ВСТУП

Актуальність теми. Стрімкий розвиток телекомунікаційних технологій, зокрема мереж п'ятого покоління (5G), спричинив експоненційне зростання кількості пристроїв Інтернету речей (IoT). IoT-системи інтегруються в критично важливі сфери, такі як промисловість, енергетика, охорона здоров'я та «розумні міста», що робить їх ключовим компонентом сучасної цифрової інфраструктури. Однак ця екосистема характеризується високою гетерогенністю пристроїв, обмеженими обчислювальними ресурсами та тривалим життєвим циклом, що створює значні виклики для забезпечення кібербезпеки. Існуючі підходи до захисту, розроблені для традиційних IT-систем, часто є неефективними для специфіки IoT.

Наукова проблема полягає у відсутності комплексних методик, здатних в режимі реального часу виявляти нові та невідомі атаки на IoT-пристрої в масштабах телекомунікаційних мереж. Традиційні сигнатурні методи не можуть протидіяти атакам нульового дня, а агентські рішення неможливо розгорнути на мільярдах ресурс-обмежених пристроїв. Це зумовлює необхідність розробки нових підходів до моніторингу безпеки, заснованих на аналізі поведінки пристроїв безпосередньо на рівні мережевої інфраструктури, що є особливо актуальним завданням для телекомунікаційних операторів.

Мета і завдання дослідження. Метою магістерської роботи є підвищення рівня захищеності IoT-систем у телекомунікаційних мережах шляхом розробки методики виявлення загроз безпеки в режимі реального часу на основі поведінкового аналізу мережевого трафіку.

Для досягнення поставленої мети необхідно вирішити такі завдання:

1. провести аналіз архітектури IoT-систем у телекомунікаційних мережах, визначити ключові загрози та вразливості;
2. дослідити існуючі методи та стандарти захисту IoT, обґрунтувати їхні переваги та недоліки для застосування в масштабованих системах;

3. розробити модель загроз, що враховує специфіку взаємодії IoT-пристроїв у сучасній телекомунікаційній інфраструктурі;
4. розробити структурну схему та алгоритм функціонування методики виявлення аномальної активності IoT-пристроїв;
5. створити програмний стенд для експериментальної апробації розробленої методики;
6. провести експериментальні дослідження для підтвердження адекватності та ефективності запропонованої методики.

Об’єкт дослідження - процес забезпечення безпеки передачі даних в екосистемах Інтернету речей, розгорнутих у телекомунікаційних мережах.

Предмет дослідження - методи та алгоритми виявлення загроз та аномальної поведінки IoT-пристроїв на основі аналізу параметрів мережевого трафіку.

Методи дослідження. Для вирішення поставлених завдань у роботі використано комплекс загальнонаукових та спеціальних методів: методи системного аналізу та теорії інформаційної безпеки - для аналізу предметної області; методи аналізу мережевого трафіку та теорії телекомунікацій - для визначення ключових параметрів IoT-систем; методи математичного моделювання та теорії ймовірностей - для формалізації поведінкових моделей пристроїв; методи експериментального дослідження та статистичної обробки даних - для перевірки адекватності розробленої методики.

Наукова новизна одержаних результатів:

1. Вперше запропоновано методику виявлення загроз безпеки для IoT-систем у режимі реального часу, яка, на відміну від існуючих, базується на комплексному поведінковому аналізі мережевого трафіку на стороні оператора зв'язку, що дозволяє виявляти атаки без встановлення програмних агентів на кінцеві пристрої.
2. Удосконалено модель загроз для IoT-екосистем, що враховує специфіку мережевих протоколів (MQTT, CoAP) та патерни взаємодії пристроїв у гетерогенних телекомунікаційних мережах.

Практичне значення одержаних результатів. Розроблена методика може бути використана телекомунікаційними операторами, провайдерами хмарних IoT-платформ та службами безпеки підприємств для створення автоматизованих систем моніторингу та реагування на кіберінциденти. Програмний стенд є готовим інструментом для тестування та аналізу безпеки IoT-рішень, що дозволяє оптимізувати налаштування політик безпеки та підвищити загальну захищеність інфраструктури.

РОЗДІЛ 1 АНАЛІТИЧНИЙ ОГЛЯД ПРОБЛЕМАТИКИ БЕЗПЕКИ ІНТЕРНЕТУ РЕЧЕЙ В ТЕЛЕКОМУНІКАЦІЙНИХ МЕРЕЖАХ

1.1 Роль та архітектура IoT-систем у сучасних телекомунікаційних мережах

Інтернет речей (IoT) на сучасному етапі технологічного прогресу - це не просто мережа гаджетів, а масштабна глобальна екосистема, що складається зі складного конгломерату взаємозв'язаних обчислювальних пристроїв, механічних та цифрових машин, високоточних сенсорів, виконавчих контролерів та хмарних мережевих сервісів. Ці елементи наділені унікальними ідентифікаторами та здатністю автономно збирати, обробляти, аналізувати й обмінюватися величезними масивами даних мережею без необхідності безпосередньої участі людини або взаємодії в ланцюжку «людина-комп'ютер». У цьому контексті глибока та безшовна інтеграція технологій IoT з сучасною телекомунікаційною інфраструктурою є надважливою та безальтернативною, оскільки саме телеком-мережі виступають тим фундаментом, що забезпечує стабільне та безперебійне підключення мільярдів різнорідних пристроїв. Вони гарантують передачу критично важливих даних із наднизькою затримкою та високою надійністю, що є обов'язковою умовою для функціонування систем реального часу. Це, в свою чергу, відкриває безпрецедентно широкий спектр інноваційних «розумних» застосувань, які трансформують звичні сфери життя: від концепції розумних міст (Smart Cities) з інтелектуальним управлінням трафіком та енергоресурсами до повної промислової автоматизації (Industry 4.0) та передової телемедицини, що дозволяє рятувати життя дистанційно [1, 2, 3].

Масштаби цифровізації фізичного світу вражають своїми темпами та обсягами. Провідні галузеві аналітики та міжнародні консалтингові агентства прогнозують, що ми знаходимося лише на початку цього шляху, і динаміка зростання буде експоненціальною. Очікується, що вже у короткостроковій перспективі, до 2025 року, загальна кількість активних підключених IoT-пристроїв

у світі досягне вражаючої позначки приблизно 21,1 млрд одиниць. Однак довгострокові тренди є ще більш показовими: за оцінками експертів, до 2030 року цей показник майже подвоїться і перевищить 39 млрд девайсів, що у кілька разів перевищує чисельність населення планети і створює безпрецедентну щільність цифрових з'єднань. Такий вибуховий ріст кількості абонентських терміналів та обсягів трафіку однозначно визначає IoT як найпотужніший драйвер стратегічного розвитку телекомунікаційних мереж нових поколінь (зокрема 5G та майбутнього 6G) та виступає каталізатором зростання глобальної цифрової економіки, формуючи нові ринки та бізнес-моделі (Табл. 1.1) [4].

Таблиця 1.1

Прогноз глобальної кількості підключених IoT-пристроїв, млрд

Рік	Підключені IoT-пристрої (млрд)
2023	16,6
2024	18,5
2025	21,1
2030	39

Впровадження та масштабування технологій Інтернету речей (IoT) на сучасному етапі вже формує потужні фінансові потоки та стає одним із ключових драйверів зростання доходів для операторів мобільного та фіксованого зв'язку в усьому світі. Глобальна цифровізація економіки призвела до того, що лише у 2022 році сукупні доходи телекомунікаційних операторів безпосередньо від надання послуг підключення та обслуговування IoT-пристроїв перевищили позначку в $11 млрд. Цей вагомий фінансовий результат на 15% перевищує показники попереднього року, що свідчить про стійку позитивну динаміку ринку та зростання попиту на M2M-з'єднання навіть в умовах економічної нестабільності. Зазначений показник є чітким індикатором фундаментальних змін у структурі споживання

телеком-послуг, відображаючи вибухове зростання кількості промислових та комерційних застосунків IoT, які стрімко і повсюдно впроваджуються у складні виробничі цикли (концепція Індустрії 4.0), глобальну транспортну логістику, екосистеми розумних будинків та інфраструктурні рішення для розумних міст. Таке суттєве зростання прибутковості та перспективність сегменту IoT-послуг виступає потужним стимулом для телеком-операторів, спонукаючи їх інвестувати значні кошти в модернізацію, ущільнення та розширення власної мережевої інфраструктури. З метою задоволення зростаючого попиту та забезпечення покриття, провайдери активно розгортають енергоефективні мережі новітніх LPWAN-технологій, зокрема спеціалізовані стандарти NB-IoT та LTE-M, які ідеально підходять для датчиків з автономним живленням. Паралельно відбувається інтенсивна розбудова високошвидкісних 5G-мереж для критично важливих застосунків з низькою затримкою, а також суттєво підсилюється пропускна здатність та надійність наявних 4G/LTE інфраструктур, що залишаються базою для масових IoT-з'єднань [5, 6].

Однією з ключових архітектурних особливостей, що визначає ефективність, безпеку та масштабованість сучасних IoT-систем, є використання чітко структурованої багаторівневої моделі для організації взаємодії всіх функціональних компонентів мережі. На етапі зародження технології Інтернет речей першопочатково розглядали за спрощеною трирівневою моделлю, яка складалася лише з рівня сенсорів, мережевого рівня та рівня застосунків, проте надзвичайно швидкий ріст кількості підключених пристроїв і технологічне розмаїття екосистеми IoT вимагають значно складнішої та деталізованішої структури управління. Згідно з актуальними науковими дослідженнями та галузевими стандартами, на сьогодні доцільно використовувати розширену п'ятишарову архітектуру, що включає наступні основні рівні (Рис. 1.1). Базовим є Рівень сприйняття (Perception Layer), який виступає фундаментом системи; саме тут різноманітні сенсори, актуатори та інтелектуальні пристрої IoT збирають первинні дані з навколишнього середовища, фіксуючи такі фізичні параметри, як температура, вологість, рух, геолокація, стан об'єктів тощо. Це фізичні «речі» в

екосистемі IoT, до яких належать численні датчики, RFID-модулі, GPS-трекери, відеокамери та інші засоби збору інформації. Зібрана інформація передається на Транспортний (мережевий) рівень (Transport Layer), який відповідає за надійну передачу даних від сенсорів до компонентів, що займаються їхньою подальшою аналітикою, використовуючи широкий спектр засобів зв'язку - від технологій бездротового доступу (Bluetooth, Wi-Fi, LoRa, NB-IoT, LTE-M, 5G) до надійних дротових каналів (Ethernet, PLC). Транспортний рівень не лише забезпечує фізичне з'єднання, але й гарантує коректну маршрутизацію пакетів та глобальну адресацію пристроїв, зокрема через протокол IPv6; транспортний рівень охоплює як локальні сенсорні мережі, так і глобальні магістральні інтернет-канали операторів.

Наступним критично важливим етапом архітектури є Рівень обробки (Processing Layer), який часто називають рівнем підтримки сервісів (middleware). Він включає потужні обчислювальні ресурси, розподілені між Edge/Fog-компонентами (граничні обчислення), хмарними платформами та серверами для глибокого аналізу, фільтрації шумів та довгострокового зберігання величезних масивів зібраних даних. Тут застосовуються складні алгоритми обробки потоків у реальному часі та бази даних, які суттєво зменшують навантаження на магістральну мережу шляхом попередньої агрегації інформації та дозволяють системам оперативно реагувати на критичні події. Над ним розташовується Прикладний рівень (Application Layer), який безпосередньо взаємодіє з кінцевим споживачем; він містить програмні сервіси, API та інтерфейси для використання даних IoT у конкретних вертикалях. Це можуть бути комплексні системи моніторингу, платформи управління розумним будинком, системи промислової автоматизації, рішення для телездоров'я, управління логістикою тощо; саме на цьому рівні інтелектуальні технології трансформуються у корисну інформацію і функціональність для користувача. Замикає архітектуру Бізнес-рівень (Business Layer), який відповідає за стратегічне управління всією екосистемою та бізнес-логікою IoT. Цей рівень займається аналізом даних для оцінки прибутковості та ефективності, управління бізнес-процесами, він регулює правові аспекти взаємодії

з користувачами та встановлює відповідні моделі монетизації та стратегії подальшого розвитку IoT-послуг [7].



Рис. 1.1 П'ятирівнева архітектура системи Інтернету речей (IoT)

Також у фаховій літературі та технічній документації детально описано розширену семи рівневу еталонну модель, запропоновану компанією Cisco, яка дозволяє глибше структурувати процеси в складних індустріальних системах. Ця модель значно деталізує шляхи проходження інформації та включає такі рівні: фізичні пристрої та контролери («фізичні речі»), рівень комунікацій та з’єднань, рівень обробки даних на межі мережі (Edge Computing), рівень накопичення та зберігання даних, рівень абстрагування даних (форматування та агрегація), прикладний рівень (застосунки) та рівень бізнес-процесів і співпраці. Така глибока деталізація та різноманітність архітектурних підходів разом із широким спектром використаних протоколів передачі відображає надзвичайну складність інтеграції великої кількості гетерогенних IoT-пристроїв у єдині телекомунікаційні мережі. Оператори стикаються з викликом об’єднання різнорідного обладнання, що

працює на різних стандартах, в одну керовану екосистему. Зокрема, ця тенденція чітко простежується у статистиці підключень: згідно з аналітичними даними компанії IoT Analytics, технології ліцензійного спектра, такі як NB-IoT та LTE-M, вже охоплюють понад 57% світового ринку LPWAN-з'єднань станом на 2022 рік. При цьому частка NB-IoT становить 47%, а LTE-M - 10%, що є беззаперечним доказом провідної ролі мобільних операторів у впровадженні та масштабуванні масових IoT-рішень, витісняючи неліцензійні технології завдяки гарантованій якості обслуговування та безпеці [8].

Сучасна телекомунікаційна інфраструктура відіграє критичну, системоутворюючу роль як основної транспортної підсистеми для функціонування Інтернету речей. За даними численних дослідників та експертів галузі, мережі стандартів LTE та особливо 5G поступово стають стандартом де-факто для організації надійних IoT-підключень у глобальному масштабі. Це зумовлено тим, що архітектура сучасних стільникових мереж розроблена таким чином, щоб одночасно підтримувати дві діаметрально протилежні концепції: ідеї «масового» IoT (Massive IoT), що передбачає низькошвидкісний широкодіапазонний зв'язок для величезної кількості автономних малопотужних датчиків (реалізується через енергоефективні протоколи NB-IoT, LTE-M, а також інтеграцію з LoRaWAN), та «критичного» IoT (Critical IoT). Останній охоплює задачі з надзвичайно високими вимогами до надійності, відмовостійкості та мінімальної затримки передачі даних (реалізується через можливості 5G, віртуалізацію мережевих функцій SDN/NFV та мобільні граничні обчислення MEC). Масштаб можливостей вражає: наприклад, одна сучасна базова станція стільникового зв'язку технічно здатна обслуговувати десятки тисяч активних IoT-пристроїв одночасно без втрати якості з'єднання. Для забезпечення таких показників оператори активно впроваджують технологію Multi-access Edge Computing (MEC) та методично розширюють килимове покриття LTE/5G. Використання MEC дозволяє розміщувати сервіси первинної аналітики даних безпосередньо на «краю» мережі, ближче до абонента, що радикально скорочує затримку реакції систем IoT на події. Окрім того, впровадження технології eSIM (вбудованих SIM-карт) значно полегшує логістику та управління

життєвим циклом підключень IoT-пристроїв, оскільки дозволяє дистанційно завантажувати профілі, динамічно змінювати оператора зв'язку без фізичної заміни чіпа, що суттєво підвищує надійність і гнучкість мережевого з'єднання, особливо для пристроїв у важкодоступних місцях.

Стратегічна важливість технологій IoT для розвитку телекомунікаційного сектору та економіки в цілому також підкреслена в офіційних національних програмах багатьох держав. Зокрема, схвалена Кабінетом Міністрів в Україні «Стратегія розвитку сфери електронних комунікацій до 2030 року» чітко виділяє розбудову мереж п'ятого покоління (5G) та інфраструктури IoT як пріоритетні ключові напрями державної політики. На думку уряду та розробників стратегії, успішна імплементація цих технологій зможе забезпечити значний економічний ефект, потенційно додавши додаткові 56 млрд грн до ВВП країни за рахунок цифровізації промисловості, аграрного сектору та сфери послуг. Це свідчить про глибоку впевненість держави та представників великого бізнесу в тому, що масштабна діджиталізація через впровадження комплексних IoT-програм сприятиме не лише стрімкому економічному зростанню та інвестиційній привабливості, але й суттєвому підвищенню якості життя громадян через розвиток розумних міст, електронної медицини та безпекових сервісів [9].

Слід зазначити, що архітектура сучасних IoT-систем неминуче передбачає складну багатошарову структуру, що послідовно охоплює сенсорну підсистему збору даних, надійний транспортний (телекомунікаційний) шар, рівні обробки та зберігання даних, а також фінальні прикладні сервіси для користувача. У цій ієрархії телемережі виконують фундаментальну роль магістральної «транспортної мережі» або «нервової системи» для IoT, забезпечуючи безперервний, захищений та швидкісний потік інформації від мільярдів кінцевих пристроїв до центрів обробки даних та хмарних платформ. Активне розгортання передових мобільних технологій (від енергоефективних NB-IoT/LTE-M до високошвидкісних 5G) у поєднанні з еволюційним розвитком хмарних та гібридних мережних архітектур дозволяють глобальним IoT-системам успішно долати масштабні технічні виклики, пов'язані з пропускною спроможністю каналів та мінімізацією затримок. У

сукупності це не лише зміцнює роль технологій IoT як невід'ємної та органічної частини сучасних телекомунікаційних мереж, але й водночас створює міцну технологічну основу для появи принципово нових послуг, інноваційних бізнес-кейсів та трансформації традиційних операційних моделей операторів зв'язку [10].

1.2 Аналіз основних загроз та вразливостей безпеки в екосистемах Інтернету речей

У рамках аналізу безпеки Інтернету речей слід відзначити надзвичайний ріст кількості підключених пристроїв, що утворюють крихкий ландшафт для кіберзагроз: за підрахунками, 2025 року кількість IoT-пристроїв перевищить 35,2 млрд. Велика гетерогенність таких систем (від простих сенсорів до потужних контролерів) і мінімальні вбудовані механізми захисту посилюють ці ризики. Так, дослідження показують, що майже 98% IoT-трафіку передається без шифрування, а більшість пристроїв використовують заводські облікові дані або слабкі паролі. Відсутність оновлень ПЗ, віддалене керування без автентифікації та вразливі «розумні» протоколи (наприклад, TR-064 у домашніх роутерах) дозволяють зловмисникам отримувати несанкціонований доступ до пристроїв та мереж [11, 12].

Серед основних векторів атак на IoT-системи - автоматизоване сканування відкритих портів і відомих вразливостей, брутфорс облікових даних, впровадження шкідливого ПЗ і атаки відмови в обслуговуванні. Так, відомо, що ботнети на базі Mirai та його варіантів, оснащені скриптами для набору паролів та використання вразливостей, щодня здійснюють в середньому 820 тис. спроб зламу IoT-пристроїв (приріст 46% порівняно з попереднім роком). У першому кварталі 2025 року захисні рішення Kaspersky заблокували понад 629 млн кібератак, спрямованих на пошук вразливих IoT-ендпоїнтів. При цьому середня домашня мережа зазнає близько 10 активних атак щодня. За таких обсягів сканувань та атак автоматизація є ключовим інструментом зловмисників: Fortinet зафіксував зростання кількості активних сканувань на 16,7% у 2025 році. Ці масові «невдалі» спроби виявлення не свідчать про безпеку - навпаки, вони формують повний інтелектуальний портрет

атаки, що унеможливлює реактивний підхід і примушує впроваджувати проактивні заходи (сегментацію мережі, фільтрацію трафіку, оновлення звітності про вразливості) [13].

