КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 1 (33), 2026
ISSN 2663 – 4023
DOI 10.28925/2663-4023.2026.33.1258
УДК 004.056:004.7:004.75

Довженко Надія Михайлівна
кандидат технічних наук, доцент
доцент кафедри інформаційної та кібернетичної безпеки імені професора Володимира Бурячка
Київський столичний університет імені Бориса Грінченка, м. Київ, Україна
ORCID: 0000-0003-4164-0066
n.dovzhenko@kubg.edu.ua

Іваніченко Євген Вікторович
кандидат технічних наук, доцент
доцент кафедри комп'ютерних наук
Київський столичний університет імені Бориса Грінченка, м. Київ, Україна
ORCID: 0000-0002-6408-443X
y.ivanichenko@kubg.edu.ua

Соколов Володимир Юрійович
кандидат технічних наук, доцент
доцент кафедри інформаційної та кібернетичної безпеки імені професора Володимира Бурячка
Київський столичний університет імені Бориса Грінченка, м. Київ, Україна
ORCID: 0000-0002-9349-7946
v.sokolov@kubg.edu.ua

АДАПТИВНА МОДЕЛЬ ВИЯВЛЕННЯ КІБЕРЗАГРОЗ У IOT-ПІДСИСТЕМАХ ДАТА ЦЕНТРІВ

Анотація. Інтеграція технологій Інтернету речей (IoT), edge/fog-обчислень і хмарних сервісів у сучасні центри обробки даних створює передумови для підвищення ефективності моніторингу, автоматизації управління інфраструктурою, безперервного збору телеметричних даних та адаптивного керування системами охолодження, енергоспоживанням і мережевими ресурсами дата-центрів. Разом із перевагами зростає і кількість кіберзагроз, пов'язаних із розширенням поверхні атаки, використанням гетерогенних IoT-пристроїв та складністю захисту розподіленої інфраструктури. У роботі досліджено особливості впровадження IoT-компонентів у хмарні середовища та дата-центри з урахуванням сучасних загроз інформаційній безпеці. Основну увагу приділено DDoS-атакам, spoofing-атакам та компрометації вузлів інфраструктури. Запропоновано адаптивну модель виявлення кіберзагроз, яка поєднує статистичний аналіз мережевого трафіку, поведінковий аналіз вузлів та графове представлення взаємодій між компонентами системи. Для оцінювання стану інфраструктури використано інтегральний показник ризику, що враховує інтенсивність трафіку, ентропію джерел, відхилення поведінкового профілю та параметри графа взаємодій. У статті також запропоновано архітектуру адаптивної системи виявлення кіберзагроз в IoT-орієнтованому дата-центрі, яка включає IoT-рівень, edge/fog-рівень попередньої обробки, аналітичний cloud-рівень, модуль графової кореляції та рівень автоматизованого реагування на кіберінциденти.

Ключові слова: IoT, сенсор, дата-центр, ЦОД, хмарне середовище, кібербезпека, DDoS-атаки, spoofing, edge computing, граф, аналіз, оцінювання ризику, компрометація.

ВСТУП

Стрімке зростання обсягів цифрових даних, розвиток хмарних сервісів, систем штучного інтелекту та розподілених обчислень обумовлюють необхідність постійної модернізації сучасних центрів обробки даних (ЦОД). Одним із ключових напрямів такого розвитку є інтеграція технологій Інтернету речей (IoT) у серверну та мережеву інфраструктуру. Адже використання IoT-компонентів дозволяє реалізувати постійний моніторинг стану обладнання, автоматизоване керування інженерними системами, балансування навантаження та інтелектуальний контроль енергоспоживання. Як наслідок, формується оновлена концепція дата-центру, у якому фізична інфраструктура, периферійні пристрої та хмарні сервіси функціонують як об'єднана система [1].

Тому і не дивно, що провідні ІТ-компанії вже активно впроваджують концептуально різні IoT-рішення у власні ЦОД. Наприклад, Amazon Web Services (AWS), Google Cloud та Microsoft Azure використовують інтелектуальні системи моніторингу для прогнозування технічного стану та особливостей обслуговування обладнання, автоматичного балансування навантаження та оптимізації енергоспоживання. Такі компанії як IBM, Cloudflare і Cisco інтегрують системи автоматизованого виявлення кіберзагроз, механізми швидкого реагування на інциденти та інструменти захисту від DDoS-атак в інфраструктури своїх дата-центрів. Schneider Electric, Siemens і Huawei розробляють нові підходи до енергоефективності, оптимізації охолодження, керування живленням та зменшення витрат електроенергії на основі IoT. У свою чергу, Dell Technologies, Intel та NVIDIA активно використовують edge computing і AI-складові для підвищення швидкості обробки даних, зниження латентності та підтримки високопродуктивних обчислень.

