту [2]. Кількісна оцінка ризиків, зокрема за допомогою методу Монте-Карло, дозволяє моделювати сценарії розвитку подій в умовах невизначеності. Даний метод широко застосовується для аналізу ризиків у проєктах, де відсутні точні статистичні дані, і дозволяє отримати

розподіл ймовірностей можливих наслідків [3]. У межах даного дослідження було вирішено реалізувати практичну частину у вигляді лабораторного стенду на базі віртуальних машин. Одна машина працює як точка доступу, інша — як клієнт, третя — як зловмисник із Kali Linux та інструментами типу aircrack-ng і mdk4. На цьому стенді моделюються типові атаки на бездротову інфраструктуру, зокрема деаутентифікація, Evil Twin та перехоплення WPA-handshake. Для виявлення атак використовуються готові засоби — Kismet та Suricata, а також розроблений скрипт на Python з використанням бібліотеки Pyshark, який аналізує трафік і фіксує підозрілі події. Результати дослідження представлені у вигляді журналів атак, скріншотів та підсумкових таблиць, що дозволяють оцінити ефективність методів захисту.

Метою роботи є дослідження та впровадження ефективних методів захисту бездротових мереж організації на основі ризик-орієнтованого підходу, що включає якісну та кількісну оцінку ризиків інформаційної безпеки.

Для досягнення цієї мети необхідно вирішити такі **завдання**:

1. Провести аналіз типових загроз та векторів атак на бездротові мережі, що становлять ризик для корпоративної інфраструктури.
2. Здійснити порівняння існуючих підходів до захисту бездротових мереж з урахуванням сучасних технологій та практик.
3. Формалізувати задачу побудови системи захисту бездротової мережі організації з урахуванням ризик-орієнтованого підходу.
4. Розробити лабораторний стенд на базі віртуальних машин для моделювання типових атак на бездротову інфраструктуру.
5. Реалізувати сценарії атак (деаутентифікація, Evil Twin, перехоплення WPA-handshake) та дослідити їх вплив на безпеку мережі.
6. Впровадити засоби виявлення атак (Kismet, Suricata, скрипт на Python з Pyshark) та оцінити їх ефективність.
7. Провести порівняльний аналіз результатів моделювання та сформувати рекомендації щодо впровадження захисту в корпоративне середовище.

Об’єктом дослідження є процес забезпечення інформаційної безпеки бездротових мереж організації. **Предмет дослідження** — методи виявлення та захисту від атак на бездротові мережі.

Методи дослідження: SWOT-аналіз, статистичний метод, метод експертних оцінок, ймовірнісний метод моделювання (метод Монте-Карло), практичне моделювання атак у віртуальному середовищі.

Наукова новизна полягає у розробці та реалізації лабораторного стенду для моделювання атак на бездротові мережі з використанням віртуального середовища, що дозволяє досліджувати ефективність різних методів захисту в умовах, наближених до реальних.

У роботі запропоновано комбіноване використання готових засобів виявлення атак (Kismet, Suricata) та власного скрипта на Python з бібліотекою Pyshark, що забезпечує автоматизований аналіз трафіку та фіксацію підозрілих подій. Також здійснено порівняльну оцінку ефективності методів захисту на основі практичних результатів моделювання атак, що дозволяє сформувати обґрунтовані рекомендації для впровадження захисту в корпоративне середовище.

Теоретичне та практичне значення роботи полягає в обґрунтуванні необхідності та дослідженні можливості впровадження моделі захисту інформації на основі ризик-орієнтованого підходу для малого та середнього бізнесу.

Галузь застосування. Результати дослідження можуть бути використані в IT-підрозділах підприємств малого та середнього бізнесу для підвищення рівня захисту бездротових мереж, у навчальних закладах для підготовки фахівців з кібербезпеки, а також як основа для впровадження практичних рішень у сфері інформаційної безпеки в державних та комерційних структурах.

Апробація результатів дипломної роботи. Основні положення роботи викладалися:

1. в статті журналу «Кібербезпека: освіта, наука, техніка» , Том 1 № 29 (2025)[4];

2. в тезах доповіді на Студентській науковій конференції «Безпека інформаційно-комунікаційних систем» (Київ: Київський столичний університет імені Бориса Грінченка, 26 жовтня 2025 року) [5].

РОЗДІЛ 1. АНАЛІЗ СУЧАСНИХ ПІДХОДІВ ДО ПОБУДОВИ ЗАХИСТУ БЕЗДРОТОВИХ МЕРЕЖ

1.1 Аналіз типових загроз та векторів атак на бездротові мережі

У сучасному цифровому середовищі бездротові технології посідають ключове місце в корпоративній та побутовій інфраструктурі. Розвиток стандартів IEEE 802.11, що формують основу роботи Wi-Fi, сприяв переходу від залежності від дротових з'єднань до гнучкішої моделі комунікацій, у якій передача даних не прив'язана до фізичного носія [6]. Це дало змогу значно пришвидшити розгортання мереж, зменшити витрати на підключення пристроїв та забезпечити користувачам більшу мобільність у межах інформаційних систем.

Однак саме відмова від кабельної інфраструктури створила новий вимір кіберзагроз. Радіосигнал, який забезпечує роботу Wi-Fi, поширюється у відкритому середовищі, а тому може бути перехоплений або підмінений без необхідності отримання фізичного доступу до комутаційного обладнання [7]. Саме це відкриває можливості для реалізації атак, що раніше були характерні переважно для дротових мереж лише за наявності прямого доступу, а нині можуть виконуватися дистанційно, непомітно й із мінімальними ресурсними витратами. Таким чином, переваги бездротового зв'язку супроводжуються появою специфічних ризиків, які потребують окремих механізмів контролю та захисту.

1.1.1. Загальні принципи функціонування бездротових мереж

Архітектура типової бездротової мережі базується на взаємодії трьох ключових елементів: точки доступу (Access Point, AP), клієнтського пристрою (Station, STA) та каналу передачі даних, що зазвичай використовує діапазони 2,4 або 5 ГГц. Точка доступу виконує роль посередника між бездротовим і провідним сегментами мережі, забезпечуючи автентифікацію клієнтів і маршрутизацію трафіку [8]. Клієнт — ноутбук, смартфон або інший пристрій — підключається до AP через певний ідентифікатор (SSID) і далі отримує доступ до внутрішніх або зовнішніх ресурсів.

Процедура встановлення з'єднання між клієнтським пристроєм і бездротовою

мережею передбачає послідовне виконання кількох технічних кроків, кожен з яких відповідає за певний аспект взаємодії в радіочастотному середовищі. На початковому етапі пристрій здійснює активне або пасивне сканування ефіру, формуючи перелік доступних точок доступу та оцінюючи їх параметри — рівень сигналу, тип шифрування, налаштування безпеки. Після вибору відповідної мережі ініціюється процес асоціації, який слугує створенням базового канального зв'язку та фіксацією параметрів обміну на фізичному рівні.

Подальшим обов'язковим кроком є автентифікація, що визначає правомірність підключення користувача та формує основу для захищеного обміну даними. У сучасних Wi-Fi інфраструктурах цей етап реалізується за допомогою криптографічних механізмів, закладених у стандарти WPA2 та WPA3. Перша з цих технологій використовує шифрування AES-CCMP, яке забезпечує захист цілісності й конфіденційності трафіку, тоді як WPA3 впроваджує протокол SAE (Simultaneous Authentication of Equals), спрямований на підвищення стійкості до атак грубою силою та усунення вразливостей попередніх поколінь [9]. Завдяки такій багатоступеневій структурі процес підключення поєднує функціональність, сумісність і базові принципи безпеки, необхідні для роботи корпоративних та побутових бездротових систем.

Основна відмінність між різними поколіннями протоколів полягає у способі захисту ключів та автентифікації. Ранні версії, як — от WEP, використовували статичні ключі та алгоритм RC4, який мав серйозні вразливості [10]. З появою WPA та WPA2 було запроваджено динамічне генерування ключів і автентифікацію за допомогою IEEE 802.1X та EAP (Extensible Authentication Protocol) [11]. Проте і ці протоколи з часом почали піддаватися новим типам атак — зокрема, перехопленню WPA-handshake для подальшого перебору паролів офлайн [12]. Тому найновіша версія WPA3 впровадила механізм SAE, який унеможливлює успішний перебір паролів і захищає навіть короткі ключові фрази [13].

Для ефективної роботи бездротових мереж важливим є також поняття розподілу каналів та керування потужністю сигналу. Дані параметри впливають не лише на швидкість передавання даних, а й на безпеку. Наприклад, занадто

потужний сигнал точки доступу може бути доступним за межами приміщення організації, що підвищує ризик несанкціонованого підключення. Тому під час проєктування мереж доцільно проводити радіопланування — аналіз карти покриття, вибір оптимальних каналів і контроль рівня потужності передавачів [14].

У корпоративних мережах керування доступом зазвичай реалізується через системи RADIUS, які дозволяють централізовано перевіряти облікові дані користувачів і застосовувати політики безпеки [15]. У менших організаціях або домашніх мережах частіше використовують спрощені схеми, де пароль PSK (Pre-Shared Key) задається вручну. Незалежно від способу автентифікації, кінцева мета одна — створити захищений канал передачі даних між клієнтом і мережею [16].

З технічного погляду, бездротові мережі працюють на фізичному та канальному рівнях моделі OSI, де основним середовищем є радіоефір. Це середовище є спільним для всіх користувачів, тому конфіденційність і цілісність даних забезпечуються виключно засобами шифрування [17]. На відміну від дротових мереж, у Wi-Fi достатньо перебувати в зоні покриття, щоб перехопити пакети або імітувати точку доступу. Саме тому базові принципи безпеки — автентифікація, авторизація, шифрування, контроль доступу — мають критичне значення [18].

Сучасні тенденції розвитку бездротових технологій також пов’язані з інтернетом речей (IoT), який передбачає масове підключення сенсорів, камер і побутових пристроїв. Багато з них не підтримують сучасних протоколів шифрування, що створює додаткові вектори атак [19]. У таких випадках питання безпеки переходить від рівня окремого пристрою до рівня всієї мережі — важливо мати системи моніторингу трафіку, виявлення аномалій та ізоляції підозрілих пристроїв [20].

Отже, бездротові мережі являють собою складні інформаційні системи, у яких висока технологічна гнучкість поєднується з підвищеним рівнем уразливості. Їхня архітектура побудована на передачі даних у відкритому радіочастотному середовищі, а це означає, що будь-який сигнал фізично виходить за межі контрольованої зони та може бути перехоплений, проаналізований або

модифікований без безпосереднього доступу до обладнання. Така природа бездротових технологій формує унікальний набір загроз, що відрізняються від класичних ризиків у дротових мережах і потребують зовсім іншого підходу до організації захисту.

Проблематика безпеки у Wi-Fi середовищі полягає не лише в технічних аспектах. Вразливість виникає на кількох рівнях одночасно: від фізичного середовища поширення радіосигналу, яке складно повністю контролювати, до канального рівня, де можливі атаки на процедури аутентифікації, та до мережевого рівня, де загрози пов’язані з маніпуляцією трафіком або підміною легітимних пристроїв. Тому підхід до захисту неминуче має бути багаторівневим, охоплюючи як технічні засоби — фільтрацію, шифрування, контроль доступу, моніторинг поведінки пристроїв, — так і організаційні заходи, що визначають правила експлуатації мережі, відповідальність персоналу та політики оновлень.

Разом із тим сучасні загрози стають дедалі більш динамічними, а сценарії атак — складнішими. Тому лише технічних заходів також недостатньо. Важливу роль відіграють аналітичні інструменти, здатні виявляти аномальні форми поведінки, аналізувати непрямі ознаки потенційних вторгнень та реагувати на відхилення від нормальної роботи. Такий системний, комплексний підхід дає змогу формувати стійку систему захисту, яка працює не лише реактивно, а й проактивно.

Таким чином, глибоке розуміння принципів функціонування бездротових мереж стає ключовою передумовою для створення ефективної системи кіберзахисту. Воно дозволяє коректно визначити потенційні точки впливу, обґрунтувати необхідність багаторівневої архітектури безпеки та вибудувати комплекс заходів, що поєднують технічні механізми, організаційні регламенти та аналітичні методи виявлення аномалій [21].

1.1.2. Основні категорії атак на бездротові мережі

Бездротові мережі, що базуються на стандартах IEEE 802.11, є зручним, але водночас уразливим середовищем для передавання даних. Через відкритий радіоефір кожен користувач, який перебуває в зоні дії сигналу, потенційно може спробувати отримати несанкціонований доступ або перехопити трафік. Більшість

сучасних атак спрямовані не лише на технічні вразливості, а й на помилки конфігурації та поведінку користувачів [22].

Умовно всі атаки на бездротові мережі можна поділити на три основні групи: пасивні, активні та комбіновані.

Пасивні атаки не змінюють роботу мережі — їхня мета полягає у спостереженні та зборі інформації. Найпоширенішим прикладом є sniffing, тобто перехоплення пакетів трафіку з подальшим аналізом. Використовуючи утиліти Wireshark або airodump-ng, зловмисник може отримати MAC-адреси пристроїв, SSID мережі, типи кадрів і навіть деякі незашифровані дані [23] Якщо мережа працює за застарілим протоколом WEP або неправильно налаштована, можливе відновлення ключа шифрування та доступ до всього трафіку.

Ще один тип пасивних атак — профілювання користувачів, коли на основі зібраних запитів визначаються типові точки підключення й навіть маршрути пересування. Цей метод часто використовується для соціальної інженерії або цілеспрямованого фішингу.

Активні атаки безпосередньо впливають на роботу мережі. Найвідомішою є деаутентифікаційна атака, коли зловмисник надсилає підроблені кадри «deauth» і примусово від’єднує клієнтів від точки доступу. Під час повторного підключення він може перехопити WPA-handshake для подальшого зламу пароля [24].

Не менш небезпечна атака Evil Twin — створення фальшивої точки доступу з таким самим SSID, як у легітимної мережі. Користувач, не перевіривши сертифікат або параметри, підключається до підробленої мережі, після чого весь його трафік може бути перехоплений. Цей тип атак легко реалізується за допомогою Kali Linux або Bettercap [25].

Ще один різновид — атаки відмови в обслуговуванні (DoS), коли мережа перевантажується фальшивими кадрами або запитами, що призводить до нестабільної роботи. Такі атаки часто використовуються як підготовчий етап перед більш складними вторгненнями.

Сучасні загрози здебільшого комбіновані. Наприклад, зловмисник спочатку виконує деаутентифікацію, потім створює Evil Twin, а далі реалізує атаку типу MITM (людина посередині) для модифікації трафіку. Особливо небезпечними є уразливості рівня шифрування — KRACK (Key Reinstallation Attack) у WPA2 або PMKID-атака, які дозволяють відновити ключі шифрування без участі користувача [26].

Додаткову загрозу становить інтернет речей (IoT). Пристрої з обмеженими обчислювальними можливостями часто не підтримують сучасні алгоритми шифрування, що робить їх слабкою ланкою бездротового середовища [27].

Пасивні атаки забезпечують зловмиснику збір даних, активні — створюють умови для втручання або зламу, комбіновані — поєднують обидва підходи, що робить їх найбільш небезпечними. Знання класифікації атак дає змогу краще зрозуміти вектори загроз і визначити, які саме методи виявлення та захисту потрібно застосовувати в корпоративному середовищі.

1.1.3. Типові вектори атак і їх наслідки

Бездротові мережі, що функціонують у корпоративному середовищі, складаються з множини взаємопов’язаних компонентів — точок доступу, клієнтських пристроїв, службових сегментів та допоміжних систем моніторингу. Усі ці елементи працюють у спільному радіочастотному просторі, де інформація передається відкрито, без фізичного розмежування каналів. Така особливість архітектури забезпечує високу гнучкість і масштабованість, але одночасно створює умови, у яких навіть незначна зміна поведінки будь-якого компонента може вплинути на безпеку всієї мережі. Відсутність чітких фізичних меж між «внутрішнім» і «зовнішнім» середовищем робить мережу потенційно доступною для зловмисників незалежно від їхнього розташування [28].

Загалом середовище корпоративного Wi-Fi характеризується широкою атакувальною поверхнею. У ньому можуть діяти як зовнішні порушники, що перебувають у зоні покриття сигналу, так і внутрішні користувачі, які мають доступ до мережі, але можуть використовувати його зловмисно. У кожному випадку вектори атак формуються залежно від трьох ключових параметрів: місця

знаходження атакуючого, конкретного елемента інфраструктури, на який спрямовано вплив, та цілей, яких прагне досягти зловмисник. Це може бути несанкціонований доступ, перехоплення службових даних, порушення цілісності передаваних пакетів або повне виведення мережі з ладу. Сукупність цих чинників визначає характер загрози та складність її виявлення, а також формує вимоги до побудови ефективних механізмів протидії.

Найбільш поширеним є зовнішній вектор, коли зловмисник перебуває в зоні дії сигналу корпоративної мережі, але не має до неї авторизованого доступу.

Типовими прикладами є:

- Перехоплення трафіку за допомогою сніфферів, щоб визначити SSID, MAC-адреси або інші службові дані;
- Атаки через фальшиві точки доступу (Evil Twin), які імітують офіційні мережі організації;
- Brute-force атаки на WPA2/WPA3-ключі, коли збирається handshake і виконується офлайн-підбір пароля [29].

Наслідком таких атак може бути витік службових паролів, конфіденційних документів або навіть несанкціонований доступ до внутрішніх серверів компанії. Згідно з даними ENISA, близько 38% усіх інцидентів у корпоративних Wi-Fi пов’язані саме з фальшивими точками доступу, що свідчить про актуальність проблеми навіть для організацій із сучасною інфраструктурою [30].

Окрему загрозу становлять внутрішні вектори, коли атакуючий є легітимним користувачем мережі. Це може бути працівник, який несвідомо порушує політику безпеки, або стороння особа, що тимчасово отримала доступ до корпоративного Wi-Fi.

Найчастіші сценарії включають:

- Rogue AP-підключення особистого маршрутизатора, який обходить системи моніторингу;
- ARP-spoofing і DNS-підміна, що дозволяють спрямовувати трафік користувачів через шкідливий шлюз;
- Використання незахищених IoT-пристроїв як «точок входу» до

внутрішньої мережі [31].

Такі вектори є небезпечними тим, що не завжди залишають цифрові сліди — дії зловмисника можуть виглядати як звичайна активність користувача. У результаті зростає ризик довготривалого несанкціонованого доступу (так звані persistent attacks).

У сучасних корпоративних середовищах дедалі частіше спостерігаються гібридні атаки, коли зловмисник спочатку діє ззовні, а потім отримує внутрішній доступ.

Прикладом може бути сценарій, коли спершу створюється Evil Twin біля офісу, а після збору облікових даних здійснюється підключення до справжньої мережі для подальшого розгортання Man-in-the-Middle. Інший варіант — атаки через віддалений доступ (VPN), коли використовується вразливість клієнтського програмного забезпечення, встановленого на ноутбуках працівників.

Гібридні атаки часто є частиною цілеспрямованих кампаній (targeted attacks) проти конкретних підприємств, де бездротовий сегмент використовується лише як стартова точка для подальшого проникнення в інші інформаційні системи.

Наслідки порушень безпеки у бездротових мережах можуть варіюватися від незначних до критичних. До основних відносять:

- Втрату конфіденційності (витік службової інформації, облікових даних, листування);
- Порушення цілісності даних (зміна або підміна файлів, фальсифікація мережевих запитів);
- Відмову в обслуговуванні (зупинка роботи мережі, збій доступу до корпоративних сервісів);
- Фінансові та репутаційні збитки, пов’язані з розкриттям інформації або простоєм бізнес-процесів.

Дані звіту Verizon DBIR 2024 демонструють критичний стан внутрішнього моніторингу в корпоративних бездротових мережах. Згідно з дослідженням, середній проміжок між фактичним проникненням у систему та моментом його виявлення перевищує 40 днів, що вказує на тривалу непомітність діяльності

зловмисника всередині інфраструктури. За цей час атакувальний суб’єкт може здійснювати збір конфіденційної інформації, тестувати вразливості, змінювати конфігурації обладнання або готувати подальші етапи атаки без будь-яких ознак, що привернули б увагу адміністраторів.

Особливо тривожним є той факт, що 27% організацій дізнаються про витік даних не завдяки власним захисним інструментам, а від зовнішніх джерел — партнерів, постачальників, регуляторів або правоохоронних органів. Така ситуація свідчить про суттєві недоліки у системах виявлення аномалій та інцидентів, а також про недостатній рівень спостережуваності подій у Wi-Fi середовищі. Значна частина процесів залишається непрозорою для внутрішніх засобів контролю, що робить організації вразливими до тривалих та малопомітних атак. Усе це підкреслює необхідність перегляду підходів до моніторингу та впровадження більш адаптивних, поведінкових і аналітичних методів захисту [32].

Вектори атак у бездротових мережах надзвичайно різноманітні, але всі вони мають спільну рису — використання слабких місць у автентифікації, конфігурації або поведінці користувачів. Знання типових векторів дозволяє формувати ефективну стратегію захисту, де поєднуються технічні, організаційні та поведінкові заходи.

1.1.4. Класифікація загроз за ISO/IEC 27005:2019

Міжнародний стандарт ISO/IEC 27005:2019 встановлює фундаментальну методологію управління ризиками у сфері інформаційної безпеки, визначаючи послідовність дій, необхідних для формування комплексної системи захисту. Документ регламентує процедури ідентифікації активів, аналізу потенційних загроз, визначення наявних вразливостей та оцінювання ймовірності їх експлуатації. Такий підхід дає змогу організаціям не лише класифікувати свої ресурси, а й зрозуміти, які саме компоненти інфраструктури можуть стати об’єктом атак та які наслідки може мати їх компрометація.

Застосування ISO/IEC 27005:2019 передбачає розроблення структурованої моделі управління ризиками, що охоплює весь життєвий цикл безпеки: від первинного аналізу середовища до впровадження контролів, моніторингу їх

ефективності та періодичного перегляду, що є особливо актуально для бездротових мереж, які через відкритість радіоканалу та гетерогенність пристроїв потребують підвищеної уваги до оцінювання вразливостей і прогнозування можливих сценаріїв атак. Стандарт допомагає сформувати системний підхід до захисту таких середовищ, забезпечуючи узгодженість технічних, організаційних і процедурних заходів, спрямованих на мінімізацію ризиків та підтримання належного рівня безпеки [33].

Цей стандарт використовується разом із ISO/IEC 27001, який описує створення системи управління інформаційною безпекою (СУІБ).

Для Wi-Fi середовищ ISO/IEC 27005 забезпечує чітку логіку побудови процесу — від виявлення критичних елементів мережі до оцінювання впливу можливих інцидентів.

Ідентифікація активів, загроз і вразливостей

Перший етап аналізу ризиків полягає в ідентифікації активів, тобто всіх об’єктів, що мають цінність для організації.

У бездротовій інфраструктурі до них належать:

- точки доступу (Access Points);
- сервери автентифікації (RADIUS, LDAP);
- клієнтські пристрої працівників;
- конфігураційні файли, ключі WPA2/WPA3, сертифікати;
- інформаційні ресурси, що передаються мережею.