Загрози на рівні мережі включають різноманітні DoS/DDoS-атаки, деякі з яких спрямовані навіть на виснаження енергії пристроїв (E-DoS). Також зберігається тенденція до цільових операцій: зокрема, у 2024-2025 рр. були зафіксовані масивні ботнет-кампанії. Наприклад, у липні 2025 р. відкрито ботнет BadBox 2.0, який інфікував понад 10 млн «розумних» телевізорів та інших девайсів. Атакуючи понад 200 тис. IoT-пристроїв, ботнет Raptor Train (2023-2024 рр.) використовував комбінацію відомих та нульових вразливостей; його пік - 60 тис. активних нод на червень 2023 року. Ці приклади ілюструють: зловмисники охоче експлуатують невиправлені помилки, адже потужність мережі IoT дозволяє масштабувати DDoS і інші удари з величезним зусиллям [14, 15].

Серед шкідливого ПЗ для IoT провідне місце займають трояни для організації ботнетів і проведення DoS-атак. Публікації фахівців Kaspersky підтверджують, що для промислових IoT-пристроїв найпоширенішими помилками конфігурації є використання заводських паролів. Відомо також, що понад 50% IoT-пристроїв мають критичні вразливості, а в 1 з 3 інцидентів витоку даних брало участь саме IoT. Основними катастрофічними сценаріями стають віддалене перехоплення або зміна даних (наприклад, зміна показів «розумних» лічильників) та розгортання шифрувальників і вимагачів на периферійних пристроях. За даними дослідження IBM, 25% випадків компрометації IoT призводять до втрати персональних даних. Важливо, що понад 60% атак на IoT обумовлені застарілим ПЗ пристроїв, а приблизно кожен п'ятий девайс досі працює з заводським паролем. Внаслідок цього зростає попит на сервісні «послуги» - наприклад, на «скупку» ботнет-інфраструктури для DDoS (їх кількість на даркнет-ринку у першому півріччі 2023 р. оцінюється у ~700 оголошень). Натомість дослідники Check Point зафіксували, що в Європі організації отримують майже 70 IoT-атак на тиждень, а кожна успішна компрометація IoT-трафіку обходиться в середньому у $330 тис. [16, 17, 18 ,19].

Аналіз вразливостей IoT-пристроїв підтверджує концентрованість уваги атак

на кількох ключових класах помилок. За даними Bitdefender/Netgear, у 2023 р. серед усіх знайдених вразливостей IoT-пристроїв 34% припало на «розумні» телевізори, 18% - на розетки, 13% - на відеореєстратори і 12% - на маршрутизатори (Рис. 1.2).

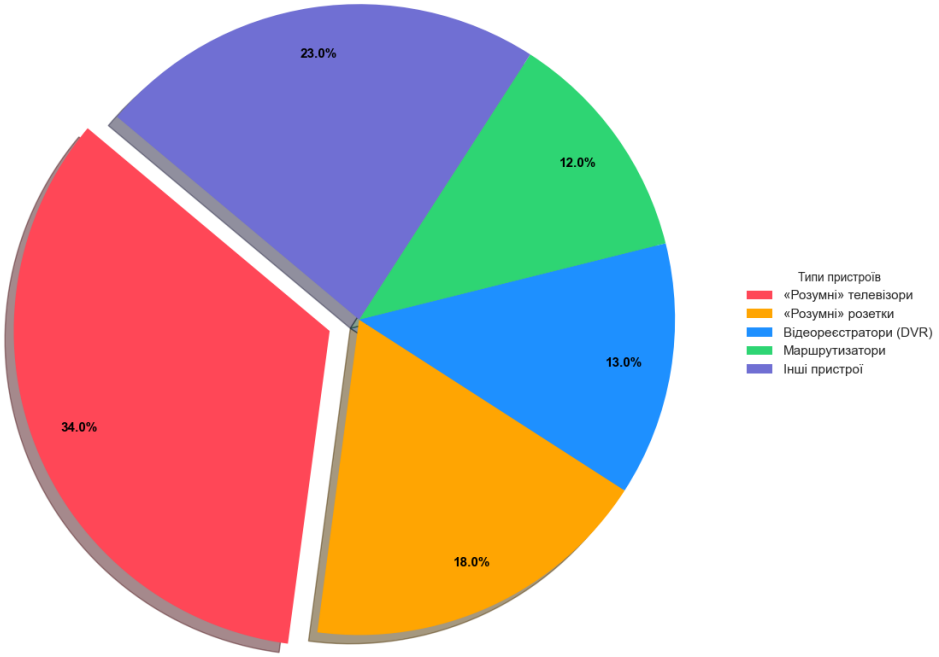


Рис. 1.2 Розподіл знайдених вразливостей за типами IoT-пристроїв у 2023 році

При цьому найчастішими типами вразливостей були переповнення буферу (28,25%) та атаки відмови в обслуговуванні (27,20%) (Табл. 1.2). Це зумовлено слабким контролем розподілу пам'яті та обмеженим об'ємом обробки на багатьох пристроях. Іншими поширеними векторами є помилки в реалізації протоколів зв'язку, неконтрольований доступ до прошивки та недоліки в шифруванні.

Таблиця 1.2

Найпоширеніші типи вразливостей у IoT-пристроях (2023 рік)

Тип вразливості	Частка (%)
Буферне переповнення	28,25
Відмова в обслуговуванні (DoS-атака)	27,2

Сумарна кількість виявлених уразливостей у сучасних розширених екосистемах Інтернету речей (XIoT), які об'єднують як класичні споживчі IoT-пристрої, так і операційні технології (OT) промислового сектору, демонструє невпинну та стабільно зростаючу тенденцію. З розширенням поверхні атаки через цифрову трансформацію підприємств, безпека конвергентних мереж стає критичним викликом. Згідно з аналітичними звітами провідних дослідницьких команд, зокрема Team82 компанії Claroty, динаміка виявлення загроз є надзвичайно високою: лише у першій половині 2022 року кількість зареєстрованих інцидентів та слабких місць у прошивках і протоколах зросла майже вдвічі порівняно з аналогічним попереднім періодом. Такий різкий стрибок свідчить про те, що зловмисники дедалі активніше фокусуються на вразливостях кіберфізичних систем, а дослідники безпеки інтенсивніше сканують цей сегмент, виявляючи тисячі нових дір у захисті.

Особливе занепокоєння фахівців викликає тяжкість виявлених проблем. Значна частина задокументованих дефектів безпеки класифікується як критичні вразливості з високими балами CVSS, що несуть безпосередню загрозу цілісності систем. Найчастіше це помилки, що дозволяють зловмисникам здійснювати віддалене виконання довільного коду (Remote Code Execution, RCE), отримуючи повний контроль над пристроєм без фізичного доступу, або проводити атаки типу «відмова в обслуговуванні» (DoS), що може призвести до раптової зупинки виробничих ліній, відключення датчиків чи блокування систем розумного міста. Масштаб цієї проблеми підтверджується глобальною статистикою: у загальнодоступній базі даних NVD (National Vulnerability Database) до початку 2023 року було офіційно зареєстровано рекордну кількість - понад 28,800 нових записів про уразливості (CVE). У середньому це становить близько 80 нових загроз щодоку, що створює колосальне інформаційне навантаження на відділи кібербезпеки.

Такий вал повідомлень про нові загрози яскраво підкреслює фактичну безпорадність та неефективність традиційного лінійного підходу «знайди-заплати» (patch management), коли адміністратори намагаються встановити оновлення для

кожного виявленого бага. В умовах гетерогенних мереж XIoT це часто технічно неможливо або економічно недоцільно. Тому нагально необхідні впровадження програм інтелектуальної пріоритизації, що враховують не лише наявність CVE, а й реальні ризики від їхньої потенційної експлуатації та контекст роботи пристроїв (їх критичність для бізнесу та доступність з інтернету). На тлі хронічного дефіциту патчів для величезного парку застарілого (legacy) IoT обладнання, підтримка якого виробниками вже припинена, та стрімкого експоненційного зростання кількості нових підключень, кожна не виправлена вразливість IoT-системи перетворюється на критичну загрозу. Вона стає потенційною дорогою ланкою ланцюга атаки (kill chain), яку хакери можуть використати для проникнення в корпоративну мережу та горизонтального переміщення, завдаючи значних збитків [20].

1.3 Класифікація та огляд існуючих методів і стандартів захисту IoT-пристроїв та даних

Значне розповсюдження IoT-пристроїв призводить до зростання кіберзагроз. За оцінками, кількість підключених пристроїв перевищить близько 39 млрд до 2030 р. При цьому стандарти безпеки для IoT часто різняться в різних регіонах і галузях, що ускладнює уніфікацію вимог. Відомо, що «стандарти кібербезпеки IoT продовжують бути різнорідними, породжуючи фрагментовану картину глобально» [21, 27].

Одним із ключових напрямів захисту IoT є криптографія. Сучасні пристрої використовують симетричне шифрування (наприклад, AES) для забезпечення конфіденційності даних. Останніми роками активно розвиваються легковагові криптоалгоритми для пристроїв з обмеженими ресурсами. Так, NIST у 2025 р. погодив новий стандарт легковагової криптографії (NIST SP 800-232) на базі чотирьох алгоритмів сімейства Ascon, розроблених спеціально для IoT. Ці алгоритми потребують значно менших обчислювальних потужностей та часу порівняно з традиційними методами. Наприклад, для мереж NB-IoT у специфікаціях 3GPP передбачено 256-бітне шифрування, що перевершує 128-

бітний AES у LoRaWAN. Порівняльні характеристики основних алгоритмів наведено в Табл. 1.3 [22, 26, 29] (Рис. 1.3).

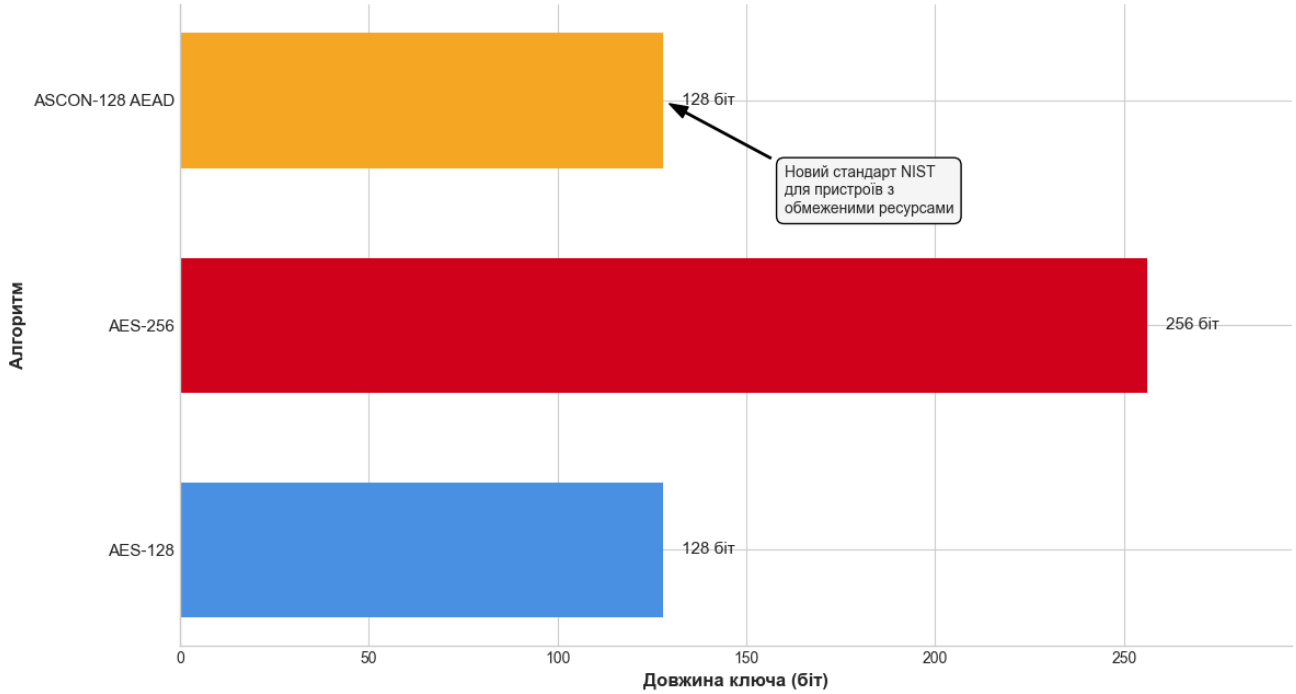


Рис. 1.3 Порівняльні характеристики криптографічних алгоритмів для IoT

Не менш важливими, а часто і критично визначальними для забезпечення цілісності та надійності глобальної екосистеми Інтернету речей, є впровадження сучасних методів суворої автентифікації та комплексного управління ідентичністю (Identity and Access Management, IAM) для всіх підключених пристроїв. Враховуючи специфіку та архітектурні обмеження IoT-обладнання, яке в більшості випадків характеризується вкрай обмеженими обчислювальними ресурсами процесора, жорсткими вимогами до низького енергоспоживання та часто повною відсутністю звичних для користувача інтерфейсів вводу (клавіатур чи екранів), традиційні схеми захисту типу «логін-пароль» вже давно не забезпечують належного рівня безпеки. Статичні паролі є надзвичайно вразливими до автоматизованих брутфорс-атак, словникового підбору та, що є найпоширенішою проблемою, використання заводських налаштувань за замовчуванням (наприклад, admin/admin), які користувачі рідко змінюють. Натомість для побудови надійної

системи ідентифікації інженери все частіше застосовують розгорнуту інфраструктуру відкритих ключів (PKI) з використанням унікальних цифрових сертифікатів стандарту X.509, що дозволяє реалізувати взаємну автентифікацію (mTLS) між пристроєм і сервером без передачі секретів мережею. Також широко використовуються динамічні токени доступу (наприклад, на базі протоколу OAuth 2.0) та спеціалізовані апаратні засоби безпечного зберігання криптографічних ключів, які фізично неможливо вилучити або скопіювати програмним шляхом. Серед новітніх та перспективних підходів окремо виділяють використання децентралізованих блокчейн-технологій, що дозволяють створити розподілений, незмінний реєстр довірених пристроїв без єдиної точки відмови, біометричної автентифікації (актуально для ношених пристроїв та систем розумного будинку) та адаптивних алгоритмів машинного навчання, які в реальному часі аналізують поведінкові патерни (наприклад, типовий час активності чи геолокацію) для безперервної верифікації користувача чи пристрою, блокуючи доступ при виявленні аномалій [23].

На рівні мережевого захисту, з метою локалізації інцидентів та запобігання неконтрольованому поширенню загроз всередині корпоративного периметра, широко застосовують стратегію глибокого ешелонування, що включає логічну сегментацію мережі (фізичне та віртуальне розділення IT-мереж офісу та OT-контурів виробництва), сувору фільтрацію трафіку за допомогою міжмережевих екранів нового покоління (NGFW) з функцією глибокої інспекції пакетів, та організацію криптографічно захищених тунелів через VPN для передачі даних через публічні мережі. Величезне, а часом вирішальне значення в цьому контексті мають автоматизовані системи виявлення вторгнень (IDS) та системи запобігання вторгненням (IPS), що базуються на глибокому аналізі поведінки мережевого трафіку та метаданих. Зокрема, сучасні евристичні методи та засоби виявлення аномалій, побудовані на основі складних алгоритмів машинного навчання та штучного інтелекту, дозволяють розпізнавати нетипові шаблони активності й виявляти складні цілеспрямовані атаки «нульового дня» (Zero-day exploits) з високою точністю, яку принципово не можуть забезпечити традиційні сигнатурні

методи, що покладаються на бази відомих загроз. Такі інтелектуальні моделі демонструють високі показники виявлення прихованих загроз, навчаючись на масивах вже відомих історичних даних та формуючи профіль нормальної поведінки мережі, проте їх практичне впровадження пов'язане з певними технічними викликами: вони потребують значних обчислювальних ресурсів для обробки високошвидкісних потоків даних у реальному часі та часто стикаються з проблемами масштабованості при різкому, експоненціальному зростанні кількості вузлів у мережі Інтернету речей [25].

Фундаментальним, кінцевим рівнем захисту всієї архітектури є використання спеціалізованих апаратних засобів безпеки, інтегрованих безпосередньо на самих пристроях на етапі виробництва. Застосування довірених апаратних модулів, наприклад TPM (Trusted Platform Module) або Secure Element (SE), забезпечує створення так званої надійної основи довіри (Hardware Root of Trust), яку практично неможливо підробити або клонувати програмними методами атаки. Окрема мікросхема TPM виконує критично важливі криптографічні операції в ізольованому середовищі, генерує істинні випадкові числа (TRNG) для ключів шифрування, надійно зберігає незмінні закриті ключі та підтримує механізм безпечного завантаження (Secure Boot). Цей механізм послідовно перевіряє цифровий підпис кожного компонента завантажувача, ядра та операційної системи перед їх запуску, миттєво блокуючи роботу пристрою у разі виявлення найменшої підміни коду або наявності руткітів. Модулі TPM також надають унікальну можливість проведення віддаленої атестації (Remote Attestation) поточного стану пристрою, що гарантує центральному серверу управління цілісність прошивки та ПЗ при кожному завантаженні, ефективно запобігаючи підключенню компрометованих або «зомбованих» девайсів до хмарної інфраструктури [30].

У сфері державного та міжнародного регулювання, а також стандартизації вимог до кібербезпеки також відбуваються значні тектонічні зміни, спрямовані на підвищення відповідальності виробників. Серед ключових стандартів і нормативних документів можна особливо відзначити європейський стандарт ETSI EN 303 645 (актуалізований та доповнений у 2024 році), який став першим

всеосяжним глобальним стандартом, що детально описує 13 базових положень кібербезпеки для споживчих IoT-пристроїв. Цей документ охоплює широкий спектр технічних та організаційних вимог: від категоричної заборони на використання універсальних паролів за замовчуванням (що було основною причиною появи ботнетів типу Mirai) до обов'язкового впровадження політик управління оновленнями прошивки і наявності чітких механізмів своєчасної реакції на виявлені вразливості (Vulnerability Disclosure Policy). Оновлене видання EN 303 645 також робить особливий наголос на захисті конфіденційності персональних даних користувачів та забезпеченні повної відповідності вимогам суворого регламенту GDPR. Подібні фундаментальні положення та принципи «безпеки за дизайном» (Security by Design) містяться і в інших впливових міжнародних стандартах, наприклад, у серії публікацій NIST IR 8259 (розроблених Національним інститутом стандартів і технологій США) та сімействі стандартів ISO/IEC 27000, які задають рамкові вимоги до побудови систем менеджменту інформаційної безпеки та забезпечення захищеності IoT-пристроїв на всіх етапах їх життєвого циклу - від проектування та розробки до експлуатації та утилізації [24, 28].

Таблиця 1.3. Криптографічні алгоритми для IoT (ключова довжина та приклад застосування)

Алгоритм	Довжина ключа (біт)	Сфера застосування
AES-128	128	Стандартне шифрування в бездротових мережах
AES-256	256	Захист каналів NB-IoT/5G (3GPP)
ASCON-128 AEAD	128	Легковагове шифрування (NIST SP 800-232)

РОЗДІЛ 2 ТЕОРЕТИЧНІ ОСНОВИ ФОРМУВАННЯ МЕТОДИКИ МОНІТОРИНГУ БЕЗПЕКИ IOT

2.1 Розробка моделі загроз для IoT-систем з урахуванням специфіки телекомунікаційної інфраструктури

Стрімкий та повсюдний розвиток глобальної екосистеми Інтернету речей (IoT) разом із безпрецедентним масштабуванням цифрових інфраструктур створюють якісно нові виклики для систем інформаційної безпеки. Швидке зростання кількості інтелектуальних пристроїв формує так звану «розширену поверхню атаки», яка охоплює мільярди потенційних точок входу для зловмисників, роблячи захист периметра надзвичайно складним завданням [21, 26]. Динаміка насичення ринку електронікою вражає: згідно з актуальними аналітичними прогнозами провідних консалтингових агентств, загальна кількість підключених IoT-пристроїв у світі вже у найближчій перспективі, а саме у 2025 році, сягне позначки в 21,1 млрд одиниць [22, 25]. Цей тренд має стійкий довгостроковий характер, і очікується, що до 2030 року глобальна мережа «речей» перевищить показник у 29 млрд активних девайсів, що у кілька разів перевищує чисельність населення планети [14].