Сучасний розвиток IoT у дата-центрах тісно пов’язаний із переходом до розподілених моделей обробки даних, у межах яких частина аналітичних функцій переноситься ближче до джерел генерації інформації. Використання edge та fog computing дозволяє суттєво скоротити затримки передачі даних, знизити навантаження на центральні хмарні компоненти та загалом підвищити швидкість реагування. Звичайно, для дата-центрів це особливо важливо в умовах обробки значних обсягів службових запитів, телеметрії, функціонування систем автоматичного керування охолодженням, розподілу навантаження між серверними стійками та підтримки сервісів штучного інтелекту.

Варто згадати і те, що інтеграція IoT-компонентів сприяє розвитку концепцій Green IT та сталого функціонування цифрової інфраструктури. Значна частина енергоспоживання дата-центрів припадає саме на системи охолодження, резервного живлення та підтримки серверного обладнання, тому використання інтелектуальних сенсорних систем дозволяє адаптивно змінювати режими роботи інфраструктури залежно від поточного навантаження. У сучасних ЦОД дедалі активніше використовуються цифрові двійники, які забезпечують моделювання фізичного стану дата-центру та прогнозування потенційних відмов обладнання. Поєднання IoT, AI-аналітики та цифрових моделей дозволяє не лише зменшити витрати електроенергії, а й підвищити надійність та стійкість інфраструктури [2].

Однак разом із перевагами впровадження IoT у хмарні середовища та дата-центри виникають все нові виклики. Насамперед, ускладнюються підходи до забезпечення інформаційної безпеки. Велика кількість периферійних пристроїв, використання гетерогенних протоколів, регулярні зміни мережевих топологій, масштабування та високий рівень розподіленості потенційно збільшують мапу атак. Особливо небезпечними залишаються DDoS-атаки, реалізовані через IoT-ботнети, spoofing-атаки, компрометація edge-вузлів, спроби несанкціонованого доступу до телеметричних систем дата-центрів і т.д. Додатковим викликом можна зазначити те, що значна частина IoT-компонентів має все ж обмежені обчислювальні ресурси та не підтримує повноцінні механізми криптографічного захисту.

Якщо розглядати класичні підходи до забезпечення інформаційної безпеки, які засновані на статичних правилах і сигнатурному аналізі, то вони не демонструють достатньої ефективності при впровадженні в такі середовища. Сучасні атаки мають адаптивний та багаторівневий характер. Вони можуть тривалий час маскуватися під легітимну активність сенсорів, котрі імплементовані в інфраструктуру дата-центру, або ж використовувати складні схеми поширення через взаємодію IoT, edge-вузлів та хмарних сервісів. У зв’язку з цим виникає необхідність розроблення адаптивних методів виявлення кіберзагроз, що поєднують статистичний аналіз мережевого трафіку, поведінкове моделювання, графові підходи та механізми інтегрального оцінювання ризику [3].

ПОРІВНЯЛЬНИЙ ТА СТАТИСТИЧНИЙ АНАЛІЗ КІБЕРЗАГРОЗ У IoT-ОРІЄНТОВАНИХ ДАТА-ЦЕНТРАХ

Як вже було зазначено, інтеграція технологій Інтернету речей (IoT) у сучасні центри обробки даних суттєво змінює підходи до функціонування не лише серверної інфраструктури, а й всіх систем моніторингу та автоматизованого керування ресурсами. На відміну від традиційних дата-центрів, IoT-орієнтована інфраструктура використовує значну кількість компонентів, які здійснюють постійну генерацію телеметричних даних у режимі реального часу. Оскільки вони мають суттєві обмеження ресурсів, спрощені, а подекуди й зовсім невраховані механізми автентифікації та недостатній рівень криптографічного захисту, це, своєю чергою, створює додаткові ризики компрометації всієї інфраструктури. Навіть один скомпрометований IoT-вузол може використовуватися як точка проникнення до критичних сегментів дата-центру або як елемент розподіленого ботнету, що призведе до успішної атаки та суттєвих збитків [4].

Особливу небезпеку для сучасних дата-центрів, як і раніше, становлять DDoS-атаки. Однак при інтеграції технологій Інтернету речей вони частіше реалізуються через ботнети. На відміну від класичних

DDoS-атак, сучасні ботнети використовують тисячі або навіть мільйони заражених IoT-пристроїв, розповсюджених у глобальній мережі. Використання таких ботнетів дозволяє формувати надзвичайно високі обсяги трафіку, здатні перевантажувати канали зв'язку, мережеву інфраструктуру та сервіси хмарних платформ. Додаткову складність створює використання low-rate DDoS-атак, які генерують трафік із меншою інтенсивністю, але здатні тривалий час залишатися непоміченими для класичних сигнатурних систем захисту.

