

ОГЛЯД ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ ДЛЯ МОНІТОРИНГУ ТА АУДИТУ БЕЗПЕКИ ІОТ-ПРИСТРОЇВ

Українець Д.С., науковий керівник Коваленко О.Є.

Парадигма Інтернету речей (надалі IoT) змінює обчислювальні системи сьогодення, формуючи нову еру, де фізичні об'єкти, які оснащені сенсорами, мікроконтролерами та мережевими модулями, співіснують у цифровому просторі. Такі пристрої беруть активну участь в обміні інформацією, збираючи, обробляючи та транслюючи дані у режимі реального часу. Але разом з тим, швидке розширення кількості IoT-пристроїв супроводжується зростанням викликів кібербезпеці. Вразливості в програмному забезпеченні (надалі ПЗ), використання старих протоколів, відсутність шифрування, недостатня аутентифікація та недоліки в оновленнях ПЗ це є типовими проблемами, що відкривають шлях для різноманітного спектру атак різної складності. Нажаль, більшість таких пристроїв розробляються з мінімальними вимогами до безпеки, адже їх основна мета – надання основної функціональності за низькою ціною, що ускладнює впровадження традиційних методів захисту інформації. Таким чином, упродовж останніх років кількість кібератак на IoT-пристрої стрімко збільшилась та зберігає цю тенденцію досі. Наприклад, лише у 2022 році було зафіксовано понад 112 мільйонів таких інцидентів у всьому світі [1].

Відповіддю на такі виклики розробляються програмні інструменти моніторингу та аудиту середовищ IoT, що дають змогу здійснювати пасивний та активний контроль мережових подій, виявляти аномальну поведінку пристроїв, фіксувати спроби проникнення, порушення політики доступу, витоки інформації або збій компонентів системи. Таке ПЗ є проміжною ланкою між фізичною інфраструктурою (сенсори, пристрої збору даних) і логічним рівнем управління (сервери обробки, адміністративні панелі, хмарні сервіси), забезпечуючи безперервний моніторинг, аналіз і реагування. А до основних функцій можна віднести наступне: збирання телеметрії, фільтрація та нормалізація даних, формування журналів, кореляція подій, виявлення загроз за сигнатурами або моделями поведінки, автоматичне сповіщення або блокування підозрілої активності; а з врахуванням стрімкого розвитку сфери штучного інтелекту та машинного навчання, інтеграція таких елементів в ПЗ позитивно впливає на ефективність запобігання та виявленню загроз [2].



Рисунок 1 – Архітектура ПЗ для моніторингу та аудиту IoT-пристроїв

Архітектура такого ПЗ (див. рис. 1), зазвичай, складається з п'яти основних рівнів: збір даних (це агенти на пристроях або моніторинг мережевого трафіку), обробка (це парсинг, нормалізація, агрегація), аналітика (це використання правил, машинного навчання, сигнатур), реагування та захист (це створення сповіщень, інтеграція з системами управління інцидентами) та взаємодія з користувачем або адміністратором.

Такий підхід дозволяє масштабувати систему (що є важливим в контексті IoT), адаптувати її до гібридного середовища, інтегрувати з хмарними рішеннями, контейнерами або серверною інфраструктурою без необхідності зміни функціонування апаратного забезпечення.

Практики безпеки IoT застосовують як легкі, вузькоспеціалізовані утиліти, так і складні фреймворки. Серед відкритих рішень популярні мережеві аналізатори такі як Zeek та Wireshark, які забезпечують аналіз трафіку, виявлення відхилень від нормальної закономірності поведінки, спроб сканування або підключення невідомих вузлів, тощо. Інструменти Nmap та OpenVAS реалізують активне сканування пристроїв для виявлення відкритих портів, відомих вразливостей та помилок конфігурації. У великих інфраструктурах широко застосовуються рішення, як-от Forescout, Cisco Cyber Vision та Azure Defender for IoT, що інтегруються з хмарними сервісами, реалізують централізовану політику доступу, підтримують автоматичну інвентаризацію пристроїв і можуть ізолювати скомпрометовані вузли у режимі реального часу.