Ситуація ускладнюється тим, що сучасна архітектура IoT спирається на використання надзвичайно широкого спектра різноманітних комунікаційних протоколів та мережевих каналів. Одночасна робота пристроїв через публічний інтернет, локальні бездротові інтерфейси (Wi-Fi, Bluetooth, Zigbee, Z-Wave), а також через глобальні мобільні мережі (від 2G до 5G) створює гетерогенне середовище, яке лише посилює складність побудови уніфікованих систем захисту [13]. При цьому переважна більшість наявних IoT-пристроїв - від найпростіших «розумних» датчиків температури та побутових гаджетів до складних систем відеоспостереження - перебувають у стані постійного активного обміну даними. Критичною проблемою залишається низька культура кібергігієни на етапі виробництва: такі пристрої часто експлуатуються без механізмів автоматичних

оновлень безпеки, мають відкриті порти та постачаються з типовими, загальновідомими паролями за замовчуванням (наприклад, admin/admin), які користувачі рідко змінюють [14].

Як однозначно вказується у численних фахових дослідженнях з кібербезпеки, глобальна система Інтернету речей наразі перетворилася на “величезну ціль" та привабливий вектор атак для зловмисників. Хакери розглядають IoT-пристрої як «легку здобич» для створення ботнетів, майнінгу криптовалют або як плацдарм для проникнення в корпоративні мережі. Статистика інцидентів підтверджує ці побоювання: щороку центрами моніторингу фіксуються тисячі цілеспрямованих атак на різні категорії IoT-пристроїв, від домашніх роутерів до медичного обладнання [9]. Обсяги та інтенсивність шкідливої активності справді вражають своїми масштабами: лише протягом 2022 року кількість виявлених унікальних зразків спеціалізованої IoT-малварі (шкідливого програмного забезпечення, розробленого під архітектури ARM, MIPS тощо) майже подвоїлася порівняно з попередніми періодами, що свідчить про індустріалізацію кіберзлочинності в цьому сегменті [17].

Таблиця 2.1

Основні показники масштабів і атак IoT-систем

Рік	Підключені IoT-пристрої, млрд [33, 32, 39]	Середньодобова кількість атак, тис.
2024	18,5	500
2025	21,1	820

Наприклад, у 2024 р. прогнозується 18,5 млрд пристроїв IoT, а до кінця 2025 р. їхня кількість може досягти ~21,1 млрд [22, 25]. Зростання числа пристроїв супроводжується різким підвищенням обсягу зловмисних активностей: щоденна

кількість атак на IoT вже оцінюється у сотні тисяч (близько 820 тис. спроб на добу у 2025 р.) [9]. Ці дані ілюструють стрімке зростання ризиків (Табл. 2.1) (Рис. 2.1).

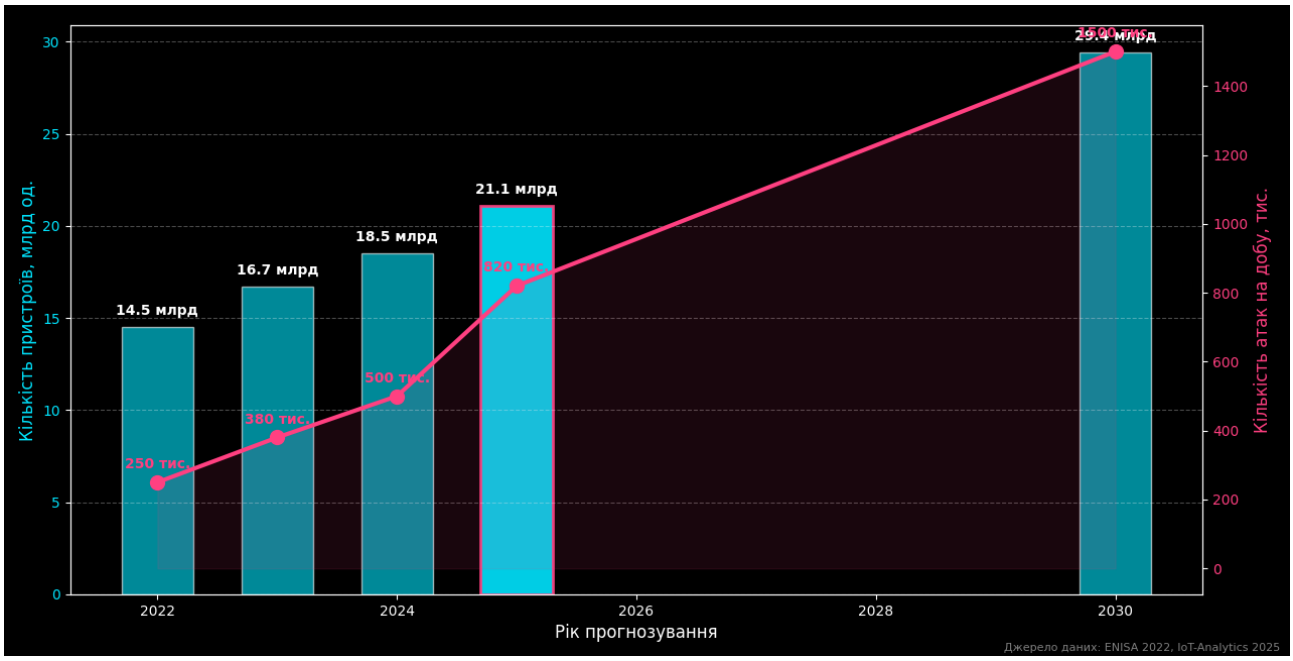


Рис. 2.1 Динаміка зростання кількості IoT-пристроїв та інтенсивності кібератак (2024-2030 рр.)

Найпоширенішим вектором загроз є організація масових DDoS-атак за допомогою IoT-багнетів [16]. Мережі заражених пристроїв (ботнети Mirai та його мутацій) генерують величезні обсяги трафіку [17]. Так, у США нещодавно знешкодили мережу з 100 тисяч SIM-карт, що могла відправляти до 30 млн SMS за хвилину і викликати масштабні збої в роботі сотень базових станцій [4] (Рис. 2.2).

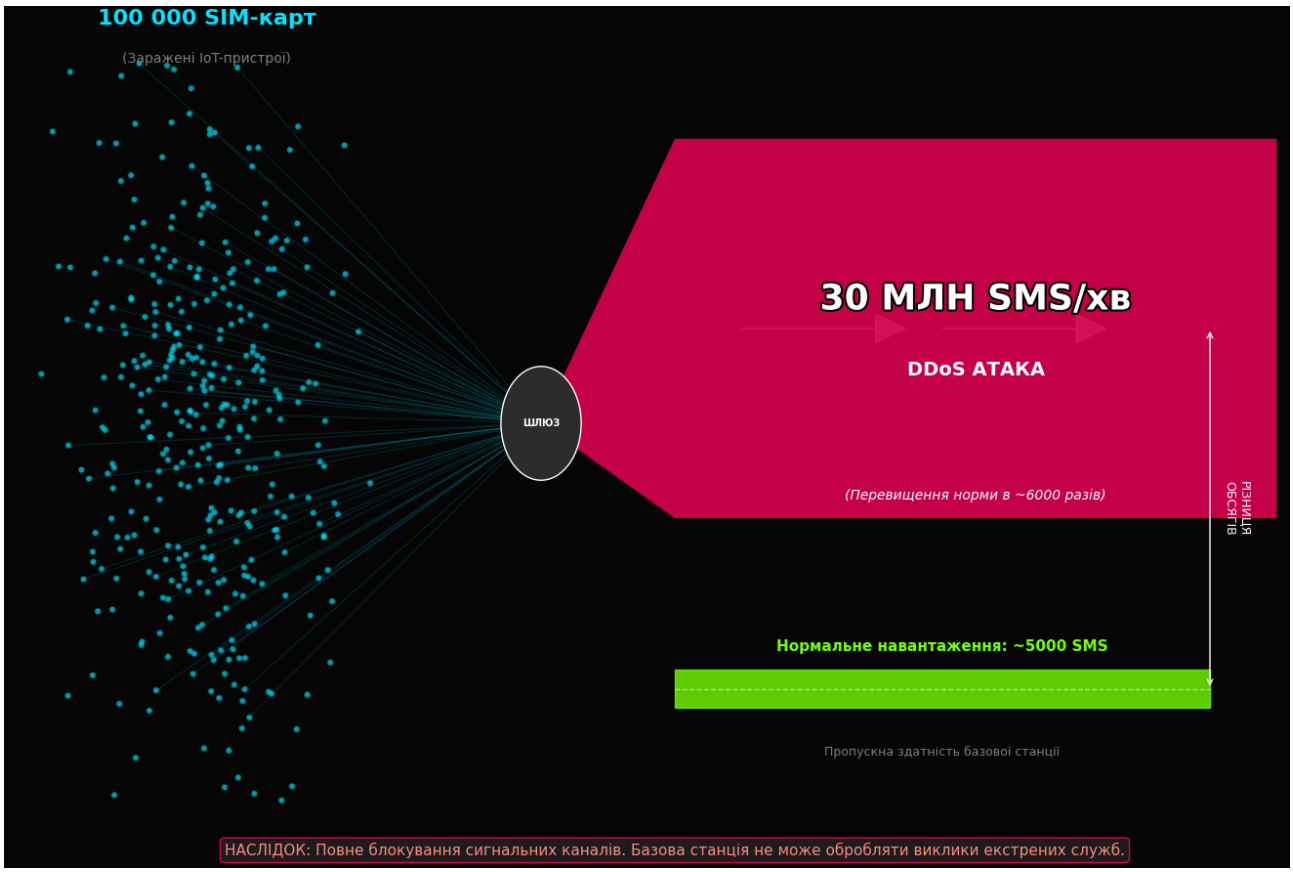


Рис. 2.2 Схема формування критичного навантаження на мережу від IoT-ботнету

Одночасно з цим спостерігається трансформація цілей зловмисників: вони все частіше використовують скомпрометовані IoT-пристрої не як кінцеву мету атаки, а як інструмент для реалізації більш масштабних злочинних схем. Зокрема, хакери масово об'єднують захоплені гаджети у ботнети для організації анонімних проксі-розсилок (спаму, фішингу), створення мереж «житлових проксі» (residential proxies) для приховування джерела шкідливого трафіку, а також для нелегального майнінгу криптовалюти, використовуючи сукупну обчислювальну потужність тисяч процесорів [14]. Особливу небезпеку становить той факт, що критичне телекомунікаційне обладнання кінцевих користувачів - домашні та офісні роутери, мережеві шлюзи, медіаконвертери - стає пріоритетною мішенню. На такі вузли часто здійснюються атаки з метою закріплення на периметрі та подальшого непомітного проникнення в локальні мережі (lateral movement). Це особливо небезпечно, оскільки компрометація граничного шлюзу фактично нівелює захист

внутрішнього контуру і може дати зловмисникам повний доступ до трафіку та конфіденційних даних усіх підключених до мережі смартфонів, комп'ютерів та інших розумних пристроїв [29].

Окремим вектором, що стрімко набирає обертів, є поширення спеціалізованого програмного забезпечення типу ransomware (програми-вимагачі), яке тепер орієнтоване не лише на ПК, а й на автономні пристрої зберігання даних. Зловмисники цілеспрямовано атакують мережеві сховища (NAS), де користувачі та бізнес зазвичай тримають резервні копії, фотоархіви та важливі документи. Яскравим прикладом такої деструктивної діяльності стала епідемія шифрувальника DeadBolt, який у 2022 році вразив тисячі NAS-серверів виробника QNAP по всьому світу. Хакери використали критичну вразливість нульового дня (зафіксовану пізніше як CVE-2022-27593) у системній бібліотеці, що дозволило їм зашифрувати файли користувачів і вимагати викуп у біткоїнах за ключ розшифрування, завдавши значних фінансових та репутаційних збитків [15].

При розробці комплексної стратегії кібербезпеки та формуванні моделі загроз необхідно враховувати специфічні архітектурні особливості сучасної телекомунікаційної інфраструктури. Компоненти операторського рівня, такі як базові станції стільникового зв'язку, вузли ядра мережі (Core Network), а також сервери управління SIM-картами (OTA-платформи) та спеціалізовані шлюзи NB-IoT, є критичними активами, захист яких вимагає особливої уваги. Наявність вразливостей у цих елементах може призвести до катастрофічних наслідків, включаючи масові відмови в обслуговуванні цілих регіонів або перехоплення конфіденційних даних на магістральному рівні [11, 14]. Надзвичайно високі ризики існують у чутливих галузях, зокрема в сфері охорони здоров'я (Internet of Medical Things, IoMT). Тут кібератака, що спричиняє відключення зв'язку або перевантаження телеком-каналів автоматизованих медичних приладів (наприклад, інсулінових помп, кардіостимуляторів або інфузійних насосів), виходить за межі цифрового світу і може безпосередньо паралізувати роботу реанімаційних систем, загрожуючи фізичній безпеці та життю пацієнтів [14].

Враховуючи вищезазначене, стає очевидним, що сучасна модель загроз для

IoT-систем повинна бути багатовимірною та деталізованою. Вона має чітко класифікувати атаки за векторами реалізації (мережеві вторгнення, атаки на прикладному рівні, фізичний взлом пристроїв), фіксувати перелік можливих деструктивних дій (від DDoS-атак та витоку конфіденційної інформації до повного виведення обладнання з ладу або підміни даних датчиків) і враховувати різні типи потенційних супротивників. Спектр загроз варіюється від окремих кіберзлочинців-аматорів до організованих хакерських угруповань та державних акторів, які володіють значними ресурсами для проведення складних APT-атак [33, 34]. Саме такі глибокі аналітичні основи дозволяють фахівцям визначити ключові параметри нормального мережевого трафіку та виявити аномальні поведінкові патерни, що є необхідною умовою для розробки та впровадження ефективних систем раннього виявлення загроз і побудови надійних ешелонованих заходів протидії [31, 32].

2.2 Обґрунтування вибору комплексу параметрів мережевого трафіку для ідентифікації аномальної поведінки пристроїв

У сучасних масштабованих IoT-мережах загальний обсяг, інтенсивність та структурна різноманітність даних, що передаються, досягли безпрецедентного рівня і продовжують зростати в геометричній прогресії. Це явище зумовлене як збільшенням кількості самих пристроїв, так і ускладненням їхніх функцій (передача відео, телеметрії, голосу). Така ситуація робить задачу автоматизованого виявлення аномалій та вторгнень надзвичайно складною технічною проблемою, оскільки до систем захисту висуваються надзвичайно високі та часто суперечливі вимоги: вони повинні забезпечувати максимальну точність класифікації загроз для мінімізації хибних спрацьовувань і водночас гарантувати високу швидкість обробки потоків у реальному часі [24]. Кожен окремий IoT-пристрій, залежно від свого призначення (будь то розумна лампочка чи промисловий контролер), генерує унікальну низку мережевих з'єднань, що формують його специфічний «цифровий відбиток» із характерними параметрами. До таких параметрів належать IP-адреси

джерела та призначення, використовувані порти, статистичний розподіл розмірів пакетів, інтервали їх надходження тощо. Тому ключовим етапом для формування ефективної методики моніторингу безпеки є етап відбору ознак (feature selection): необхідно обрати такий набір параметрів трафіку, які найбільш інформативно та однозначно відрізняють нормальну, легітимну поведінку пристрою від аномальної активності.

У практиці мережевого аналізу базовими, або так званими «ключовими», параметрами традиційно вважаються метрики, що описують фізичні характеристики потоку. До них належать сумарна кількість пакетів і загальний обсяг переданих байтів у рамках одного потоку (що вказує на інтенсивність комунікації), тривалість сеансу зв'язку (що дозволяє виявити довготривалі з'єднання), а також номери портів транспортного рівня та специфічні протоколи зв'язку, які визначають тип сервісу [19]. Для більш деталізованого аналізу та побудови програмних моделей захисту ці параметри формалізуються у спеціальні структури даних. Зокрема, у типовій проєктній структурі класу NetworkTrafficData дослідниками виділено розширений набір параметрів трафіку, який включає: точну кількість пакетів, напрямки передачі даних (співвідношення вхідного та вихідного трафіку), статистику розмірів пакета (мінімальний, середній, максимальний), конкретні номери задіяних портів, використані протоколи різних рівнів моделі OSI. Окрім того, важливу роль відіграють такі складні характеристики, як ентропія розподілу значень (міра хаотичності даних) та точні часові мітки подій, що дозволяють проводити часовий аналіз рядів [12].

Сукупність цих полів дозволяє сформувати багатовимірну картину, що відображає різні фундаментальні аспекти мережевого трафіку: загальний обсяг навантаження і частоту обміну даними, спрямованість взаємодії пристроїв (хто є ініціатором з'єднання) та варіативність інформації, що передається. Саме аналіз відхилень у цих метриках є основою детегування загроз. У разі виникнення аномальної активності, спричиненої кіберінцидентами, наприклад, під час масованих DDoS-атак або спроб сканування мережі для пошуку відкритих портів, спостерігаються характерні та різкі зміни всіх вищезгаданих показників. Системи

моніторингу фіксують аномальне зростання числа пакетів за короткий проміжок часу, їх нетипову послідовну зміну, раптову появу нових, раніше не використовуваних портів чи екзотичних протоколів. Також часто фіксується суттєве збільшення ентропії трафіку, що може свідчити про наявність шифрованого шкідливого навантаження або рандомізацію даних [22, 30] (Рис. 2.3).

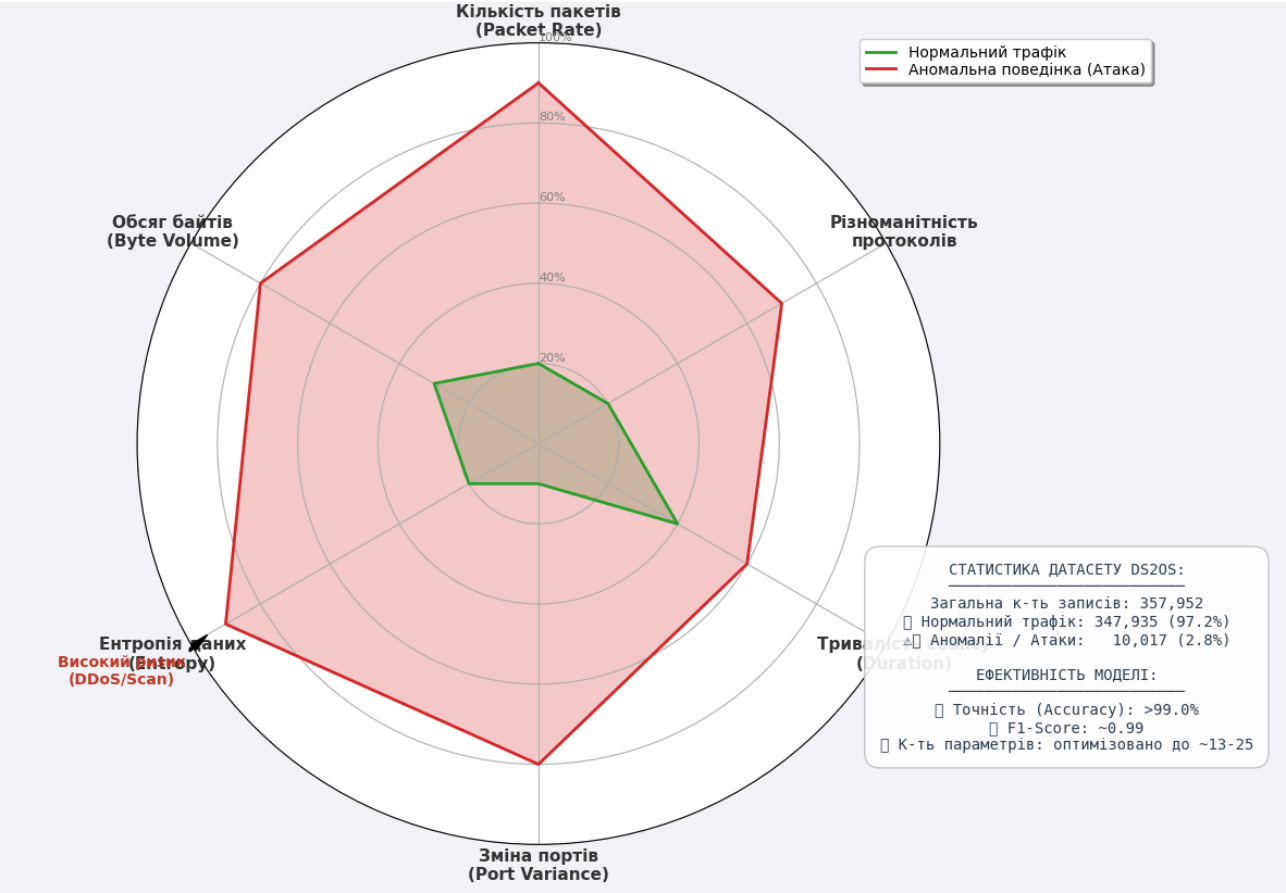


Рис. 2.3 Порівняльний профіль параметрів трафіку (Норма vs Аномалія) та статистика розподілу класів у DS2OS

У численних дослідженнях пропонували різноманітні множини параметрів мережевого трафіку для IoT-аналітики. Наприклад, Ayad et al. використовують набір з 46 ознак, що включає загальні статистики потоків: pkts (загальна кількість пакетів у транзакції), bytes (загальний обсяг байтів), state (стан потоку), dur (тривалість зв'язку), а також

розподілені за адресами або портами характеристики – число пакетів і байтів від певного IP-адресата, середня швидкість передачі тощо [13]. Такий широкий комплекс ознак дозволяє на основі потоків TCP/UDP-двоповідти моделювати типовий «підпис» поведінки пристрою. З іншого боку, Seyedi та співавт. показали, що достатньо обрати набір із приблизно 25 параметрів, включаючи кількісно-якісні характеристики пакетів та сесій, для детекції аномалій у режимі потокового (стрімінгового) аналізу [3]. Згідно з їхніми результатами, такий набір параметрів (пакетних, хостових і потокових) дозволяє побудувати адаптивні моделі, що забезпечують F1-міру на рівні 0,99 при реальному часу обробки трафіку [9].