Не менш критичними є атаки на edge-вузли та IoT/OT-протоколи. Варто згадати, що сучасні системи автоматизації дата-центрів активно використовують MQTT, CoAP, BACnet та Modbus, проте значна частина цих протоколів спочатку не проєктувалася з урахуванням зростаючих вимог кібербезпеки. Як наслідок, відсутність шифрування, слабкі механізми автентифікації та недостатній рівень сегментації мережі створюють умови для перехоплення телеметрії, spoofing-атак, компрометації систем та порушення роботи інженерної інфраструктури.

Окрему категорію загроз формують атаки, пов'язані з компрометацією прошивок IoT-пристроїв, edge-контролерів або компонентів систем керування. У сучасних дата-центрах такі атаки становлять особливу небезпеку через високу взаємозалежність програмного та апаратного забезпечення. Крім того, останніми роками спостерігається активне використання штучного інтелекту для автоматизації фішингових кампаній, генерації адаптивних сценаріїв атак та обходу традиційних механізмів захисту [5].

Основні кіберзагрози для IoT-орієнтованих дата-центрів наведені у таблиці 1.

Таблиця 1.

Основні кіберзагрози для IoT-орієнтованих дата-центрів

Загроза	Характеристика	Основні вектори атаки	Потенційні наслідки	Рівень критичності
DDoS-атаки на основі IoT-ботнетів	Масоване перевантаження інфраструктури через заражені/скомпрометовані IoT-пристрої	Mirai, Aisuru, TurboMirai, UDP/SYN flood	Відмова сервісів, перевантаження каналів, недоступність хмарних сервісів	Критичний
Ransomware	Шифрування критичних даних та серверної інфраструктури	Фішинг, експлуатація вразливостей IoT	Втрата доступу до даних, фінансові збитки, простої ЦОД	Критичний
Компрометація edge-вузлів	Атаки на периферійні обчислювальні вузли	Zero-day, insecure firmware, слабка автентифікація	Підміна даних, порушення аналітики, несанкціонований доступ	Високий
Атаки на IoT/OT-протоколи	Експлуатація промислових та IoT-протоколів	Modbus, BACnet, MQTT, CoAP	Порушення автоматизації, дестабілізація систем управління	Високий
Витік конфіденційних даних	Несанкціонований доступ до телеметрії та службових даних	API exploitation, credential theft	Компрометація інформації, порушення GDPR/ISO вимог	Середній-високий
Атаки з використанням AI	Використання ШІ для автоматизації атак	Генерація фішингу, адаптивні DDoS-атаки	Ускладнення виявлення та реагування	Високий

Аналіз сучасних тенденцій демонструє стрімке зростання кількості атак, орієнтованих саме на IoT-інфраструктуру дата-центрів. За даними Cloudflare, у 2025 році кількість DDoS-атак, які розповсюджувалися на мережевому рівні, зросла більш ніж утричі порівняно з 2024 роком. Дані NETSCOUT також підтверджують збереження високої інтенсивності DDoS-активності, зокрема понад 8 млн атак у другій половині 2025 року [6]. Подібні атаки реалізуються переважно через глобальні IoT-ботнети, до складу яких входять маршрутизатори, IP-камери, smart-девайси та периферійні edge-вузли.

Паралельно зростає кількість атак на OT- та IoT-протоколи. За даними Forescout, у 2025 році активність атак із використанням OT-протоколів зросла на 84 %, причому серед найбільш помітних напрямів фіксувалися Modbus, EtherNet/IP та BACnet, що свідчить про зміщення фокусу атакувальників у

бік кіберфізичної інфраструктури [7]. Це створює ризики не лише для серверних компонентів дата-центрів, а й для систем енергоживлення, охолодження, автоматизованого керування та телеметрії [8].

Динаміку зростання основних кіберзагроз у IoT-орієнтованих дата-центрах наведено на рис. 1.

Рис.1. Динаміка зростання ключових кіберзагроз у IoT-інфраструктурі дата-центрів

Представлені статистичні дані демонструють, що найбільш критичними залишаються високорозподілені DDoS-атаки та атаки на IoT/OT-протоколи. Їхня небезпека полягає не лише у здатності порушувати доступність сервісів, а й через потенційний шкідливий вплив на інженерну інфраструктуру дата-центрів. У випадку компрометації edge-вузлів або систем автоматизованого керування зловмисники можуть вносити зміни в роботу систем охолодження, енергоживлення та розподілу навантаження, що, знову ж таки, потенційно створює ризик порушення функціонування всієї інфраструктури.