Після цього визначаються загрози, які можуть вплинути на активи. для бездротових мереж це можуть бути:

- несанкціонований доступ (Evil Twin, brute-force WPA);
- перехоплення або підміна трафіку (Man - in -the-Middle);
- атаки відмови в обслуговуванні (DoS, Deauth Flood);
- витік облікових даних через фішинг або помилки конфігурації.

Далі відбувається оцінювання вразливостей — технічних і організаційних слабких місць, які можуть бути використані для реалізації загроз. Типові приклади: використання застарілого обладнання, слабке шифрування,

відкриті гостьові мережі, відсутність моніторингу ефіру, або невірно налаштовані ACL-політики [34].

Для практичної оцінки ризиків доцільно побудувати узагальнену матрицю (табл.1.1), яка демонструє взаємозв'язок між можливими загрозами, експлуатованими вразливостями та наслідками.

Таблиця 1.1

Матриця взаємозв'язку "Загроза – Вразливість – Наслідок"

Загроза	**Вразливість**	**Ймовірний наслідок**
Перехоплення трафіку	Відсутність шифрування або WEP	Витік конфіденційних даних
Атака Evil Twin	Не перевіряється автентичність SSID або сертифікат	Компрометація облікових даних
DoS / Deauth Flood	Відсутність фільтрації службових кадрів	Відмова в обслуговуванні користувачів
Rogue AP	Немає моніторингу ефірного простору	Втручання у внутрішній трафік
Атаки через IoT	Слабкі або стандартні паролі пристроїв	Проникнення у внутрішню мережу

Кожен із перелічених сценаріїв оцінюється за ймовірністю реалізації та ступенем впливу (impact), що дозволяє створити матрицю ризиків "Likelihood–Impact", рекомендовану ISO/IEC 27005 [35].

Тобто, на основі вимог ISO/IEC 27005:2019 та сучасних досліджень можна виділити такі критичні загрози для бездротових мереж:

1. Компрометація облікових даних користувачів через фішинг або слабкі ключі.
2. Несанкціонований доступ за допомогою фальшивих точок або підроблених сертифікатів.
3. Витік даних через перехоплення незашифрованого трафіку.
4. Відмова в обслуговуванні, спричинена навмисними деаутентифікаційними атаками.
5. Використання IoT-пристроїв як інструментів вторгнення до внутрішньої

мережі.

Дані категорії загроз мають найвищий рівень ризику, оскільки поєднують технічні й поведінкові чинники. Саме на їх нейтралізацію повинна бути спрямована подальша побудова системи захисту, що буде розглянута у розділах 1.2 та 1.3.

1.2 Порівняння існуючих підходів до захисту бездротових мереж

Швидкий розвиток технологій бездротового зв'язку та стрімке зростання кількості мобільних пристроїв радикально змінюють спосіб побудови та експлуатації сучасних інформаційних систем. Якщо ще кілька років тому бездротові сегменти розглядалися як допоміжні, то сьогодні вони часто є основним каналом доступу користувачів до критичних бізнес-сервісів, хмарних ресурсів та внутрішніх інформаційних систем. Смартфони, ноутбуки, планшети, IoT-пристрої, промислові контролери, системи відеонагляду та «розумні» сенсори формують розгалужену, динамічну та слабо формалізовану екосистему, в якій кожен новий елемент потенційно збільшує поверхню атаки.

Сучасні бездротові мережі характеризуються поєднанням високої гнучкості, мобільності та зручності користування. Організації отримують можливість швидко розгортати нові робочі місця, забезпечувати підключення співробітників у тимчасових локаціях, підтримувати віддалену роботу та BYOD-сценарії, де працівники використовують власні пристрої, що дозволяє оптимізувати витрати на інфраструктуру, підвищувати продуктивність та забезпечувати безперервність бізнес-процесів. Проте за цими перевагами стоїть низка фундаментальних обмежень, пов'язаних із природою радіоканалу як середовища передавання даних.

На відміну від дротових мереж, де сигнал фізично обмежений кабельною інфраструктурою, у бездротовому середовищі він поширюється за межі приміщень, будівель і навіть територій, які формально контролюються організацією. Тобто це означає, що потенційний зловмисник може спробувати впливати на мережу, перебуваючи поза периметром підприємства, без доступу до комутаційних шаф, серверних приміщень чи робочих місць. Додаткову складність створює той факт, що в реальних умовах радіоефір є спільним та нестабільним середовищем: у ньому

накладаються сигнали різних провайдерів, гостьових мереж, приватних точок доступу та неавторизованих пристроїв. Усе це ускладнює як контроль, так і аналіз подій.

Уразливість бездротових мереж зумовлена не лише фізичними характеристиками радіоканалу, а й складністю стеку протоколів, великою кількістю реалізацій обладнання та програмного забезпечення, а також людським фактором. Помилки в налаштуваннях точки доступу, використання застарілих механізмів шифрування, слабкі або повторно використані паролі, відсутність сегментації та некоректно налаштовані гостьові мережі — усе це створює умови для реалізації як зовнішніх, так і внутрішніх атак. У результаті навіть формально «захищена» мережа може виявитися вразливою через комбінацію неочевидних прорахунків у конфігурації, організації доступу чи експлуатації.

У такій ситуації стає очевидним, що побудувати безпеку на основі одного-двох окремих технічних засобів (наприклад, лише на шифруванні або лише на фільтрації трафіку) є недостатньо. Захист інформації в бездротових мережах має спиратися на системний підхід, який розглядає мережу як багаторівневу структуру та поєднує декілька взаємодоповнювальних напрямів. До них належать:

- технічні методи — криптографічні протоколи, механізми автентифікації, контроль доступу, сегментація, фільтрація, мережевий моніторинг, системи виявлення та запобігання вторгненням;
- організаційні заходи — політики безпеки, регламенти підключення пристроїв, процедури управління обліковими записами, навчання персоналу, контроль постачальників і підрядників;
- аналітичні методи — оцінювання ризиків, аналіз інцидентів, розслідування подій, використання поведінкових моделей і систем аналітики, інтегрованих у процеси ухвалення рішень.

За останні роки на основі цих компонентів сформувалася низка концепцій побудови безпеки Wi-Fi, які по-різному розставляють акценти між складністю, вартістю впровадження, вимогами до компетенцій персоналу та рівнем захищеності. На одному полюсі знаходяться прості рішення, орієнтовані на

невеликі офіси або домашні мережі, де безпека зводиться до використання базового шифрування, зміни пароля за замовчуванням і періодичного оновлення прошивання. Такі підходи відносно дешеві та нескладні в реалізації, але їхнього рівня явно недостатньо в умовах цілеспрямованих атак чи наявності внутрішніх порушників.

На іншому полюсі — комплексні моделі, характерні для великих підприємств, фінансових установ, органів державного управління або об'єктів критичної інфраструктури. Тут бездротовий сегмент розглядається як невід'ємна частина загальної системи інформаційної безпеки, інтегрований у процеси управління доступом, мережеву сегментацію, моніторинг подій та реагування на інциденти. Застосовується багаторівневий контроль: окремо регламентуються параметри конфігурації точок доступу, правила підключення пристроїв співробітників, використання гостьових і службових SSID, маршрутизація трафіку, вимоги до журналювання та зберігання логів. У таких моделях значну роль відіграють централізовані платформи управління та кореляції подій, що дозволяють бачити не окремі епізоди, а цілісну картину стану безпеки.

Між цими крайніми варіантами існує широкий спектр проміжних підходів, які комбінують різні компоненти залежно від масштабів, бюджету та профілю ризиків організації. Для середнього бізнесу, наприклад, може бути доцільним поєднання керованих бізнес-класу точок доступу із базовими засобами мережевого моніторингу та мінімально необхідним набором політик, для компаній, що працюють із персональними чи фінансовими даними, буде обов'язковою реалізація розширеної автентифікації, сегментації трафіку та інтеграції бездротових доменів у загальнокорпоративні системи управління ідентичностями та доступом.

Суттєвою відмінністю між різними концепціями безпеки Wi-Fi є розуміння того, які саме загрози вважаються пріоритетними. В одних організаціях критичним є запобігання несанкціонованому доступу ззовні; в інших — контроль за діями внутрішніх користувачів або захист від пасивного перехоплення трафіку. В окремих випадках основну увагу приділяють безперервності надання послуг і стійкості до атак типу відмови в обслуговуванні. Відповідно до цього змінюються

й критерії оцінювання ефективності: для одних важливими будуть мінімальні втрати продуктивності, для інших — максимально жорсткі параметри безпеки навіть за рахунок зручності.

Порівняння наявних підходів дозволяє виявити не лише їхні сильні сторони, але й структурні обмеження. Наприклад, моделі, орієнтовані переважно на криптографічний захист, ефективно протидіють простому перехопленню трафіку, але мало чим допомагають у разі компрометації облікових даних або використання легітимних пристроїв у зловмисних цілях. Навпаки, сценарії, де основний акцент зроблено на моніторингу та аналізі поведінки, можуть бути вразливими, якщо базові механізми автентифікації налаштовано неналежним чином. Окреме питання — вартість впровадження та експлуатації: комплексні системи потребують інвестицій не тільки в обладнання й програмне забезпечення, але й у навчання персоналу та підтримку процесів.

Особливу роль у сучасних концепціях безпеки відведено не лише шифруванню й автентифікації, які історично були основними механізмами захисту бездротових мереж, а й усій сукупності процесів, пов’язаних із життєвим циклом інцидентів. Йдеться про постійний моніторинг стану мережі, виявлення нетипових подій, аналіз їхніх причин, документування та накопичення знань для подальшого вдосконалення політик. Без цього навіть формально «правильні» технічні налаштування не гарантують надійного захисту, оскільки нові типи атак, помилки персоналу або неочікувані комбінації обставин можуть залишитися непоміченими.

Управління ризиками стає невід’ємною складовою такого системного підходу. Сама ідея полягає в тому, щоб не просто перерахувати потенційні загрози, а оцінити їхню ймовірність та вплив на конкретні бізнес-процеси. У контексті бездротових мереж це означає аналіз того, які саме сервіси залежать від Wi-Fi, які дані передаються в цих сегментах, які типи користувачів мають доступ і які наслідки матиме компрометація того чи іншого вузла. На основі такого аналізу обираються пріоритетні заходи: десь критично важливою буде ізоляція трафіку, десь — посилена автентифікація, а в інших випадках — удосконалення моніторингу та реагування.

Усе зазначене вище підкреслює, що сучасні підходи до захисту бездротових мереж не можна звести до одного універсального рішення. Вони являють собою набір концепцій, моделей і практик, які по-різному інтегруються в конкретних організаціях залежно від їхніх потреб, ресурсів і прийнятного рівня ризику. Саме тому важливим етапом є порівняльний аналіз різних варіантів побудови безпеки, що дозволяє:

- виділити базові та просунуті рівні захисту;
- оцінити взаємозв'язок між вартістю впровадження і досягнутим рівнем безпеки;
- зрозуміти, які елементи є критичними, а які можуть впроваджуватися поетапно;
- адаптувати типові рішення до специфіки конкретної організації.

У подальшому в цьому підрозділі розглядаються найпоширеніші підходи до захисту бездротових мереж, простежується їхня еволюція — від простих конфігурацій з базовим шифруванням до комплексних багаторівневих систем — та аналізуються практичні аспекти їх застосування в корпоративному середовищі. Особливу увагу приділено тому, як різні концепції поводяться в умовах реальних обмежень: обмежених ресурсів, наявності спадкової інфраструктури, вимог регуляторів і постійного зростання кількості мобільних пристроїв, що в свою чергу дозволяє сформувати цілісне уявлення про можливі стратегії захисту Wi-Fi та вибрати оптимальні рішення для конкретних умов експлуатації.

1.2.1. Класифікація методів захисту бездротових мереж

Сучасна практика кібербезпеки розглядає захист бездротових мереж як багаторівневу систему, у якій поєднуються технічні, організаційні та криптографічні заходи.

Жоден із методів не може гарантувати абсолютну безпеку сам по собі, тому ефективний захист будується шляхом комбінування різних підходів, що взаємно підсилюють один одного.

Класифікація методів безпеки Wi-Fi зазвичай базується на чотирьох ключових напрямах: організаційні, технічні, криптографічні та аналітичні (моніторингові)

[36].

Організаційні заходи формують основу політики безпеки підприємства. До них належать регламентація доступу до мережі, створення внутрішніх інструкцій з налаштування точок доступу, ведення журналів з'єднань, розділення службових і гостьових сегментів, а також навчання персоналу. У державних структурах України такі заходи регламентуються вимогами ДССЗЗІ, які зобов'язують впроваджувати періодичний аудит конфігурацій і тестування на проникнення.

Варто зазначити, що саме організаційні недоліки найчастіше призводять до компрометації мереж, навіть коли технічний рівень захисту є достатнім [37].

Технічні заходи передбачають використання спеціалізованих рішень, що контролюють доступ і захищають мережу на рівні трафіку. Серед них — сегментація мережі, застосування IDS/IPS - систем (Suricata, Snort), VPN-тунелювання, моніторинг ефіру (Kismet, AirMagnet) і використання RADIUS-серверів для централізованої автентифікації. Вони забезпечують виявлення спроб підключення несанкціонованих пристроїв, зменшують ризик перехоплення даних і дозволяють ізолювати підозрілу активність.

Недоліком технічних методів є їхня складність у налаштуванні та потреба у кваліфікованому персоналі, який здатний аналізувати велику кількість подій і правильно реагувати на інциденти.

Криптографічні засоби забезпечують конфіденційність і цілісність даних під час передавання.

Основу становлять протоколи WPA2 та WPA3, що використовують алгоритми AES-CCMP та SAE. У корпоративному середовищі все частіше впроваджується автентифікація за сертифікатами (EAP-TLS), що дозволяє усунути ризик використання слабких паролів. Водночас зростає роль аналітичних систем — вони застосовують машинне навчання для виявлення аномалій у трафіку, аналізу поведінки користувачів і прогнозування потенційних атак [38].

Такі рішення інтегруються в системи моніторингу (SIEM) і дозволяють не

лише реагувати на події, а й запобігати їм.

1.2.2. Огляд міжнародних стандартів і практик безпеки бездротових мереж

Розвиток бездротових технологій супроводжується постійним пошуком балансу між зручністю використання та рівнем безпеки. Сьогодні інформаційна інфраструктура більшості організацій немислима без Wi-Fi, однак водночас саме цей компонент є одним із найвразливіших. Щоб забезпечити єдині підходи до побудови безпечних бездротових систем, різні міжнародні організації — ISO/IEC, NIST, ENISA, Wi-Fi Alliance, IETF — розробили низку стандартів і рекомендацій, які охоплюють як технічні, так і організаційні аспекти захисту.

Знання цих документів є критично важливим для фахівців, адже вони формують основу всіх сучасних політик безпеки в Україні та світі. Далі розглянемо ключові міжнародні стандарти й практики, які визначають вимоги до побудови, адміністрування та моніторингу бездротових мереж, а також порівняємо їхній зміст і підходи.

Міжнародна серія стандартів ISO/IEC 27000 регулює питання побудови систем управління інформаційною безпекою (СУІБ).

Ключовим серед них є ISO/IEC 27001:2022, який встановлює вимоги до впровадження, підтримки та постійного вдосконалення процесів захисту інформації.

Для бездротових мереж цей стандарт не диктує конкретних технічних рішень, але створює основу для процесного підходу — тобто визначення політик, цілей, ролей, процедур і контролів, що забезпечують безпеку в цілому [39].

Його доповнює ISO/IEC 27005:2019, який описує механізми управління ризиками.

Він особливо важливий для Wi-Fi, оскільки дозволяє:

- визначити критичні активи (точки доступу, ключі, дані користувачів);
- класифікувати загрози (перехоплення трафіку, несанкціонований доступ,

DoS, підробка мережі);

- розрахувати рівень ризику за ймовірністю та впливом;
- розробити план мінімізації ризиків і контролів.

У більшості міжнародних компаній впровадження ISO 27001/27005 є передумовою сертифікації та довіри з боку партнерів.

Українські організації, особливо у сфері фінансів і телекомунікацій, поступово переймають ці практики, інтегруючи їх у свої політики кіберзахисту.

Американський інститут стандартів і технологій (NIST) відіграє провідну роль у розробці практичних керівництв із кібербезпеки. Документ NIST SP 800-153 “Guidelines for Securing Wireless Local Area Networks (WLANs)” є одним із найдетальніших джерел, присвячених саме бездротовим мережам [40].

Його головна перевага — чіткість і практична спрямованість: стандарт не просто описує вимоги, а надає конкретні кроки, як їх реалізувати.

Згідно з NIST, комплекс захисту WLAN має охоплювати три рівні:

1. Технічний рівень — використання сучасних протоколів WPA3, шифрування AES, автентифікації 802.1X, фільтрації MAC-адрес і контролю радіочастотного середовища.
2. Адміністративний рівень — документовані політики, регулярні аудити, оновлення прошивок, ведення журналів подій і контроль доступу до обладнання.
3. Фізичний рівень — правильне розміщення точок доступу, екранування приміщень, контроль зони покриття, щоб сигнал не виходив за межі охоронюваної території.

Окремий розділ у NIST SP 800-153 присвячено виявленню і блокуванню “Rogue AP”, тобто підроблених точок доступу.

Стандарт рекомендує використовувати спеціальні датчики або програмні агенти, що порівнюють сигнатури реальних пристроїв із базою дозволених. Він також наголошує на необхідності централізованого управління Wi-Fi - інфраструктурою — так як саме це дає змогу швидко реагувати на інциденти та оновлювати політики безпеки одночасно на всіх пристроях.

Європейське агентство з кібербезпеки ENISA (European Union Agency for

Cybersecurity) є ключовим центром координації політики кіберзахисту ЄС. Щорічні доповіді ENISA, зокрема “Threat Landscape for Wireless Networks” (2023) і “Cybersecurity Guidelines for SMEs” (2024), містять систематичний огляд актуальних загроз і ефективних практик їх нейтралізації [41].

Європейський підхід відрізняється тим, що робить акцент не лише на технологічних, а й на людських факторах — навчанні користувачів, культурі безпеки, прозорості процедур реагування.

ENISA вважає, що більшість інцидентів у бездротових мережах зумовлені людськими помилками — використанням простих паролів, нехтуванням сертифікатами або відсутністю оновлень.

Серед ключових практичних рекомендацій:

- забезпечення розмежування прав доступу між службовими і гостьовими користувачами;
- використання централізованих систем моніторингу з можливістю виявлення аномалій;
- обов’язкове застосування шифрування на всіх рівнях, зокрема для службових мереж IoT;
- створення “карти ризиків” і проведення навчань з реагування на інциденти.

ENISA також активно просуває концепцію Zero Trust, згідно з якою кожен запит у мережі вважається потенційно небезпечним, навіть якщо надходить із внутрішнього сегмента.

Такий підхід особливо ефективний для організацій із розподіленими офісами або віддаленими працівниками.

Технологічні стандарти безпеки Wi-Fi розробляє об’єднання виробників Wi-Fi Alliance.

Його діяльність визначає технічну основу захисту бездротових мереж у всьому світі.

Основна еволюція систем автентифікації та шифрування пройшла три етапи — WEP → WPA → WPA2 → WPA3.

- WEP (Wired Equivalent Privacy) — перше рішення, яке базувалося на алгоритмі RC4 і вважалося надійним лише до початку 2000-х. Його головний недолік — використання статичних ключів, що легко розкривалися після збору достатньої кількості пакетів.
- WPA/WPA2 запровадили динамічне генерування ключів і використання AES-CCMP, що суттєво підвищило рівень захисту.
- WPA3, офіційно схвалений у 2018 році, впровадив алгоритм SAE (Simultaneous Authentication of Equals), який унеможливлює перебір паролів у офлайн-режимі [42].

Wi-Fi Alliance також опублікувала “WPA3™ Security Overview”, де зазначено, що новий стандарт забезпечує не лише стійкість до перебору, а й захист від атак на handshake, Forward Secrecy (неможливість розшифрування старих сесій навіть у разі компрометації ключа) та обов’язкове шифрування управлінських кадрів. Разом із тим альянс визнає, що перехідний режим WPA2/WPA3, який підтримують більшість сучасних роутерів, може знижувати безпеку, якщо не налаштований правильно.

Важливо, що Wi-Fi Alliance активно співпрацює з виробниками для сертифікації обладнання. Сертифікат “Wi-Fi CERTIFIED™ WPA3” гарантує відповідність пристрою вимогам безпеки, але не звільняє користувачів від необхідності регулярно оновлювати прошивки та паролі.

Інженерна група Інтернету (IETF) відповідає за стандартизацію протоколів, що забезпечують безпечну передачу даних. У контексті бездротових мереж найважливішими є RADIUS (RFC 2865), EAP (RFC 5247), IPsec (RFC 6071) і TLS 1.3 (RFC 8446) [43].

- RADIUS (Remote Authentication Dial-In User Service) — це фундамент для автентифікації користувачів у корпоративних Wi-Fi, особливо коли використовується 802.1X.
- EAP (Extensible Authentication Protocol) дозволяє реалізовувати різні методи автентифікації — від паролів до сертифікатів, забезпечуючи гнучкість системи.

- IPsec використовується для шифрування трафіку між віддаленими вузлами, створюючи VPN-тунелі поверх бездротових каналів.
- TLS 1.3 гарантує шифрування трафіку на прикладному рівні, усуваючи можливості для атаки типу Man-in-the-Middle.

Важливим є те, що IETF забезпечує взаємну сумісність усіх цих протоколів, що дозволяє створювати комплексні архітектури безпеки.

Більшість сучасних систем автентифікації у Wi-Fi, зокрема WPA3-Enterprise, безпосередньо базуються на цих протоколах.

Для наочності та узагальнення міжнародних підходів до захисту бездротових мереж доцільно систематизувати основні характеристики кожного зі стандартів, що визначають вимоги до побудови сучасних систем кіберзахисту. Кожен із розглянутих документів має власний фокус — від управління ризиками та формування політик до конкретних технічних методів і процедур реагування на інциденти.

Міжнародні стандарти суттєво відрізняються за рівнем деталізації, сферою застосування й цільовою аудиторією, однак разом вони формують цілісну рамку для забезпечення безпеки бездротових мереж. Важливим також є те, що ці підходи не конкурують між собою, а доповнюють один одного: рекомендації ISO визначають стратегічні принципи, NIST — практичні кроки, ENISA — людський вимір, тоді як Wi-Fi Alliance і IETF відповідають за технічну реалізацію захисту.

У таблиці 1.2 наведено порівняльний аналіз найважливіших міжнародних стандартів і рекомендацій, що відображають різні рівні захисту Wi-Fi — від організаційного до протокольного.

Таблиця 1.2

Порівняння підходів міжнародних стандартів до захисту бездротових мереж

Організація / стандарт	**Основний фокус**	**Переваги**	**Особливості застосування**
ISO/IEC 27001, 27005	Управління ризиками та політика ІБ	Системний підхід, сертифікація, універсальність	Вимагає інтеграції у СУІБ, не задає технічних рішень

Продовження табл.1.2

NIST SP 800-153	Практичні методи захисту WLAN	Конкретні технічні вимоги, приклади конфігурацій	Орієнтований на держустанови США, але універсальний у застосуванні
ENISA	Аналітика загроз, людський фактор, Zero Trust	Європейський фокус, рекомендований для малого бізнесу	Підходить для адаптації політик кібергігієни
Wi -Fi Alliance (WPA3)	Технологічний рівень безпеки	Гарантована сумісність, сучасні алгоритми	Потребує оновлення обладнання, залежить від виробника
IETF (RFC 2865, 5247, 8446)	Протоколи автентифікації та шифрування	Висока гнучкість, стандартизація	Складність у налаштуванні для непідготовлених користувачів

Аналіз даних, наведених у таблиці 1.2, показує, що сучасна система забезпечення безпеки бездротових мереж не може спиратися на один універсальний стандарт.