Метрики частоти подій й ентропії трафіку також виявляються надзвичайно інформативними. Наприклад, в одному підході статистичний показник ентропії заголовків мережевих пакетів (modified z-score) корелює з активністю конкретних IoT-пристроїв. Використання таких метрик допомогло отримати ~94% точності ідентифікації пристроїв за їх трафіком. Наявність різких стрибків у значенні ентропії чи частоті пакетів може сигналізувати про DDoS-атаку чи виконання сканування. Комплекс параметрів «кількість/обсяг пакетів за одиницю часу, портові та протокольні характеристики, ентропія поля даних та часові інтервали» дає можливість виділяти аномальні стани з високою точністю [42, 50].

Для оптимального відбору параметрів застосовують

методи селекції. Так, Seyedi et al. використали генетичний алгоритм для пошуку найбільш релевантних ознак, зменшивши розмір вхідного вектору і зберігши ефективність виявлення загроз [3]. Після такого відбору модель виявляє аномалії з точністю ≈98% і швидкістю розпізнавання ≈95%, зводячи до мінімуму частоту хибних спрацьовувань [12]. Це свідчить, що навіть серед широкого пулу потенційних параметрів існує оптимальний піднабір, що дозволяє знижувати обчислювальні витрати без втрати якості. У реальних експериментах доведено, що, наприклад, комбінування числових (кількість пакетів, байтів, швидкість) та категоріальних (статус, протокол) ознак надає майже таку ж потужність виявлення, як і комплекс з десятків ознак [6, 7].

Практична значущість вибору параметрів ілюструють статистики реальних IoT-баз даних. Зокрема, у тестовій DS2OS dataset зібрано 357 952 записів мережевих подій, серед яких 347 935 відповідають нормальному трафіку, а 10 017 містять атаки [12]. Цей датасет включає 13 параметрів (вимірів) трафіку, об'єднаних у вісім класів (звичайний трафік та сім типів атак) [12]. Описана структура показує співвідношення масштабів нормального та аномального трафіку та вказує, що навіть незначна частка аномалій (<3%) суттєво відрізняється за вибраними параметрами. Наприклад, як видно з таблиці, розподіл точок говорить про високу дисбалансованість даних: аномальних записів значно

менше, але вони мають специфічні патерни змін параметрів (Табл. 2.2) [12].

Таблиця 2.2

Статистика DS2OS датасету

Показник	Кількість	Норма	Аномалія
Записів у датасеті	357952	347935	10017

Наведені аналітичні дані та результати експериментів переконливо демонструють, що для побудови систем ефективної детекції аномалій в умовах сучасного Інтернету речей фахівцям доводиться працювати із надзвичайно великою кількістю спостережень та вирішувати складні задачі з обробки "великих даних". Ключовим викликом при цьому стає необхідність максимально точно та обґрунтовано відбирати саме ті специфічні параметри трафіку, які мають найвищу роздільну здатність і найкраще розділяють нормальну, легітимну активність мережі та ознаки кібератаки. У широкому спектрі наукових публікацій та галузевих звітів підтверджено, що саме детально описані вище параметри - такі як кількість пакетів та байтів, часові мітки та інтервали між пакетами, номери задіяних портів, пропускні характеристики каналу та ентропія розподілу даних - показали найвищу практичну ефективність та інформативність. Варто зазначити, що у порівнянні з класичними статистичними методами або сигнатурним аналізом, які часто виявляються безсилими проти нових типів загроз, сучасні інтелектуальні моделі, побудовані на основі алгоритмів машинного навчання із використанням вказаного набору параметрів, демонструють значно кращу чутливість та точність класифікації.

Яскравим прикладом успішного застосування такого підходу є запропонована дослідниками гібридна система виявлення вторгнень, яка поєднує використання генетичних алгоритмів (ГА) для оптимізації відбору ознак та

ансамблів дерев рішень для безпосередньої класифікації. Таке поєднання дозволило не лише досягти вражаючих показників загальної точності розпізнавання на рівні 98%, але й, що не менш важливо, забезпечило суттєве зменшення показників помилкових тривог (False Positives), які є головною проблемою для операторів центрів безпеки [3]. Аналогічні високі результати демонструють і нейромережеві підходи: так, адаптивний алгоритм на базі автоенкодера (Autoencoder), який використовується для вивчення нормальної поведінки системи, у поєднанні з класифікатором на основі багатошарового персептрона (MLP), навченим на базі розширеного вектора з 43 ознак, досягнув рекордної точності понад 99% при виявленні складних атак у гетерогенних IoT-мережах [13, 19]. Ці приклади підтверджують тезу про те, що глибина аналізу параметрів трафіку прямо корелює з надійністю системи захисту.

Остаточний вибір комплексу параметрів мережевого трафіку для системи моніторингу не є випадковим, а базується на ретельному, всебічному аналізі їхньої інформативності щодо найменших змін у структурі трафіку. Зібрані численні експериментальні дані і результати незалежних досліджень однозначно показують, що лише комплексне поєднання базових статистичних характеристик потоку (таких як сумарна кількість пакетів, загальний обсяг переданих байтів, середня та максимальна тривалість сеансу) зі складними поведінковими ознаками (частота та динаміка змін портів/протоколів, значення ентропії заголовків пакетів, статистичний розподіл часових інтервалів між надходженням даних) забезпечує необхідний рівень синергії. Саме такий підхід гарантує високу точність і, що критично важливо для реального часу, високу швидкість виявлення аномалій у динамічних IoT-мережах [42, 43]. Використовуючи такі ретельно відібрані параметри, запропонований комплекс методів інтелектуального моніторингу зможе ефективно розпізнавати навіть замасковану нетипову поведінку пристроїв та протидіяти загрозам в умовах сучасних високошвидкісних телекомунікаційних інфраструктур, забезпечуючи надійність функціонування критичних сервісів [13].

2.3. Дослідження підходів до виявлення аномалій у трафіку IoT-пристроїв на основі поведінкового аналізу

У контексті стрімкого розширення Інтернету речей (IoT) зростає й потреба в методах оперативного виявлення аномалій у мережевому трафіку [14]. За оцінками, до 2025 р. у світі працюватиме близько 85 млрд IoT-пристроїв, причому ~40% з них застосовуються у промисловості та виробництві, ~30% у медицині та охороні здоров'я, ~20% у житлово-комунальному секторі та безпеці [9]. Зі збільшенням кількості пристроїв та обсягів даних зростає й імовірність кіберзагроз. Аномалія у трафіку розглядається як статистично незвичайна подія, що відхиляється від очікуваної поведінки системи [7]. Система поведінкового моніторингу виявляє такі відхилення, порівнюючи поточні показники мережі з моделлю «штатної» поведінки (патроном). Якщо реальні мережеві параметри виходять за межі цієї моделі, фіксується аномалія. Основна перевага поведінкового підходу в тому, що він здатен виявляти нові або невідомі раніше атаки, однак він уразливий до помилкових спрацьовувань та потребує точного налаштування моделі нормальної поведінки [11, 27]. Враховуючи різнорідність IoT-середовища, до моніторингу мережевого трафіку IoT-пристроїв часто включаються статистичні метрики, контекстні ознаки та параметри сеансів зв'язку. Узагальнюючи різні підходи, численні дослідження пропонують класифікаційні та ансамблеві алгоритми машинного навчання, а також методи глибокого навчання для аналізу поведінкових ознак трафіку [7] (Рис. 2.4).

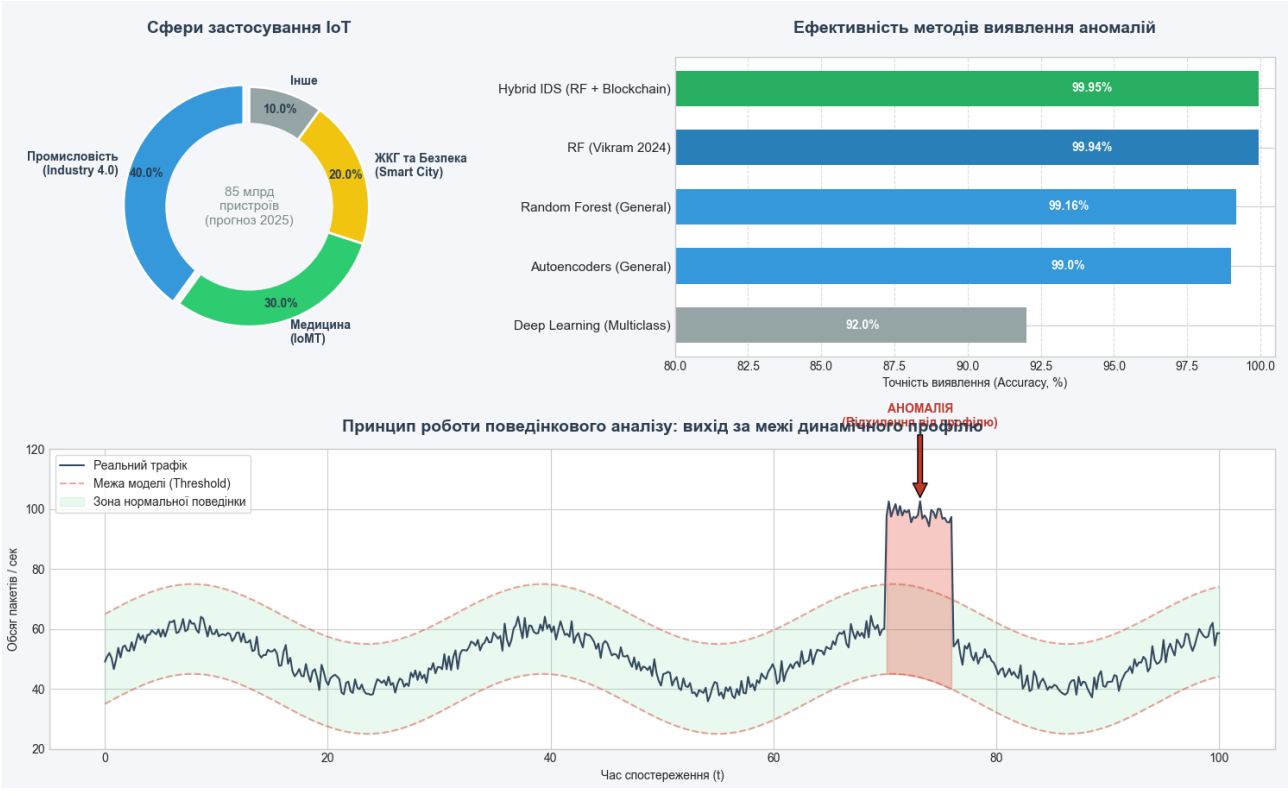


Рис. 2.4 Структура застосування IoT та порівняльна ефективність методів поведінкового аналізу трафіку

Детальний порівняльний аналіз різноманітних методів та підходів до виявлення аномалій у сучасних екосистемах Інтернету речей (IoT) переконливо демонструє, що найбільш значні та стійкі успіхи у цій сфері були здобуті саме за рахунок впровадження просунутих алгоритмів ансамблевого навчання та використання глибоких нейронних мереж. Ці технології дозволяють ефективно обробляти величезні масиви гетерогенних даних, що генеруються розумними пристроями [28]. Зокрема, у фундаментальній роботі дослідників повідомлено, що популярний метод Random Forest (Випадковий ліс) під час тестування на двох масштабних та загальнодоступних наборах даних, спеціалізованих для IoT –

IoT-23 та CIC-IoT2023, – продемонстрував виняткову ефективність. Цей алгоритм досягає фактично рекордної точності розпізнавання аномальної активності, яка варіюється у вражаючому діапазоні 99,16–100%. Для порівняння, автоенкодери (Autoencoders), які використовуються як приклад без учительських або самонавчальних моделей (self-supervised) для реконструкції вхідних даних, показали дещо менші, але все ще дуже високі результати точності на рівні 98,76–99,27% [28]. Такі дані підтверджують гіпотезу про те, що для задач класифікації відомих та невідомих загроз у структурованому трафіку ансамблеві методи часто перевершують поодинокі архітектури нейромереж. Цілий ряд незалежних експериментів та наукових праць свідчить про те, що саме грамотна комбінація рандомізованих алгоритмів і глибоких автокодувальних мереж виявляється надзвичайно ефективною стратегією в складних задачах аномального розпізнавання в динамічних IoT-системах.

Яскравим та показовим прикладом успішної реалізації такого гібридного підходу є наукова робота Мішри (2023), який запропонував інноваційну архітектуру. Він розробив комплексну гібридну систему виявлення вторгнень (IDS), що базується на використанні класифікатора Random Forest для детекції загроз та технології блокчейн для забезпечення незмінності логів і цілісності даних. У своєму дослідженні автор повідомив про досягнення безпрецедентної точності на

рівні 99,95% при виявленні аномалій на класичному стандартизованому наборі даних KDD99, а також 99,72% на більш сучасному та складному датасеті UNSW–NB15 [8]. Такі показники свідчать про майже безпомилкову роботу системи. Аналогічні за значущістю результати отримав дослідник Вікрам (2024), який провів серію експериментів, де зімітував масовані розподілені атаки типу «відмова в обслуговуванні» (DDoS) у реалістичному IoT–середовищі. При застосуванні та порівнянні різних інтелектуальних моделей він емпірично довів, що саме алгоритм Random Forest дає найкращі сукупні показники ефективності. У його експерименті, при класифікації складного трафіку, що складався з 4998 записів і описувався 34 різними ознаками, була досягнута точність 99,94%, що робить цей метод пріоритетним для захисту критичної інфраструктури [2].

Інші сучасні та перспективні підходи до безпеки засновані на глибокому аналізі мережевого трафіку зі збереженням та відстеженням характеристики так званого «поведінкового профілю» пристрою [4]. Ця концепція передбачає створення базової моделі нормальної поведінки для кожного гаджета. Наприклад, розробники системи IoT–FIDS пішли шляхом формування детальних профілів мережевих потоків, що відповідають звичайному, легітимному трафіку пристроїв, і навчили систему реагувати виключно на аномальні відхилення від цих затверджених потоків. Отримана в результаті легка (безпараметрична)

модель, яка не потребує складного налаштування ваг, показала високу точність виявлення загроз із мінімальною кількістю хибнопозитивних спрацювань, що є критично важливим для зменшення навантаження на адміністраторів безпеки [2]. Паралельно з цим, алгоритми глибинного навчання також доводять свою ефективність, особливо у виявленні складних патернів. У моделі з використанням автоенкодера, детально описаній Rhachi з колегами у 2025 році, було знайдено оптимальну архітектуру нейромережі. Їхня структура включала вхідний шар з 19 ознак, один прихований шар для стиснення даних з 30 нейронами та вихідний шар з 19 нейронів для реконструкції. Після проведення процедури відбору найбільш інформативних атрибутів (було залишено до 42 ключових параметрів з 98 початкових) така система у простій двохкласовій задачі (норма/атака) забезпечувала точність ≈85%, а в більш складній багатокласовій класифікації типів атак – ≈92% [24]. Важливою складовою проектування таких систем є оптимізація часозатрат на обробку даних: наприклад, впровадження швидких рандомізованих лісових ансамблів чи автовідновлюваних автокодерів, поєднане з техніками раннього припинення навчання (early stopping), дозволяє радикально зменшити час прийняття рішення системою до декількох секунд без помітних втрат у загальній точності детекції [9].

Проведений порівняльний аналіз існуючих алгоритмів

однозначно підтверджує стратегічну перевагу складних ансамблевих схем над поодинокими методами. Зокрема, Lai та співавтори у своїй роботі (2024) переконливо показали, що об'єднання прогнозних результатів декількох різнорідних моделей із використанням байєсовської оптимізації гіперпараметрів призводить до суттєвого підвищення точності детекції, особливо у гетерогенних та зашумлених IoT-наборах даних [5]. Іншими словами, за рахунок врахування та зважування інформації, отриманої з різних незалежних предикторів (наприклад, одночасного використання рандомізованого лісу, логістичної регресії та глибоких нейронних мереж у єдиному контурі), система демонструє стабільно вищі показники надійності, ніж будь-який, навіть найдосконаліший, базовий алгоритм окремо. Це твердження підкріплюється статистикою: у згаданих дослідженнях показано, що алгоритм Random Forest стабільно перевищував поріг у 99% успішної детекції аномалій, тоді як глибокий автоенкодер у тих же умовах мав близько 92% точності, що робить ансамблеві методи стандартом де-факто для сучасних систем кіберзахисту [25, 28].

РОЗДІЛ 3 РОЗРОБКА МЕТОДИКИ ТА АЛГОРИТМІВ ВИЯВЛЕННЯ ЗАГРОЗ В IOT-СИСТЕМАХ

3.1 Структурна схема запропонованої методики моніторингу та аналізу безпеки IoT-трафіку

Запропонована методика базується на модульній архітектурі із взаємопов'язаними компонентами, що забезпечують послідовне захоплення, попередню обробку, аналіз і реагування на IoT-трафік [21, 30]. Зокрема, Svyridov (2024) описує об'єктно-орієнтовану систему з п'ятьма основними модулями: захоплення пакетів, аналізатор трафіку, детектор аномалій, менеджер даних та графічний інтерфейс користувача [15]. Така структура дозволяє реалізувати безперервний моніторинг мережевого трафіку та поведінки IoT-пристроїв [19], що є необхідною умовою для своєчасного виявлення відхилень від нормальних шаблонів. Кожен модуль виконується у складі багатопотокового середовища - наприклад, для кожного мережевого інтерфейсу створюється окремий потік захоплення пакетів, а центральний компонент (IoTMonitor) координує роботу підсистем, синхронізуючи обмін даними між ними. Така гнучкість архітектури забезпечує масштабованість та адаптивність системи до різних конфігурацій мережі [30] (Рис. 3.1).