Важливою особливістю кібератак, які спрямовані на IoT компоненти, є їхній комбінований характер. DDoS-активність часто супроводжується spoofing-атаками, компрометацією API, використанням викрадених облікових даних та спробами латерального переміщення між сегментами інфраструктури. У таких умовах класичні сигнатурні засоби захисту є недостатньо ефективними, оскільки вони не враховують поведінкову динаміку системи та складні взаємозв'язки між її компонентами.

Таким чином, забезпечення кіберстійкості сучасних IoT-орієнтованих дата-центрів потребує комплексного підходу, який повинен поєднувати Zero Trust архітектуру, сегментацію IoT-мереж, багаторівневий захист від DDoS-атак, поведінковий аналіз, графові методи кореляції подій та AI/ML-системи виявлення аномалій. Саме така інтеграція методів статистичного, поведінкового та графового аналізу є основою для побудови адаптивних систем виявлення кіберзагроз у сучасних хмарних середовищах з інтегрованими IoT-компонентами [9].

АДАПТИВНА МОДЕЛЬ ВИЯВЛЕННЯ ТА ПРОГНОЗУВАННЯ КІБЕРЗАГРОЗ У ХМАРНОМУ СЕРЕДОВИЩІ З ІНТЕГРОВАНИМИ IoT-КОМПОНЕНТАМИ

На відміну від традиційних мережевих середовищ, IoT-орієнтовані дата-центри функціонують у режимі постійної генерації телеметричних даних. Своєю чергою це створює умови, за яких мережевий трафік має виражений динамічний характер, а межа між нормальною та аномальною активністю стає менш очевидною. У зв'язку з цим ефективне виявлення кіберзагроз потребує не лише аналізу окремих параметрів трафіку, а й врахування взаємозв'язків між поведінкою вузлів, структурою мережевої взаємодії та часовою динамікою розвитку атак.

Для підвищення ефективності виявлення кіберзагроз доцільно розглянути адаптивну модель, що поєднує статистичний аналіз мережевого трафіку, поведінковий аналіз вузлів та графове представлення взаємодій між компонентами системи. Модель описується множиною:

$$M = (O, G, F, R), \quad (1)$$

де O – множина об'єктів інфраструктури, G – граф взаємодій, F – множина функцій аналізу, R – інтегральна оцінка ризику.

Для формалізованого опису стану системи в момент t вводиться множина параметрів:

$$S(t) = \{\lambda(t), H(t), \Delta(t), deg^{-}(v,t)\} \quad (2)$$

де $\lambda(t)$ – характеризує інтенсивність трафіку, $H(t)$ – ентропія джерел трафіку , $\Delta(t)$ – відхилення поведінкового профілю вузла інфраструктури, $deg^{-}(v,t)$ – вхідний ступінь вузла у графі взаємодій.

Для виявлення атак типу DDoS ключовим параметром є інтенсивність трафіку, яка визначається як відношення кількості пакетів до інтервалу часу:

$$\lambda(t) = \frac{N(t)}{\Delta t} \tag{3}$$

де $N(t)$ – кількість пакетів за часовий інтервал Δt. У нормальному режимі значення $\lambda(t)$ є відносно стабільним, тоді як під час DDoS-атаки спостерігається різке або поступове збільшення цього параметра.

Для сучасних IoT-ботнетів характерним є поступове нарощування інтенсивності трафіку, що дозволяє атаці тривалий час залишатися малопомітною для класичних IDS-систем. У таких умовах зміна трафіку може бути описана експоненційною залежністю:

$$\lambda(t) = \lambda_0 e^{k(t-t_a)} \tag{4}$$

де $t_a -$ момент початку атаки, а $k -$ коефіцієнт інтенсивності зростання трафіку.

У сценарії для перевірки роботи запропонованого підходу значення $\lambda(t)$ задано в діапазоні від 100 до 2900 пак/с. Для подальшого використання у функції інтегрального оцінювання ризику виконується нормалізація параметра:

$$\lambda_{\text{norm}}(\text{t}) = \frac{\lambda(\text{t})}{\lambda_{max}} = \frac{\lambda(\text{t})}{2900}$$

Окрему роль у моделі відіграє ентропійний аналіз. На відміну від централізованих атак, DDoS-атаки на основі IoT-ботнетів характеризуються високою розподіленістю джерел трафіку. Для оцінювання цього ефекту використовується ентропія джерел трафіку:

$$H = -\sum_{i=1}^{n} p_i \, log p_i, \tag{5}$$

де p_i – частка трафіку від і-го джерела.

Ентропійний підхід є важливим саме для IoT-середовищ, оскільки дозволяє оцінити ступінь розподіленості атаки та виявляти ситуації, коли велика кількість периферійних пристроїв починає генерувати аномальний трафік. У дослідженні значення $H(t)$ змінюються в межах від 2 до 4.7.