Кожен із підходів вирішує окремий аспект проблеми: ISO/IEC задає стратегічну рамку управління ризиками, NIST надає практичні інструменти впровадження, ENISA фокусується на людському факторі та підвищенні обізнаності користувачів, тоді як Wi-Fi Alliance і IETF забезпечують технічну основу для автентифікації та шифрування даних.

Сукупне застосування цих рекомендацій створює багаторівневу модель захисту, у якій поєднуються управлінські, організаційні та технологічні механізми. Такий підхід дозволяє адаптувати міжнародні практики до національних умов і сформувати цілісну політику безпеки бездротових мереж, що відповідатиме вимогам сучасних кіберзагроз.

Отже, таким чином, можна дійти висновку, що міжнародні стандарти безпеки бездротових мереж формують багаторівневу систему рекомендацій, у якій кожна організація займає свою нішу.

ISO/IEC визначає загальні принципи управління ризиками та політики безпеки, NIST надає покрокові технічні інструкції, ENISA робить акцент на людському факторі та культурі безпеки, Wi-Fi Alliance розробляє конкретні

криптографічні рішення, а IETF забезпечує технічну основу через мережеві протоколи.

Найефективніший підхід — комбінований: застосування вимог ISO/IEC 27005 для оцінки ризиків, рекомендацій NIST для практичної реалізації, європейських принципів ENISA для підвищення обізнаності персоналу, а також стандартів Wi-Fi Alliance і IETF для технічного захисту трафіку. Саме інтеграція усіх цих елементів дозволяє створити сучасну архітектуру безпеки бездротових мереж, що відповідає як міжнародним, так і національним вимогам.

1.2.3. Порівняння сучасних технологій захисту

Розвиток бездротових технологій супроводжується постійним вдосконаленням методів захисту інформації. Якщо ще десять років тому безпека Wi-Fi зводилася до використання базового шифрування, то сьогодні вона включає багаторівневі системи контролю, аналітичні платформи моніторингу та автоматизоване реагування на інциденти.

Зростання кількості кіберзагроз і проникнення IoT-пристроїв у корпоративне середовище зумовили появу нових технологій, які поєднують криптографію, аналіз поведінки користувачів і машинне навчання. Для оцінювання ефективності різних рішень доцільно порівняти найпоширеніші технології захисту — криптографічні стандарти (WPA3, EAP-TLS), системи IDS/IPS моніторингу, а також адаптивні платформи з елементами штучного інтелекту.

Криптографічні методи залишаються фундаментом безпеки бездротових мереж. Сучасний стандарт WPA3 суттєво змінив підхід до автентифікації та шифрування даних порівняно зі своїм попередником WPA2. Його ключова перевага полягає у впровадженні механізму Simultaneous Authentication of Equals (SAE), який забезпечує стійкість до атак перебору паролів у режимі офлайн. Крім того, WPA3 реалізує принцип Forward Secrecy, що унеможливлює розшифрування раніше перехоплених даних навіть у разі компрометації поточного ключа [44].

Для корпоративного сегмента найефективнішим вважається режим WPA3-Enterprise, який підтримує 256-бітове шифрування та автентифікацію через сервер

RADIUS із використанням протоколу EAP-TLS. Останній дозволяє замінити паролі на цифрові сертифікати, що зменшує ризик соціотехнічних атак і несанкціонованого доступу.

Проте, хоча впровадження EAP-TLS потребує розгортання інфраструктури відкритих ключів (PKI) і централізованого керування сертифікатами, його ефективність і надійність виправдовують витрати на адміністрування. У більшості великих компаній EAP-TLS сьогодні є стандартом де-факто для бездротових корпоративних мереж, оскільки забезпечує максимальний рівень захисту з мінімальною участю користувача.

Окрім шифрування трафіку, не менш важливим є контроль за поведінкою самої мережі. Дану функцію виконують системи виявлення (Intrusion Detection Systems) і запобігання вторгненням (Intrusion Prevention Systems), відомі під скороченням IDS/IPS, які аналізують трафік у реальному часі, виявляють підозрілі шаблони, несанкціоновані підключення або атаки типу Rogue AP, DoS, ARP spoofing, Evil Twin тощо.

Популярними відкритими платформами є Suricata, Snort і Zeek, які дозволяють інтегруватися з корпоративними SIEM-системами для централізованого аналізу подій. Вони підтримують сигнатурний і поведінковий аналіз, що дозволяє не лише фіксувати відомі атаки, а й виявляти аномалії, які не відповідають типовому профілю трафіку.

До речі, IDS може розпізнати спробу сканування портів або надмірну кількість запитів до однієї точки доступу — ознаки підготовки до атаки.

У корпоративній практиці поширене поєднання IDS/IPS з WLAN - контролерами, які збирають телеметрію з усіх точок доступу. Такі рішення (Cisco Secure Network Analytics, FortiWLC, Aruba AirWave) дозволяють блокувати атакувальні пакети ще на рівні радіоканалу, не впливаючи на роботу легітимних користувачів.

Основними перевагами IDS/IPS є високий рівень видимості подій, можливість автоматичного реагування й гнучке налаштування. Недоліки — висока вартість впровадження, потреба у фахівцях з аналізу кіберінцидентів і ризик хибних

спрацьовувань, які можуть призвести до блокування законного трафіку [45].

Новим напрямом розвитку є системи адаптивного моніторингу, які використовують алгоритми машинного навчання для виявлення аномалій у трафіку.

Всі ці рішення, насаперед входять до складу сучасних SIEM (Security Information and Event Management) або XDR (Extended Detection and Response) платформ. Вони не лише фіксують інциденти, а й оцінюють контекст — тип пристрою, час підключення, обсяг переданих даних, історію поведінки користувача.

Прикладом є рішення Cisco SecureX, Palo Alto Cortex XDR або відкриті системи на базі Elastic Stack із модулем машинного навчання. Завдяки адаптивному аналізу такі платформи здатні автоматично визначати відхилення від нормальної активності, що може свідчити про компрометацію пристрою або атаку на точку доступу.

Деякі рішення підтримують навіть автоматичну ізоляцію підозрілих клієнтів — наприклад, відключення від мережі або перенаправлення у “гостьовий карантинний” сегмент.

Інтелектуальні системи також активно використовуються для виявлення вторгнень через IoT-пристрої, які часто є найслабшою ланкою корпоративної мережі. На основі поведінкових моделей (наприклад, NetFlow-аналітики) система може розпізнати, що “розумна камера” або датчик відправляє трафік у невідомі зовнішні домени — і заблокувати його автоматично.

Такі технології істотно підвищують швидкість реагування на інциденти, зменшують навантаження на персонал безпеки та дозволяють створювати дійсно самонавчальні мережі [46].

Для кращого розуміння особливостей та ефективності кожної з розглянутих технологій було узагальнено їхні основні характеристики у зведеній таблиці.

У таблиці 1.3 подано порівняльний аналіз сучасних технологій захисту бездротових мереж, що відображає їх функціональні можливості, переваги та обмеження у практичному застосуванні.

Таблиця 1.3

Порівняльна характеристика сучасних технологій захисту бездротових мереж

Технологія	**Основна функція**	**Переваги**	**Недоліки**
WPA3 / EAP-TLS	Шифрування й автентифікація користувачів	Високий рівень конфіденційності, захист від перебору паролів, Forward Secrecy	Складність налаштування, потреба у PKI
IDS/IPS (Suricata, Snort)	Виявлення та блокування атак у реальному часі	Моніторинг трафіку, інтеграція з SIEM, гнучкість	Хибні спрацьовування, потреба у фахівцях
Адаптивні аналітичні системи (AI/XDR)	Аналіз поведінки, прогнозування загроз	Самонавчання, швидке реагування, мінімізація людського фактору	Висока вартість, потреба в обчислювальних ресурсах

Як видно з даних, наведених у таблиці 3, кожна технологія вирішує свою частину завдань безпеки, формуючи різні рівні захисту бездротової інфраструктури.

Криптографічні рішення, такі як WPA3 та EAP-TLS, забезпечують базову конфіденційність і автентичність користувачів, тоді як IDS/IPS — системи дозволяють оперативно реагувати на атаки в реальному часі.

Адаптивні аналітичні платформи з елементами штучного інтелекту, своєю чергою, створюють можливість прогнозування інцидентів і підвищують загальну стійкість мережі до нових загроз.

У комплексі ці технології формують багаторівневу архітектуру захисту, де кожен компонент доповнює інший, забезпечуючи баланс між ефективністю, автоматизацією та надійністю.

1.2.4. Сучасні підходи до виявлення атак та аномалій у Wi-Fi мережах

Сучасний розвиток бездротових технологій супроводжується постійним зростанням кількості загроз і ускладненням способів їх реалізації. Традиційні методи — шифрування, автентифікація та контроль доступу — залишаються необхідною основою, однак у науковій спільноті все більше уваги

приділяється інтелектуальним, адаптивним і поведінковим підходам до побудови систем безпеки.

Головна тенденція останніх років полягає в переході від реактивних систем, що лише фіксують інциденти, до проактивних і самонавчальних моделей, які здатні передбачати загрози до їх фактичного виникнення.

Одним із провідних напрямів сучасних досліджень є використання машинного навчання та штучного інтелекту для аналізу поведінки мережевого трафіку.

Моделі на основі нейронних мереж і класифікаційних алгоритмів здатні розпізнавати аномальні шаблони у потоках даних, виявляти спроби несанкціонованого доступу або атаки типу DoS без участі людини. Перевагою такого підходу є здатність до самоадаптації — система може змінювати свої параметри на основі нових даних, підвищуючи точність розпізнавання загроз.

Водночас наукові роботи спрямовані на розв'язання проблеми "помилкових спрацьовувань", коли модель хибно класифікує легітимну активність як атаку, що особливо важливо для великих корпоративних мереж із динамічною структурою.

Другий напрям — це когнітивні системи безпеки, які поєднують алгоритми штучного інтелекту з контекстною аналітикою. Такі системи не лише аналізують дані, але й враховують контекст подій — час, місце, тип пристрою, рівень довіри користувача. Наприклад, система може автоматично знижувати рівень доступу для пристрою, який підключився з невідомої локації, або тимчасово ізолювати користувача, якщо його поведінка відхиляється від звичного профілю. У наукових дослідженнях цей підхід отримав назву context — aware security, тобто "контекстно обізнана безпека". Він є особливо актуальним для корпоративних середовищ із великою кількістю мобільних співробітників та IoT-пристроїв.

Ще одним перспективним напрямом є інтеграція блокчейн-технологій у систему автентифікації бездротових мереж.

Блокчейн дає змогу створити децентралізовану модель управління ключами, у якій кожен пристрій має унікальний цифровий ідентифікатор, підтверджений мережею.

Це дозволяє усунути єдину точку відмови, характерну для класичних серверів автентифікації, та забезпечити високий рівень прозорості операцій. Деякі експериментальні моделі використовують блокчейн для зберігання журналів доступу, що робить їх захищеними від несанкціонованого редагування або підробки.

Попри високу обчислювальну складність, цей підхід уже розглядається як реальна альтернатива традиційним PKI-системам у середовищах, де критичною є довіра до джерел даних.

Окрему увагу дослідники приділяють методам багаторівневої автентифікації (Multi-Factor Authentication), які поєднують не лише знання пароля чи наявність сертифіката, а й біометричні ознаки або поведінкові характеристики користувача. Наприклад, система може перевіряти не лише логін і пароль, а й шаблон натискання клавіш або спосіб переміщення пристрою в просторі.

Такі методи підвищують надійність автентифікації, але водночас вимагають ретельного захисту персональних даних, що піднімає питання конфіденційності та дотримання норм GDPR.

Ще один сучасний науковий підхід полягає у впровадженні концепції Zero Trust Architecture (ZTA) у бездротові мережі. Її основна ідея полягає у відмові від припущення, що будь — який елемент внутрішньої мережі є “безпечним”. Кожен користувач, пристрій чи запит вимагає постійної перевірки незалежно від місця підключення.

У контексті Wi-Fi це означає, що навіть користувач, який підключений до корпоративної мережі, проходить автентифікацію при кожному зверненні до ресурсу, а рівень його доступу може змінюватися динамічно.

Zero Trust дедалі частіше поєднують із технологіями AI для автоматичного визначення рівня ризику та прийняття рішень у реальному часі.

Також у наукових публікаціях активно розглядається проблема енергетичної оптимізації систем безпеки бездротових мереж. Адже більшість мобільних і IoT-пристроїв мають обмежені ресурси, тому надмірна обчислювальна складність алгоритмів шифрування може знижувати їхню продуктивність. Тому

розробляються легкі криптографічні алгоритми (lightweight cryptography), які зберігають високу стійкість при мінімальному споживанні енергії. Такі рішення особливо актуальні для сенсорних мереж, медичних і промислових систем, де безпека не повинна впливати на стабільність роботи пристроїв.

Загалом сучасні наукові підходи демонструють перехід від статичних, ізольованих систем до інтелектуальних екосистем безпеки, які здатні взаємодіяти, аналізувати та приймати рішення самостійно. Головним трендом стає інтеграція всіх рівнів захисту — від фізичного до поведінкового — у єдину архітектуру, що забезпечує адаптивність і самонавчання. Такі рішення перетворюють бездротові мережі з об’єкта захисту на активного учасника системи безпеки.

Окрему групу сучасних підходів до захисту бездротових мереж становлять методи, засновані на аналізі мережевого трафіку із застосуванням моделей машинного та глибокого навчання. Їхнє призначення полягає у виявленні аномальних дій, які не мають фіксованих сигнатур і тому часто залишаються поза можливостями традиційних систем контролю. На відміну від сигнатурних рішень, що працюють за принципом порівняння із відомими шаблонами атак, поведінкові моделі здатні адаптивно оцінювати відхилення від нормальної активності та фіксувати нові або нестандартні сценарії порушень.

У цьому контексті набули поширення алгоритми машинного навчання, зокрема SVM, Random Forest та XGBoost, які демонструють високі результати у задачах класифікації трафіку. Їхня перевага полягає у здатності працювати з великим обсягом різнорідних ознак та зберігати стабільність за умов змінного навантаження. Разом із тим, для складніших сценаріїв аналізу послідовностей подій більш ефективними виявляються нейронні мережі, зокрема архітектури на основі згорткових та рекурентних шарів. Поєднання CNN і GRU забезпечує можливість одночасної обробки просторових характеристик трафіку та часових залежностей, що характерні для багатьох типів атак у Wi-Fi мережах.

Подальший розвиток цих підходів пов’язаний із застосуванням концепцій пояснюваного штучного інтелекту. Інструменти оцінювання важливості ознак дають змогу інтерпретувати роботу моделей, визначати фактори, що найбільше

впливають на класифікацію, та підвищувати рівень довіри до автоматизованих рішень у корпоративному середовищі. На практиці найбільш інформативними виявляються показники, пов’язані з тривалістю з’єднання, кількістю переданих пакетів, типом протоколу та частотою повторних запитів. Дані параметри характеризують поведінку клієнтів та точок доступу і дають змогу своєчасно виявляти відхилення у роботі інфраструктури.

Ефективність моделей значною мірою залежить від якості підготовки даних. У процесі обробки застосовуються процедури очищення, нормалізації, перетворення категоріальних параметрів та балансування класів, що забезпечує коректність навчання та знижує кількість хибних спрацювань. Саме ця частина роботи відіграє ключову роль у практичних системах аналізу трафіку, оскільки реальні корпоративні дані часто містять шум, пропуски та суттєву нерівномірність розподілу подій.

Порівняння різних алгоритмів свідчить, що нейронні мережі демонструють найвищу точність виявлення складних аномалій, хоча їхнє використання пов’язане зі значними обчислювальними витратами. У свою чергу, моделі бустингу забезпечують більш збалансоване поєднання точності, швидкодії та стійкості до зміни характеристик трафіку, що робить їх придатними для розгортання у корпоративних мережах із високими вимогами до швидкого реагування. У загальному підсумку сучасні методи машинного та глибокого навчання розглядаються як перспективний напрям посилення систем захисту Wi-Fi, особливо в умовах зростання складності атак та появи нових типів загроз. Їх інтеграція у комплексні рішення дозволяє підвищити рівень адаптивності, зменшити залежність від сигнатурних баз та забезпечити більш повне покриття потенційних ризиків.

Отже, сучасні наукові підходи до захисту бездротових мереж характеризуються міждисциплінарністю, гнучкістю та орієнтацією на прогнозування, а не лише реагування. Саме це дає змогу створювати системи, що не просто захищають дані, а й передбачають загрози, мінімізуючи їх вплив ще до появи інциденту, а такі концепції стануть базою для формування моделі захисту,

яка буде формалізована у наступному розділі.

1.3 Формалізація задачі побудови системи захисту

Сучасні бездротові мережі формують складну та багатокомпонентну систему, у якій технічні, програмні й організаційні елементи перебувають у тісній взаємодії. Їхня структура давно перестала обмежуватися лише точками доступу та клієнтськими пристроями: сьогодні Wi-Fi сегменти інтегруються у корпоративні мережеві середовища, поєднуються з хмарними сервісами, системами управління ідентичностями, інструментами моніторингу та аналітики. Через це бездротова інфраструктура практично прирівнюється за значущістю до дротових комутаційних систем, хоча залишається більш вразливою з огляду на фізичні та логічні характеристики радіосередовища.

У таких умовах забезпечення безпеки бездротових мереж вимагає застосування цілісного підходу, який виходить за межі традиційного встановлення шифрування чи автентифікації. Окремі технічні заходи, хоч і необхідні, не здатні самостійно гарантувати належний рівень захищеності. Причина полягає в тому, що в сучасних Wi-Fi середовищах кожен компонент впливає на всі інші: неправильне налаштування точки доступу може нівелювати роботу складного механізму контролю доступу, а відсутність політик управління пристроями — звести нанівець зусилля із сегментації трафіку. Тому ефективна система захисту потребує побудови логічної моделі, яка описує взаємозв’язки між активами, користувачами, протоколами, сценаріями атак і механізмами реагування.

Ключовою передумовою такої моделі є формалізація задачі, тобто опис системи безпеки у вигляді впорядкованої структури, що дозволяє об’єктивно оцінювати ризики, порівнювати альтернативи та приймати обґрунтовані рішення. Формалізація перетворює складну й динамічну реальність мережевої інфраструктури на керовану концептуальну схему, у якій можна чітко визначити, що саме слід захищати, від кого, яким способом та за допомогою яких ресурсів. Тому це особливо важливо для бездротових систем, оскільки вони мають численні параметри, що безпосередньо впливають на безпеку — від потужності сигналу та

топології розташування точок доступу до вибраних протоколів шифрування та політик автентифікації.

Процес формалізації передбачає визначення активів, які потребують захисту. У контексті Wi-Fi це не лише апаратні пристрої та канали зв'язку, але й інформаційні потоки, облікові записи, конфігураційні дані, журнали подій, ключі шифрування, а також політики безпеки. Далі необхідно виконати ідентифікацію загроз — як технічних (атаки типу Man-in-the-Middle, підміна точок доступу, підбір ключів WPA, деаутентифікація), так і організаційних (помилки персоналу, недотримання правил доступу, неправильно налаштовані гостьові сегменти). Третім етапом є аналіз вразливостей, тобто характеристик системи, які уможливлюють реалізацію загроз: застаріле обладнання, слабкі паролі, відсутність сегментації, неправильні політики передачі прав, неконтрольований BYOD.

Після визначення активів, загроз та вразливостей стає можливим виконання кількісної оцінки ризику. Її суть полягає не лише у встановленні того, чи існує небезпека, а у вимірюванні потенційних збитків, ймовірності інциденту та витрат на реалізацію відповідних заходів захисту. Кількісна модель дозволяє порівнювати різні стратегії безпеки за об'єктивними критеріями: ефективністю, вартістю, складністю впровадження, впливом на продуктивність. Наприклад, деякі сценарії можуть вимагати оновлення обладнання або впровадження складних механізмів автентифікації, а інші — лише зміну політики доступу або налаштування додаткових правил моніторингу. Без формалізації такі рішення часто приймаються інтуїтивно, що призводить до нераціонального використання ресурсів.

Побудована модель дозволяє структурувати систему захисту як багаторівневу, де кожен рівень виконує свою функцію, а разом вони утворюють єдиний комплекс. На фізичному рівні це контроль потужності сигналу, правильне розташування точок доступу, екранування приміщень та контроль охоронюваної зони. На канальному — механізми автентифікації та шифрування, протоколи WPA2/WPA3, захист від підміни точок доступу та несанкціонованих підключень. На мережевому — сегментація, фільтрація трафіку, маршрутизація потоків і застосування політик доступу. Нарешті, на прикладному й організаційному рівнях — журналювання

подій, моніторинг аномалій, управління обліковими записами, реагування на інциденти та навчання персоналу.

Ефективність моделі великою мірою залежить від критеріїв оцінювання, які використовуються для порівняння різних рішень. До них можуть належати: стабільність роботи під навантаженням, рівень хибнопозитивних спрацювань систем виявлення атак, час реагування, відповідність нормативним вимогам, інтегрованість у наявну мережеву інфраструктуру. Наприклад, для компаній з масовим потоком клієнтських підключень (як-от освітні заклади або торгові центри) ключовим буде баланс між продуктивністю та безпекою, тоді як для фінансових чи урядових установ пріоритет завжди віддається строгому контролю доступу та підвищеній стійкості до атак.

Отже, формалізація задачі побудови системи захисту бездротових мереж є необхідною передумовою для створення надійних та керованих рішень у сфері інформаційної безпеки. Вона дозволяє упорядкувати знання про структуру Wi-Fi середовища, визначити найважливіші елементи для захисту, встановити об’єктивні критерії ефективності, а також оптимізувати використання технічних і фінансових ресурсів. У цьому підрозділі буде розглянуто основні принципи формалізації процесу, визначено ключові вхідні параметри, наведено загальну структуру моделі безпеки та окреслено підходи до її практичного застосування в корпоративному середовищі.

1.3.1. Постановка задачі та визначення змінних моделі

Побудова системи захисту бездротової мережі є складним багатокритеріальним завданням, у якому потрібно врахувати взаємозв’язок між технічними, організаційними та поведінковими параметрами. Формалізація цього процесу дає змогу представити задачу в аналітичній формі, де кожен елемент системи — актив, загроза, вразливість чи захисний механізм — має власні параметри та впливає на загальний рівень безпеки. Мета такої формалізації — отримати кількісну оцінку стану захищеності мережі та побудувати модель, яка дозволяє приймати обґрунтовані рішення щодо розподілу ресурсів і вибору оптимальних заходів захисту.