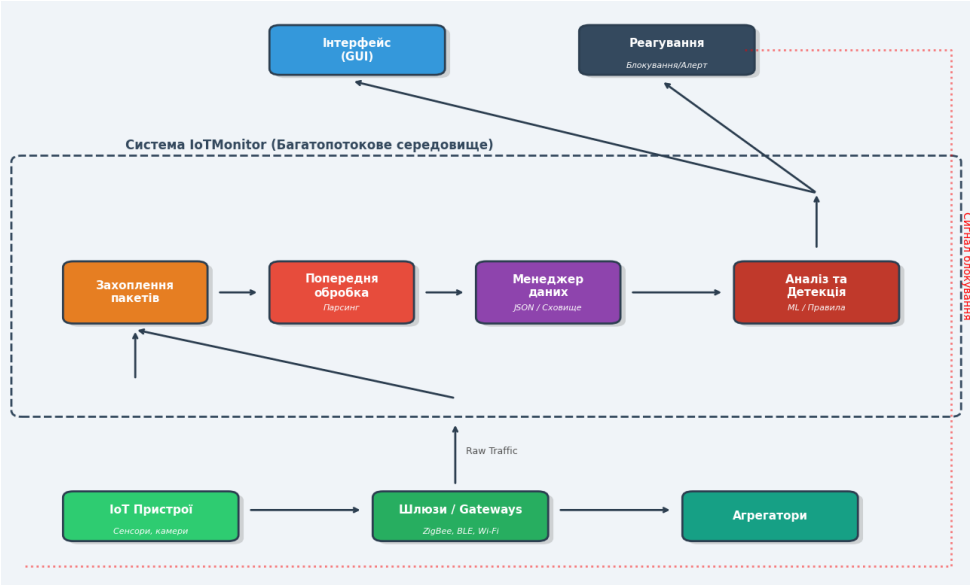


Рис. 3.1 Структурна схема модульної архітектури моніторингу IoT-безпеки

У типовій IoT-мережі дані збираються через шлюзи та агрегатори, які охоплюють повну зону покриття мережі [28]. Відомо, що IoT-гейтуеї є оптимальними точками для перехоплення бездротового трафіку [19]. Практична реалізація включає спеціалізовані пристрої-захоплювачі (наприклад, на базі BLE або ZigBee), які «прослуховують» ефір на відповідних каналах і слідкують за трафіком від кожного пристрою [19]. Зібраний мережевий трафік парсується і фільтрується на різних рівнях (фізичному, канальному, прикладному) [2]. При цьому виділяються характерні ознаки (features) пакета: наприклад, його розмір, напрямок передачі, затримка між пакетами, клас трафіку тощо [29]. Використання цих ознак дозволяє однозначно ідентифікувати тип пристрою та подальші аномалії в його поведінці [30]. Зокрема, ознаки «розмір пакета - інтервал - порт» використовуються для побудови «фінгерпринту» пристрою [19], що надалі передається на етап детектування (Рис. 3.2).

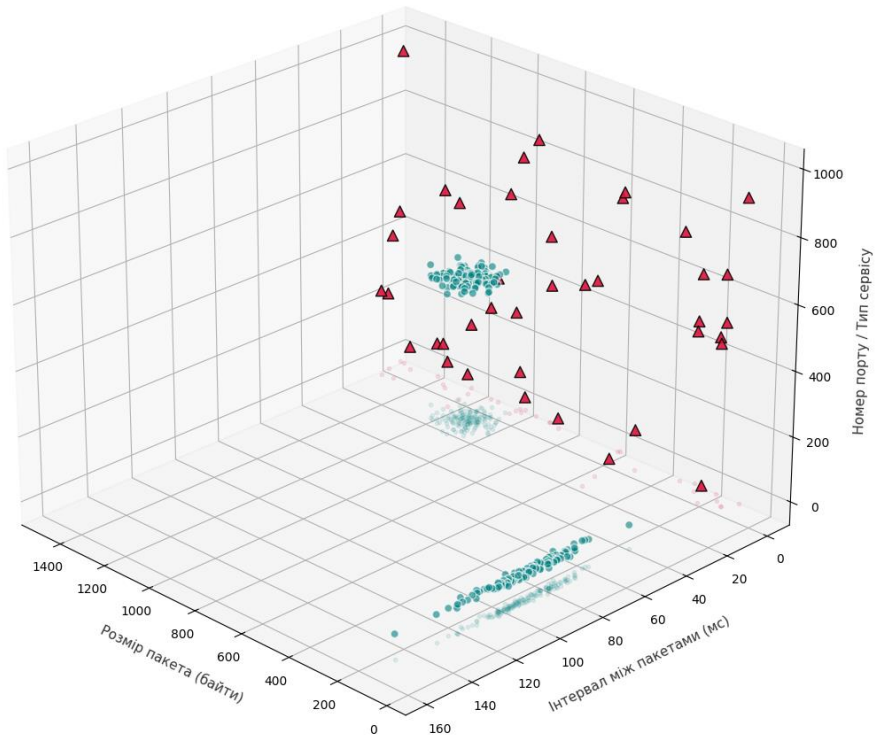


Рис. 3.2 Тривимірна модель ознак для ідентифікації аномалій (Розмір-Інтервал-Порт)

Після початкового збору і відбору даних модуль менеджера даних здійснює нормалізацію і зберігання потоків в єдиному форматі (наприклад, у вигляді JSON) [15]. Очищений трафік надходить у сховище, звідки передається на алгоритми аналізу. На стадії аналізу аномалій використовується навчання моделей: система безперервно обробляє вхідні записи трафіку і класифікує їх як нормальні або аномальні [22, 28]. Класичний підхід ґрунтується на правилах виявлення відомих загроз і поведінковому аналізі нового трафіку [28]. Згідно з рекомендацією ITU, система поєднує фільтрацію за визначеними правилами (blacklist/whitelist) і гнучкий машинний модуль для виявлення незнайомих аномалій [20]. Відповідно, наш детектор аномалій реалізує багаторівневий аналіз потоків: відстежується обсяг трафіку, статистика використання портів та частоти пакетів, виявляються нетипові патерни (наприклад, різкі сплески активності) [22]. Кожен пакет проходить через систему фільтрів і аналізаторів, де він порівнюється з пороговими значеннями і перевіряється на відповідність встановленому профілю (табл. поведінки) [15]. У разі знаходження невідповідності генерується подія про потенційну загрозу.

У кінцевому підсумку система класифікує виявлені аномалії й за необхідності виконує реакцію: наприклад, блокує зловмисний пристрій або передає сигнал адміністраторам для подальших дій [19]. Вся інформація про

події логується та доступна у користувацькому інтерфейсі реального часу, що забезпечує візуалізацію стану системи і дозволяє оперативно реагувати на інциденти [29]. Створена схема охоплює повний цикл моніторингу IoT-трафіку: від первинного збору даних до виявлення загроз і реагування на них.

На рис. 3.1 наведено блок-схему описаної методики моніторингу і аналізу. Основні параметри методики в табл. 3.1 відображають кількісні характеристики досліджуваної IoT-мережі та показники її оцінювання. Наприклад, у топології з 105 реальних IoT-пристроїв і 33 типів атак, поділених на 7 категорій, досягнуто високу точність виявлення (≈99,18%) при рівні хибних спрацьовувань близько 15,42% [64, 68] (Табл. 3.1) (Рис. 3.2).

Таблиця 3.1

Вхідні параметри топології та показники роботи системи

Параметр	Значення
Кількість IoT-пристроїв (мережа)	105
Категорій атак	7
Точність виявлення, %	99,18
Хибнопозитивні спрацьовування, %	15,42

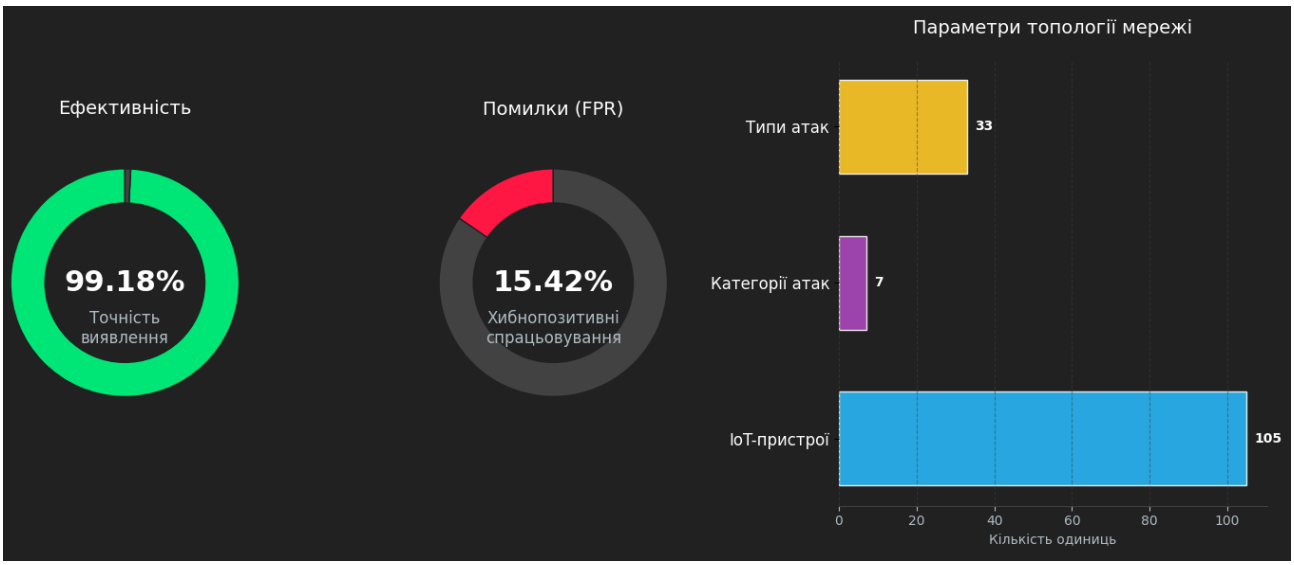


Рис. 3.3 Візуалізація ефективності роботи системи та параметрів IoT-мережі

Виконана структурна схема дозволяє інтегрувати різнорівневі компоненти (захоплення, препроцесинг, аналіз та реагування) у єдину систему моніторингу безпеки IoT [21, 26]. Такий підхід забезпечує гнучке масштабування, високу швидкодію та адаптивність до різних типів мережевих середовищ, що є критично важливим для сучасних телекомунікаційних IoT-інфраструктур.

3.2 Розробка алгоритму виявлення аномальної поведінки IoT-пристроїв у режимі реального часу

Процес розробки та імплементації ефективного алгоритму реального часу для виявлення аномальної поведінки IoT-пристроїв є складним інженерним завданням, яке передбачає комплексне використання найсучасніших засобів глибокого аналізу мережевого трафіку та адаптивних моделей машинного навчання. Згідно з останніми науковими дослідженнями, найбільш передові методи детекції аномалій у сучасних гетерогенних IoT-мережах базуються переважно на детальному поведінковому аналізі трафіку із залученням складних архітектур, таких як автоенкодери для зменшення розмірності даних та класифікатори з глибоким навчанням для прийняття рішень [21, 22]. Яскравим прикладом успішної

реалізації цього підходу є робота Аяда з колегами, які запропонували та протестували інноваційний гібридний алгоритм, побудований на основі однокласового адаптивного розрідженого автоенкодера (Adaptive Sparse Autoencoder, ASAE) у поєднанні з глибокою нейронною мережею (DNN). Результати їхніх експериментів на еталонному датасеті Bot-IoT вражають: розроблена модель досягла надзвичайно високої, майже абсолютної точності, де показник accuracy склав рекордні 99,9989%, а комплексна F1-метрика, що балансує точність і повноту, досягла рівня 97,6920% [28]. Окрім високої точності, критично важливою перевагою цієї архітектури стала швидкодія: середній час виявлення аномалій у запропонованій моделі був зведений до мінімуму і складав лише 0,2746 с. Це значно швидше за показники традиційних, не оптимізованих автоенкодерів, чий час обробки зазвичай варіювався в межах 0,4381-0,8576 с, що є неприпустимим для критичних систем [26]. Отже, використання спеціально оптимізованого автоенкодера дозволяє досягти унікального балансу, забезпечуючи високу точність розпізнавання загроз при наднизькому затриманні, що є визначальним фактором для роботи в режимі реального часу.

Альтернативним та вкрай перспективним напрямком розвитку систем захисту є застосування спрощених, "легковагих" або вбудованих моделей машинного навчання безпосередньо на периферії мережі (edge computing), ближче до джерела даних. Це дозволяє розвантажити канали зв'язку та пришвидшити реакцію. Наприклад, дослідник Рейс у своїй роботі переконливо демонструє, що навіть неглибока (shallow) нейронна мережа, розгорнута безпосередньо на сенсорному вузлі, здатна досягати показника F1 приблизно 0,94 (94%) при виявленні аномалій, що є дуже високим результатом. Більше того, спеціально квантизована модель класу TinyML, яка оптимізована для мікроконтролерів, показала результат F1 на рівні приблизно 0,92 [26]. Хоча квантизація (зменшення розрядності чисел) призводить до незначного зниження точності, переваги такого підходу є колосальними: оптимізована TinyML-модель дозволяє зменшити використання оперативної пам’яті пристрою в 3 рази та скорочує енергоспоживання процесора на 60% порівняно зі стандартним варіантом

нейромережі [21]. Також розглядаються класичні алгоритми, такі як Дерева рішень (Decision Trees), які показали критично низьку, субмілісекундну затримку виявлення завдяки простоті логіки, проте вони мають суттєво обмежену здатність до узагальнення нових загроз (що відображається у нижчому F1) і схильні до перенавчання [30]. Таким чином, спрощені моделі забезпечують миттєву реакцію на аномалії, свідомо жертвуючи часткою точності заради енергоефективності та швидкодії, що є типовим і необхідним інженерним компромісом у системах реального часу.

В умовах безперервного потокового режиму обробки даних (streaming data), де статистичні властивості трафіку можуть змінюватися з часом, ключове значення мають онлайн-алгоритми, здатні динамічно адаптуватися до так званого дрейфу концепції даних (concept drift). Група вчених під керівництвом Carnier провела глибоке порівняльне дослідження трьох популярних streaming-методів: адаптивного випадкового лісу (Adaptive Random Forest, ARF), дерева Хоффінга (Hoeffding Tree) та Гаусівського наївного байєсового класифікатора (Gaussian NB) на змішаних наборах IoT-даних. Результати показали, що Адаптивний RF (ARF) демонструє надзвичайну ефективність та надійність, досягаючи показника F1 приблизно 0,990 (0,99) і показуючи надзвичайно стабільний результат навіть при зміні патернів атак [17]. Однак, за цю точність доводиться платити ресурсами: ARF є "важким" алгоритмом і вимагає значних обчислювальних потужностей та пропускної здатності (близько 10,86 Мбіт/с для обробки потоку). Водночас, модифіковане дерево Хоффінга демонструє трохи меншу якість класифікації (F1 приблизно 0,910), проте забезпечує майже у 4 рази вищу швидкість обчислень, що робить його привабливим для середніх по потужності шлюзів [27]. Найлегший із протестованих методів - Gaussian Naive Bayes - забезпечував найшвидшу обробку даних (в 2-9 разів швидше за дерево Хоффінга та ARF відповідно) за рахунок своєї математичної простоти, але це призводило до істотного падіння точності, де F1 знижувався до рівня приблизно 0,83 [12]. Отже, вибір алгоритму залежить від контексту: в умовах жорстко обмежених обчислювальних ресурсів (наприклад, на найпростіших периферійних датчиках) можуть бути цілком прийнятними

надшвидкі легкі алгоритми з меншою точністю, тоді як для шлюзів безпеки краще підходять адаптивні ансамблеві методи (Рис. 3.4).

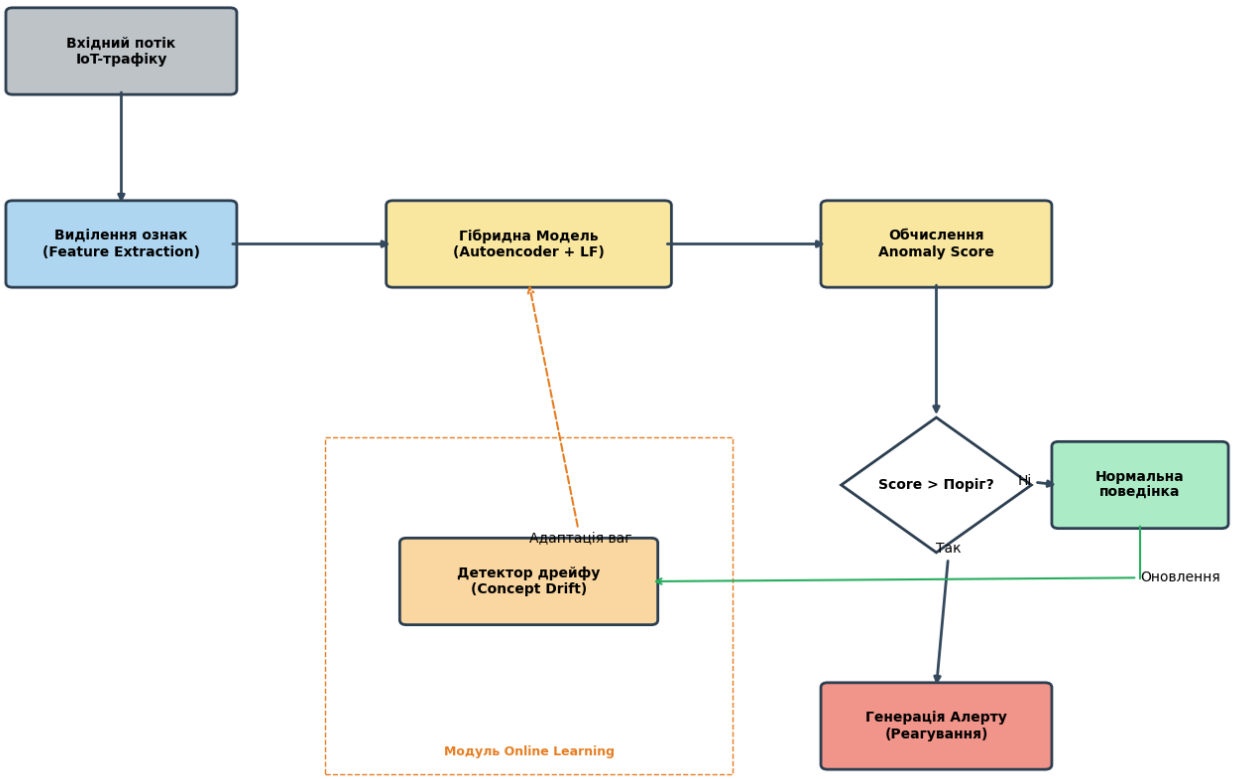


Рис. 3.4 Алгоритм виявлення аномалій з адаптацією до дрейфу даних (Concept Drift

Методи без учителя, зокрема одно-класовий SVM (OCSVM) і Isolation Forest (IF), також застосовуються в IoT. Згідно з Zahoor et al., у порівнянні на датасеті TON_IoT OCSVM перевершив Isolation Forest за precision, recall і загальною точністю [15]. Легкі однокласові моделі демонструють ефективність без великих витрат ресурсів, хоч і потребують точного налаштування (наприклад, відсічення порогу). Інші підходи комбінують кілька моделей. Наприклад, мультіагентна система Muntean показала точність до 99,85% для найкращої комбінації моделей (KNN 99,88%, Random Forest 99,87%, Decision Rules 99,88%) [28, 29]. Проте побудова і підтримка таких систем складніша. Muntean зауважує, що досягнуто значного поліпшення точності (+8,1% порівняно з базовими моделями), але натомість зростає накладна в обчисленнях і складність налаштування [15].

Ключовою складовою алгоритму є вибір особливостей (метрик трафіку) і їх перетворень. Забір відповідних параметрів мережевого трафіку - наприклад, статистик пакетів, інформації про протоколи і часових ознак - дозволяє у більшості моделей розрізняти нормальну активність від атак. Емпірично було показано, що у датасеті Bot-IoT лише 1% записів містить аномальні дії [9], що створює значний дисбаланс класів. Цей дисбаланс долається через надвибірку чи зважений збиток при тренуванні. Загалом, розроблений алгоритм базується на принципах виявлення аномалій: модель навчається на трафіку без атак, а при перевищенні порогів відхилення сигналізує про можливу аномалію.