Нормалізація параметра виконується за формулою:

$$\text{H}_{\text{norm}}(\text{t}) = \frac{\text{H}(\text{t}) - H_{min}}{H_{max} - H_{min}} = \frac{\text{H}(\text{t}) - 2}{4.7 - 2}$$

Важливою особливістю сучасних атак є використання spoofing-механізмів для підміни ідентифікаційних параметрів вузлів. У таких випадках шкідливий вузол намагається імітувати поведінку легітимного IoT-пристрою, що суттєво ускладнює виявлення загрози. Для аналізу таких аномалій використовується поведінковий підхід, заснований на порівнянні еталонного та спостережуваного профілів активності:

$$\Delta(t) = \left\| X_{observed}(t) - X_{expected}(t) \right\| \tag{6}$$

де $X_{observed}(t)$ – фактичний профіль активності вузла, а $X_{expected}(t)$ – еталонний профіль.

Значне зростання параметра $\Delta(t)$ свідчить про невідповідність між заявленими ідентифікаційними характеристиками вузла та його реальною поведінкою. Для дата-центрів це особливо важливо, оскільки spoofing-атаки можуть бути спрямовані на системи телеметрії, edge-шлюзи або компоненти автоматизованого керування інженерною інфраструктурою.

Параметр $deg^{-}(v,t)$ визначає кількість вхідних з'єднань до вузла та використовується як один із ключових індикаторів DDoS-активності. У межах графового представлення мережі різке збільшення кількості вхідних зв'язків до окремого вузла свідчить про спробу перевантаження ресурсу або концентрацію аномальної активності. У проведеному дослідженні значення параметра змінюються від 10 до 170, тому для забезпечення коректного інтегрального аналізу застосовується нормалізація:

$$deg^{-}{}_{norm}(t) = \frac{deg^{-}(v,t)}{170}$$

Методика передбачає інтеграцію цих параметрів у єдину функцію оцінювання стану системи:

$$R(t) = \alpha_1\lambda(t) + \alpha_2 H(t) + \alpha_3\Delta(t) + \alpha_4 deg^{-}(v,t) \quad (7)$$

що дозволяє здійснювати комплексний аналіз та підвищувати точність виявлення атак.

Коефіцієнти $\alpha_1, \alpha_2, \alpha_3, \alpha_4$ є ваговими параметрами, що визначають внесок кожного показника у загальну оцінку ризику. Їх значення обрано на основі нормалізації параметрів та експериментального аналізу впливу кожного показника на точність виявлення атак:

$$\alpha_1 = 0.35, \alpha_2 = 0.2, \alpha_3 = 0.25, \alpha_4 = 0.2$$

З урахуванням нормалізації інтегральна оцінка ризику набуває вигляду:

$$R(t) = 0.35 * \lambda_{norm}(t) + 0.2 * \mathrm{H_{norm}(t)} + 0.25 * \Delta(t) + 0.2 * deg^{-}{}_{norm}(v,t)$$

Значення $R(t)$ буде знаходитися в інтервалі [0;1] та інтерпретується як рівень ризику функціонування системи.

Для прийняття рішення вводяться порогові значення: при $R(t) < 0.3$ система вважається стабільною, у діапазоні $0.3 \le R(t) < 0.6$ фіксується потенційна загроза, а при $R(t) \ge 0.6$ – активна фаза атаки [10].

На рис. 2 представлено графік зміни інтенсивності трафіку $\lambda(t)$. До 50 секунди система функціонує у штатному режимі, після чого спостерігається різке експоненціальне зростання навантаження, характерне для DDoS-атаки.

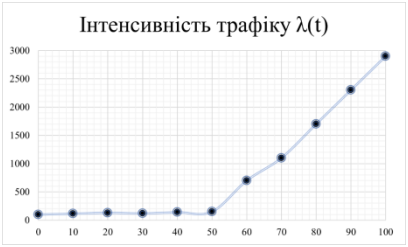

Рис.2. Приклад зміни інтенсивності трафіку під час DDoS-атаки

Поступове збільшення трафіку після 60 секунди свідчить про активацію IoT-ботнету та залучення нових вузлів до атаки. Така динаміка може відповідати сценарію high-volume DDoS-атаки, у якому інтенсивність трафіку зростає внаслідок поетапного залучення скомпрометованих IoT-пристроїв.

Рис. 3 відображає зміну ентропії джерел трафіку $H(t)$. До моменту активації атаки значення ентропії залишаються відносно стабільними, що відповідає нормальному режиму роботи інфраструктури.