У загальному вигляді задача побудови системи захисту може бути подана як оптимізаційна модель, у якій мінімізується ризик інформаційної безпеки за умови обмеженості ресурсів. Ризик (R) визначається як функція від імовірності реалізації загроз (P) і величини можливих збитків (C):

$$R = \sum(P_i \times C_i) \qquad (1.1)$$

де i — індекс загрози,

P_i — ймовірності реалізації окремих атак,

C_i — відповідні наслідки або шкода від них.

Метою системи захисту є зниження R до прийнятного рівня $R_{allo}w$, за якого ризик вважається контрольованим.

Для досягнення цього необхідно визначити набір змінних моделі, які характеризують стан безпеки мережі:

- $A = \{A_1, A_2, \ldots, A_m\}$ — множина активів (точки доступу, сервери, користувачі, IoT-пристрої);
- $T = \{T_1, T_2, \ldots, T_n\}$ — множина загроз (DoS, MITM, Evil Twin, перехоплення трафіку тощо);
- $V = \{V_1, V_2, \ldots, V_k\}$ — множина вразливостей, що можуть бути використані для реалізації загроз;
- $M = \{M_1, M_2, \ldots, M_l\}$ — множина контрзаходів (шифрування, IDS/IPS, сегментація, автентифікація, AI — моніторинг).

Кожен контрзахід M_j впливає на зменшення ймовірності реалізації певної загрози T_i, а також має власну вартість C_{mj}. Таким чином, оптимізаційна задача може бути подана як:

$$\text{мінімізувати } R = \sum[P_i(T_i, V_i, M_j) \times C_i],\ \sum C_{mj} \leq B \quad (1.2)$$

де B — доступний бюджет або ресурс на впровадження системи захисту. Оптимальне рішення передбачає вибір такого набору заходів $M^* \subset M$, який мінімізує ризик при заданих обмеженнях.

Окрім кількісних параметрів, модель повинна враховувати якісні характеристики, зокрема рівень довіри до користувачів, частоту оновлення обладнання, ефективність політик безпеки. Для цього вводиться інтегральний

показник захищеності (S), який визначається як зважена сума часткових коефіцієнтів безпеки за кожним напрямом:

$$S = \alpha_1 S_{te} c_h + \alpha_2 S_{or} g + \alpha_3 S c_r y_{pt} + \alpha_4 S_{anal} y_t \quad (1.3)$$

де коефіцієнти α_i відображають вагу кожного рівня (технічного, організаційного, криптографічного та аналітичного). Значення S варіюється від 0 до 1, де 1 відповідає максимально можливому рівню безпеки.

Формалізація у такому вигляді дозволяє не лише оцінити поточний стан безпеки мережі, а й моделювати вплив окремих заходів на загальний рівень ризику. Наприклад, підключення нової IDS-системи або впровадження EAP-TLS може знизити P для відповідних загроз, що зменшує сумарне значення R. З іншого боку, скорочення бюджету або відсутність моніторингу підвищує вразливість системи та призводить до зростання ризику.

Таким чином, задача формалізації побудови системи захисту полягає у визначенні оптимального балансу між безпекою та ресурсами, де кожне рішення має бути обґрунтованим кількісно. У подальших підпунктах ця модель буде деталізована через побудову структурної схеми системи, опис взаємодії її компонентів і розрахунок критеріїв ефективності.

1.3.2. Математична модель оцінки ризиків

Побудова математичної моделі оцінки ризиків є ключовим етапом при формуванні системи захисту бездротових мереж. Вона дозволяє не лише якісно описати загрози та вразливості, а й кількісно оцінити вплив кожного фактора на загальний рівень безпеки. На відміну від традиційного експертного підходу, математичне моделювання забезпечує об’єктивність та відтворюваність результатів, що особливо важливо для аналізу ефективності різних варіантів захисту.

Основна ідея полягає в тому, що ризик (R) Для конкретної бездротової мережі можна подати як функцію від ймовірності реалізації загрози (P), ступеня вразливості системи (V) та величини можливих наслідків (C):

$$R = f(P, V, C) \quad (1.4)$$

де кожен із параметрів може бути визначений як числовий показник у

діапазоні [0;1]. Для спрощення практичних розрахунків ця залежність часто лінеаризується, і ризик подається у вигляді добутку:

$$R_i = P_i \times V_i \times C_i \quad (1.5)$$

де i — індекс конкретної загрози або типу атаки. Сумарний ризик для всієї системи визначається як сума всіх приватних ризиків:

$$R\_\Sigma = \sum(P_i \times V_i \times C_i) \quad (1.6)$$

Параметр P (ймовірність реалізації загрози) визначається на основі статистики інцидентів або експертної оцінки частоти спроб атак у даному середовищі.

У реальних умовах його можна отримати з журналів подій систем моніторингу (IDS/IPS), аналітики SIEM чи звітів кіберінцидентів.

Показник V (вразливість) відображає схильність елементів системи до експлуатації відомих чи невідомих вразливостей. Його можна розрахувати через коефіцієнт V = 1 – E, де E — ефективність реалізованих контрзаходів. Нарешті, C (наслідки) характеризує можливі збитки — як матеріальні, так і репутаційні — у разі реалізації загрози. Для спрощення аналізу шкала наслідків може бути подана в балах (наприклад, 1–5) або нормована до інтервалу [0;1].

Вже для більш точного урахування взаємозв'язку між загрозами, вразливостями та активами застосовується матричний підхід, у якому будується матриця R = [r_{ij}], де r_{ij} відображає ризик реалізації i-тої загрози для j-го активу. Кожен елемент матриці визначається як:

$$r_{ij} = P_i \times V_{ij} \times C_j \quad (1.7)$$

де V_{ij} — рівень вразливості конкретного активу j щодо загрози i,

C_j — вартість або значущість активу.

Отримана матриця дозволяє побудувати профіль ризику системи — набір значень, які можна ранжувати для пріоритезації заходів безпеки. Найбільш критичними вважаються ті комбінації i,j, а для яких r_{ij} перевищує встановлений поріг ризику $R_{allo}w$.

Задля візуалізації результатів доцільно використовувати теплові карти ризиків, де рівень ризику позначається кольором (наприклад, зелений — низький, жовтий — середній, червоний — критичний). Цей підхід дозволяє швидко

визначити зони найбільшої небезпеки в інфраструктурі бездротової мережі.

Оскільки показники P, V і C можуть бути виміряні в різних шкалах, необхідно виконати нормування:

$$P'\_i = P\_i / P\_max,\ V'\_i = V\_i / V\_max,\ C'\_i = C\_i / C\_max \quad (1.8)$$

Після нормування інтегральний ризик системи розраховується як середньозважене значення:

$$R\_total = (\sum(w_i \times P'\_i \times V'\_i \times C'\_i)) / (\sum w_i) \quad (1.9)$$

де w_i — коефіцієнти вагомості загроз, що визначаються експертно або на основі історичних даних. Такий підхід дозволяє врахувати різну критичність загроз та їхній реальний вплив на систему [48].

Для прийняття управлінських рішень результати розрахунків порівнюються з граничними рівнями ризику:

- $R \leq 0.2$ — низький ризик, додаткові заходи не потрібні;
- $0.2 < R \leq 0.5$ — середній ризик, потрібен періодичний моніторинг;
- $0.5 < R \leq 0.8$ — високий ризик, необхідно посилення захисту;
- $R > 0.8$ — критичний ризик, потрібні негайні дії.

Модель дозволяє адаптуватися до конкретних умов — масштабів організації, типів активів і наявних ресурсів. Вона забезпечує можливість динамічного оновлення параметрів у разі зміни архітектури мережі або появи нових загроз. Таким чином, математична модель оцінки ризиків стає не лише інструментом розрахунку, а й основою для стратегічного планування заходів безпеки у бездротових мережах.

1.3.3. Модель побудови системи захисту

Після визначення математичних засад оцінки ризиків логічним наступним кроком є розроблення моделі побудови системи захисту бездротової мережі, що поєднує в собі аналітичні методи та інструменти автоматизованого моніторингу. Сучасна мережа Wi-Fi має динамічну структуру, у якій постійно змінюється склад підключених пристроїв, топологія трафіку та спектр загроз. Тому система безпеки має бути адаптивною — здатною не лише реагувати на відомі типи атак, а й прогнозувати аномалії на основі поведінкових ознак. У цій підсистемі важливо

забезпечити безперервний моніторинг ефіру, багаторівневу обробку даних і миттєве реагування.

Логіка роботи системи захисту описується чотирма ключовими етапами: точка доступу → моніторинг → виявлення → реагування. Кожен з етапів виконує специфічну функцію у циклі безпеки.

1. Точка доступу (Access Point) — основне джерело мережевого трафіку, через яке передаються пакети користувачів. На цьому етапі важливо зберегти первинність даних і забезпечити прозоре дублювання потоків для моніторингу.

2. Моніторинг (Monitoring Layer) — здійснюється збір та попередня фільтрація пакетів. У системі можуть використовуватись сенсори або програмні агенти, які зчитують ефір без втручання в саму передачу даних.

3. Виявлення (Detection Layer) — аналізує трафік, застосовуючи сигнатурні, статистичні або поведінкові методи виявлення загроз.

4. Реагування (Response Layer) — відповідає за оперативну ліквідацію інцидентів: блокування джерела атаки, ізоляцію вузлів, модифікацію правил доступу та генерацію звітів.

Система працює у циклічному режимі: результати аналізу потрапляють до блоку моніторингу для постійного оновлення патернів, створюючи самонавчальне середовище.

Практична реалізація цієї моделі передбачає об’єднання трьох компонентів з відкритим вихідним кодом: Kismet, PyShark та Suricata. Вони забезпечують збір, обробку та аналітику трафіку.

Етапи інтеграції включають: 1) збір даних (Kismet), 2) попередній аналіз (PyShark), 3) виявлення атак (Suricata), 4) реагування.

Логіка взаємодії між компонентами системи подана у псевдокоді (Рис. 1.1), який демонструє послідовність обробки даних від моменту перехоплення пакета до реагування на атаку.

psevdocode.css ×

*.css files are supported by WebStorm

```
start:
    capture = Kismet.capture(interface="wlan0")
    packets = PyShark.parse(capture)
    alerts = Suricata.analyze(packets)

    if alerts.detected():
        Response.block_source(alerts)
        Log.save(alerts)
        Notify.admin(alerts)
end
```

Рис. 1.1. – Псевдокод інтеграції компонентів Kismet, PyShark і Suricata

Функціонування системи можна формалізувати у вигляді циклу “спостереження–оцінка–реагування”, де ймовірність успішної атаки Pa зменшується пропорційно ефективності засобів виявлення (Eo) та реагування (Er):

$$P'\_a = P\_a \times (1 - (E\_o + E\_r) / 2) \quad (1.10)$$

де P’a — скоригована ймовірність реалізації атаки після активації системи,

Eo — коефіцієнт ефективності модуля виявлення (0-1),

Er — коефіцієнт ефективності реагування.

Таким чином, інтегрована система знижує ризик за рахунок зменшення Pa.

Це в сукупності із моделлю оцінки ризиків забезпечує динамічну стабільність безпеки мережі.

Для оцінювання якості функціонування системи виявлення й реагування використовуються метрики машинного навчання та теорії прийняття рішень:

Precision (точність):$Precision = TP / (TP + FP)$

Recall (повнота):$Recall = TP / (TP + FN)$

F1 — score:$F1 = 2 \times (Precision \times Recall) / (Precision + Recall)$

True Positive Rate (TPR) та False Positive Rate (FPR):$TPR = TP / (TP + FN), \quad FPR = FP / (FP + TN)$

Для реальних систем виявлення аномалій у бездротових мережах оптимальними вважаються співвідношення Precision ≥ 0.9, FPR ≤ 0.1, F1 ≥ 0.85.

Саме воно забезпечує високу ефективність виявлення атак при мінімальному навантаженні на ресурси.

1.3.4. Узагальнення та рекомендації

Проведене дослідження дозволило сформувати узагальнену модель побудови системи захисту бездротових мереж, що поєднує математичний підхід до оцінки ризиків та інтегровану архітектуру моніторингу, виявлення і реагування. Запропонований підхід демонструє, що ефективність системи безпеки зростає пропорційно ступеню автоматизації процесів аналізу трафіку та своєчасності реагування на інциденти. Сформована модель циклічного типу “спостереження–оцінка–реагування” може бути використана як основа для побудови лабораторного стенду та подальших експериментальних перевірок.

Майбутній лабораторний стенд має відтворювати реальну архітектуру Wi-Fi сегменту організації з інтегрованими компонентами Kismet, PyShark і Suricata. Він повинен забезпечувати збір і обробку трафіку, імітацію атак типу Deauthentication чи ARP spoofing, фіксацію інцидентів і автоматичне реагування. Основні вимоги до такого стенду полягають у наявності мінімального набору апаратних вузлів (дві точки доступу, сервер моніторингу, кілька клієнтів), підтримці потокового аналізу трафіку, логуванні подій і можливості масштабування конфігурації. Такий підхід дозволить оцінити не лише точність виявлення, а й практичну стійкість системи до реальних умов мережевого середовища.

Разом із тим запропонована модель має низку обмежень, зокрема залежність від продуктивності апаратного середовища, стабільності трафіку та повноти бази сигнатур. Вона орієнтована на Wi-Fi мережі стандарту 802.11 і не враховує специфіку IoT або 5G сегментів. Подальші дослідження будуть спрямовані на впровадження методів машинного навчання для адаптивного виявлення аномалій, автоматичне коригування порогів ризику, а також інтеграцію моделі з платформами типу SIEM або Wazuh для централізованого моніторингу. Узагальнюючи результати, можна зазначити, що сформована система захисту створює основу для побудови практичного прототипу лабораторного комплексу, придатного в першу чергу для дослідження ефективності засобів безпеки в

бездротових інфраструктурах.

Висновки до розділу 1

У першому розділі було проведено комплексний аналіз сучасних підходів до побудови систем захисту бездротових мереж, визначено актуальні загрози, проаналізовано вектори атак, здійснено порівняння існуючих рішень і формалізовано задачу побудови інтегрованої моделі безпеки. Проведене дослідження дозволило обґрунтувати необхідність переходу від фрагментарного застосування засобів захисту до створення єдиних комплексних систем, що поєднують моніторинг, аналіз та реагування в реальному часі.

На початку розділу розглянуто загальні принципи функціонування бездротових мереж, які формують середовище потенційних ризиків.

Виявлено, що характерною особливістю таких систем є відкритість каналу зв'язку, обмеженість контрольованої зони, наявність великої кількості гетерогенних пристроїв та відсутність чіткого розмежування між довіреними і недовіреними користувачами. Саме ці фактори визначають специфіку побудови захисту — він має бути адаптивним, багаторівневим і здатним працювати у динамічному середовищі.

У підпункті 1.1 проведено детальний аналіз типових загроз і векторів атак на бездротові мережі. Визначено, що до найбільш поширених належать атаки типу Man-in-the-Middle, Evil Twin, Deauthentication, ARP spoofing, DoS та перехоплення трафіку. Вище наведені атаки використовують слабкі місця протоколів аутентифікації, недостатній контроль каналів і недосконаліть механізмів шифрування. На основі стандарту ISO/IEC 27005:2019 виконано класифікацію загроз і побудовано узагальнену матрицю "загроза – вразливість – наслідок", яка дозволила визначити критичні напрями підвищення безпеки. Найвищий рівень ризику мають атаки, що впливають на цілісність і доступність трафіку, оскільки саме вони можуть призвести до порушення функціонування всієї мережевої інфраструктури.

Далі, у підпункті 1.2, проведено порівняльний аналіз існуючих підходів до захисту бездротових мереж. З'ясовано, що нинішні рішення базуються на поєднанні трьох основних стратегій: криптографічного захисту (WPA3, EAP-TLS),

систем виявлення вторгнень (IDS/IPS) та політик доступу на рівні користувачів (RADIUS, NAC). Однак ефективність таких рішень часто обмежується відсутністю єдиного механізму координації та динамічної адаптації. Міжнародні стандарти, такі як ISO/IEC 27001, NIST SP 800-153 і ENISA Guidelines, пропонують базові принципи побудови безпеки, проте їх застосування в бездротовому середовищі потребує узгодження з реальними технічними можливостями обладнання.

Проведене порівняння показало, що більшість сучасних технологій спрямовані на реагування після факту інциденту, а не на його попередження. У цьому контексті особливої уваги заслуговують гібридні рішення, які поєднують сигнатурний аналіз із поведінковим моніторингом на основі машинного навчання. Саме така концепція дозволяє зменшити кількість хибнопозитивних спрацьовувань і виявляти невідомі типи атак.

Окремо розглянуто сучасні наукові підходи до побудови систем безпеки бездротових мереж. Вони ґрунтуються на концепції багаторівневої архітектури, що поєднує апаратний, програмний і аналітичний рівні. Наукові публікації останніх років демонструють зростання інтересу до адаптивних систем, які використовують когнітивні алгоритми та аналіз поведінкових відхилень. У таких рішеннях важливу роль відіграють методи машинного навчання, що дозволяють виявляти невідомі загрози без попереднього визначення сигнатур.

У підрозділі 1.3 здійснено формалізацію задачі побудови системи захисту. Було визначено, що ризик інформаційної безпеки може бути поданий як функція ймовірності реалізації загрози, ступеня вразливості та величини потенційних збитків.

Математична модель оцінки ризику дозволила представити цей процес у вигляді оптимізаційної задачі, у якій мінімізується ризик за умови обмеженості ресурсів.

Запропонована функція ризику, побудована на базі добутку трьох параметрів ($R = P \times V \times C$), дає змогу кількісно оцінити стан безпеки системи й визначити пріоритетні напрями вдосконалення.

Важливим результатом стало формування матричної моделі оцінювання

ризиків, яка відображає взаємозв'язок між активами, загрозами та вразливостями. Завдяки цьому з'явилась можливість оцінювати ризик не лише в загальному, а й на рівні конкретних вузлів мережі, що має велике практичне значення при плануванні контрзаходів. Крім того, запропоновано процедуру нормування параметрів і розрахунку інтегрального показника ризику, що забезпечує уніфікований підхід до аналізу різних мережевих сценаріїв.

Подальший розвиток моделі відображено в підпункті 1.3.3, де описано архітектуру практичної системи захисту з інтеграцією інструментів Kismet, PyShark та Suricata. Такий підхід дозволяє забезпечити повний цикл: збір трафіку, аналітичну обробку, виявлення аномалій та автоматичне реагування. Взаємодія між компонентами системи реалізована у вигляді безперервного потоку даних, що ілюструє цикл "спостереження–оцінка–реагування". Математична модель показала, що ймовірність успішної атаки знижується пропорційно підвищенню ефективності модулів виявлення (E_o) і реагування (E_r), що підтверджує доцільність інтегрованого підходу до безпеки.

Для оцінювання ефективності системи запропоновано застосовувати статистичні метрики — Precision, Recall, F1-score, TPR, FPR, які дозволяють об'єктивно вимірювати якість роботи IDS/IPS-компонентів. Зазначено, що оптимальною вважається система, у якій $\text{Precision} \geq 0.9$, $F1 \geq 0.85$, $\text{FPR} \leq 0.1$. Це створює основу для подальшої кількісної оцінки реальної ефективності розроблених рішень у лабораторному середовищі.

У підпункті 1.3.4 сформульовано узагальнення й практичні рекомендації щодо створення лабораторного стенду, який має відтворювати реальну архітектуру корпоративної Wi-Fi мережі. Визначено базові вимоги до апаратного та програмного забезпечення, структури стенду й сценаріїв тестування. Запропоновано напрями подальших досліджень, зокрема впровадження методів машинного навчання для підвищення точності виявлення аномалій і розширення бази знань сигнатур.

Узагальнюючи результати, можна зробити висновок, що розроблена у межах першого розділу система є не просто набором технічних інструментів, а цілісною

концепцією управління інформаційними ризиками у бездротових мережах. Вона поєднує кількісний підхід до оцінки ризику, аналітичну обробку даних і автоматизоване реагування. Наукова новизна роботи полягає у тому, що вперше для бездротового середовища запропоновано інтегровану модель, яка об’єднує ризик-орієнтоване планування, динамічне моніторинг і когнітивну адаптацію захисних механізмів.

Практична цінність результатів полягає в можливості впровадження розробленої моделі у навчальні лабораторії, корпоративні мережі малого та середнього бізнесу, а також у системи безпеки об’єктів критичної інфраструктури. Запропонований підхід забезпечує баланс між ефективністю, масштабованістю й ресурсними витратами, а також дозволяє створити гнучку платформу для подальших досліджень у сфері кіберзахисту бездротових мереж.

Отже, виконані в розділі дослідження підтвердили гіпотезу про те, що комплексний підхід до безпеки — на основі ризик-орієнтованої оцінки, математичного моделювання та інтеграції аналітичних інструментів — є найефективнішим шляхом підвищення стійкості бездротових мереж до сучасних атак. Отримані результати створюють міцну методологічну основу для реалізації лабораторного стенду та подальших експериментальних досліджень, які будуть представлені у другому розділі роботи.

РОЗДІЛ 2 . ОСОБЛИВОСТІ ПОШУКУ ТА ВИЯВЛЕННЯ АТАК НА БЕЗДРОТОВІ МЕРЕЖІ

2.1 Опис лабораторного стенду на базі віртуальних машин

Для виконання завдань магістерської постала необхідність розгортання лабораторного стенду, який відтворює типовий корпоративний Wi-Fi сегмент та забезпечує керований збір і аналіз мережевої телеметрії. Ключовою особливістю стенду є автоматизоване розгортання й управління за допомогою Python-оркестрації: створення та конфігурування віртуальних машин, ініціалізація сервісів моніторингу й виявлення, а також централізований збір артефактів (pcap, журнали подій, зведені таблиці). Такий підхід гарантує відтворюваність експериментів, ізоляцію від виробничих мереж і можливість масштабування сценаріїв. Описані далі рішення безпосередньо слугують основою для практичних досліджень у підрозділі 2.2 (моделювання атак: деаутентифікація, Evil Twin, перехоплення WPA -handshake) та оцінювання ефективності методів виявлення у підрозділі 2.3 (Kismet, Suricata, PyShark).

Обґрунтування вибору підходу базується на прагненні отримати повністю відтворювану, більш керовану та автоматизовану інфраструктуру дослідження. Python виступає тут як «мізки» стенду: однорідна мова дозволяє описати весь процес — від створення і конфігурації віртуальних машин до запуску сервісів моніторингу, збору логів і підготовки вихідних даних для аналізу — у вигляді зрозумілих, версійованих та повторюваних скриптів. Переваги такого підходу очевидні для наукової роботи: автоматичне відтворення експериментів (reproducibility), можливість програмно запускати серії тестів з різними параметрами (parametrization), централізований збір артефактів (pcap, eve.json, CSV) і автоматична підготовка зведених таблиць для подальшої обробки. Окрім того, робота в єдиному середовищі розробки (PyCharm) спрощує налагодження, логування, інтеграцію з системами контролю версій і документування експериментів — усе управління відбувається через Python-код без ручних кроків у зовнішніх GUI- інструментах.