Актуальним трендом є розвиток платформ розподіленої обробки даних, які реалізують принципи периферійних обчислень [3]: аналітика виконується якнайближче до джерела даних, що зменшує затримки та не вимагає постійного підключення до центрального сервера. Це вкрай важливо в умовах обмеженої пропускної здатності мережі або високої чутливості до затримок, наприклад, як у випадку з автономними автомобілями, розумною енергетикою або виробничими процесами з критично важливим управлінням у режимі реального часу. Такі системи можуть поєднувати базову обробку на периферійних вузлах з поглибленим аудитом у хмарі, таким чином досягається баланс між швидкістю реагування та якістю виявлення загроз.

Отже, у перспективі, важливими напрямками розвитку такого ПЗ для аудиту безпеки IoT є створення полегшених агентів з вбудованими механізмами машинного навчання [4], здатних працювати автономно, а також стандартизація форматів обміну подіями безпеки, що уніфікує звіти та спрощує інтеграцію з рішеннями SIEM (Security Information and Event Management). Розробка контейнеризованих рішень на основі самооновлюваних ML-моделей для виявлення нових загроз забезпечує динамічну адаптованість до наявних ресурсів пристрою з мінімальним впливом на продуктивність, збереженням функціональності та стабільності у середовищах з нестійким з'єднанням та з обмеженими ресурсами. Забезпечення ефективного аудиту без шкоди для функціональності та стабільності – це «ключ» в сучасних дослідженнях у сфері інформаційної безпеки систем IoT.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Annual number of IoT attacks global 2022. *Statista* : веб-сайт. URL: <https://www.statista.com/statistics/1377569/worldwide-annual-internet-of-things-attacks/> (дата звернення: 07.04.2025).
2. Minhaj Ahmad Khan. IoT security: Review, blockchain solutions, and open challenges. *Future Generation Computer Systems*. 2018. Vol. 82, no. 395–411. URL: <https://doi.org/10.1016/j.future.2017.11.022> (дата звернення: 07.04.2025).
3. Weisong Shi, Jie Cao. Edge Computing: Vision and Challenges. *IEEE Internet of Things Journal*. 2020. Vol. 3, no. 5. URL: <https://doi.org/10.1109/JIOT.2016.2579198> (дата звернення: 07.04.2025).
4. Hossein Ahmadvand, Chhagan Lal. Privacy-Preserving and Security in SDN-Based IoT: A Survey. *IEEE Access*. 2023. Vol. 11. P. 44772–44786. URL: <https://ieeexplore.ieee.org/document/10103687> (дата звернення: 07.04.2025).

**НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ БІОРЕСУРСІВ І
ПРИРОДОКОРИСТУВАННЯ УКРАЇНИ
ФАКУЛЬТЕТ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ**



**ТЕОРЕТИЧНІ ТА ПРИКЛАДНІ
АСПЕКТИ РОЗРОБКИ
КОМП'ЮТЕРНИХ СИСТЕМ**

**ЗБІРНИК НАУКОВИХ ПРАЦЬ ЗА МАТЕРІАЛАМИ
VII ВСЕУКРАЇНСЬКОЇ НАУКОВО-ПРАКТИЧНОЇ КОНФЕРЕНЦІЇ
СТУДЕНТІВ І АСПІРАНТІВ
*24 квітня 2025 року***

Київ 2025

УДК 004

Відповідальна за випуск: М.І. Лендел

Збірник наукових праць за матеріалами VII Всеукраїнської науково-практичної конференції студентів і аспірантів «ТЕОРЕТИЧНІ ТА ПРИКЛАДНІ АСПЕКТИ РОЗРОБКИ КОМП'ЮТЕРНИХ СИСТЕМ '2025», 24 квітня 2025 року, НУБіП України, Київ. – 452 с. (електронне видання)

Відповідальність за зміст публікацій несуть автори.

Передрук матеріалів, а також використання їх будь-якій формі допускається лише з дозволу авторів