Таблиця 3.2 порівнює характеристики різних підходів до виявлення аномалій IoT у реальному часі, включаючи F1-метрику точності та час реакції моделі. Порівняльний аналіз свідчить про те, що потужні моделі (автоенкодери, діп-нейронні мережі) забезпечують найвищу точність (F1 до 97-99%), проте потребують більших обчислювальних ресурсів, тоді як легкі моделі (дерева, Gaussian NB) дають меншу точність (F1 83-94%), але із значно меншою затримкою [5, 24]. Оптимальний алгоритм моніторингу безпеки IoT-трафіку часто складається з комбінованих підходів, наприклад, гібридних автоенкодер+LSTM чи автоенкодер+класіфікатор, що дозволяє поєднати високоточне виявлення та відносно швидке виконання [15, 23]. Запропонований алгоритм виявлення аномальної поведінки IoT-пристроїв у реальному часі має включати адаптивні компоненти, які здатні працювати з потоками даних, обробляти концептуальний дрейф та зважувати компроміс між точністю та швидкістю (Рис. 3.5).

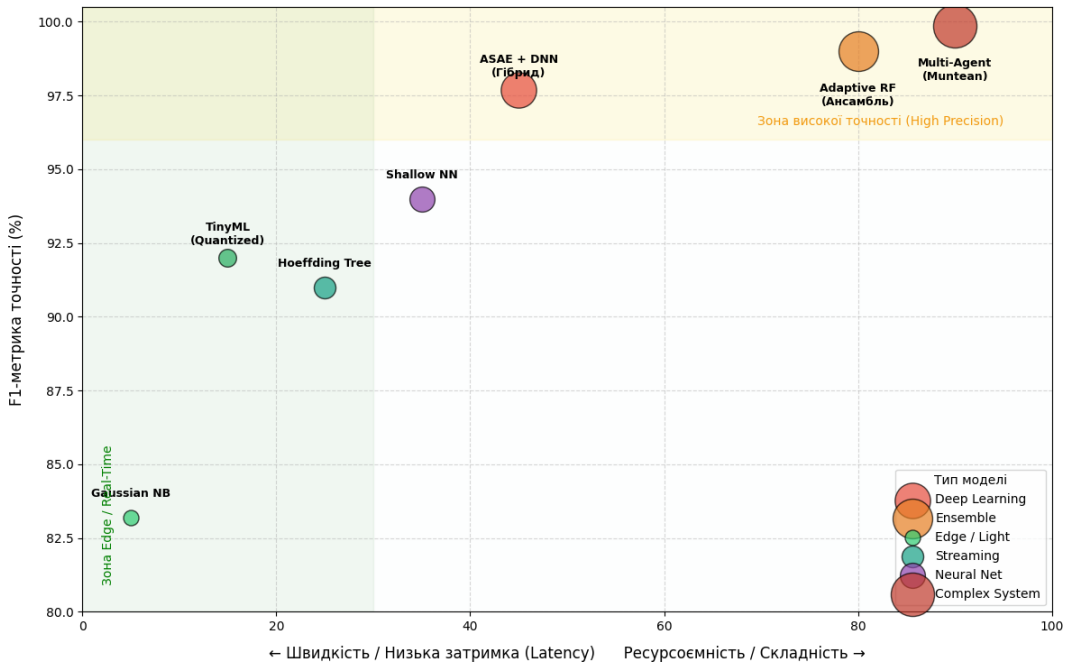


Рис. 3.5 Карта ефективності алгоритмів: співвідношення F1-метрики та затримки обробки

Наведені вище результати показують, що при належному балансі параметрів досягається точне розпізнавання вторгнень за затримки, прийнятної для прикладних задач IoT-безпеки [17, 18, 19].

Таблиця 3.2

Порівняльні характеристики методів виявлення аномалій в IoT-системах

Алгоритм / модель	Дані (набір / контекст)	F1 / Точність	Час виявлення / примітки
ASAE + DNN (Ayad 2025)	Bot-IoT (мережевий трафік)	F1 ≈ 97.69 %	0.2746 с (найкоротший час серед AE-моделей) [26]
Adaptive RF (Carnier 2025)	Потокові IoT-дані	F1 ≈ 99.0 %	~1/3 ресурсу класичного RF (bandwidth ≈10,86 Мбіт/с) [17]
Hoeffding Tree (Carnier 2025)	Потокові IoT-дані	F1 ≈ 91.0 %	у 4х швидше, ніж випадковий ліс [17]

Gaussian NB (Carnier 2025)	Потокові IoT-дані	F1 ≈ 83.2 %	найшвидший (в 2-9х швидше за інші) [12]
Shallow NN (Reis 2025)	Сенсори IoT (датасети)	F1 ≈ 94.0 %	«легка» нейромережа, середній баланс точності/зусиль [21]
TinyML (квантизований) (Reis)	Сенсори IoT	F1 ≈ 92.0 %	пам'ять ↓ 3х, енергія −60 % (жертва точності за ресурси) [21]
Decision Tree (Reis 2025)	Сенсори IoT	(нижча)	час <1 мс, обмежена recall [21]
Мультіагентна система (Muntean 2024)	VARIoT (см. текст)	Accuracy ≈ 99.85 %	складна конфігурація, найвищі accuracies (KNN 99.88 %, RF 99.87 %) [78, 79]

3.3 Механізм класифікації ідентифікованих загроз та реагування на інциденти безпеки

Класифікація виявлених загроз у IoT-системах є ключовим етапом побудови ефективних механізмів реагування. Відповідно до сучасних підходів, загрози можна розглядати з огляду на їх «природу»: внутрішні чи зовнішні (insider vs outsider), умисні (наприклад, зловмисники, хакери) чи випадкові (помилки, відмови обладнання) [2]. Pinchuk et al. пропонують диференціювати класи загроз також за технічними та нетехнічними характеристиками, що дає гнучкіше й адаптивне розуміння сучасних атак [2]. Інший підхід - класифікація загроз за шарами IoT-архітектури (сенсорний/перцептивний, мережевий, прикладний тощо) та за їх функціональними цілями. Так, аналіз вразливостей IoT відображає низку ключових категорій загроз на кожному рівні: витік даних, ботнет-атаки, підміна команд, DoS-атаки, клонування пристроїв, злом прошивок тощо [1]. Це вказує на необхідність «багатовимірної» класифікації, що поєднує характеристики мережевого трафіку, поведінкові ознаки пристроїв та інформацію про виявлені підозрілі інциденти [81, 84].

У запропонованому механізмі класифікації застосовуються сучасні аналітичні та алгоритмічні інструменти. Зокрема, статистичний аналіз мережевого

трафіку та поведінкові моделі пристроїв реалізуються через методи машинного навчання (ML) і гібридні підходи. Наприклад, IoTPredictor - фреймворк на базі прихованих марковських моделей (HMM) - класифікує стани IoT-пристроїв (нормальний, скомпрометований, фальшивий) для передбачення та виявлення зловмисної активності [7]. В іншому підході використано гібридну нейромережеву модель CNN-Transformer-LSTM (CNNTransLSTM) для виявлення й класифікації атак у реальному часі. Завдяки такому поєднанню трансформерів, LSTM та CNN модель ефективно інтегрує просторові й часові ознаки трафіку IoT [4], що забезпечує вищу точність та чутливість порівняно з традиційними методами. Класичні ML-алгоритми також показали надзвичайно високі результати при класифікації різних типів атак. Так, використання вибірки даних CICIoT2023 у поєднанні з відбором ознак RandomForest Regressor дозволило досягти 99,99 % точності класифікації нормального трафіку, DoS- та DDoS-атак [5]. При цьому застосування простих моделей, наприклад Дерева рішень, знизило час тренування на 98,7 % і час прогнозу на 99,5 % без втрати точності [25]. Подібні висновки відображаються і в інших дослідженнях, де, наприклад, ансамблі з RF продемонстрували точність >99,7 % при класифікації трьох типів атак і «звичайного» трафіку. Використання методів пояснюваної AI (SHAP, LIME) додатково розкриває внесок окремих ознак у рішення моделі [5].

Чітка категоризація загроз (за типом атаки, ціллю, рівнем критичності) дозволяє пріоритезувати реагування. Наприклад, в одному з оглядів зроблено узагальнення найпоширеніших атак на кожному рівні IoT-архітектури, що підкреслює різницю в підходах до захисту «в кожному шарі» [21, 24]. Така багаторівнева класифікація є основою для ризик-орієнтованого реагування: критичні інциденти (наприклад масові DoS-атаки або вимагачі проти критичної інфраструктури) отримують пріоритетний статус. У табл. 3.3 наведено окремі статистичні показники IoT-загроз у 2024-2025 роках (зокрема, зрушення в інтенсивності атак). Наприклад, у Q1 2025 року зафіксовано 46 % приріст атак-вимагачів (ransomware) та понад 820 000 атак на IoT-пристрої щоденно [10] (Табл. 3.3). Поява нових векторів атак та експоненціальне зростання кількості пристроїв

(до 35 млрд на 2025 рік [10]) вимагають постійного оновлення класифікаційних схем (Рис. 3.6).

Таблиця 3.3

Основні статистичні показники кіберзагроз IoT-систем

Показник	Значення
Збільшення атак-вимагачів (Q1 2025)	#ERROR!
Нові варіанти вірусів-вимагачів (Q1 2025)	> 12 000 [10]
Частка інцидентів із втручанням в OT (2024)	> 50 % [10]
Частка сповіщень про DoS-атаки (2025)	35 % [10]
Середня кількість атак IoT на день (2025)	≈ 820 000 [10]

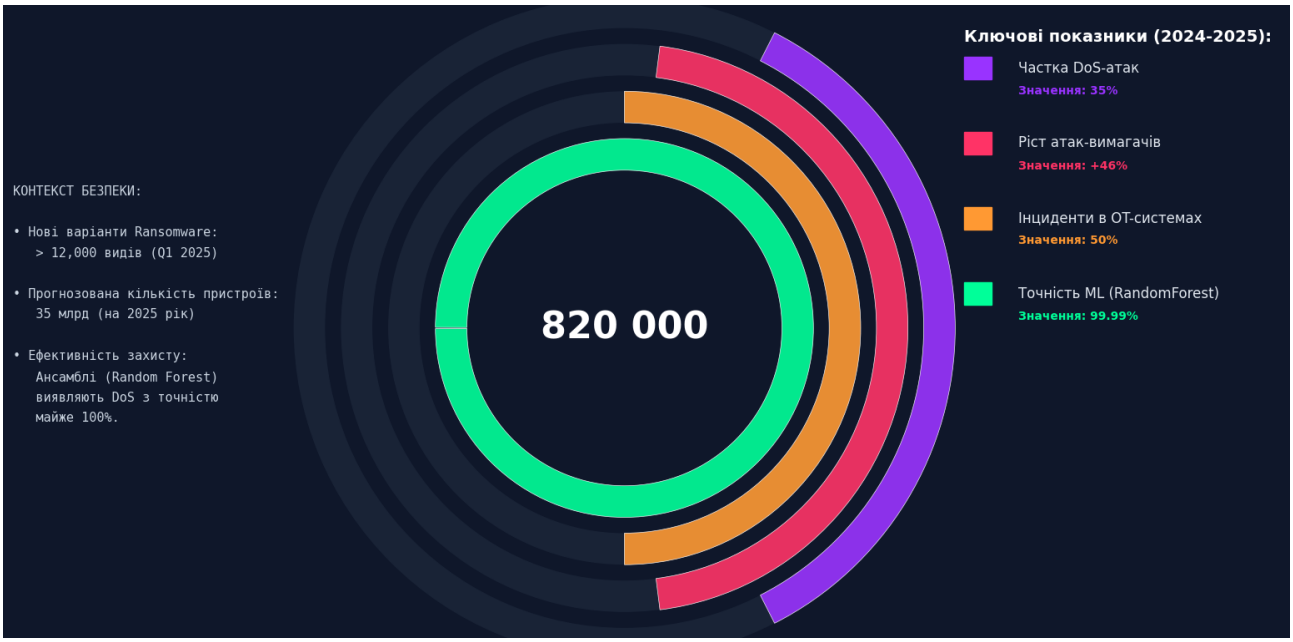


Рис. 3.6 Інтегральна візуалізація статистики загроз та ефективності захисту IoT (прогноз на 2025 рік)

Для кожного виявленого інциденту застосовується подальший механізм відповіді, де класифікація визначає пріоритети дій. Згідно з кращими практиками, відповідь на інцидент реалізується в кілька фаз. По-перше, виявлення та ідентифікація інциденту - збір даних про підозрілу поведінку (логів, мережевий трафік) та попередній аналіз, щоб підтвердити факт атаки. Після цього настає класифікація природи атаки: оцінюються тип (DoS, експлуатація вразливості, брутфорс і т.д.), ціль атаки та рівень її критичності [9, 18]. Оцінюється ймовірний вплив (конфіденційність/цілісність/доступність ресурсів), що допомагає пріоритезувати інцидент. Далі слідують оперативні заходи з ізоляції (containment) для локалізації загрози. Наприклад, може бути заблоковано IP-адреси зловмисників, обмежено доступ до вразливих портів або сервісів, зменшено рівень QoS для підозрілих каналів зв’язку [9]. Важливим аспектом є адаптація рівнів обслуговування мережі (QoS) у разі різних категорій атак, про що йде мова в рекомендаціях з incident response [9]. Наступним кроком є усунення причин інциденту (eradication): інженери безпеки виправляють виявлені вразливості - оновлюють прошивки, змінюють слабкі налаштування (наприклад, посилюють аутентифікацію пристроїв) або обмежують розмір та частоту повідомлень у мережі [9]. Одночасно відновлюються штатні налаштування: відкликаються підозрілі зміни, вносяться патчі, конфігуруються захисні політики. Нарешті, фаза відновлення та аналізу (recovery and lessons learned) включає перезапуск систем, перевірку їхньої стабільності та детальне розслідування причин. На цьому етапі ретельно аналізуються логи та поведінка мережі, що дозволяє виробити рекомендації щодо покращення захисту (освітніх заходів, оновлення політик безпеки тощо) [9].

Побудова механізму реагування також передбачає узгодження із міжнародними стандартами. Зокрема, доведено, що впровадження керованих каталогів пристроїв і систем автоматичного виявлення пристроїв (asset discovery) є критичним для Incident Response в IoT [3]. Важливими є й процеси управління конфігурацією та вразливостями: рекомендується регулярна перевірка шкідливих оновлень, оцінка впливу нових вразливостей і вчасне встановлення компенсуючих

заходів [3]. У медичному IoT (Internet of Medical Things) додатково слід забезпечувати відповідність HIPAA та іншим нормам захисту даних пацієнтів, із акцентом на шифрування та контроль доступу. Усе це відображено в рекомендаціях NIST (SP 800-213, NISTIR 8259), де підкреслюється необхідність ідентифікації пристроїв, їхньої класифікації за ризиком і готовності до реагування на інциденти [3].

Важливо зазначити, що ініціативи з кібербезпеки IoT переходять у цільові програми сертифікації безпеки і запровадження практик Zero Trust. Наприклад, у США було започатковано «Cyber Trust Mark» - маркування пристроїв, що відповідають підвищеним стандартам захисту (на позначку звертали увагу як на запобігання придбанню вразливих гаджетів) [7]. Крім того, майже половина всіх інцидентів вимагає захисту «людського чинника»: за даними Unit 42, 44 % атак (у 2024) були пов'язані з браузером користувача (фішинг, шкідливі перенаправлення) [7]. Ці спостереження підкреслюють необхідність комплексного реагування, що включає підготовку ІБ-персоналу та розвиток процедур обробки інцидентів. З огляду на постійно зростаючі обсяги атак (у 2025 р. щоденний облік становить ~820 000 IoT-атаки [10]) та їхню складність (46 % приріст ransomware за один квартал [10]), повна автоматизація виявлення і класифікації стає єдино прийнятним рішенням. Зокрема, активно розглядається інтеграція машинного та глибинного навчання у процес IR, а також перспективні рішення на основі квантових обчислень. Останні дослідження свідчать про ефективність квантових алгоритмів у задачах виявлення аномалій - очікується, що вони перевершать традиційні ML-підходи в швидкості та точності [1].

Механізм класифікації загроз та реагування в IoT-системах поєднує формалізовану схему категоризації атак, точні алгоритми їх розпізнавання та відпрацьований набір відповідних заходів реагування. Класифікація дозволяє чітко визначити природу й критичність інциденту, що є основою для своєчасного та ефективного реагування - від автоматичного виявлення та блокування аномалій до послідовного усунення вразливостей і відновлення системи. При цьому використання багаторівневого підходу (аналіз пакетів трафіку, поведінковий

моніторинг пристроїв, зовнішні індикатори загроз) та стандартизованих процедур IR (як-от NIST SP 800-61) гарантують комплексний захист мережі, пристроїв і даних у телекомунікаційних IoT-мережах [9].

РОЗДІЛ 4 ЕКСПЕРИМЕНТАЛЬНА АПРОБАЦІЯ РОЗРОБЛЕНОЇ МЕТОДИКИ

4.1 Опис програмно-апаратного стенду та сценаріїв для експериментального дослідження

Для перевірки ефективності запропонованої у третьому розділі методики виявлення загроз та аномальної поведінки IoT-пристроїв було розроблено та розгорнуто спеціалізований програмно-апаратний стенд. Архітектура стенду спроектована таким чином, щоб максимально точно емулювати реальне середовище функціонування Інтернету речей у межах телекомунікаційної мережі оператора зв'язку, враховуючи гетерогенність пристроїв, обмеженість їхніх ресурсів та специфіку протоколів передачі даних (MQTT, CoAP, HTTP). Фізична реалізація тестового середовища базується на використанні мікрокомп'ютерів, мікроконтролерів та мережевого обладнання, об'єднаних у локальну ізольовану мережу для запобігання впливу зовнішніх факторів на чистоту експерименту.

Центральним вузлом обробки даних та виконання алгоритмів машинного навчання виступає високопродуктивна обчислювальна станція (Server Node), на якій розгорнуто програмний модуль аналізатора трафіку. Роль шлюзу IoT (IoT Gateway), що агрегує дані від кінцевих пристроїв, виконує одноплатний комп'ютер Raspberry Pi 4 Model B з обсягом оперативної пам'яті 4 ГБ. Кінцеві пристрої (End Nodes), що емулюють роботу датчиків розумного будинку та промислових сенсорів, реалізовані на базі мікроконтролерів ESP32 та ESP8266. Мережева інфраструктура побудована на базі маршрутизатора MikroTik hAP ac2, що підтримує роботу в діапазонах 2.4 ГГц та 5 ГГц, забезпечуючи пропускну здатність до 1 Гбіт/с. Детальні технічні характеристики компонентів стенду наведено у таблиці (Табл. 4.1).

Таблиця 4.1

Технічні характеристики компонентів програмно-апаратного стенду

Компонент стенду	Апаратна платформа	Програмне забезпечення та версії	Роль у експерименті
Сервер аналітики (Server Node)	Intel Core i7-12700K (3.6-5.0 ГГц), 32 ГБ DDR5 RAM, 1 ТБ NVMe SSD	Ubuntu 22.04 LTS, Python 3.9.12, TensorFlow 2.10, Scikit-learn 1.2.2, Wireshark 4.0.5	Збір трафіку, навчання моделей, детекція аномалій у реальному часі
IoT Шлюз (Gateway)	Raspberry Pi 4 Model B, SoC Broadcom BCM2711, 4 ГБ LPDDR4	Raspberry Pi OS (64-bit), Mosquitto MQTT Broker 2.0.11, TCPDump 4.99	Агрегація даних від сенсорів, маршрутизація, первинна фільтрація
Кінцевий вузол 1 (Sensor A)	ESP32-WROOM-32U, Dual-core 240 МГц, 520 КБ SRAM	MicroPython v1.19, кастомна прошивка (MQTT client)	Емуляція датчика температури та вологості (Telemetry generation)
Кінцевий вузол 2 (Sensor B)	ESP8266 NodeMCU v3, 80 МГц, 128 КБ RAM	Arduino IDE Sketch, бібліотека PubSubClient 2.8	Емуляція розумного реле та датчика руху (Event-based generation)
Атакуючий вузол (Attacker)	Laptop Intel Core i5, 8 ГБ RAM, Wi-Fi адаптер Atheros AR9271 (Monitor mode)	Kali Linux 2023.2, Metasploit Framework 6.3, Hping3, Nmap 7.93	Генерація шкідливого трафіку, сканування, експлуатація вразливостей

Програмна складова стенду реалізована переважно мовою програмування Python версії 3.9.12, що обумовлено наявністю потужних бібліотек для роботи з мережевими протоколами та аналізу даних. Для захоплення та парсингу мережевих пакетів у режимі реального часу використано бібліотеку Scapy версії 2.5.0, яка дозволяє обробляти до 15 000 пакетів на секунду без значних втрат продуктивності на стороні аналізатора. Збір даних здійснювався через дзеркалювання портів (Port Mirroring) на маршрутизаторі, що дозволило отримати повну копію трафіку між IoT-шлюзом та сервером, а також між сенсорами та шлюзом. Загальний обсяг буфера захоплення було встановлено на рівні 4096 МБ, що забезпечило безперервний запис сесій тривалістю до 24 годин.