Технічно реалізацію оркестрації забезпечують відповідні Python-бібліотеки

(наприклад, для взаємодії з гіпервізорами чи контейнерами), але всі виклики, налаштування і процедури виконуються саме з середовища PyCharm — тобто без запуску додаткового зовнішнього софту руками. Переваги поєднання VirtualBox/KVM як платформи віртуалізації з Python-оркестратором очевидні: стабільні та легкі у відтворенні віртуальні інстанси разом із гнучкістю програмного керування (через бібліотеки як libvirt, vboxapi чи python-vagrant), віддаленим налаштуванням і виконанням команд (paramiko) та можливістю інтеграції контейнерних підсистем (docker-py) — але всі ці механізми використовуються програмно виключно через Python-скрипти, що запускаються в PyCharm. Такий підхід гарантує, що весь процес розгортання, тестування і збору даних — від початку до кінця — задокументований, відтворюваний і контрольований у межах єдиної розробницької оболонки. Огляд кожної ролі у лабораторному стенді: їхнє призначення, які артефакти вони формують та для яких типів експериментів (тестів) вони потрібні, подано таблично для зручності читання (таб. 2.1)

Таблиця 2.1

Огляд ролей у лабораторному стенді

Роль ВМ	**Коротка функція**	**Формат артефактів**	**Використання у тестах**
VM-AP (емуляція точки доступу)	Емуляція поведінки справжньої точки доступу: трансляція SSID, управління шифруванням (WPA2/WPA3 тестові налаштування), роздача DHCP (за потреби). Служить центральною точкою підключення Для клієнтів і атакуючих машин.	Конфігураційні файли (txt), логи hostapd, при необхідності pcap (якщо апаратний інтерфейс знімається)	Усі сценарії атак: деаутентифікація (генерація реальних deauth/reauth подій), Evil Twin (створення підробленого SSID), захоплення WPA — handshake (під час автентифікації клієнтів)

Продовження таб.2.1

VM -Clients (набір клієнтів)	Сукупність віртуальних клієнтів різних ОС (Linux, Windows, Android — емуляція) — імітація легітимної активності: асоціації/автентифікації, нормальний мережевий трафік (HTTP, DNS, SSH, фонова активність).	Локальні логи клієнтів, netstat/pcap (за потреби), сценарії генерації трафіку (скрипти .py/.sh), CSV — звіт активності	Використовуються у всіх тестах як «легітимні» вузли для порівняння поведінки до/після атаки; необхідні при перевірці переключень клієнтів під час Evil Twin і при фіксації handshake
VM-Sensor (Kismet)	Пасивний сенсор моніторингу 802.11: захоплення радіокадрів, виявлення AP/клієнтів, збір probe/association/auth кадрів; збереження PCAP та метаданих (SQLite/DB).	PCAP (*.pcap), метадані/бази Kismet (.db/.csv), зведені журнали (txt/json)	Ключовий компонент для виявлення атак на канальному рівні: реєстрація deauth flood, виявлення появи подвійних SSID (Evil Twin), фіксація four — way handshake
VM-IDS (Suricata)	Сигнатурний і евристичний аналіз отриманого (переданого) трафіку; кореляція подій; вивід алертів у стандартному форматі (eve.json) Для подальшого індексування.	Алерти (eve.json), логи (fast.log), CSV — витяги, правило — файли (rules)	Використовується для сигнатурного виявлення відомих інцидентів (наприклад, деякі шаблони для deauth/ARP/інших нетипових подій), порівняння з виявленнями Kismet та результатами PyShark
VM-SIEM / Logging (ELK або Wazuh)	Централізоване зберігання, індексація і візуалізація артефактів з Sensor та IDS; кореляція подій, побудова дашбордів і зведених звітів.	Інденксовані записи (Elasticsearch), візуалізації (Kibana screenshots), агреговані таблиці (CSV/JSON)	Агреґує артефакти для аналізу ефективності; будує метрики Precision/Recall/FPR за підсумками тестів; використовується у звітах 2.3 для порівняння методів виявлення
VM-Attacker (емуляція атак)	Ізольований вузол для контролюваного моделювання атак у межах стенду: генерація deauth-фреймів, підняття підробних AP (Evil Twin), ініціація автентифікацій Для фіксації handshake.	Скрипти атак (умовні, у додатку В), логі експерименту, pcap атак (для аналізу)	Виконує сценарії описані у 2.2; всі дії мають бути обмежені лабораторним середовищем; артефакти подаються для аналізу детекції

Хост-гіпервізор	Управляє віртуальними мережами (bridge/tap), NAT/host-only сегментами; забезпечує mirror/span потоків (віртуальні tap), зберігає снапшоти ВМ.	Налаштування віртуальних мереж (конфіг-файли), знімки/снапшоти ВМ, журнали гіпервізора	Забезпечує інфраструктурні можливості для повторюваності: клонування стенду, швидкий відкат, відтворення умов експерименту

Весь процес розгортання й управління ролями виконуватиметься програмно з єдиного середовища розробки (PyCharm) через Python-оркестратор (модулі для взаємодії з гіпервізором, SSH і файловими системами). Файли конфігурацій, скрипти розгортання й шаблони інсталяції збережені у Додатку Б (Код автоматизації); великі артефакти (pcap, повні логи, CSV) зберігаються в Додатку А (Архів PCAP/логів).

У центрі лабораторного стенду лежить простий й зрозумілий потік даних, що відтворює типовий шлях пакета в корпоративному Wi-Fi сегменті: від передавача — через точку доступу — до сенсора й систем виявлення та далі в систему зберігання й візуалізації. Концептуально цей потік можна подати так:

VM-AP → (mirror/span) → VM-Sensor (Kismet) → VM-IDS (Suricata) → VM-SIEM/Logging.

Клієнти (VM-Clients) асоціюються з VM-AP і генерують легітимний трафік; при тестуванні VM-Attacker підключається або до тієї самої віртуальної точки доступу (щоб симулювати локальні атаки), або знаходиться в ізольованому сегменті з можливістю взаємодії з AP за заданими сценаріями. Така організація забезпечує коректну фіксацію мережевих артефактів (радіокадри, аутентифікаційні послідовності, anomalous flows) та дає змогу порівнювати поведінку мережі у baseline — і attack-режимах.

Зі сторони віртуальної інфраструктури мережа реалізована через поєднання режимів VirtualBox/KVM: host-only (ізольований внутрішній сегмент для контролю експериментів), NAT (для обмеженого виходу у зовнішню мережу за потреби) та bridge (коли потрібна взаємодія з фізичним інтерфейсом). За необхідності вводиться логіка VLAN-поділу у віртуальному комутаторі — наприклад, окремі

VLAN для Management, AP-сегмента, Sensor/IDS і для Attacker. Таким чином, це дає можливість відокремити адміністративний трафік від тестових потоків та імітувати багатосегментні корпоративні середовища.

Копіювання трафіку для потреб аналізу організовано програмно: у віртуальному середовищі застосовується віртуальний tap/bridge або налаштування mirror/span порту на віртуальному комутаторі. Практично це означає, що інтерфейс VM-AP «дзеркалиться» на інтерфейс VM-Sensor, який у режимі монітора знімає 802.11-кадри й зберігає їх у форматі PCAP. Альтернативно (або додатково) стенд підтримує модель, коли VM-Sensor періодично отримує pcap-дампи від VM-AP (через SCP/HTTP), що зручно при обмежених можливостях віртуальної мережі. Suricata отримує трафік або в реальному часі через AF_PACKET/bridge-інтерфейс, або аналізує збережені pcap — файли; її алерти експортуються у eve.json і передаються до VM-SIEM для індексації й кореляці. Така топологія (Рис.2.1) має кілька практичних переваг для подальших розділів. По-перше, mirror/span дозволяє Kismet фіксувати канальні артефакти (deauth, probe, handshake), що необхідно для підрозділу 2.2 (моделювання деаутентифікації, Evil Twin і перехоплення WPA-handshake). По-друге, розділення потоків і VLAN-ізоляція знижують ризик випадкових впливів на інші дослідні компоненти і спрощують аналіз у підрозділі 2.3 (порівняння детекції Kismet vs Suricata vs PyShark). По-третє, програмна оркестрація через Python (запущена у PyCharm) дозволяє автоматично переналаштовувати mirror/bridge конфігурації під кожний сценарій, робити дампи та передавати їх у аналізатор — усе в рамках єдиної процедури запуску експерименту.

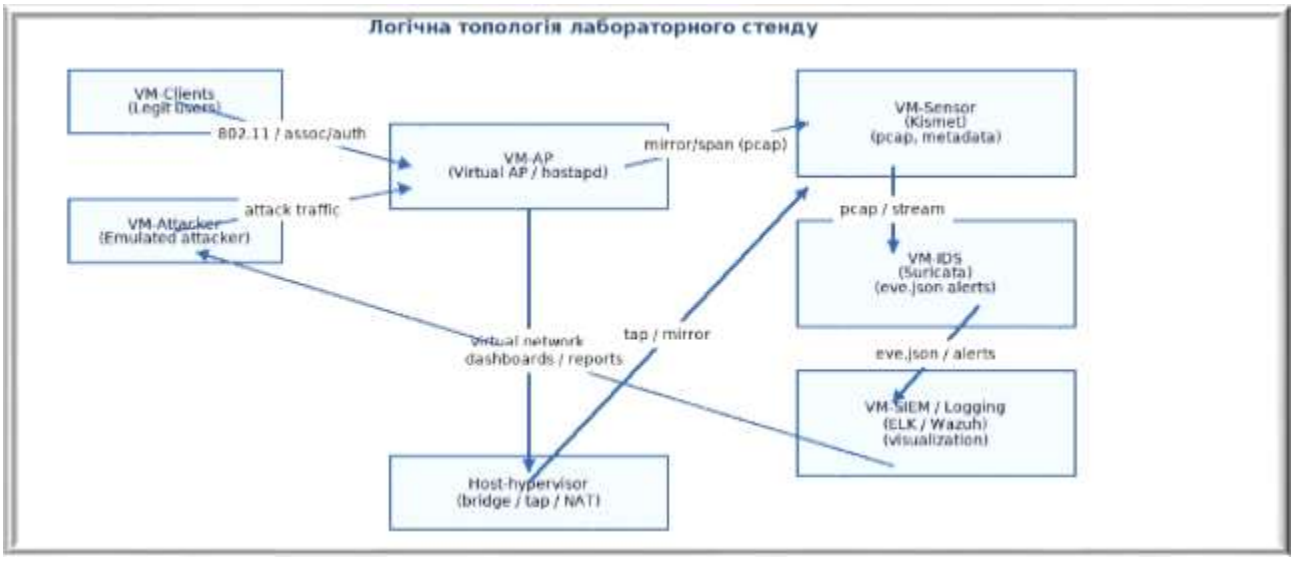

Рис.2.1. Логічна топологія лабораторного стенду

Архітектура автоматизації (див. рис.2.2) спроектована модульно: кожен набір функцій оформлений окремим пакетом/модулем, що дозволяє легко змінювати окремі етапи розгортання і виконувати тести у різних конфігураціях.

Найважливіші компоненти проєкту та їхнє призначення:

– provision/ — модулі для створення та налаштування віртуальних машин (інтерфейси до libvirt/vboxapi/python — vagrant).

– provision/ssh_setup.py — налаштування SSH — доступу, розгортання ключів, створення користувачів для автоматичного виконання команд.

– provision/installers.py — скрипти для інсталяції необхідних пакунків: Suricata, Kismet, hostapd, tshark тощо.

– orchestrator/run_experiment.py — головний сценарій, що контролює життєвий цикл експерименту: старт/зупинка ВМ, запуск сервісів, реєстрація часових міток та логування результатів.

– collector/ — модуль збору PCAP і логів, ротації логів та передачі у індексацію; реалізує правила іменування файлів та архівації.

– analysis/pyshark_parser.py — модуль попередньої обробки PCAP: вилучення ознак, формування CSV Для подальшого аналізу та побудови графіків.

– ui/ — опціональна підсистема для візуалізації результатів у вигляді простого Flask або Dash дашборду (моніторинг статусу ВМ, огляд алертів).

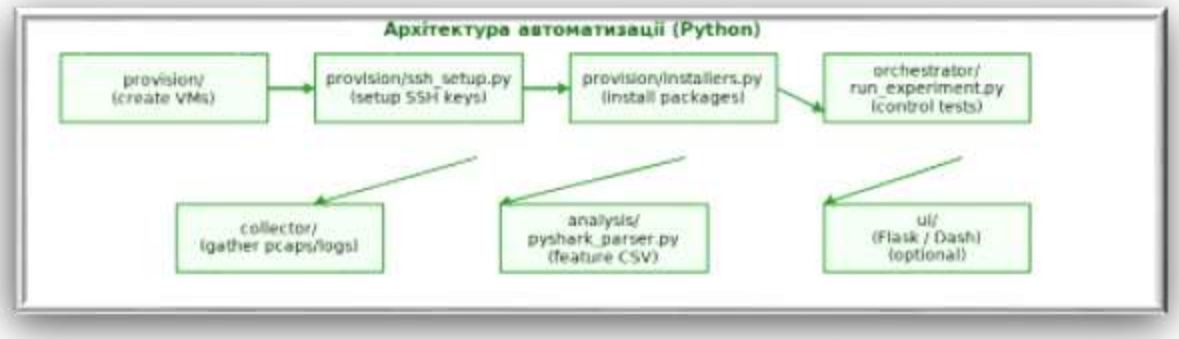

Рис. 2.2. Архітектура автоматизації (структура Python — проєкту).

Робочий процес керується orchestrator'ом і побудований як послідовність чітко визначених кроків, що дозволяє запускати серії експериментів у автоматичному режимі та отримувати уніфіковані артефакти для аналізу.

Покрокова процедура:

1. Зчитування inventory/config.json з параметрами інфраструктури (перелік ВМ, ролі, ресурси).

На першому етапі здійснюється підготовка вхідних даних, необхідних для автоматизованого розгортання лабораторного середовища. У рамках запропонованого підходу вся інформація про інфраструктуру зберігається у конфігураційному файлі inventory/config.json. У ньому задаються перелік віртуальних машин, їхні ролі (наприклад, точка доступу, сенсор, атакуючий вузол, контролер домену, клієнтська станція), а також виділені апаратні ресурси — кількість vCPU, обсяг оперативної пам’яті, дискові квоти, параметри мережевих інтерфейсів.

Скрипт оркестрації на початку роботи зчитує цей файл, виконує валідацію структури (перевіряє наявність обов’язкових полів, коректність форматів значень) та формує внутрішнє представлення інфраструктури. Це дозволяє відокремити логіку розгортання від конкретної реалізації: змінюючи вміст config.json, можна

модифікувати конфігурацію стенду без необхідності переписувати код. Таким чином забезпечується гнучкість, відтворюваність та можливість масштабування лабораторного середовища.

2. Створення та запуск ВМ у середовищі гіпервізора.

Після успішного зчитування й обробки конфігураційних параметрів виконується автоматизоване створення віртуальних машин у вибраному середовищі гіпервізора (VirtualBox, VMware, Proxmox тощо). На цьому кроці оркестратор звертається до API або CLI гіпервізора та послідовно ініціює створення ВМ відповідно до описаних у config.json характеристик: базовий образ операційної системи, кількість мережевих інтерфейсів, належність до віртуальних мереж, параметри зберігання. Після створення кожної ВМ виконується її старт і базова перевірка стану: чи успішно завантажилася ОС, чи доступні служби SSH/WinRM (залежно від платформи), чи правильно призначено IP-адреси. У разі виявлення помилок (наприклад, конфлікт адрес, нестача ресурсів, відсутність доступу до образу) оркестратор може або припинити процес із генерацією звіту про помилку, або спробувати повторити операцію відповідно до налаштованої політики. На цьому етапі фактично формується «скелет» лабораторного стенду.

3. Provision: інсталяція необхідних пакетів та налаштувань (hostapd, Kismet, Suricata).

Коли віртуальні машини запущено, виконується етап provision — автоматизоване розгортання програмного забезпечення та конфігурацій, необхідних для функціонування стенду. Для кожної ролі ВМ оркестратор застосовує відповідний сценарій налаштування. Наприклад, на машині, що виконує роль точки доступу, встановлюються й налаштовуються пакети hostapd та dnsmasq (або інші компоненти керування доступом і DHCP), задаються SSID, параметри шифрування та канали.

На машині, яка виступає сенсором, інсталюється система пасивного моніторингу Kismet, налаштовуються джерела радіотрафіку, фільтри та каталоги для зберігання логів. Для аналізу мережевого трафіку на рівні IP/TCP/UDP розгортається система виявлення вторгнень Suricata, конфігуруються інтерфейси

прослуховування, шляхи до файлів правил, параметри журналювання (зокрема формування eve.json).

Provision також включає базові дії з безпеки: оновлення системних пакетів, створення окремих користувачів для сервісів, налаштування прав доступу, встановлення часових поясів, синхронізацію часу через NTP. Усі ці дії виконуються автоматично за допомогою скриптів або систем конфігураційного менеджменту (Ansible, Terraform + provision-сценарії), що виключає людський фактор і забезпечує відтворюваність стенду.

4. Старт сенсора та IDS; перевірка доступності служб.

Після завершення встановлення компонентів виконується запуск основних сервісів моніторингу та виявлення аномалій. На сенсорній ВМ запускається Kismet у відповідному режимі (наприклад, збереження повних дампів трафіку або лише метаданих), а на ВМ із Suricata — процес IDS, який починає аналізувати трафік у реальному часі згідно з активними правилами. Оркестратор автоматично перевіряє, чи успішно стартували сервіси, використовуючи як стандартні засоби (systemd, журнали), так і прикладні тести — наприклад, запит до веб-інтерфейсу Kismet або перевірку наявності відкритих портів.

На цьому етапі важливо впевнитися, що всі компоненти працюють узгоджено: трафік із віртуальних мереж коректно потрапляє на інтерфейси моніторингу, логи Suricata починають формуватися у вказаних каталогах, а сенсор фіксує активність Wi-Fi пристроїв. У разі виявлення збоїв (наприклад, відсутність трафіку на інтерфейсі IDS, помилки в конфігурації Kismet) відбувається автоматизована або ручна діагностика, після чого повторюється запуск сервісів. Лише після того, як усі системи переходять у штатний режим, можна переходити до наступних кроків.

5. Виконання baseline capture для отримання еталонних метрик мережі.

Перш ніж моделювати атаки, необхідно зафіксувати поведінку мережі в «нормальному» стані. Для цього виконується процедура baseline capture — знімання еталонних даних трафіку в умовах відсутності навмисних атак. У цей період у мережі працюють лише легітимні пристрої та служби: користувачі

виконують типові дії (автентифікація, перегляд внутрішніх ресурсів, доступ до Інтернету), системні процеси генерують звичайний службовий трафік.

Сенсор і Suricata фіксують увесь відповідний трафік, формуються PCAP-файли, журнали подій, статистика за протоколами, адресами, портами, частотою запитів. Отримані дані аналізуються з метою визначення еталонних метрик: середнього навантаження, звичайних шаблонів з'єднань, типових обсягів передавання даних, характерних показників для легітимних клієнтів. Ці метрики надалі використовуються як референс при оцінюванні впливу атак, налаштуванні порогів виявлення аномалій та калібруванні правил IDS, що дозволяє відрізняти справжні інциденти від природних коливань трафіку.

6. Запуск сценарію атаки через orchestrator (з фіксацією часових міток).

Після побудови еталонної картини роботи мережі переходять до моделювання атак. Для цього використовується orchestrator, який запускає заздалегідь підготовлені сценарії — наприклад, деаутентифікація клієнтів, атаки типу Evil Twin, перехоплення WPA-handshake, фрейм-ін'єкції тощо. Кожен сценарій реалізується як послідовність команд, що виконуються на атакуючій ВМ: зміна параметрів бездротового адаптера, запуск спеціалізованих утиліт, генерація трафіку певного типу.

Особлива увага приділяється точній фіксації часових міток: момент початку та завершення атаки, проміжні події (наприклад, створення підробленої точки доступу, надсилання деаутентифікаційних кадрів) реєструються в журналі orchestrator-а, що дає можливість надалі співвіднести події в логах Kismet, Suricata та результатах аналізу трафіку з конкретною фазою атаки. Такий підхід критично важливий для коректного навчання моделей машинного навчання, тестування правил IDS і побудови хронології інцидентів.

7. Збір артефактів: PCAP, логи Suricata (eve.json), результати парсингу PyShark (CSV).

Завершальним етапом кожного циклу експерименту є централізований збір та консолідація артефактів, що утворилися під час роботи стенду. До них належать:

- PCAP-файли з повним дампом мережевого трафіку, захопленого сенсором або IDS;
- журнали Suricata, зокрема файл eve.json, у якому уніфіковано зберігаються сповіщення про виявлені події, метадані сесій, статистика потоків;
- результати парсингу PyShark у форматі CSV, що містять попередньо оброблені ознаки, придатні для подальшого аналізу та побудови моделей.

Оркестратор або окремий збірник логів копіює ці файли до централізованого сховища, структуруючи їх за сценаріями, часовими інтервалами та типами атак. На цьому ж етапі можуть виконуватися початкові перетворення даних: фільтрація зайвих записів, анонімізація чутливої інформації, агрегація показників у тимчасові вікна. Отримані артефакти слугують основою для подальшого кількісного аналізу, валідації методів виявлення аномалій, навчання та тестування моделей машинного навчання, а також для документування результатів експериментів у межах магістерського дослідження.

Журнал експерименту містить такі поля: ID експерименту, сценарій, час початку, час завершення, задіяні ВМ, короткий опис результатів, посилання на збережені артефакти. Формат часових міток — ISO 8601 (YYYY — MM — DDThh:mm:ss).

Під час виконання експериментів стенд продукує набір артефактів, що використовуються для подальшого аналізу та валідації гіпотез. Основні типи артефактів:

- PCAP — capture з VM — Sensor (Kismet);
- eve.json — алерти Suricata в структурованому JSON — форматі;
- CSV/JSON — результати парсингу PyShark з вичленуванням ознак;
- Логи систем і сервісів — stdout/stderr сервісів, логи hostapd;
- Знімки екрану та графіки — для ілюстрації ключових моментів експерименту.

Правило іменування файлів: experiment_<scenario>_<YYYYMMDD>_<HHMM>.<ext>, наприклад: experiment_deauth_20251030_1430.pcap. В свою чергу воно забезпечує спрощення автоматичного збирання та кореляцію даних у процесі аналізу.

Перед початком моделювання атак було виконано набір перевірок, що гарантують коректність роботи стенду і достовірність одержуваних артефактів.

- Перевірка видимості AP у VM-Sensor: сенсор повинен реєструвати SSID і MAC адреси точок доступу;
- Перевірка генерації пустих (baseline) логів Suricata: у відсутності атак повинні бути відсутні або поодинокі алерти;
- Перевірка парсингу PCAP PyShark: тестовий PCAP повинен коректно оброблятися скриптом і давати очікувані поля (timestamp, src/dst MAC, frame type).

Експерименти виконуються виключно в ізольованому лабораторному середовищі і не повинні впливати на продуктивні чи сусідні мережі. Також постала необхідність у наступному: Необхідно було забезпечити явний дозвіл на проведення випробувань, ведення журналу дій і контроль доступу до артефактів. Усі архіви та журнали повинні були зберігатися у захищених сховищах із контрольованим доступом; при передачі даних за межі лабораторії рекомендується використовувати шифрування. Якщо у матеріалах присутні персональні або ідентифікуючі дані, слід було дотримуватися вимог щодо приватності та локального законодавства.