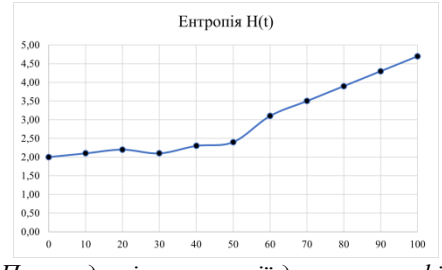

Рис.3. Приклад зміни ентропії джерел трафіку $H(t)$

Після 60 секунди спостерігається зростання ентропії, яке підтверджує збільшення кількості розподілених джерел трафіку та використання великої кількості IoT-пристроїв у структурі ботнету. У поєднанні з графіком інтенсивності трафіку це дозволяє відокремлювати розподілені атаки від локальних аномалій або короткочасних перевантажень мережі.

На рис. 4 представлено зміну параметра Δ(t), що характеризує ступінь відхилення поведінкового профілю вузлів.

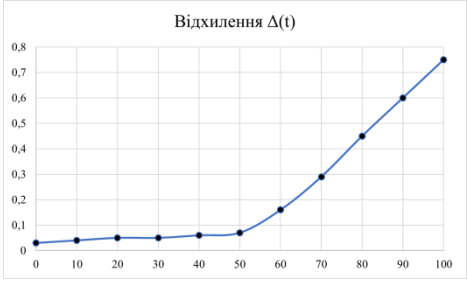

Рис.4. Зміна поведінкового профілю $\Delta(t)$

До початку атаки значення параметра мають незначні коливання, однак після 60 секунди спостерігається різке зростання відхилення між еталонним та фактичним профілем активності. У свою чергу це може свідчити про появу spoofing-аномалій та порушення відповідності між ідентифікаційними ознаками вузлів і їхньою реальною поведінкою.

На рис. 5 наведено графік інтегрального показника ризику $R(t)$. До моменту активації атаки система перебуває у межах нормального функціонування, після чого спостерігається швидке зростання рівня ризику.

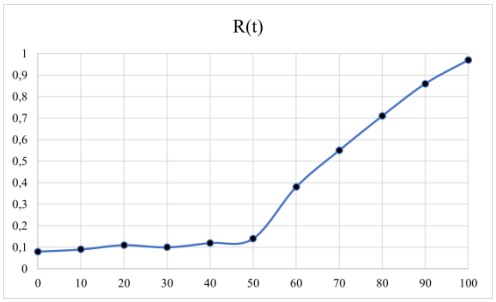

Рис. 5. Інтегральний показник ризику $R(t)$

Узгоджена зміна $\lambda(t), H(t), \Delta(t)$ та $deg^{-}(v,t)$ підтверджує ефективність запропонованого підходу для виявлення комбінованих DDoS/spoofing-атак у IoT-орієнтованих дата-центрах. На відміну від класичних сигнатурних підходів, модель дозволяє враховувати часову динаміку розвитку атак, особливості IoT-ботнетів та складні взаємозв'язки між компонентами хмарної інфраструктури дата-центру.

АРХІТЕКТУРНА РЕАЛІЗАЦІЯ АДАПТИВНОЇ СИСТЕМИ ВИЯВЛЕННЯ КІБЕРЗАГРОЗ В ІОТ-ОРІЄНТОВАНОМУ ДАТАЦЕНТРІ

Архітектурна реалізація запропонованої моделі передбачає побудову багаторівневої системи, яка забезпечує безперервний збір телеметричних даних, попередню обробку мережевого трафіку, графову кореляцію подій, обчислення інтегрального показника ризику та автоматизоване реагування на виявлені кіберзагрози. На відміну від класичних систем IDS/IPS, така архітектура повинна враховувати специфіку IoT-компонентів у дата-центрах, зокрема велику кількість сенсорів, контролерів енергоспоживання, систем охолодження, smart-rack-пристроїв, edge-шлюзів та сервісів хмарної інфраструктури[11].

Як вже було зазначено, сучасні IoT-орієнтовані дата-центри фактично є складними кіберфізичними системами, у яких фізична інфраструктура тісно інтегрована з цифровими платформами керування. У таких середовищах будь-яка аномальна поведінка окремих компонентів або ж компрометація периферійного вузла можуть впливати не лише на доступність певних мережевих чи хмарних сервісів, а й на роботу всіх критично важливих для функціонування ЦОД систем. Саме тому архітектура повинна забезпечувати не просто ізольований аналіз окремих подій, а більш глибинне, комплексне оцінювання поведінки всієї інфраструктури з урахуванням взаємозв'язків між її компонентами.