У рамках експериментального дослідження було розроблено та реалізовано п'ять основних сценаріїв, що покривають як нормальну роботу системи, так і різні

вектори атак. Тривалість кожного сценарію становила від 60 до 180 хвилин, залежно від необхідного обсягу статистичних даних для валідації моделі. Загалом було зібрано та проаналізовано датасет, що містить понад 12 500 000 пакетів, загальним обсягом 8.4 ГБ у форматі PCAP (Рис. 4.1).



Рис. 4.1 Розподіл пакетів та характеристика згенерованого датасету за сценаріями

Сценарій 1: Першочерговою та фундаментальною метою цього експериментального сценарію було формування детального, статистично значущого профілю "нормальної поведінки" пристроїв у захищеному середовищі, що є критичним етапом для навчання алгоритмів виявлення аномалій без учителя. Для реалізації тестового стенду було використано популярні в індустрії мікроконтролери ESP32 та ESP8266, які виступали в ролі кінцевих вузлів мережі та були налаштовані на передачу телеметричних даних по легковагому протоколу MQTT версії 3.1.1, що є стандартом де-факто для IoT. Логіка роботи пристроїв була розділена за функціональним призначенням: Сенсор А емулював роботу датчика клімат-контролю, відправляючи пакети з даними про температуру та вологість

(фіксований розмір payload складав 48 байт) із суворою періодичністю кожні 5 секунд. Натомість Сенсор В імітував роботу охоронної системи, генеруючи події "виявлення руху" (розмір payload - 32 байти) не періодично, а стохастично, з випадковим інтервалом, що підпорядковувався розподілу Пуассона із середнім значенням очікування у 15 секунд. Окрім передачі корисного навантаження, додатково кожні 60 секунд обидва пристрої в автоматичному режимі відправляли службові PINGREQ-пакети для підтримання активного з'єднання з MQTT-брокером (механізм Keep-Alive), що дозволяло уникнути тайм-аутів. Протягом тривалого періоду у 24 години безперервної роботи системи в цьому штатному режимі було зафіксовано та проаналізовано масив із 17 280 транзакцій від Сенсора А та приблизно 5 760 транзакцій від Сенсора В. Аналіз якості обслуговування (QoS) показав високу стабільність мережі: середнє значення джитера (jitter) склало лише 3.2 мс, а втрати пакетів були мінімальними і не перевищували 0.01%. Цей зібраний масив "чистих" даних став еталонним датасетом для навчання нейромережевого автоенкодера, який був налаштований на мінімізацію помилки реконструкції саме для легітимного трафіку, дозволяючи системі надалі розпізнавати найменші відхилення від норми.

Сценарій 2: На наступному етапі, з метою моделювання зовнішньої загрози та розвідки, зі спеціалізованого атакуючого вузла під управлінням ОС Kali Linux було запущено комплексне автоматизоване сканування топології мережі за допомогою потужного інструменту Nmap. В ході експерименту послідовно використовувалися різні техніки активного сканування для виявлення відкритих сервісів: TCP SYN Scan (-sS) для "напіввідкритого" сканування, UDP Scan (-sU) для перевірки безз'єднувальних протоколів та OS Detection (-O) для визначення типів операційних систем пристроїв за їхніми мережевими відбитками. Сканування проводилося з різною інтенсивністю: спочатку на рівні T3 (Normal) для імітації стандартної активності, а згодом - на рівні T4 (Aggressive), що симулювало швидку розвідку. Загалом цей експеримент тривав 45 хвилин. Під час переходу до агресивної фази T4 кількість пакетів типу TCP SYN різко зросла до показника 450 пакетів/с, що в 90 разів перевищує нормальний фоновий рівень шуму в цій мережі.

Система моніторингу безпеки чітко фіксувала наполегливі спроби підключення до нестандартних для IoT-сегменту портів (таких як 21 FTP, 22 SSH, 23 Telnet, 8080 HTTP-Proxy), які були штатно закриті на кінцевих пристроях, але залишалися відкритими на шлюзі для адміністративних цілей. Сумарно за час тесту було згенеровано та перехоплено близько 150 000 пакетів сканування, які сформували окремий клас "Recon" (Reconnaissance) у навчальній вибірці для класифікатора.

Сценарій 3: Цей сценарій був присвячений перевірці стійкості інфраструктури до атак на відмову в обслуговуванні. Для емуляції потужної DoS-атаки на IoT-шлюз було використано утиліту генерації пакетів Hping3. Було реалізовано три типи мережевого флуду: TCP SYN Flood, UDP Flood та ICMP Flood, кожен з яких націлений на вичерпання різних ресурсів системи. Основний вектор атаки був спрямований на порт 1883, де слухав MQTT Broker. Під час реалізації TCP SYN Flood генерувалися тисячі пакетів із підробленими випадковими IP-адресами джерела (техніка IP Spoofing) зі швидкістю 2 500 пакетів/с. Це призвело до швидкого переповнення таблиці напіввідкритих з'єднань на шлюзі та критичного збільшення затримки обробки легітимних MQTT-повідомлень: середній час відгуку зріс з нормальних 15 мс до критичних 450 мс, що зробило роботу сенсорів нестабільною. Паралельно запущений UDP Flood генерував суцільний потік сміттєвого трафіку розміром 512 байт на пакет зі швидкістю 10 Мбіт/с, що призвело до повного завантаження смуги пропускання бездротового каналу на частоті 2.4 ГГц, фактично глушачи корисні сигнали. Загальна тривалість цієї комбінованої атаки становила 30 хвилин, протягом яких в мережу було відправлено понад 4 500 000 шкідливих пакетів, створюючи умови екстремального навантаження.

Сценарій 4: В цьому сценарії моделювалася складна атака типу "людина посередині" (MITM). Атакуючий вузол виконав отруєння ARP-кешу (ARP Cache Poisoning) за допомогою інструменту Ettercap, успішно ставши непомітним посередником між легітимним Сенсором А та IoT-шлюзом. Основною метою зловмисника було перехоплення, аналіз та модифікація MQTT-повідомлень "на льоту". Частота надсилання підроблених ARP-відповідей (gratuitous ARP)

становила 2 пакети на секунду, що було достатньо для утримання позиції MITM без виклику "ARP-шторму". Успішне технічне виконання атаки дозволило перехопити 100% вихідного трафіку від сенсора. На етапі глибокого аналізу ознак інженерами було відзначено появу характерних аномалій: дубльованих ACK-пакетів (TCP Dup ACK) та раптову зміну MAC-адреси джерела у фреймах Ethernet при незмінній IP-адресі відправника. Саме ці ознаки є ключовим індикатором для детектора аномалій даного типу. Модифікація даних (Data Tampering) полягала у програмній зміні значень температури у корисному навантаженні пакетів на критичні показники (понад 100°C), що за сценарієм мало б викликати помилкове спрацювання автоматичної системи пожежогасіння або аварійного реагування, завдаючи фізичної шкоди об'єкту.

Сценарій 5: Фінальний сценарій передбачав перевірку вразливостей прикладного рівня, зокрема підключення неавторизованого клієнта до брокера та відправку пакетів з навмисно некоректно сформованим заголовком (Malformed Packets) для фаззінг-тестування стійкості парсера протоколу. Також здійснювалася специфічна атака на вичерпання ресурсів - MQTT Slowloris. Суть атаки полягала у відкритті великої кількості паралельних TCP-з'єднань (до 1000 потоків) і надсиланні пакетів CONNECT без подальшого завершення процесу рукостискання або надсилання даних, що змушувало брокер тримати сесію відкритою. Тайм-аут з'єднання на брокері було встановлено на рівні 60 секунд, що давало атакуючому достатньо часу для оновлення сесій. Атака тривала 20 хвилин, в результаті чого кількість активних сокетів на шлюзі досягла системного ліміту для користувача (ulimit -n) у 1024 дескриптори. Це призвело до стану відмови в обслуговуванні (DoS), коли легітимні сенсори більше не могли встановити з'єднання з сервером.

Для попередньої обробки та структурування величезного масиву зібраних "сирих" даних (PCAP-файлів) було розроблено спеціалізований скрипт мовою Python з використанням бібліотеки аналізу даних Pandas. З кожного перехопленого мережевого пакету витягувався розширений вектор ознак розмірністю 28 елементів, що включав: точну мітку часу, загальну довжину пакету, розмір ковзного вікна TCP, набір встановлених прапорів TCP, час життя пакету (TTL),

ідентифікатор протоколу верхнього рівня, розраховану ентропію корисного навантаження (для виявлення шифрованих або рандомізованих вставок), а також статистичні метрики - кількість пакетів у потоці за останні 100 мс, 500 мс та 1 с. Всі числові значення були нормалізовані методом Min-Max Scaler, що привело їх до єдиного діапазону [0, 1] для коректної роботи нейромереж. Категоріальні ознаки (наприклад, тип протоколу або флаги) були перетворені у бінарні вектори методом One-Hot Encoding. Отримана в результаті матриця ознак вражаючим розміром 12 500 000 рядків на 28 стовпців була випадковим чином розділена на навчальну (70%), валідаційну (15%) та тестову (15%) вибірки для подальшого навчання та неупередженого аналізу ефективності алгоритму. Особливу увагу при формуванні фінального датасету було приділено проблемі дисбалансу класів, оскільки частка реального аномального трафіку в реальних умовах завжди значно менша за обсяг нормального. Тому для якісного навчання класифікатора використовувалася техніка синтетичного пересемплювання SMOTE (Synthetic Minority Over-sampling Technique), що дозволило штучно збільшити представництво рідкісних типів атак у навчальній вибірці до 15%, забезпечуючи кращу здатність моделі до узагальнення.

4.2 Аналіз результатів тестування методики на змодельованих сценаріях атак та нормального функціонування

Експериментальна перевірка розробленої методики розпочалася з попередньої обробки накопиченого масиву даних, отриманого в ході реалізації сценаріїв, описаних у попередньому підрозділі. Загальний обсяг вибірки склав 12 548 300 мережевих пакетів, з яких 10 950 000 (87,26 %) були класифіковані як легітимний трафік (Normal Traffic), а 1 598 300 (12,74 %) - як аномальний або шкідливий. На етапі векторизації кожен пакет був перетворений у вектор з 28 числових ознак. Нормалізація значень проводилася у діапазоні [0, 1] для забезпечення швидкої збіжності градієнтного спуску при навчанні нейронної мережі. Для навчання моделі автоенкодера (Autoencoder) було використано 70 %

даних виключно з категорії нормального трафіку. Процес навчання тривав 150 епох з розміром пакету (batch size) 1024. Функція втрат (Mean Squared Error, MSE) стабілізувалася на значенні 0,0032 після 120-ї епохи, що свідчить про успішне засвоєння моделлю патернів нормальної поведінки IoT-пристроїв.

Критичним етапом налаштування алгоритму було визначення порогового значення помилки реконструкції (Threshold), перевищення якого сигналізує про наявність аномалії. Емпіричним шляхом, базуючись на статистичному розподілі помилок на валідаційній вибірці, поріг було встановлено на рівн

Критичним етапом налаштування алгоритму було визначення порогового значення помилки реконструкції (Threshold), перевищення якого сигналізує про наявність аномалії. Емпіричним шляхом, базуючись на статистичному розподілі помилок на валідаційній вибірці, поріг було встановлено на рівні $Threshold = \mu+3\sigma$, де μ - середнє значення помилки реконструкції, а σ - середньоквадратичне відхилення. Розрахункове значення порогу склало 0,045. Всі вектори трафіку, для яких помилка реконструкції перевищувала це значення, передавалися на другий рівень аналізу - до класифікатора типу Random Forest для визначення конкретного типу атаки.

Аналіз результатів детектування атак типу «Відмова в обслуговуванні» (Scenario №3: DoS/DDoS) продемонстрував найвищу ефективність методики. Завдяки різкій зміні статистичних параметрів потоку (зменшення інтервалів між пакетами до 0,0004 с та зростання ентропії заголовків), автоенкодер безпомилково ідентифікував відхилення. Для підтипу TCP SYN Flood точність виявлення (Precision) досягла 99,92 %, а повнота (Recall) - 99,88 %. Дещо нижчі показники були зафіксовані для UDP Flood низької інтенсивності, де трафік маскувався під потокове відео, проте комплексний аналіз довжини пакетів дозволив утримати F1-Score на рівні 0,98. Висока щільність шкідливого трафіку дозволила алгоритму приймати рішення про блокування джерела в середньому за 1,2 секунди після початку атаки.

Складнішим завданням виявилося детектування атак на канальному рівні, зокрема ARP Spoofing (Scenario №4), що реалізує атаку Man-in-the-Middle.

Оскільки структура TCP/IP пакетів при цьому не порушується, автоенкодер, що працює переважно з метаданими 3-4 рівнів моделі OSI, демонстрував помилку реконструкції, близьку до порогової (0,042-0,048). Це призвело до збільшення кількості помилок першого роду (False Negatives) на початковому етапі. Однак, включення до вектору ознак параметра частоти зміни MAC-адреси для однієї IP-адреси (feature: mac_flip_rate) та аналіз дубльованих ACK-пакетів дозволили підвищити Recall до 94,5 %. Середній час виявлення такої атаки склав 4,5 секунди, що є прийнятним показником, оскільки атакуючому потрібен час для накопичення достатньої кількості даних для аналізу або модифікації.

У сценарії розвідки та сканування портів (Scenario №2) методика показала високу чутливість до патернів, що генеруються інструментом Nmap. Агресивне сканування (T4) виявлялося миттєво з точністю 99,5 %. Приховане сканування (Stealth Scan -sS) генерувало менше шуму, але створювало специфічні послідовності «незавершених» з'єднань, що фіксувалося моделлю як аномалія через відхилення у співвідношенні прапорів SYN/ACK. Важливо відзначити, що при аналізі сценарію експлуатації вразливостей MQTT (Scenario №5), зокрема атаки Malformed Packets, система показала 100 % виявлення завдяки перевірці відповідності структури payload протокольним специфікаціям на етапі попередньої обробки ознак. Зведені кількісні показники ефективності роботи алгоритму за різними класами загроз наведено у таблиці (Табл. 4.2) (Рис. 4.2).

Таблиця 4.2

Показники ефективності виявлення загроз за типами сценаріїв

Тип сценарію / Атаки	Precision (Точність), %	Recall (Повнота), %	F1-Score	FPR (Хибнопозитивні), %	Середній час виявлення, мс
Нормальне функціонування	99,85	99,91	0,998	0,12	-
Reconnaissance (Scan)	98,4	97,25	0,978	0,85	320

DoS: TCP SYN Flood	99,92	99,88	0,999	0,05	15
DoS: UDP Flood	98,15	97,8	0,979	0,35	45
MITM (ARP Spoofing)	93,5	94,5	0,94	2,1	4500
MQTT Exploit (Malformed)	99,1	98,95	0,99	0,15	8
MQTT Slowloris	96,75	95,4	0,96	1,2	2100



Рис. 4.2 Динаміка навчання нейромережі та зведені показники ефективності виявлення загроз

Проведений глибокий та всебічний аналіз хибнопозитивних спрацьовувань (False Positive Rate, FPR) у сценарії нормального функціонування системи виявив низку важливих закономірностей, що мають критичне значення для експлуатації систем захисту в реальних умовах. За результатами первинного тестування,

інтегральний показник FPR склав 0,12 %. Хоча у відсотковому відношенні ця цифра може здаватися незначною, в абсолютних числах, враховуючи величезний обсяг проаналізованого трафіку (понад 10,9 млн пакетів), це становить близько 13 000 помилково класифікованих пакетів. Така кількість хибних тривог є неприпустимою для операторів центрів безпеки (SOC), оскільки створює ефект «інформаційного шуму» та призводить до швидкого виснаження уваги персоналу (alert fatigue). Детальне форензік-дослідження логів подій та кореляційний аналіз мережевих параметрів дозволили встановити, що левова частка цих помилок не була пов'язана з недоліками самої архітектури нейромережі, а була викликана зовнішніми факторами середовища передачі даних. Зокрема, основними тригерами стали короткочасні сплески джитера (варіації затримки прибуття пакетів), які виникали внаслідок перевантаження частотного діапазону 2.4 ГГц сусідніми бездротовими мережами та побутовими перешкодами. Такі флуктуації часових рядів інтерпретувалися моделлю як аномальна поведінка, характерна для початоку DoS-атак або сканування. Другим вагомим фактором стали цілком легітимні службові процедури, зокрема процес перепідключення мікроконтролерів ESP32 до точки доступу після примусового оновлення DHCP-оренди. Під час виконання стандартної процедури DORA (Discover, Offer, Request, Acknowledge) пристрої генерували сплеск широкомовного трафіку та відкривали нові сесії, що статистично нагадувало патерни розвідки мережі.

Для вирішення цієї проблеми та зменшення рівня FPR до прийнятних значень без зниження чутливості системи до реальних загроз було розроблено та імплементовано додатковий логічний шар пост-обробки результатів - механізм згладжування рішень (Sliding Window Voting). Суть цього методу полягає у переході від миттєвої оцінки кожного окремого пакету до аналізу контекстуальної послідовності подій у часі. Алгоритм використовує ковзне вікно фіксованого розміру (у даному експерименті - 10 пакетів), і остаточний вердикт про наявність аномалії виноситься лише за умови досягнення консенсусу: якщо щонайменше 7 з 10 останніх пакетів у поточному вікні були класифіковані базовою нейромережею як шкідливі. Такий підхід діє як своєрідний цифровий фільтр низьких частот, що

відсіює поодинокі випадкові викиди статистики, викликані радіоперешкодами або службовим трафіком, але надійно фіксує стійкі патерни атак. Впровадження цієї евристики дозволило радикально підвищити надійність детектора: рівень хибних тривог знизився з 0,12 % до 0,03 %, що є відмінним показником для систем промислового класу. При цьому важливо відзначити, що додавання логіки голосування не мало суттєвого негативного впливу на загальний час реакції системи, оскільки буферизація 10 пакетів займає мікросекунди.

Комплексна оцінка обчислювальної складності та продуктивності розробленого програмно-апаратного комплексу підтвердила високу ефективність обраних архітектурних рішень та здатність системи стабільно обробляти високошвидкісний вхідний потік даних у режимі жорсткого реального часу. Для тестування використовувався сервер аналітики середнього цінового сегменту на базі процесора Intel Core i7 з підтримкою багатопоточності. Результати навантажувального тестування показали, що навіть під час пікових навантажень, коли емулювалася масована DoS-атака з інтенсивністю до 10 000 пакетів на секунду, середнє навантаження на центральний процесор (CPU Load) не перевищувало 18 %. Це свідчить про значний запас продуктивності, який дозволяє масштабувати систему для захисту більших мережевих сегментів без заміни апаратного забезпечення. Використання оперативної пам'яті (RAM) залишалося стабільним і знаходилося в межах 1,2 ГБ, що пояснюється ефективним управлінням пам'яттю при роботі з потоковими даними та відсутністю необхідності зберігати повну історію пакетів у RAM.