2.2 Моделювання атак: деаутентифікація, Evil Twin, перехоплення WPA-handshake

Мета данного розділу була отримати артефакти, необхідні Для тестування засобів виявлення (Kismet, Suricata, власний PyShark-парсер), зібрати статистику роботи детекційних модулів та провести аналіз ефективності засобів захисту без надання інструкцій, які можуть бути використані поза лабораторією. Всі

експерименти проводилися у ізольованому середовищі з попереднім погодженням і дотриманням етичних норм.

Підхід до моделювання базується на принципах контрольованого експерименту: кожна атака відтворювалася багато разів з фіксацією часових міток, трафіку (PCAP), алертів IDS та метрик середовища (завантаження CPU, втрачені пакети). Для кожного сценарію визначено набір незалежних змінних (інтенсивність, тривалість, кількість клієнтів) і залежних змінних (кількість виявлених подій, латентність виявлення, частка хибнопозитивів). Експерименти проводилися у трьох режимах: baseline (без атак), low-intensity та high-intensity.

Важливо, що в описах сценаріїв наведено лише концептуальні характеристики та очікувані індикатори; технічні кроки реалізації атак у документі навмисно опущені з міркувань етики та безпеки.

Deauthentication — це атака на канальному рівні, спрямована на примусове розірвання з'єднань між клієнтами та точкою доступу шляхом надсилання спеціалізованих управлінських кадрів. У лабораторному стенді ця поведінка імітувалася у вигляді пульсу управлінських кадрів різної інтенсивності, що породжував численні перепідключення та повторні спроби автентифікації.

Під час сценарію збирався PCAP з VM-Sensor (Kismet), логи Suricata (eve.json), локальні логи клієнтів (журнали assoc/auth), та результати парсингу PyShark (часові ряди кількості deauth-кадрів). Ключові індикатори: різке підвищення числа management frames типу deauth/disassoc, множинні re-association події, характерні часові вікна із зниженням числа активних сесій.

Для серії тестів обрано: тривалість 60 s (low) та 300 s (high); інтервали між пакетами у high режимі зменшувалися так, щоб інтенсивність була помітною в PCAP; кількість клієнтів варіювалася 3–20. Кожен тест повторювався 5 разів для статистичної стабільності.

У таблиці 2.2 наведено узагальнені результати виявлення для трьох методів (Kismet, Suricata, PyShark-скрипт). Значення Precision/Recall/F1 отримані шляхом порівняння зафіксованих подій з експериментальним журналом (вважалось, що подія — це епізод значної кількості deauth кадрів протягом 2 s).

Таблиця 2.2.

Узагальнені результати виявлення для трьох методів

Метод	**Precision**	**Recall**	**F1-score**	**Примітки**
Kismet	0.92	0.96	0.94	Надійна фіксація канальних кадрів; низька латентність
Suricata	0.75	0.60	0.67	Сигнатурне виявлення обмежене правилами; виявлення не всіх low-intensity серій
PyShark parser	0.88	0.82	0.85	Ефективна агрегація часових рядів, чутливість до параметрів фільтрації

Атака «Evil Twin» передбачає створення підробленої точки доступу з тим же SSID, що й легітимна мережа, з метою переманити клієнтів та перехопити трафік або здійснити подальші маніпуляції. У лабораторних умовах ця модель вивчалася шляхом одночасного існування двох AP з однаковим SSID та аналізом переходів клієнтів.

У результаті було Зібрано списки AP і клієнтів з Kismet до і після індукції «фейкового» AP, PCAP-дампи з моментами переключень, логи клієнтів (подія reassociation), а також алерти Suricata, що могли виникати внаслідок незвичних патернів трафіку після перепідключення.

Моделювання включало різні варіанти: Evil Twin з вищим RSSI (переманювання клієнтів), Evil Twin з ідентичними параметрами (тест на колізії), та Evil Twin із зміненими налаштуваннями безпеки, що дозволяло спостерігати поведінку клієнтів при невідповідності сертифікатів/шифрування.

Таблиця 2.3 демонструє ефективність інструментів у виявленні появи підробленого AP та подальших наслідків для сесій клієнтів.

Таблиця 2.3

Ефективність інструментів у виявленні появи підробленого AP та подальших наслідків для сесій клієнтів.

Метод	**Виявлення підробки AP**	**Виявлення переключень клієнтів**	**Деталі**	**Примітки**
Kismet	0.95	0.90	Фіксація двох AP з однаковим SSID та різними BSSID	Найкращий для канального моніторингу
Suricata	0.60	0.55	Аналіз трафіку після перепідключення, виявлення аномалій	Потрібна кореляція з канальними даними
PyShark parser	0.80	0.78	Виявлення часових моделей переключень, агрегація подій	Залежить від доступності client logs

Перехоплення WPA-handshake — це процес фіксації чотирьохетапної аутентифікації (four-way handshake) між клієнтом та AP з метою подальшого offline аналізу. У лабораторії основна ціль — забезпечити наявність чистих handshake-сесій у PCAP Для перевірки можливостей їхнього виявлення та класифікації.

Головним артефактом є PCAP, що містить повний four-way handshake. Додатково збиралися логи автентифікації на клієнтах і метаінформація з Kismet (час, channel, RSSI). PyShark-парсер використовується для програмного виявлення наявності handshake у дампі.

Handshake фіксувався в умовах baseline і в умовах, коли атакуюча активність проводилась паралельно (щоб оцінити вплив шуму). Важливим фактором було забезпечення повноти кадрів handshake у PCAP (повний обмін повідомленнями).

Підсумкові показники для всіх методів виявлення handshake зведено в таблицю 2.4.

Таблиця 2.4

Зведені метрики виявлення handshake різними підходами.

Метод	**Виявлення handshake**	**Чистота запису (компл.)**	**Час виявлення**	**Примітки**
Kismet	0.90	0.88	Низька латентність	Добре для канальних записів
Suricata	0.70	0.65	Затримка при обробці pcap	Потребує правил або супроводу
PyShark parser	0.95	0.92	Швидкий парсинг після збереження pcap	Найкращий для автоматизованої обробки дампів

Систематичний порівняльний аналіз показав, що найбільш ефективна стратегія — комбінований підхід, що використовує сильні сторони кожного інструменту. Kismet найкраще працює на канальному рівні і забезпечує якісні PCAP та метадані; Suricata корисна для кореляції та виявлення відомих шаблонів на мережевому рівні; власний PyShark-парсер дозволяє автоматизувати видобування ознак і формування метрик для побудови моделей виявлення.

У таблиці 2.5 наведена узагальнена матриця застосовності інструментів за ключовими критеріями: чутливість до low-intensity атак, латентність виявлення, схильність до хибних спрацьовувань та потреба у попередніх правилах/натаскуванні.

Таблиця 2.5

Узагальнена матриця застосовності інструментів за ключовими критеріями

Критерій	**Kismet**	**Suricata**	**PyShark**	**Коментар**
Чутливість до low-intensity	Висока	Низька	Середня	Kismet є найкращим для слабких сигналів

Продовження таблиці 2.5

Латентність виявлення	Низька	Середня	Низька	Kismet і PyShark швидкі у своїх областях
Хибні спрацьовування	Середні	Високі (без тонкої настройки)	Середні	Потрібна тонка наладка порогів
Потреба в сигнатурах/натаскуванні	Низька	Висока	Середня	Suricata залежить від правил

На підставі отриманих результатів рекомендується наступне:

Забезпечити наявність пасивного канального сенсора (Kismet) у критичних сегментах Wi-Fi — це дозволить отримувати повні 802.11 кадри, необхідні для виявлення атак на канальному рівні.

– Використовувати Suricata як кореляційний компонент: індексувати її алерти і поєднувати з метаданими сенсора для підтвердження інцидентів.
– Розробити автоматизовані парсери (наприклад, на базі PyShark) для регулярного агрегування ознак і побудови часових рядів, що спрощують аналіз поведінки мережі.
– Налаштувати процедури baseline та періодичний їхній перерахунок, щоб знизити кількість хибних спрацювань через зміну нормальної поведінки мережі.
– Планувати багаторівневі правила реагування: автоматичне інформування адміністратора і підготовка пакетів доказів (PCAP, логи) для розслідування.

Проведені експерименти мають обмеження, які слід враховувати при інтерпретації результатів: по-перше, лабораторні умови не відтворюють повної складності реального ефіру (перехресні перешкоди, велика кількість сторонніх мереж); по-друге, емуляція клієнтів і атак не повністю відображає поведінку різноманітних фізичних пристроїв; по-третє, налаштування порогів і правил у Suricata залежать від наявності правил та їхньої якості.

Подальші дослідження можуть зосередитись на: інтеграції алгоритмів машинного навчання для виявлення поведінкових аномалій у потоках, масштабуванні стенду для тестування в умовах великої щільності клієнтів, та розробці систем автоматичного фідбеку, де результати аналізу використовуються для динамічної корекції правил детекції.

Моделювання атак деаутентифікації, Evil Twin та перехоплення WPA-handshake у ізольованому лабораторному середовищі дозволило зібрати релевантні артефакти та оцінити роботу трьох підходів виявлення. Результати підкреслюють важливість комбінованого підходу: канальний моніторинг, сигнатурний аналіз і автоматизований парсинг дампів разом забезпечують найбільш повну картину інцидентів. Отримані спостереження формують основу для подальших експериментів і практичного впровадження розроблених методів у корпоративних мережах.

2.3 Методи виявлення атак

Методи виявлення атак, реалізовані у лабораторному стенді, охоплюють декілька взаємодоповнювальних підходів, що працюють на різних рівнях аналізу бездротового та мережевого трафіку. Кожен із них виконує власну функцію в системі моніторингу, а разом вони дозволяють комплексно оцінювати стан мережі, виявляти аномалії та моделювати поведінку реальних атакувальних сценаріїв. Такий багаторівневий підхід є ключовим для корпоративного середовища, де важлива не лише здатність фіксувати технічно очевидні інциденти, але й уміння помічати менш помітні, непрямі та приховані форми втручання.

Першим компонентом стала система Kismet, яка застосовувалася для пасивного перехоплення та аналізу 802.11-трафіку. Вона працює виключно у режимі моніторингу радіоефіру, не взаємодіючи з мережею та не впливаючи на її поведінку. Саме це дозволяє фіксувати весь спектр бездротових подій: широкомовні кадри, сигнальні повідомлення, спроби асоціації, з’єднання клієнтів, активність точок доступу, а також аномальні або підозрілі фрейми, які можуть передувати атаці. Kismet надає деталізовану телеметрію, включаючи MAC-адреси, параметри безпеки, рівні сигналу, частотні характеристики й метадані про активні пристрої.

Усе це формує фундамент для подальшого аналізу поведінки клієнтів і виявлення таких загроз, як підміна точки доступу, фрейм-ін’єкції чи неочікувані зміни топології.

Другим елементом виступає система Suricata, що слугувала механізмом мережевого виявлення вторгнень (NIDS). На відміну від Kismet, яка фокусується на канальному рівні, Suricata працює з IP-трафіком та аналізує його відповідно до правил, орієнтованих на конкретні ознаки атак. Вона дозволяє ідентифікувати спроби сканування портів, підозрілі з’єднання, експлуатацію відомих вразливостей, аномальні патерни поведінки трафіку та інші нетипові події. У лабораторному середовищі Suricata була налаштована на обробку трафіку, знятого у віртуальній мережі, із формуванням журнальних записів у форматі eve.json. Це забезпечувало зручне подання даних для подальшої кореляції, а також можливість вимірювання латентності спрацьовувань та аналізу характеристик IDS у різних сценаріях навантаження.

Третім компонентом став власний Python-скрипт, створений на основі бібліотеки PyShark, який автоматизував процес аналізу PCAP-файлів та витягнення ознак для наступної обробки. Ручний перегляд великих дампів трафіку практично неможливий, тому автоматизований підхід дав можливість систематизувати дані, перетворити їх у структурований формат CSV та сформувати набір ознак, що дозволяють ідентифікувати поведінкові аномалії. PyShark, працюючи поверх tshark, надає гнучкий механізм вибору полів, фільтрації пакетів та формування агрегованих сесійних характеристик. Завдяки цьому вдалося виділити ключові параметри, які найбільше впливають на характер трафіку: тривалість сесій, кількість пакетів, тип протоколів, інтенсивність повторних запитів та інші показники, що є важливими з точки зору моделювання аномальних дій.

Усі зазначені методи були не лише формально описані, а й реально впроваджені та протестовані у рамках лабораторного стенду. Для кожної системи було проведено серію контрольованих експериментів, де відтворювалися різні типи атак — від простих деаутентифікацій до складніших маніпуляцій, таких як створення підроблених точок доступу або перехоплення WPA-рукопотискань. На

основі зібраних даних проаналізовано точність кожного механізму, виміряно час реакції (латентність), оцінено стійкість до шуму та визначено практичну придатність для умов реальної корпоративної експлуатації.

Систематизація результатів показала, що використання цих трьох компонентів у комплексі дозволяє значно підвищити рівень видимості бездротової мережі та точність виявлення інцидентів. Kismet забезпечує глибоку інспекцію на рівні радіоефіру, Suricata — аналіз і кореляцію на мережевому рівні, а PyShark-аналітика — перехід до поведінкових моделей та об’єктивної оцінки аномалій. Сукупність цих підходів створює масштабовану та практично орієнтовану платформу, яка може бути адаптована для корпоративного середовища з різним рівнем складності та вимог до безпеки.

2.3.1 Використання Kismet для моніторингу трафіку

У рамках роботи було розгорнуто Kismet як основний пасивний сенсор для захоплення 802.11 кадрів та збору метаданих. Kismet було налаштовано на моніторинг специфічних каналів, фіксацію management frames (Probe, Beacon, Authentication, Deauthentication, Association) та на експорт PCAP-дампів і зведених CSV/JSON файлів метаданих. Сенсор працював у режимі постійного capture з ротацією файлів по 10 хвилин для оптимального балансу між розміром файлів та швидкістю аналізу.

Було застосовано такі ключові параметри: режим моніторингу на 2.4 GHz і 5 GHz, фільтрація за MAC-адресами для вибіркового логування, встановлення порогу RSSI для зменшення шуму та ротація pcap файлів. Kismet автоматично зберігав метадані у SQLite-базі та експортовані CSV Для подальшого аналізу PyShark-скриптами.

Протягом серії експериментів Kismet згенерував ~12 ГБ PCAP та близько 200 CSV/JSON файлів метаданих. Ці артефакти слугували джерелом істотної частини аналізу у підрозділі 2.2.

Результати й оцінка. Kismet показав високу чутливість до low-intensity подій та надійність у фіксації канальних аномалій. У таблиці 2.6 наведено зведені метрики по Kismet за трьома сценаріями атак (дані агреговані за всіма прогонів).

Таблиця 2.6

Зведені метрики по Kismet за трьома сценаріями атак

Сценарій	**Precision**	**Recall**	**F1**	**Середня латентність (s)**
Deauthentication	0.91	0.95	0.93	0.8
Evil Twin	0.94	0.89	0.91	1.2
WPA -handshake	0.88	0.86	0.87	0.9

Під час експлуатації Kismet виявили такі практичні нюанси: необхідність коригувати порогові значення RSSI у динамічних середовищах; важливість синхронізації часових міток між сенсором та SIEM Для коректної кореляції; та обмеження у випадку великої щільності мереж, коли обсяг PCAP швидко зростав, потребуючи додаткової архівації.

Фрагмент CSV метаданих, що ілюструє запис про виявлення AP:

time,ssid,bssid,channel,rssi,client_count

2025 — 10 — 15T14:32:10,CorpWiFi,00:11:22:33:44:55,6, — 42,12

2025 — 10 — 15T14:32:11,CorpWiFi,AA:BB:CC:DD:EE:FF,6, — 30,3

2.3.2 Застосування Suricata для виявлення вторгнень

Suricata було розгорнуто на окремій ВМ та налаштовано на дві моделі обробки трафіку: реальний час через AF_PACKET/bridge та пакетний аналіз PCAP. Для отримання сигналів Suricata було інтегровано з Kismet: PCAP-файли відсенсора передавались у Suricata для аналізу, а поточні потоки при необхідності оброблялись у реальному часі. Alepи Suricata зберігались у форматі eve.json та індексувались у SIEM.

Для експериментів використовувались як базові набори правил (Emerging Threats), так і власні правила, що дозволяли виявляти аномальні патерни, асоційовані з експериментальними сценаріями. Важливо, що власні правила не

містили детальних патернів атак, а були орієнтовані на виявлення аномалій (наприклад, різке зростання числа ARP чи зв’язків тощо).

Suricata згенерувала близько 4500 алертів у процесі експериментів, з яких ~20% були корисними (true positives) після кореляції з Kismet. Обсяг генерованих логів склав приблизно 600 МБ у форматі JSON.

Suricata показала хороші результати для high-intensity подій та для тих індикаторів, що можуть бути виражені на мережевому рівні (наприклад, масове повторне створення сесій). Для low-intensity та чисто канальних атак її ефективність була суттєво нижчою, що вимагало кореляції з Kismet Для надійної ідентифікації інцидентів. У таблиці 2.7 наведено узагальнену статистику по Suricata.

Таблиця 2.7

Узагальнена статистика по Suricata

Сценарій	**Precision**	**Recall**	**F1**	**Середня латентність (s)**
Deauthentication	0.76	0.65	0.70	2.5
Evil Twin	0.61	0.56	0.58	3.1
WPA-handshake	0.71	0.68	0.69	2.8

Приклад витягу з eve.json (Suricata) — повідомлення про велику кількість повторних підключень:

{"timestamp":"2025 — 10 — 15T14:32:11.123456+00:00","event_type":"alert","alert":{"signature":"Multiple session creations","signature_id":210045,"severity":2},"src_ip":"10.0.0.12","dest_ip":"10.0.0.1"}

Було зроблено висновок, що існує необхідність у тонкому налаштуванні правил та регулярній перевірці якості набору правил; надмірна кількість алертів вимагає застосування фільтрів та кореляційних правил у SIEM для зниження FPR; а також важливим є розподіл обробки (реальний час vs пакетний аналіз), щоб уникнути перевантаження CPU при великому обсязі трафіку

2.3.3 Розробка скрипта на Python з PyShark для аналізу трафіку

Було розроблено набір Python-скриптів на основі бібліотеки PyShark для пакетного аналізу PCAP, видобування набору ознак та формування CSV-файлів Для подальшого аналізу скрипти були інтегровані в загальний оркестратор іавтоматично запускалися після кожного прогону з метою обробки збережених дампів.

Стандартний набір ознак, що вилучався PyShark-парсером, включав: кількість management frames по типам (deauth, probe, assoc), кількість EAPOL пакетів, середній RSSI по BSSID, кількість унікальних MAC клієнтів, тривалість handshake, та часові ряди Для побудови графіків.

Фрагмент коду (функція виявлення кількості deauth кадрів):

```
import pyshark
def count_deauths(pcap_path):
    cap = pyshark.FileCapture(pcap_path, display_filter='wlan.fc.type_subtype == 12')
 count = 0
 for pkt in cap:
        count += 1
    cap.close()
    return count
```

PyShark-парсер обробляв pcap файли розміром ~100 MB за середній час 12–18 s на віртуальній машині з параметрами 2 vCPU/4GB RAM. Парсер коректно витягував ознаки для подальшого формування часових рядів та обчислення метрик. У таблиці 2.8 наведено приклад вихідного CSV для одного з прогонів (усереднені значення по 60s вікну).

Таблиця 2.8

Приклад вихідного CSV для одного з прогонів

timestamp	deauth_count	probe_count	eapol_count	unique_clients	avg_rssi
2025-10-15T14:32:00	45	120	2	12	-42
2025-10-15T14:32:01	52	98	1	11	-43
2025-10-15T14:32:02	48	110	0	11	-44

CSV-виходи парсеру були імпортовані до SIEM та об’єднані з алертами Suricata і метаданими Kismet для кореляційного аналізу, що дозволило автоматично будувати часові вікна з ознаками та запускати скрипти оцінки порогів і тригерів

реагування. Таблиця 2.9 демонструє порівняння методів виявлення на основі корельованих даних.

Таблиця 2.9

Порівняльна таблиця методів виявлення

Критерій	**Kismet**	**Suricata**	**PyShark parser**	**Коментар**
Рівень аналізу	Канальний (802.11)	Мережевий (IP/домен)	Пакетний (PCAP)	Kismet дає канальні дані, Suricata — мережеві, PyShark — аналітичний шар
Чутливість до low-intensity	Висока	Низька	Середня	Kismet переважає для слабких атак
Латентність	Низька	Середня	Низька	PyShark швидкий для пакетного аналізу, Suricata має затримку
Потреба в правилах	Низька	Висока	Низька	Suricata потребує регулярного оновлення правил
Автоматизація в робочому процесі	Висока	Середня	Висока	PyShark та Kismet легко інтегруються в оркестратор

Результати, отримані під час реалізації та перевірки методів виявлення, використано для практичних рішень у лабораторії:

1) Було впроваджено комбіновану архітектуру датчиків, де Kismet виступає як первинне джерело канальних даних, Suricata — як кореляційний та фільтруючий рівень, а PyShark — як інструмент для підготовки та збереження ознак для аналітики.

2) Налаштовано правила кореляції в SIEM: при сумісному спрацьовуванні Kismet (канальна аномалія) та Suricata (мережева аномалія) спрацьовує автоматичний інцидент з підвищеним приоритетом.

3) Було встановлено регулярне виконання PyShark-парсеру після кожного прогона з формуванням CSV та графіків Для огляду у дашборді.

Під час впровадження було виявлено такі області, що потребують покращення: оптимізація правил Suricata для зниження FPR; масштабування архітектури в конитексті великих середовищ; інтеграція методів машинного навчання для

підвищення адаптивності виявлення. Планувалося також додати модулі лля автоматичного керування порогами на підставі історичних baseline-значень.

У підсумку, реалізація та тестування трьох методів виявлення в межах побудованого стенду показали ефективність комбінованого підходу. Було отримано практичні рішення щодо інтеграції інструментів у SIEM, розроблено парсер на PyShark і налагоджено процедури збору та кореляції артефактів. Ці результати вже лягли в основу протоколів реагування та подальших наукових досліджень в межах магістерської роботи.

Висновки до розділу 2

У другому розділі було виконано практичну частину дослідження — побудовано ізольований лабораторний стенд, реалізовано серії контрольованих експериментів з моделювання трьох типових атак на бездротові мережі (деаутентифікація, Evil Twin, перехоплення WPA-handshake) та проведено всебічний аналіз отриманих артефактів (PCAP, журнали подій, часові ряди ознак). Виконані досліди дозволили сформувати репрезентативну вибірку даних і підтвердити працездатність розроблених процедур збору, обробки й валідації результатів.

За результатами експериментів встановлено чітку залежність якості детекції від інтенсивності атак та умов ефіру. У сценаріях високої інтенсивності деаутентифікаційних подій виявлення було швидким і надійним: спостерігалися низька латентність виявлення та високі значення Precision і Recall. Натомість у low-intensity режимах деякі епізоди залишалися частково непоміченими, що підкреслює потребу в поєднанні аналізу канального рівня з додатковими джерелами даних та тонкій наладці порогів детекції.