На першому рівні функціонують IoT-компоненти дата-центру, які генерують первинну телеметрію та мережевий трафік. До них частіше за все можна віднести сенсори температури, вологості, енергоспоживання, контролери охолодження, пристрої моніторингу серверних стійок та периферійні вузли керування. Фактично на цьому рівні саме IoT-складові можуть бути як джерелом корисних даних для моніторингу, так і потенційною точкою компрометації при формуванні ботнетів або реалізації spoofing-атак. Додатковою проблемою є те, що значна частина IoT-компонентів використовує спрощені

механізми автентифікації та має обмежені обчислювальні ресурси, що ускладнює впровадження повноцінних механізмів криптографічного захисту безпосередньо на периферійному рівні, як вже згадувалося раніше.

На другому рівні здійснюється збір, агрегація та попередня фільтрація (опрацювання) даних. Edge/fog-вузли виконують первинне очищення трафіку, усунення шумів, нормалізацію параметрів та формування вектора ознак $X(t)$. Саме на цьому етапі обчислюються або готуються до подальшого аналізу значення $\lambda(t), H(t), \Delta(t)$ та $deg^{-}(v,t)$.

Використання edge/fog-рівня дозволяє зменшити навантаження на центральні хмарні ресурси та скоротити затримки під час обробки даних. Такий підхід особливо важливий для дата-центрів, у яких рішення щодо реагування на аномалії повинні прийматися у режимі, наближеному до реального часу[12].

На третьому рівні реалізується аналітичний модуль виявлення кіберзагроз. Він виконує окремий аналіз DDoS-активності, spoofing-аномалій та поведінкових відхилень. DDoS-аналіз базується на оцінюванні інтенсивності трафіку та ентропії джерел, тоді як spoofing-аналіз ґрунтується на порівнянні еталонного й фактичного профілів вузлів. Такий поділ дозволяє уникнути змішування різних типів атак і водночас забезпечує можливість їх подальшої кореляції. Особливістю запропонованого підходу є те, що аналіз виконується не лише на рівні окремих пакетів або потоків даних, а й з урахуванням часової динаміки розвитку аномалій. Впровадження такого підходу дозволяє виявляти low-rate DDoS-атаки та поступові spoofing-аномалії, які часто залишаються непомітними для класичних сигнатурних IDS-систем.

На четвертому рівні формується графова модель кіберзагроз. Вузлами графа є IoT-пристрої, edge-шлюзи, віртуальні машини, контейнери, API-сервіси та компоненти хмарної інфраструктури, а ребра відображають мережеві або логічні взаємодії між ними. Графовий модуль дозволяє виявляти критичні вузли, шляхи поширення атаки та аномальне зростання кількості вхідних зв'язків, що особливо важливо для аналізу DDoS-атак у дата-центрах. На відміну від традиційних мережевих моделей, графовий підхід дозволяє враховувати не лише факт взаємодії між вузлами, а й інтенсивність, частоту та контекст цих взаємодій. У результаті система отримує можливість виявляти приховані взаємозалежності між аномальними подіями та формувати узагальнену картину розвитку кіберінциденту.

На п'ятому рівні виконується інтегральне оцінювання ризику. Отримані з попередніх рівнів параметри передаються до модуля Risk Assessment, де на основі функції $R(t)$ визначається поточний стан системи. Якщо значення ризику перебуває в межах нормального режиму, система продовжує моніторинг. Якщо показник переходить у зону потенційної загрози або активної атаки, ініціюється процедура реагування. Інтегральний підхід до оцінювання ризику дозволяє враховувати не лише окремі аномалії, а й їхній сукупний вплив на функціонування інфраструктури. Для IoT-орієнтованих дата-центрів, де атаки часто мають комбінований характер і можуть одночасно впливати на мережевий, прикладний та інженерний рівні системи, це особливо важливо.

Фінальний рівень забезпечує вибір і застосування контрзаходів. Залежно від типу та інтенсивності загрози система може виконувати ізоляцію IoT-вузла, обмеження мережевого трафіку, зміну політик доступу, переналаштування SDN-маршрутизації, блокування підозрілих ідентифікаторів або переведення окремого сегмента інфраструктури у режим підвищеного контролю. Такий підхід узгоджується з принципами Zero Trust, відповідно до яких кожен вузол має постійно підтверджувати свою легітимність, а доступ до ресурсів надається лише після перевірки контексту, поведінки та рівня ризику[13]. У сучасних дата-центрах реалізація Zero Trust є особливо актуальною через високу динамічність IoT-середовища та постійну зміну кількості активних вузлів інфраструктури.

Важливою особливістю запропонованої архітектури є можливість масштабування та адаптації до змін навантаження. Оскільки IoT-інфраструктура дата-центрів характеризується значною кількістю телеметричних потоків, система повинна підтримувати горизонтальне масштабування аналітичних модулів, динамічний розподіл обчислювальних ресурсів та адаптивне переналаштування механізмів моніторингу[14]. Поєднання edge/fog-обчислень та хмарної аналітики дозволяє забезпечити баланс між швидкістю реагування, точністю виявлення аномалій та ефективністю використання ресурсів дата-центру.