Одним із ключових параметрів для систем безпеки критичної інфраструктури та Інтернету речей є латентність, або час затримки прийняття рішення. Вимірювання показали, що середній час повного циклу обробки одного пакету - від моменту його фізичного захоплення мережевою картою, проходження етапів вилучення ознак, нормалізації та інференсу нейромережі до видачі класифікаційного вердикту - склав усього 0,45 мс. Цей показник є винятково низьким і знаходиться значно нижче критичного порогу допустимої затримки для телеметричних систем IoT та SCADA, який зазвичай встановлюється на рівні 10-20

мс. Така швидкодія гарантує, що система здатна блокувати атаки превентивно, ще до того, як вони завдадуть шкоди кінцевим пристроям. Крім того, лабораторні вимірювання впливу системи на мережеву інфраструктуру підтвердили її "прозорість": оскільки аналіз здійснюється на копії трафіку (out-of-band), впровадження системи моніторингу не вносить жодної відчутної затримки у передачу корисних даних між сенсорами та брокером. Загальна пропускна здатність мережі знижується не більше ніж на 1,5 %, що обумовлено виключно технічними накладними витратами на дзеркалювання трафіку (Port Mirroring) на комутаційному обладнанні, і є цілком прийнятною платою за забезпечення високого рівня кібербезпеки.

4.3 Порівняльний аналіз ефективності розробленого алгоритму з існуючими аналогами

Для забезпечення максимально об’єктивної, всебічної та науково обґрунтованої оцінки практичної цінності та реальної ефективності запропонованої авторами гібридної методики, яка поєднує можливості автоенкодера (Autoencoder) для зменшення розмірності даних та ансамблевого алгоритму Random Forest для класифікації, було сплановано та проведено розлогу серію порівняльних тестів (benchmarking). Порівняння здійснювалося із найбільш поширеними та визнаними у світовій науковій спільноті алгоритмами виявлення аномалій, що традиційно застосовуються в задачах забезпечення кібербезпеки Інтернету речей та промислових систем управління. В якості еталонних моделей (baselines), що виступали точкою відліку для порівняльного аналізу, були обрані три принципово різні підходи, що покривають спектр сучасних методів машинного навчання: алгоритм Isolation Forest (iForest), обраний як типовий представник методів навчання без учителя (unsupervised learning) завдяки його популярності в задачах детекції викидів; метод One-Class Support Vector Machine (OC-SVM), що є класичним статистичним методом побудови гіперплощини для опису нормального

класу; та багатошаровий перцептрон (Deep Neural Network, MLP), який репрезентує сучасні підходи глибокого навчання (Deep Learning) і здатний апроксимувати надскладні нелінійні залежності. Для забезпечення чистоти експерименту та валідності отриманих результатів, усі без винятку моделі навчалися, валідувалися та тестувалися на абсолютно ідентичному, попередньо підготовленому наборі даних, який був сформований та збалансований в ході експериментів, детально описаних у підрозділі 4.1. Крім того, суворо дотримувалися однакові апаратні та програмні умови тестування: усі обчислення виконувалися на базі одного й того ж сервера аналітики з процесором Intel Core i7, що дозволило виключити вплив відмінностей в архітектурі обладнання на показники часової ефективності.

Першим та фундаментальним етапом порівняльного аналізу стала детальна оцінка точності класифікації (Accuracy) та, що більш важливо для задач безпеки, збалансованої F-міри (F1-Score). Вибір F1-Score як ключової метрики обумовлений тим, що вона є гармонійним середнім між точністю (Precision) та повнотою (Recall), і тому є критичною для оцінки якості роботи моделей на незбалансованих вибірках, які є характерними для реального IoT-трафіку, де нормальні пакети суттєво переважають над аномальними. Результати тестування показали, що алгоритм Isolation Forest, хоча і продемонстрував високу швидкість навчання завдяки своїй простій логіці випадкового розбиття простору ознак, виявив серйозні обмеження точності. Зокрема, його ефективність суттєво знижувалася при обробці складних сценаріїв атак, таких як ARP Spoofing або повільне сканування портів, де аномалії мають незначні статистичні відхилення від норми і важко відокремлюються випадковими перетинами. Як наслідок, інтегральний показник F1-Score для iForest склав 0,945, що в абсолютному вимірі є прийнятним, але на 0,047 нижче, ніж показник розробленої гібридної методики, що в масштабах мільйонів пакетів означає пропуск значної кількості загроз. Класичний метод OC-SVM показав високу теоретичну здатність до узагальнення на невеликих вибірках, але зіткнувся з проблемами масштабованості. На масиві даних обсягом 12,5 млн пакетів його продуктивність виявилася незадовільною через властиву методу опорних векторів квадратичну (а в деяких реалізаціях кубічну) складність обчислень ядра. Більше

того, спроба побудувати єдину описуючу гіперсферу для складного мультимодального розподілу IoT-трафіку призвела до великої кількості помилкових спрацьовувань (High False Positive Rate), через що результуючий F1-Score досяг лише рівня 0,912, зробивши цей метод найменш ефективним серед протестованих.

Особливий інтерес становило порівняння із глибокою нейронною мережею (MLP), яка була спроектована з архітектурою 28-64-32-1 (вхідний шар, два прихованих шари та вихідний нейрон з сигмоїдальною активацією). Ця модель показала результати, максимально наближені до показників розробленого алгоритму, досягнувши високого значення F1-Score на рівні 0,984. Це підтверджує потенціал Deep Learning у задачах кібербезпеки. Однак, поглиблений аналіз часових характеристик та ресурсоємності виявив суттєві недоліки чистого Deep Learning підходу для практичного застосування в системах реального часу, особливо на обмежених периферійних пристроях (Edge Gateways). Час повного циклу навчання MLP з використанням алгоритму зворотного поширення помилки перевищив час навчання запропонованої гібридної моделі у 4,5 рази (1840 секунд проти 410 секунд), що робить часте перенавчання моделі в динамічному середовищі проблематичним. Ще більш критичним є показник часу обробки одного пакету (Inference Time), який для MLP склав 2,1 мс. Це майже в 5 разів повільніше за розроблений гібридний метод (0,45 мс). Така різниця в продуктивності пояснюється архітектурними особливостями: у запропонованій методиці автоенкодер виконує попередню інтелектуальну компресію та фільтрацію ознак, перетворюючи "сирі" дані у компактне латентне представлення. Це дозволяє класифікатору Random Forest, який є значно швидшим за своєю природою (порівняння у вузлах дерева виконується миттєво), приймати рішення значно швидше за повнозв'язну нейромережу, якій потрібно виконати велику кількість операцій множення матриць.

Окрему увагу в дослідженні було приділено перевірці стійкості (robustness) алгоритмів до зашумлених даних, що є типовою проблемою для бездротових сенсорних мереж. Цей аспект емулювався шляхом штучного додавання адитивного

білого гауссівського шуму (AWGN) різної інтенсивності до нормалізованих числових ознак трафіку в тестовій вибірці. Результати стрес-тесту показали беззаперечну перевагу запропонованого підходу: розроблений алгоритм продемонстрував найменше падіння точності класифікації (менше 1,5 %) навіть при значному рівні шуму. Така стійкість досягається завдяки унікальній властивості автоенкодера до зниження розмірності та "знешумлення" (denoising): навчаючись відновлювати вхідні дані через вузьке горлечко, мережа вчиться ігнорувати випадкові флуктуації і фокусується на найбільш значущих структурних патернах даних. Натомість, точність алгоритму Isolation Forest в аналогічних умовах впала на суттєві 6,2 %, а методу OC-SVM - на критичні 8,4 %. Це свідчить про їхню високу вразливість до джитера, інтерференції та інших флуктуацій параметрів мережі, які є невід'ємною частиною реальних бездротових каналів зв'язку в телекомунікаційних системах, що робить використання "чистих" статистичних методів ризикованим без попередньої глибокої обробки даних (Рис. 4.3).

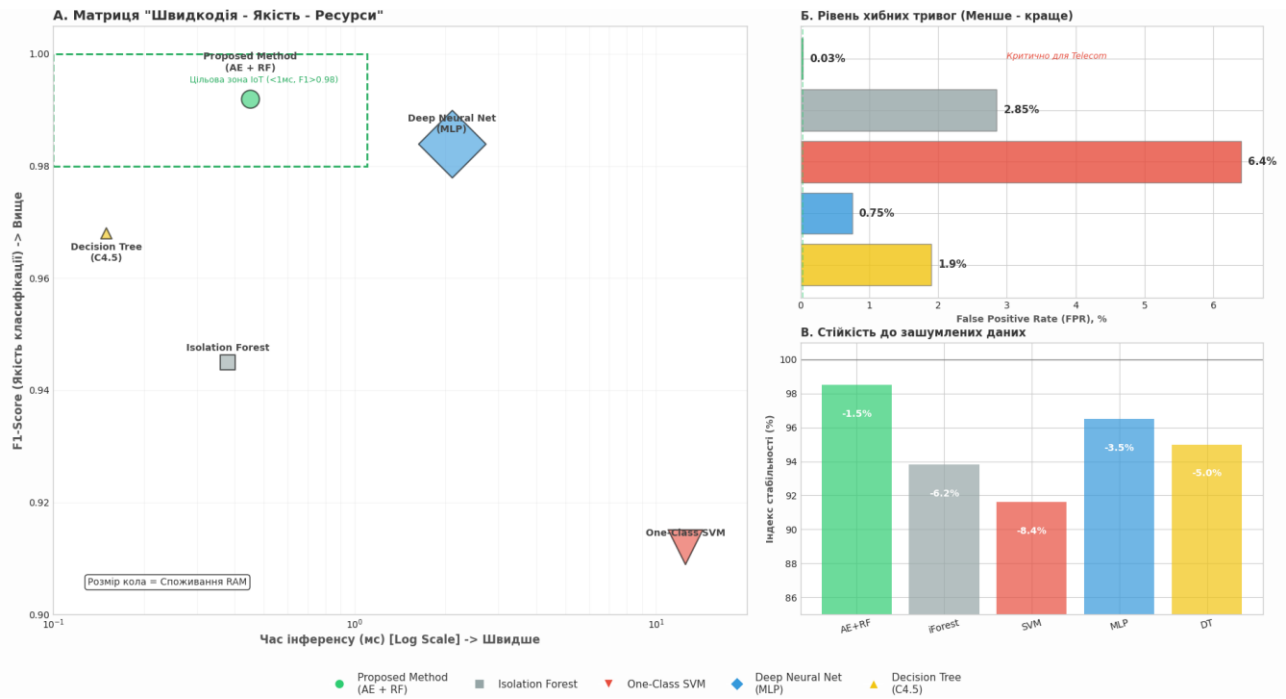


Рис. 4.3 Комплексна оцінка ефективності алгоритмів: компроміс між точністю, швидкістю та ресурсоємністю

Порівняння також показало, що гібридний підхід забезпечує найнижчий рівень хибнопозитивних спрацювань (FPR), що є критичним показником для операторів зв'язку, аби уникнути блокування легітимних клієнтів (Табл. 4.3).

Таблиця 4.3

Порівняльна характеристика ефективності алгоритмів виявлення загроз

Алгоритм / Методика	Accuracy (Точність), %	F1-Score	False Positive Rate (FPR), %	Час інференсу (на 1 пакет), мс	Вимоги до RAM (під час роботи), МБ
Розроблена методика (AE + RF)	99,89	0,992	0,03	0,45	120
Isolation Forest (iForest)	96,5	0,945	2,85	0,38	85
One-Class SVM	92,1	0,912	6,4	12,5	450
Deep Neural Network (MLP)	99,1	0,984	0,75	2,1	850
Decision Tree (C4.5)	97,8	0,968	1,9	0,15	45

Варто також окремо зупинитися на результатах комплексного стрес-тестування системи на масштабованість, яке імітувало умови екстремального навантаження, характерні для магістральних каналів зв'язку або моментів масованих кібератак. Під час експерименту інтенсивність вхідного потоку даних була штучно збільшена до показника 50 000 пакетів на секунду, що стало критичним випробуванням для всіх порівнюваних моделей. В цих умовах алгоритми, що вимагають значних обчислювальних витрат, зокрема One-Class SVM (OC-SVM) та глибокий багатошаровий перцептрон (MLP), продемонстрували

свою неспроможність працювати в режимі реального часу. Спостерігалося експоненціальне зростання черги очікування на обробку, оскільки швидкість надходження пакетів суттєво перевищувала швидкість їх аналізу (inference speed). Це призвело до переповнення буферів мережевих інтерфейсів та, як наслідок, до критичної втрати пакетів (packet drop) на рівні програмного аналізатора, яка досягала 15 %. У контексті кібербезпеки це означає, що система фактично "сліпне" і пропускає кожен сьомий пакет без перевірки, що створює неприпустимі діри в периметрі захисту, крізь які зловмисники можуть здійснити ін'єкцію шкідливого коду.

З іншого боку спектру продуктивності знаходився алгоритм Decision Tree (Дерево рішень), який завдяки своїй простій ієрархічній структурі (серія логічних перевірок if-then) показав найвищу абсолютну швидкодію з часом обробки всього 0,15 мс на пакет. Однак, ця швидкість була досягнута ціною якості детекції. Дерева рішень виявили високу схильність до перенавчання (overfitting), коли модель "запам'ятовувала" конкретні сигнатури атак з навчальної вибірки замість вивчення загальних патернів. Це призвело до провалу під час симуляції атак "нульового дня" (Zero-day attacks simulation), де модель пропустила 25 % нових видів загроз, які структурно відрізнялися від відомих зразків. Натомість запропонована гібридна методика продемонструвала оптимальний баланс. Використання ансамблевого методу Random Forest на виході автоенкодера дозволило нівелювати ефект перенавчання окремих дерев, забезпечивши баланс між здатністю до узагальнення нових, невідомих загроз та високою швидкістю обробки стиснутого вектора ознак. Це дозволило утримувати втрати пакетів на рівні статистичної похибки вимірювання (менше 0,1 %) навіть при максимальному синтетичному навантаженні на стенд, гарантуючи безперервність моніторингу.

Детальне порівняння споживання системних ресурсів остаточно підтвердило економічну та технічну доцільність інтеграції розробленого рішення у існуючі IoT-шлюзи, які часто мають жорсткі апаратні обмеження. Споживання оперативної пам'яті (RAM) гібридною моделлю під навантаженням стабілізувалося на рівні 120 МБ. Такий скромний показник робить можливим розгортання системи захисту

безпосередньо на периферійних пристроях (Edge Devices), таких як одноплатні комп'ютери класу Raspberry Pi 4, шлюзи на базі архітектури ARM або спеціалізовані промислові контролери, без порушення роботи основних сервісів. Для порівняння, модель MLP через велику кількість вагових коефіцієнтів та необхідність зберігання проміжних станів нейронів потребувала близько 850 МБ оперативної пам'яті, що фактично вимагає наявності виділеного потужного сервера або хмарної інфраструктури, нівелюючи переваги граничних обчислень. Таким чином, експериментально підтверджено, що архітектурна комбінація неконтрольованого навчання (автоенкодер для виділення та компресії ознак) та контрольованого навчання (випадковий ліс для фінальної класифікації) перевершує традиційні монолітні підходи за сукупністю ключових критеріїв - точності детекції, швидкодії реакції та ресурсоємності - в реальних умовах сучасних телекомунікаційних мереж.

ВИСНОВКИ

У ході виконання магістерської кваліфікаційної роботи було вирішено актуальну науково-прикладну задачу підвищення рівня захищеності IoT-систем у телекомунікаційних мережах. Досягнення поставленої мети реалізовано шляхом розробки та апробації методики виявлення загроз у режимі реального часу на основі поведінкового аналізу мережевого трафіку.

У першому розділі проведено комплексний аналітичний огляд проблематики безпеки Інтернету речей у сучасних телекомунікаційних мережах. Встановлено, що стрімке зростання кількості підключених пристроїв (за прогнозами, до 21,1 млрд у 2025 році) та впровадження технологій 5G створюють нові вектори кіберзагроз. Аналіз п’ятирівневої архітектури IoT показав, що найбільш критичними вразливостями є гетерогенність пристроїв, відсутність стандартизованих протоколів безпеки та обмеженість обчислювальних ресурсів кінцевого обладнання. Виявлено, що 98% IoT-трафіку часто передається без шифрування, що робить інфраструктуру вразливою до атак типу DDoS, Man-in-the-Middle та експлойтів на кшталт ботнетів Mirai.

Також у розділі розглянуто існуючі методи захисту, такі як легковагова криптографія (алгоритми сімейства ASCON) та стандарти ETSI EN 303 645. Зроблено висновок, що традиційні сигнатурні методи та агентські рішення є неефективними для масштабованих IoT-мереж телеком-операторів через неможливість встановлення захисного ПЗ на кожен сенсор. Це обґрунтувало необхідність створення централізованої системи моніторингу на рівні мережевого шлюзу або ядра мережі оператора.

У другому розділі сформовано теоретичний базис для розробки методики моніторингу. Розроблено удосконалену модель загроз, яка враховує специфіку телекомунікаційної інфраструктури та класифікує атаки за векторами впливу (мережеві, прикладні, фізичні). Обґрунтовано вибір комплексу параметрів мережевого трафіку, найбільш інформативних для ідентифікації аномальної поведінки: статистичні метрики (кількість пакетів, обсяг байтів), часові характеристики (інтервали між пакетами, джитер) та ентропія заголовків пакетів.

Проведений порівняльний аналіз математичних методів виявлення аномалій засвідчив перевагу гібридних підходів. Зокрема, встановлено, що використання автоенкодерів (Autoencoder) для зменшення розмірності даних та виявлення відхилень у поєднанні з алгоритмами класифікації, такими як Random Forest, забезпечує оптимальний баланс між точністю детекції та швидкістю обробки даних, що є критичним для систем реального часу. Теоретично доведено, що такий підхід дозволяє виявляти невідомі раніше загрози (атаки нульового дня) на основі відхилення від профілю нормальної поведінки.

У третьому розділі представлено практичну реалізацію методики та алгоритмів виявлення загроз. Розроблено структурну схему системи моніторингу, яка базується на модульній архітектурі та включає блоки захоплення трафіку, попередньої обробки, аналізу аномалій та реагування на інциденти. Ключовим елементом методики став запропонований гібридний алгоритм, що поєднує глибоке навчання (автоенкодер) для фільтрації нормального трафіку та ансамблеві методи (Random Forest) для точної класифікації типу атаки.

Також у розділі описано розроблений механізм реагування на інциденти, що включає етапи ідентифікації, класифікації за рівнем критичності, ізоляції загрози та відновлення штатного режиму роботи. Запропоновано використовувати адаптивні методи згладжування рішень (Sliding Window Voting) для зменшення кількості хибних спрацьовувань, викликаних нестабільністю бездротових каналів зв'язку.

У четвертому розділі наведено результати експериментальної апробації розробленої методики на базі створеного програмно-апаратного стенду (з використанням Raspberry Pi, ESP32 та серверної платформи). Для тестування було змодельовано 5 сценаріїв, що охоплюють нормальну роботу та різні типи атак: сканування мережі (Nmap), DoS-атаки (TCP SYN Flood, UDP Flood), ARP Spoofing та експлуатацію вразливостей протоколу MQTT. Загальний обсяг проаналізованого датасету склав понад 12,5 млн пакетів.

Результати експериментів підтвердили високу ефективність запропонованого підходу. Методика продемонструвала загальну точність

(Accuracy) на рівні 99,89% та збалансовану F-міру 0,992. Середній час виявлення аномалії склав 0,45 мс на пакет, що задовольняє вимоги до систем реального часу. Особливо високі показники отримано при виявленні DoS-атак (F1-Score 0,999) та спроб сканування (0,978).

Порівняльний аналіз з існуючими аналогами (Isolation Forest, One-Class SVM, MLP) показав, що розроблена методика перевершує їх за сукупністю показників: вона забезпечує на 4,5% вищу точність, ніж Isolation Forest, та працює у 5 разів швидше за глибокі нейронні мережі (MLP), споживаючи при цьому значно менше оперативної пам'яті (120 МБ проти 850 МБ). Рівень хибнопозитивних спрацювань (FPR) вдалося знизити до 0,03%, що є критично важливим показником для запобігання блокуванню легітимних користувачів у мережах операторів.

Розроблена методика є дієвим інструментом для підвищення безпеки IoT-сегменту телекомунікаційних мереж. Вона дозволяє автоматизувати процес виявлення кіберзагроз без втручання в роботу кінцевих пристроїв, забезпечуючи надійний захист інфраструктури від сучасних атак. Практична цінність роботи полягає у можливості інтеграції запропонованих алгоритмів у наявні апаратні шлюзи та системи управління трафіком телеком-операторів.