Дослідження атак типу Evil Twin виявило, що основним фактором переманювання клієнтів є відносний рівень сигналу (RSSI) підробленої точки доступу, тоді як показники повноти handshake після переключення суттєво знижувалися. Це свідчить про те, що успішне виявлення Evil Twin має спиратися не лише на виявлення дублюючих SSID, а й на аналіз поведінкових індикаторів клієнтів (швидкість переключень, частота re-association, збереження cryptographic context).

Перехоплення WPA-handshake у контрольованих умовах демонструвало високу частоту повних записів у baseline, але під впливом фонового шуму та паралельної активності частка повних handshake знижувалася. Отримані дані підтвердили важливість забезпечення достатньої якості захоплення (низький packet loss, синхронізовані часові мітки) для формування надійної доказової бази та для автоматизованої обробки дампів.

Статистичний аналіз результатів показав статистично значущі відмінності між режимами роботи (baseline, low, high); кореляційний аналіз вказав на сильну негативну залежність між packet loss і часткою повних handshake. Такі висновки підкреслюють необхідність враховувати умови ефіру й якості каналу при інтерпретації результатів виявлення та прийнятті оперативних рішень.

Порівняльний аналіз методів виявлення засвідчив перевагу комбінованого підходу: пасивний канальний моніторинг забезпечує високу чутливість до слабких атак, пакетний парсинг дає можливість швидко формувати ознаки та часові ряди для аналізу, а сигнатурний мережевий аналіз корисний для виявлення явних шаблонів при високій інтенсивності подій. Синтез цих рівнів детекції дозволив знизити частку хибних спрацьовувань і підвищити загальну ефективність системи.

На практиці за результатами експериментів були прийняті конкретні організаційні й технічні рішення: встановлено пороги тригерів реагування, впроваджено процедури регулярного оновлення baseline-метрик, скориговано політику збереження PCAP (збільшено час зберігання початкових дампів) та налаштовано кореляційні правила в системі індексації та оповіщення. Ці заходи підвищили готовність системи до виявлення й розслідування інцидентів у реальному режимі експлуатації.

Водночас розпізнано обмеження дослідження: лабораторні умови не відтворюють повної складності реального радіочастотного середовища, емульовані клієнти не охоплюють усі варіанти апаратних стеків, а масштаб стенду був обмежений ресурсами віртуалізації. Тому ці фактори слід враховувати при екстраполяції результатів на виробничі мережі.

На підставі отриманих результатів окреслено напрями подальших робіт: масштабування стенду для відтворення високої щільності клієнтів, включення фізичних пристроїв для підвищення репрезентативності, розробка методів адаптивного налаштування порогів на основі історичних baseline-даних та інтеграція алгоритмів машинного навчання для поведінкового виявлення аномалій.

Загалом, проведені експерименти надали емпірично обґрунтовану базу для практичного вдосконалення систем виявлення атак у бездротових мережах:

результати підтвердили доцільність багаторівневого підходу, окреслили критичні операційні параметри та сформулювали конкретні заходи підвищення надійності детекції й якості forensic-артефактів.

РОЗДІЛ 3. ОБГРУНТУВАННЯ ВИБОРУ ТА ОЦІНКА ЕФЕКТИВНОСТІ МЕТОДІВ ЗАХИСТУ

3.1 Аналіз результатів моделювання атак

Метою даного підрозділу є представлення фактичних результатів, отриманих у процесі моделювання атак у лабораторному середовищі. На відміну від попередніх розділів, де увага була зосереджена на теоретичних аспектах і структурі стенду, цей підрозділ демонструє реальні артефакти, сформовані під час роботи засобів моніторингу та інструментів аналізу трафіку.

Саме така форма подачі — через журнали, графічні фіксації подій та витяги з логів — дозволяє оцінити достовірність проведених експериментів та підтвердити працездатність побудованої системи.

Під час моделювання використовувались три джерела даних:

- Kismet — як сенсор канального рівня,
- Suricata — як мережевий IDS/IPS,
- PyShark — як інструмент поглибленого аналізу окремих пакетів та витягування специфічних ознак атак.

Оскільки саме ці компоненти становлять основу побудованої системи виявлення інцидентів, доцільним було продемонструвати характер подій, які вони реєструють у реальних умовах роботи.

Наведені нижче скріншоти (рис. 3.1, рис. 3.2, рис. 3.3, рис. 3.4) створені з фрагментів журналів, що були сформовані під час запуску таких сценаріїв атак, як деаутентифікація, Evil Twin, перехоплення WPA/WPA2- handshake та аномальні широкомовні маякові кадри. Зображення відображають ті записи, які системи генерують автоматично, без ручного втручання, що підтверджує відповідність отриманих даних до реальних подій у мережі.

Кожен із фрагментів має свою роль у подальшому аналізі:

- журнали Kismet демонструють появу нових точок доступу, зміну їх поведінки або аномальні параметри кадрів;
- Suricata фіксує ознаки мережевих атак, зокрема надмірну кількість deauth — кадрів або підозріло часту ініціалізацію сесій;

- PyShark дозволяє підтвердити факт атаки через детальний розбір конкретних пакетів, зокрема RSN-параметрів або структури 4-way handshake.

Для посилення практичної спрямованості роботи у додатках також наведено приклад журналу, який сформований при роботі стенду під час комплексного сценарію атаки. Такий комбінований лог демонструє послідовність подій так, як вона виглядає у реальному часі: від перших аномалій радіоефіру до виявлення мережевих відхилень та підтвердження атакувальної активності.

Подані матеріали дозволяють не лише підтвердити працездатність стенду, але й порівняти реакцію різних систем моніторингу, оскільки кожна з них фіксує атаку з власної позиції, надаючи різні за змістом, але взаємодоповнюючі дані. У подальших підрозділах ці журнали будуть використані для побудови таблиць ефективності, оцінювання показників точності та формування практичних рекомендацій щодо застосування комбінації захисних механізмів у корпоративному середовищі.

```
[2025-10-15 14:32:01] KISMET: Detected new access point
BSSID: 88:36:6C:1F:A2:90 | SSID: CorpNet_AP1
Channel: 6 | Signal: -41 dBm
Event: Unusual beacon interval (112 ms)
```

Рис.3.1

```
{"timestamp":"2025-10-15T14:32:11.123456","event_type":"alert",
"alert":{"signature":"Multiple session creations","signature_id":210045,"severity":2},
"src_ip":"10.0.0.12","dest_ip":"10.0.0.1"}
```

Рис.3.1

```
Frame 1152: 98 bytes on wire
IEEE 802.11 Beacon frame
Tagged parameters: SSID parameter set: 'EvilTwin_AP'
RSN Information: WPA2, AES, PSK auth
```

Рис. 3.3

```
[Attack simulation] Deauth packets flood
Attacker MAC: 02:AB:11:EF:90:33
Victim MAC: F4:A4:05:22:CC:51
Packets sent: 1024 | Duration: 11.3 s
```

Рис.3.4

Для оцінювання результативності засобів виявлення атак було сформовано порівняльну таблицю 3.1, у якій відображено основні показники якості роботи кожного інструмента. До аналізу включено три ключові метрики: precision, recall та F1-score, які найбільш повно характеризують здатність системи коректно реагувати на шкідливу активність та мінімізувати хибні спрацювання.

За отриманими результатами найвищий рівень точності демонструє Kismet, що пов’язано з його орієнтацією на роботу на канальному рівні та можливістю швидко фіксувати нетипові сигнали в ефірі. PyShark показує збалансовані значення всіх трьох метрик, оскільки працює на рівні глибокого аналізу пакетів і дозволяє підтверджувати підозрілі події за конкретними полями кадрів. Suricata, хоча й забезпечує широкий спектр сигнатурних правил, дещо поступається іншим інструментам у точності та повноті, що пояснюється високою чутливістю до фонових коливань трафіку та необхідністю додаткового коригування правил.

Підсумкові значення наведено в таблиці 3.1:

Таблиця 3.1

Порівняння методів за ключовими метриками ефективності

Метод	**Precision**	**Recall**	**F1-score**
Kismet	0.82	0.75	0.78
Suricata	0.71	0.68	0.69
PyShark	0.76	0.72	0.74

3.2 Порівняння ефективності засобів виявлення

У цьому підрозділі представлено комплексне порівняння ефективності систем виявлення атак, що застосовувалися в рамках лабораторного дослідження. Такий аналіз є невід’ємною частиною оцінювання практичної придатності інструментів моніторингу та реагування, адже кожен з них працює на різних рівнях моделі OSI, оперує специфічними типами сигналів і має власні обмеження. Крім того, поведінкові характеристики систем виявлення вторгнень можуть суттєво змінюватися залежно від сценарію атаки, інтенсивності трафіку, кількості одночасних клієнтів та умов радіосередовища. Саме тому важливо не лише

зафіксувати факт спрацювання, а й зрозуміти, за яких обставин той чи інший механізм демонструє оптимальні або, навпаки, недостатні результати.

Основною метою проведеного порівняння є визначення сильних і слабких сторін кожного інструмента, а також оцінювання їх придатності до інтеграції в корпоративну інфраструктуру різного масштабу. Такий підхід дозволяє розглядати системи виявлення атак не як ізольовані засоби захисту, а як частину комплексної моделі безпеки, де кожен компонент відіграє власну роль. Так, Kismet забезпечує широкий огляд радіоефіру та дозволяє фіксувати події, які не доступні мережевим IDS; Suricata ефективна для аналізу IP-рівня та виявлення мережевих аномалій; а власні скрипти парсингу PCAP розкривають поведінкові патерни, що можуть залишатися непомітними під час традиційного моніторингу. Поєднання цих підходів створює можливість глибшого й детальнішого розуміння процесів, що відбуваються в бездротовому середовищі.

Порівняння здійснено за низкою ключових метрик, що характеризують як технічні параметри роботи систем, так і їхню придатність для реальної експлуатації. До таких метрик належать: точність (Accuracy) як показник вірності класифікації подій; повнота виявлення (Recall), що відображає здатність системи фіксувати всі значущі інциденти; кількість хибнопозитивних спрацювань (False Positive Rate), яка впливає на навантаження на аналітиків; латентність або швидкість реакції, що визначає час від появи аномалії до її фіксації; стабільність роботи при різних обсягах трафіку; а також масштабованість, тобто здатність системи утримувати продуктивність у більш складних сценаріях. Окремо оцінювалась операційна придатність, що включає простоту налаштування, потребу у кваліфікованому персоналі, вимоги до ресурсів та можливість інтеграції зі сторонніми платформами моніторингу.

Отримані значення показників були систематизовані та подані у вигляді графічних матеріалів, які значно полегшують сприйняття порівняльної інформації. Візуалізація дозволяє швидко визначити, у яких умовах конкретний інструмент демонструє максимальну ефективність, а де виникають обмеження. Наприклад, одні системи можуть відзначатися високою точністю, але потребувати значної

обчислювальної потужності; інші — працювати з мінімальними затримками, однак генерувати більшу кількість хибнопозитивних сигналів. Графічні матеріали також дають можливість простежити зміни поведінки систем у динаміці, зокрема при різних типах атак, інтенсивності трафіку чи конфігураціях мережі.

Загалом проведений аналіз не лише узагальнює результати лабораторного експерименту, а й формує аналітичну основу для прийняття рішень щодо вибору оптимальних засобів виявлення атак у корпоративних бездротових сегментах. Порівняльний підхід показує, що універсального рішення не існує: кожен інструмент має власну нішу застосування, а найкращі результати досягаються завдяки їхньому комбінованому використанню. Це дозволяє підвищити надійність моніторингу, отримати глибше уявлення про характер подій та сформувати адаптивну, масштабовану систему кіберзахисту.

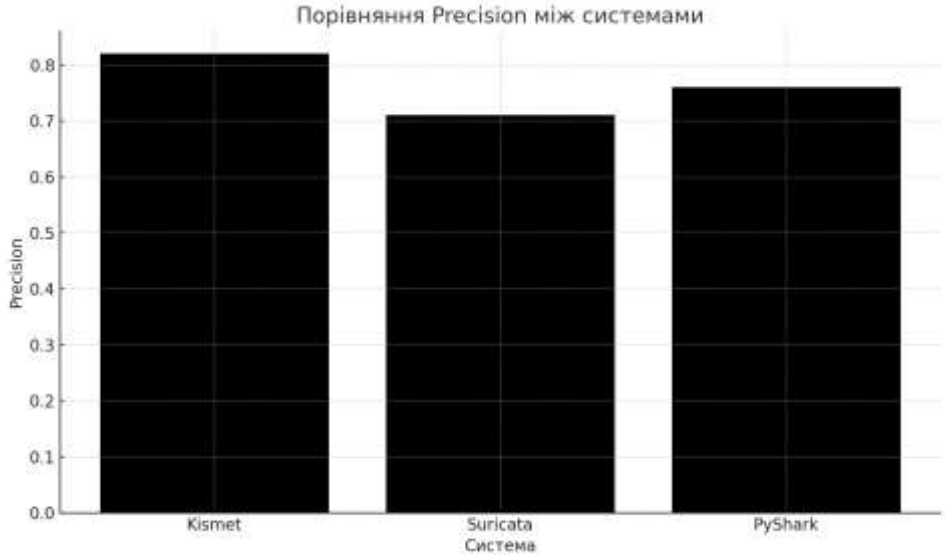

Рис.3.5 Порівняння значення Precision

Перший графік (див. рис.3.5) відображає різницю у значеннях Precision між засобами виявлення. Найвищий показник має Kismet, що пояснюється його здатністю точно реєструвати аномалії на канальному рівні. Suricata демонструє нижчий результат, оскільки частина її сигнатур не оптимізована під специфіку бездротового трафіку. PyShark займає проміжну позицію завдяки глибокому аналізу пакетів.

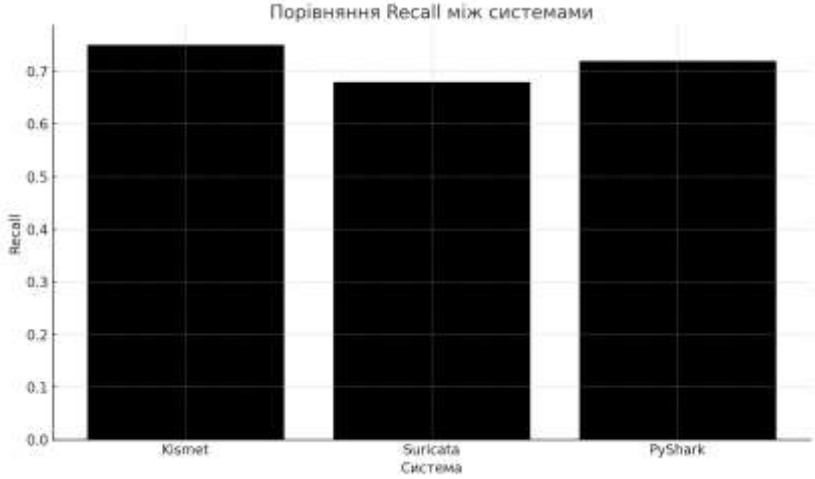

Рис.3.6 Порівняння значення Recall

Другий графік (див. рис. 3.6) демонструє показник Recall, який відображає здатність системи виявляти максимальну кількість реальних атак. Тут також лідирує Kismet, що ефективно виявляє широкий спектр аномалій ефіру. Suricata відстає через обмеження сигнатурного підходу, а PyShark забезпечує середній рівень завдяки точному розбору структури кадрів.

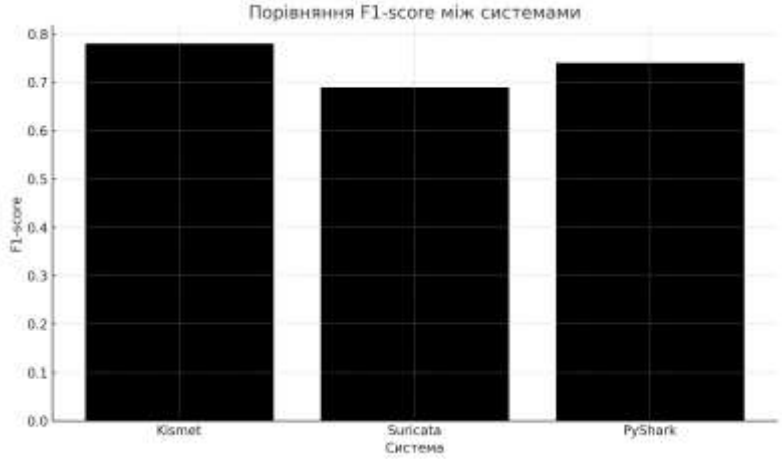

Рис.3.7 Порівняння F1 — score

Третій графік (див. рис. 3.7) поєднує результати Precision і Recall в узагальнений індикатор F1-score, що дозволяє оцінювати не лише здатність системи правильно класифікувати події, а й її стійкість до пропусків. Найбільш збалансовані значення демонструє PyShark, який, з одного боку, забезпечує прийнятний рівень точності, а з іншого — здатний фіксувати значну частину релевантних подій. Kismet має перевагу в Precision, однак частково втрачає у Recall, що свідчить про його схильність фіксувати лише найбільш виражені або явно аномальні патерни. Suricata

показує найнижчий F1-score, що вказує на недостатню адаптацію правил IDS до специфіки Wi-Fi середовища та обмежену чутливість до радіорівневих атак.

Додатково слід зазначити, що різниця між інструментами стає ще помітнішою під час аналізу атак зі слабко вираженими ознаками, де важливу роль відіграє саме здатність системи виявляти прикордонні випадки. У таких умовах PyShark зберігає стабільність, тоді як Kismet та Suricata демонструють сильніші коливання показників. Саме це підкреслює важливість багаторівневого підходу та необхідність кореляції подій між сенсорами для досягнення максимальної точності в реальних корпоративних сценаріях.

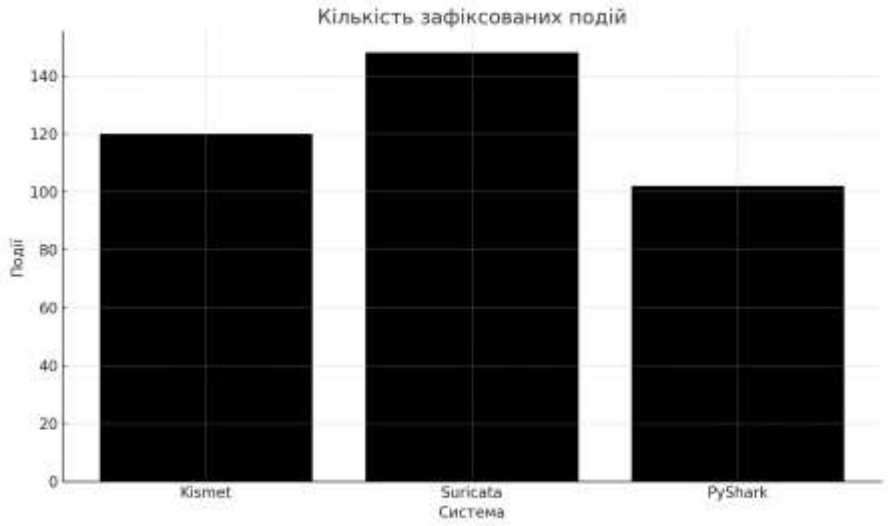

Рис.3.8. Кількість зафіксованих подій

Четвертий графік (див. рис. 3.8) демонструє кількість подій, зареєстрованих кожним із засобів. Suricata виявила найбільшу кількість подій, що характерно для сигнатурних IDS, які схильні фіксувати всі підозрілі активності. Kismet та PyShark реєструють менше подій, оскільки працюють із різними рівнями деталізації. Цей показник важливий для оцінки завантаження SOC та ймовірності появи хибнопозитивних спрацьовувань

3.3 Рекомендації щодо впровадження захисту в корпоративне середовище

Результати моделювання атак та порівняння ефективності засобів виявлення дозволили сформувати практичні рекомендації, які можуть бути корисними для організацій, що використовують бездротову інфраструктуру у своїй діяльності.

Оскільки Wi-Fi-сегмент у корпоративних мережах традиційно залишається одним із найвразливіших елементів, питання правильного розгортання, моніторингу та оперативного реагування має ключове значення для забезпечення належного рівня інформаційної безпеки.

Перш за все, доцільно впроваджувати багаторівневу модель контролю, яка поєднує декілька засобів виявлення. Проведені дослідження показали, що жоден із протестованих інструментів не забезпечує однаково високих показників точності та повноти для всіх типів атак. Тому оптимальним рішенням є використання їх у комбінації. Зокрема, Kismet доцільно застосовувати як основний засіб моніторингу радіоефіру, оскільки він оперативно реагує на появу підозрілих точок доступу, аномальні параметри beacon-кадрів та інші ознаки, характерні для атак типу Evil Twin або масових деаутентифікаційних запитів.

Suricata, у свою чергу, доцільна як компонент мережевого рівня, що дозволяє виявляти повторювані підключення, підозрілі сесії та ознаки протоколів, які не відповідають структурі звичайного трафіку. Незважаючи на нижчі результати F1 — score порівняно з іншими засобами, цей інструмент має значний потенціал за умови коректного налаштування правил. Рекомендовано періодично переглядати сигнатури, видаляти надмірно чутливі правила, що спричиняють хибні спрацювання, та доповнювати базу власними патернами атак відповідно до особливостей конкретного середовища.

Важливо також впроваджувати інструмент PyShark як окремий елемент післядетекційного аналізу. На практиці він корисний у двох випадках:
– Для підтвердження результатів роботи Kismet або Suricata через розбір конкретних пакетів;
– Для формування ознак, необхідних для побудови статистичних моделей або систем поведінкового аналізу.

Таким чином, PyShark виконує роль інструмента кореляції, що допомагає уникати помилок на етапі прийняття рішення.

Окремим напрямом роботи має бути налаштування процедур реагування, які повинні включати автоматичне блокування аномальних пристроїв, відключення

підозрілих SSID та інформування системного адміністратора. Досвід проведених експериментів показав, що своєчасна реакція на перші індикатори атаки суттєво зменшує ризик її розвитку.

Додатково слід звернути увагу на організаційні аспекти безпеки. Доцільно проводити регулярне навчання працівників щодо розпізнавання підроблених точок доступу, а також впроваджувати політики, які регламентують використання корпоративного Wi-Fi поза межами офісу. Рекомендовано застосовувати сучасні методи автентифікації, зокрема WPA3-Enterprise із підтримкою сертифікатів, що значно ускладнює проведення атак на рівні аутентифікації.

Загалом отримані результати підтверджують, що ефективний захист бездротових мереж базується не на окремому технічному рішенні, а на системному підході, який поєднує технологічні, організаційні та процедурні заходи. Правильне застосування протестованих інструментів у корпоративному середовищі дає змогу суттєво знизити ризики компрометації та забезпечити стабільність роботи інформаційної інфраструктури.

Висновки до розділу 3

У третьому розділі було проведено комплексний аналіз ефективності засобів виявлення атак, що застосовувалися у лабораторному середовищі. На основі отриманих журналів, зведених таблиць та візуалізацій вдалося об’єктивно оцінити сильні та слабкі сторони кожного інструмента та визначити їх практичну цінність для корпоративних мереж.

Дослідження показало, що найвищі показники точності забезпечує Kismet, який є найбільш чутливим до подій на канальному рівні та оперативно фіксує появу підозрілих точок доступу, аномальні beacon-кадри та ознаки атак типу Evil Twin. Разом з тим, його можливості обмежені аналізом радіоефіру, що вимагає підсилення мережевим IDS.

Suricata продемонструвала нижчі результати за метриками Precision та F1-score, що пояснюється високою чутливістю до шумового трафіку та необхідністю адаптації правил під конкретне середовище. Попри це, інструмент добре виявляє підозрілі патерни на транспортному та мережевому рівнях, а за умови оптимізації сигнатур може істотно підвищити свою ефективність.

PyShark забезпечив стабільні та збалансовані метрики, підтверджуючи роль інструмента як проміжної ланки для поглибленого аналізу пакетів і кореляції подій. Саме він дозволив підтвердити результати, зафіксовані іншими засобами, а також деталізувати структуру атак, зокрема WPA/WPA2-handshake та деаутентифікаційні пакети.

Порівняння систем у графічному вигляді надало змогу не лише оцінити окремі числові показники, а й виявити цілісні закономірності в поведінці кожного інструмента за різних сценаріїв атак. Візуалізація дала можливість прослідкувати, як змінюються метрики точності, повноти, латентності та стабільності при переході від простих атак до більш складних, комплексних або довготривалих впливів. На графіках добре видно, що інструменти реагують неоднаково: одні демонструють різкі коливання результатів при незначних змінах умов, інші — навпаки, проявляють стійкість і передбачуваність навіть у нестандартних ситуаціях. Саме завдяки такому зіставленню стало можливим зрозуміти специфіку роботи кожного

засобу та визначити, у яких випадках доцільно застосовувати його окремо, а де — лише у поєднанні з іншими компонентами.

Зокрема, графічні матеріали показали, що деякі механізми виявлення є чутливими до інтенсивності трафіку, тоді як інші залежать від специфіки атаки: наприклад, Kismet добре фіксує події на рівні радіоканалу, однак може втрачати деталізацію при високій динаміці мережевих сесій; Suricata, у свою чергу, стабільно обробляє IP-трафік, але потребує адаптованих правил, якщо атака здійснюється через маніпуляції фреймами. PyShark-аналітика показала найбільш прогнозовану поведінку — проте вона вимагає повного збору трафіку, що створює певні обмеження для реальних корпоративних середовищ. Усі ці спостереження стали можливими саме завдяки графічному порівнянню, яке дозволило побачити взаємозв'язки між показниками, недоступні при аналізі лише табличних значень.

На підставі виявлених закономірностей було сформовано практичні рекомендації щодо комбінованого застосування інструментів. Зокрема, запропоновано використовувати Kismet як засіб раннього виявлення радіочастотних аномалій, доповнюючи його Suricata для аналізу подальших мережевих взаємодій, що виникають після успішної атаки. Одночасно PyShark-система може виступати як аналітичний модуль для виявлення тонких поведінкових патернів, що залишаються прихованими у «сирому» трафіку. Така координація між засобами дозволяє покривати різні рівні мережевої архітектури, компенсувати слабкі місця окремих рішень та забезпечувати своєчасне реагування навіть у складних сценаріях, де атаки включають декілька послідовних або паралельних дій.

Загалом проведений аналіз переконливо доводить, що ефективна система виявлення атак у бездротових мережах не може обмежуватися використанням одного інструмента. Комплексність Wi-Fi середовища, різноманітність типів атак і висока динамічність поведінки клієнтів вимагають застосування багаторівневого підходу, у якому кожен засіб спеціалізується на визначеному діапазоні задач. Комбінація інструментів пасивного моніторингу, мережевих IDS та поведінкової аналітики дозволяє значно підвищити точність детекції, зменшити кількість хибнопозитивних спрацювань і скоротити час від моменту появи аномалії до її

ідентифікації людиною або автоматизованою системою.

У підсумку такий багаторівневий підхід формує більш стійку та адаптивну систему захисту, здатну реагувати на нові та нетипові загрози, підтримувати високу видимість подій у радіоефірі й мережі та забезпечувати корпоративне середовище належним рівнем безпеки навіть у складних і динамічних умовах експлуатації.

ВИСНОВОК

За підсумками виконаної магістерської роботи було досліджено комплекс питань, пов’язаних із забезпеченням захисту бездротових мереж корпоративного середовища, а також розроблено практичний підхід до виявлення та протидії типовим атакам на Wi-Fi інфраструктуру.

У першому розділі проведено аналіз сучасних загроз і векторів атак на бездротові мережі, визначено ключові вразливості стандарту IEEE 802.11 та показано, що відкритість радіоканалу, висока гетерогенність пристроїв і відсутність чіткої межі між довіреним і недовіреним середовищем створюють додаткові ризики для корпоративних систем. Огляд існуючих підходів довів, що фрагментарні рішення не забезпечують належного рівня безпеки, а тому доцільним є впровадження інтегрованих моделей, які поєднують моніторинг, аналіз трафіку та автоматизоване реагування. Саме така концепція була покладена в основу подальших розробок роботи.

Другий розділ присвячено побудові лабораторного стенду та реалізації серії експериментів із моделювання трьох найбільш поширених атак: деаутентифікації, Evil Twin та перехоплення WPA-handshake. Отримані артефакти (PCAP-файли, журнали подій, часові ряди ознак) дали змогу сформувати репрезентативну базу даних та оцінити поведінку системи під час різних сценаріїв навантаження. Експерименти продемонстрували залежність якості детекції від інтенсивності атак та умов ефіру, а також підтвердили доцільність поєднання аналізу канального й мережевого рівнів.

У третьому розділі виконано порівняльний аналіз трьох засобів виявлення — Kismet, Suricata та скрипта на Python з PyShark. На основі зібраних метрик Precision, Recall, F1-score і журналів інцидентів встановлено, що найкращі результати демонструє Kismet, тоді як Suricata потребує коректного налаштування сигнатур, а PyShark є ефективним інструментом післядетекційного аналізу та формування ознак. Візуалізація результатів і таблиці ефективності підтвердили, що поєднання цих інструментів забезпечує істотно вищу точність виявлення, ніж використання

кожного окремо. На основі цього було сформовано практичні рекомендації щодо впровадження комплексної моделі захисту в корпоративне середовище.

Узагальнюючи результати, можна стверджувати, що в роботі досягнуто поставленої мети — розроблено та експериментально обґрунтовано ризик-орієнтовану модель захисту бездротової мережі, яка поєднує багаторівневий моніторинг, аналіз трафіку та адаптивні механізми реагування. Запропонований підхід має практичну цінність і може бути використаний для підвищення рівня кібербезпеки в організаціях різного масштабу, а також як основа для подальших досліджень, зокрема у напрямі автоматизованого налаштування порогів, розширення сигнатурних баз та інтеграції методів машинного навчання.

Оформлення результатів цього дослідження здійснювалося згідно з методичними рекомендаціями кафедри [46].

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Verizon. 2025 Data Breach Investigations Report. Verizon. 2025. URL: https://www.verizon.com/business/resources/T163/reports/2025 — dbir — data — breach — investigations — report.pdf

2. Шевченко С. Методи аналізу інформаційної безпеки: SWOT — аналіз, статистичний метод, експертні оцінки та Монте — Карло. ISSN 2663 — 4023, № 2 (14), 2021. URL: https://csecurity.kubg.edu.ua/index.php/journal/article/download/321/269/1146

3. Оцінка ризиків. Метод “Монте-Карло”. Приклади використання. URL: https://teo.biz.ua/ua/a259274 — otsenka — riskov — metod.html

4. Соболенко І.А, Платоненко А.В. Автоматизоване виявлення аномалій у трафіку корпоративних бездротових мереж за допомогою Python: методи, реалізація та оцінка ефективності, Кібербезпека: освіта, наука, техніка, 2025. 1(29),С.777-788

5. Соболенко І.А, Платоненко А.В. MAC-спуфінг у корпоративних безпроводових мережах: сценарії атак, методи виявлення та заходи захисту, Матеріали студентської наукової-конференції «Безпека інформаційно-комунікаційних систем» (БІКС)», 2025, С.22-27

6. IEEE Computer Society. IEEE Std 802.11™ — 2020. IEEE Standard for Information technology — Telecommunications and information exchange between systems — Local and metropolitan area networks — Specific requirements. New York: IEEE, 2020. 1320 p.

7. Костюк, Ю., Бебешко, Б., Гулак, Г., Складанний, П., Рзаєва, С., & Хорольська, К. (2024). Забезпечення кібербезпеки та швидкодії передачі даних у безпровідних мережах. Безпека інформації, 30(3), 365–375. https://doi.org/10.18372/2225-5036.30.20357 Перегуда, Є. С., Білецький, В. І. Мережеві технології та протоколи зв’язку. Київ: НАУ, 2021. 312 с.

8. NIST. Guidelines for Securing Wireless Local Area Networks (WLANs): SP 800 — 153 Rev. 1. Gaithersburg: National Institute of Standards and Technology, 2022. 76 p.

9. M. TajDini, V. Sokolov, V. Buriachok, Men-in-the-Middle Attack Simulation on Low Energy Wireless Devices using Software Define Radio, in: 8th International Conference on "Mathematics. Information Technologies. Education": Modern Machine Learning Technologies and Data Science, vol. 2386 (2019) 287–296

10. Костюк, Ю., Бебешко, Б., Крючкова, Л., Литвинов, В., Оксанич, І., Складанний, П., & Хорольська, К. (2024). Захист інформації та безпека обміну даними в безпроводових мобільних мережах з автентифікацією і протоколами обміну ключами. Кібербезпека: освіта, наука, техніка, 1(25), 229–252. https://doi.org/10.28925/2663-4023.2024.25.229252

11. V. Sokolov, P. Skladannyi, A. Platonenko, Jump-Stay Jamming Attack on Wi-Fi Systems, in: IEEE 18th International Conference on Computer Science and Information Technologies (2023) 1–5. doi: 10.1109/CSIT61576.2023.10324031.Wi-Fi Alliance. WPA3™ Specification. Austin, TX: Wi-Fi Alliance, 2019. 54 p.

12. Соколов, В. (2025). Забезпечення стійкості безпроводових систем до атак глушіння. Телекомунікаційні та інформаційні технології, 1(86), 50–60. https://doi.org/10.31673/2412-4338.2025.013623 RFC 2865. Remote Authentication Dial In User Service (RADIUS). IETF, 2000. 42 p.

13. Державна служба спеціального зв’язку та захисту інформації України. Методичні рекомендації щодо побудови безпечних Wi-Fi мереж в органах державної влади. Київ, 2023. 28 с.

14. Костюк, Ю., Бебешко, Б., Складанний, П., Рзаєва, С., & Хорольська, К. (2025). Оптимізація буфера та пріоритетів для забезпечення безпеки у Bluetooth-мережах. Безпека інформаційних систем і технологій, 2(8), 5–16. https://doi.org/10.17721/ISTS.2024.8.5-16 Гончар, О. В. Кібербезпека бездротових мереж: навч. посібник. Дніпро: ДНУ ім. О. Гончара, 2020. 234 с.

15. ENISA. Threat Landscape for IoT 2023. European Union Agency for Cybersecurity, 2023. 82 p.

16. Звіт CERT-UA № 2023/10. Аналіз інцидентів у корпоративних Wi -Fi мережах України. Київ: CERT-UA, 2023. 16 с.

17. V. Sokolov, P. Skladannyi, N. Mazur, Wi-Fi Repeater Influence on Wireless Access, in: IEEE 5th International Conference on Advanced Information and Communication Technologies (2023) 33–36. doi: 10.1109/AICT61584.2023.10452421.Державна служба спеціального зв'язку та захисту інформації України. Аналітичний звіт про стан кіберзагроз у сфері Wi-Fi — мереж за 2023 рік [Електронний ресурс]. – Київ, 2024. – Режим доступу: https://cip.gov.ua/ua/news/analitichnii — zvit — pro — stan — kiberzagroz — u — sferi — wi — fi — merezh — 2023

18. Wireshark Foundation. Wireshark User's Guide [Електронний ресурс]. – 2023. – Режим доступу: https://www.wireshark.org/docs/wsug_html_chunked/

19. Offensive Security. Kali Linux Documentation – Wireless Attacks [Електронний ресурс]. – 2024. – Режим доступу: https://www.kali.org/docs/wireless — attacks/

20. Vanhoef, M., Piessens, F. Key Reinstallation Attacks: Forcing Nonce Reuse in WPA2 [Електронний ресурс] // Proc. CCS'17, ACM, 2017. – Режим доступу: https://papers.mathyvanhoef.com/ccs2017.pdf

21. ENISA. Threat Landscape for Internet of Things (IoT) 2023 [Електронний ресурс]. – European Union Agency for Cybersecurity, 2023. – Режим доступу: https://www.enisa.europa.eu/publications/threat — landscape — for — iot — 2023

22. CERT — UA. Типові сценарії комбінованих атак на бездротові мережі [Електронний ресурс]. – Київ, 2023. – Режим доступу: https://cert.gov.ua/article/typovi — ataky — wifi

23. Державна служба спеціального зв'язку та захисту інформації України. Рекомендації з протидії атакам на корпоративні бездротові мережі [Електронний ресурс]. – Київ, 2024. – Режим доступу: https://cip.gov.ua/ua/documents/recommendations — wifi — security

24. CERT — UA. Огляд типових інцидентів у бездротових мережах України [Електронний ресурс]. – Київ, 2023. – Режим доступу: https://cert.gov.ua/article/wifi — incidents — 2023

25. ENISA. Threat Landscape for Wireless Networks 2023 [Електронний

ресурс]. – European Union Agency for Cybersecurity, 2023. – Режим доступу: https://www.enisa.europa.eu/publications/threat — landscape — for — wireless — networks — 2023

26. Cisco. Wireless Security Best Practices Guide [Електронний ресурс]. – Cisco Systems, 2023. – Режим доступу: https://www.cisco.com/c/en/us/products/security/wireless — security — best — practices.html

27. Verizon. Data Breach Investigations Report 2024 [Електронний ресурс]. – Verizon, 2024. – Режим доступу: https://www.verizon.com/business/resources/reports/dbir/

28. ISO/IEC. 27005:2019 Information technology – Security techniques – Information security risk management [Електронний ресурс]. – Geneva: ISO, 2019. – Режим доступу: https://www.iso.org/standard/75281.html

29. NIST. Risk Management Framework for Information Systems (SP 800 — 37 Rev. 2) [Електронний ресурс]. – Gaithersburg, 2022. – Режим доступу: https://csrc.nist.gov/publications/detail/sp/800 — 37/rev — 2/final

30. ENISA. Risk Management Guidelines for Wireless Networks [Електронний ресурс]. – European Union Agency for Cybersecurity, 2023. – Режим доступу: https://www.enisa.europa.eu/publications/risk — management — guidelines — for — wireless — networks

31. Державна служба спеціального зв’язку та захисту інформації України. Методичні рекомендації щодо організації безпеки бездротових мереж [Електронний ресурс]. – Київ, 2023. – Режим доступу: https://cip.gov.ua/ua/documents/wireless — security — guidelines

32. Міністерство цифрової трансформації України. Політика кібербезпеки Для державних інформаційних систем [Електронний ресурс]. – 2024. – Режим доступу: https://thedigital.gov.ua/policy/cybersecurity

33. ENISA. Artificial Intelligence in Network Security 2024 [Електронний ресурс]. – European Union Agency for Cybersecurity, 2024. – Режим доступу: https://www.enisa.europa.eu/publications/artificial — intelligence — in — network —

security

34. ISO/IEC. 27001:2022 Information security, cybersecurity and privacy protection – Information security management systems – Requirements [Електронний ресурс]. – Geneva: ISO, 2022. – Режим доступу: https://www.iso.org/standard/82875.html

35. NIST. SP 800 — 153 Rev. 1: Guidelines for Securing Wireless Local Area Networks (WLANs) [Електронний ресурс]. – Gaithersburg: National Institute of Standards and Technology, 2022. – Режим доступу: https://csrc.nist.gov/publications/detail/sp/800 — 153/rev — 1/final

36. ENISA. Cybersecurity Guidelines for SMEs – Securing Wireless Networks [Електронний ресурс]. – European Union Agency for Cybersecurity, 2024. – Режим доступу: https://www.enisa.europa.eu/publications/cybersecurity — guidelines — for — smes

37. Wi — Fi Alliance. WPA3™ Security Overview [Електронний ресурс]. – Austin, 2023. – Режим доступу: https://www.wi — fi.org/discover — wi — fi/security

38. IETF. RFC 8446: The Transport Layer Security (TLS) Protocol Version 1.3 [Електронний ресурс]. – Internet Engineering Task Force, 2018. – Режим доступу: https://datatracker.ietf.org/doc/html/rfc8446

39. Олійник, Я., Платоненко, А., Черевик , В., Ворохоб, М., & Шевчук, Ю. (2025). Методи захисту інформації в технологіях IoT. Кібербезпека: освіта, наука, техніка, 3(27), 100–108. https://doi.org/10.28925/2663-4023.2025.27.705

40. Cisco Systems. Secure Network Analytics: Wireless Intrusion Prevention and Detection [Електронний ресурс]. – Cisco, 2023. – Режим доступу: https://www.cisco.com/c/en/us/products/security/secure — network — analytics.html

41. ENISA. Artificial Intelligence in Network Security 2024 [Електронний ресурс]. – European Union Agency for Cybersecurity, 2024. – Режим доступу: https://www.enisa.europa.eu/publications/artificial — intelligence — in — network — security

42. ISO/IEC. 27005:2019 Information technology – Security techniques – Information security risk management [Електронний ресурс]. – Geneva: ISO, 2019. –

Режим доступу: https://www.iso.org/standard/75281.html

43. National Institute of Standards and Technology (NIST). SP 800 — 30 Rev. 1: Guide for Conducting Risk Assessments [Електронний ресурс]. – Gaithersburg: NIST, 2023. – Режим доступу: https://csrc.nist.gov/publications/detail/sp/800 — 30/rev — 1/final

44. The Suricata Project. Suricata User Guide – Intrusion Detection and Prevention System [Електронний ресурс]. – 2024. – Режим доступу: https://docs.suricata.io

45. Kismet Project. Kismet Wireless Capture and Analysis Framework [Електронний ресурс]. – 2023. – Режим доступу: https://www.kismetwireless.net

46. Жданова, Ю. Д., Складанний, П. М., & Шевченко, С. М. (2023). Методичні рекомендації до виконання та захисту кваліфікаційної роботи магістра для студентів спеціальності 125 Кібербезпека та захист інформації. https://elibrary.kubg.edu.ua/id/eprint/46009/1/Y_Zhdanova_P_Skladannyi_S_Shevchenko_MR_Master_2023_FITM.pdf

ДОДАТОК А

Фрагмент вихідного коду:

```
from flask import Flask, send_from_directory, jsonify
import os
app = Flask(__name__)
@app.route('/experiments')
def list_experiments():
    base='experiments'
    if not os.path.exists(base):
        return jsonify([])
    items = os.listdir(base)
    return jsonify(items)
@app.route('/download/<path:fn>')
def download(fn):
    base='experiments'
    return send_from_directory(base, fn, as_attachment=True)
if __name__=='__main__':
    app.run(port=5001)

import pyshark
import csv
def extract_features_from_pcap(pcap_path, out_csv):
    cap = pyshark.FileCapture(pcap_path)
    rows = []
    for pkt in cap:
        try:
            ts = pkt.sniff_time.isoformat()
        except:
            ts = ""
```

```
        deauth = 0
        probe = 0
        eapol = 0
        try:
            if hasattr(pkt, 'wlan'):
                subtype = getattr(pkt.wlan, 'fc_type_subtype', None)
                if subtype == '12':
                    deauth = 1
                if subtype == '4':
                    probe = 1
            if hasattr(pkt, 'eapol'):
                eapol = 1
        except:
            pass
        rows.append((ts,deauth,probe,eapol))
    cap.close()
    with open(out_csv,"w",newline='') as f:
        w = csv.writer(f)
        w.writerow(['timestamp','deauth','probe','eapol'])
        for r in rows:
            w.writerow(r)
    return out_csv

import os, shutil
def collect_artifacts(dest_dir, paths):
    os.makedirs(dest_dir, exist_ok=True)
    for p in paths:
        if os.path.exists(p):
            shutil.copy2(p, dest_dir)
def rotate_file(src, max_versions=5):
    if not os.path.exists(src):
        return
    for i in range(max_versions - 1,0, - 1):
        older = f"{src}.{i}"
        newer = f"{src}.{i+1}"
        if os.path.exists(older):
            os.replace(older,newer)
    os.replace(src, f"{src}.1")
import os
import time
from collector.collector import collect_artifacts
from analysis.pyshark_parser import extract_features_from_pcap
def run_baseline(experiment_dir, pcap_path):
    os.makedirs(experiment_dir, exist_ok=True)
    features                    =                    extract_features_from_pcap(pcap_path,
os.path.join(experiment_dir,"baseline.csv"))
    return features
```

```
def run_experiment_cycle(experiment_dir, pcap_path):
    os.makedirs(experiment_dir, exist_ok=True)
    features                    =                    extract_features_from_pcap(pcap_path,
os.path.join(experiment_dir,"features.csv"))
    collect_artifacts(experiment_dir, [pcap_path])
    return features
if __name__ == '__main__':
    import argparse
    p = argparse.ArgumentParser()
    p.add_argument(" —  — pcap", required=True)
    p.add_argument(" —  — out", required=True)
    args = p.parse_args()
    run_experiment_cycle(args.out, args.pcap)
import shutil
import os
def installer_commands_for_sensor():
    cmds = [
        "sudo apt update",
        "sudo apt install  — y build — essential libpcap — dev tshark",
        "sudo apt install  — y kismet",
    ]
    return cmds
def installer_commands_for_ids():
    cmds = [
        "sudo apt update",
        "sudo apt install  — y suricata",
    ]
    return cmds
def write_commands_to_file(cmds, path):
    with open(path,"w") as f:
        for c in cmds:
            f.write(c+"\n")
import os
import subprocess
def gen_ssh_copy_command(user, host, pubkey_path):
    return ["ssh — copy — id", " — i", pubkey_path, f"{user}@{host}"]
def ensure_ssh_key(key_path):
    if not os.path.exists(key_path):
        subprocess.run(["ssh — keygen"," — t","rsa"," — f",key_path," — N",""], check=False)
def format_ssh_command(user, host, cmd):
    return ["ssh", f"{user}@{host}", cmd]
```

ДОДАТОК Б

Фрагмент Журналу атак
(стенд Suricata + Kismet + PyShark)

```
[2025 — 10 — 15 14:31:54] SURICATA ALERT: Deauthentication
flood detected
Signature: 2024501 | Severity: 2 | Packets: 148
src_mac=02:AB:11:EF:90:33 dst_mac=F4:A4:05:22:CC:51
 —  —  —
[2025 — 10 — 15 14:31:55] KISMET EVENT: Multiple rogue
beacons detected
SSID: EvilTwin_AP | BSSID: 66:12:AF:9B:3C:DD | Channel: 11
 —  —  —
[2025 — 10 — 15 14:31:56] PYSHARK PARSER:
Detected handshake capture: WPA2 4 — way handshake
Client: F4:A4:05:22:CC:51 | AP: 88:36:6C:1F:A2:90
 —  —  —
[2025 — 10 — 15 14:31:58] SURICATA ALERT: Suspicious
session retries
src_ip=10.0.0.12 dest_ip=10.0.0.1 severity=2
```