На рис. 6 представлена багаторівнева архітектура адаптивної системи виявлення кіберзагроз, яка забезпечує послідовне перетворення первинних даних IoT-рівня у рішення щодо реагування на кіберінциденти. На відміну від класичних IDS-систем, запропонована архітектура враховує взаємодію IoT-пристроїв, edge/fog-рівня та хмарної інфраструктури дата-центру[15]. Дані, отримані з IoT-компонентів, проходять етапи збору, фільтрації, нормалізації, аналітичної обробки, графової кореляції та інтегрального оцінювання ризику. Результатом роботи системи є класифікація стану інфраструктури та вибір відповідних контрзаходів.

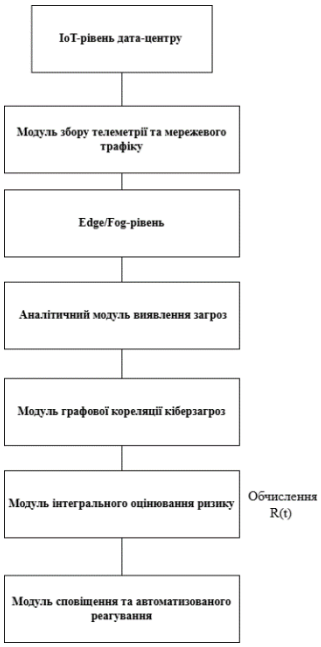

Рис. 6. Архітектура адаптивної системи виявлення кіберзагроз в IoT-орієнтованому дата-центрі

Поєднання статистичного аналізу, поведінкового моделювання, графових методів та механізмів автоматизованого реагування створює основу для побудови адаптивних систем кіберзахисту нового покоління, здатних забезпечувати стійкість сучасних дата-центрів в умовах постійного зростання кількості та складності IoT-орієнтованих кіберзагроз.

ВИСНОВКИ ТА ПЕРСПЕКТИВИ ПОДАЛЬШИХ ДОСЛІДЖЕНЬ

У статті досліджено особливості впровадження IoT-компонентів у сучасні дата-центри та хмарні середовища з акцентом на кібербезпекові ризики, що виникають унаслідок розширення поверхні атаки, використання edge/fog-рівнів, гетерогенних IoT-пристроїв та автоматизованих систем керування інфраструктурою. Показано, що найбільш критичними для IoT-орієнтованих дата-центрів є DDoS-атаки на основі ботнетів, spoofing-атаки, компрометація edge-вузлів, атаки на IoT/OT-протоколи та загрози, пов’язані з ланцюгами постачання.

Запропоновано адаптивну модель виявлення та оцінювання кіберзагроз, яка поєднує статистичний аналіз мережевого трафіку, ентропійний аналіз джерел, поведінкове профілювання вузлів та графове представлення взаємодій між компонентами інфраструктури. Для формалізації стану системи використано параметри $\lambda(t), H(t), \Delta(t)$ та $deg^{-}(v,t)$ на основі яких формується інтегральний показник ризику $R(t)$. Такий підхід дозволяє враховувати не лише окремі аномалії, а й їхній сукупний вплив на функціонування IoT-орієнтованого дата-центру.

Окремо запропоновано архітектурну реалізацію адаптивної системи виявлення кіберзагроз, що включає IoT-рівень, edge/fog-рівень попередньої обробки, аналітичний модуль виявлення атак, графову кореляцію подій, інтегральне оцінювання ризику та рівень автоматизованого реагування. Представлена архітектура забезпечує логічний перехід від збору телеметричних даних до прийняття рішень щодо ізоляції вузлів, обмеження трафіку, зміни політик доступу та застосування Zero Trust-підходу.

Перспективи подальших досліджень полягають у розширенні запропонованої моделі за рахунок автоматичного налаштування вагових коефіцієнтів для різних типів атак, поглибленні графового аналізу шляхів поширення загроз у edge/fog/cloud-архітектурах, а також у застосуванні методів машинного та глибинного навчання для динамічного профілювання IoT-пристроїв. Окрему увагу доцільно приділити верифікації моделі на реальних наборах мережевого трафіку дата-центрів, розробці засобів візуалізації динамічних графів кіберзагроз та оцінюванню ефективності запропонованого підходу з урахуванням параметрів SLA, затримки реагування та допустимого рівня хибних спрацювань.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Dovzhenko, N., Ivanichenko, Y., Ausheva, N., Shevchuk, Y., & Lukovskyi, T. (2025). Study of data center architectures with integration of IoT components to ensure energy efficiency and cyber resilience. *Cybersecurity: Education, Science, Technique, 4*(28), 547-564. https://doi.org/10.28925/2663-4023.2025.28.835
2. Dovzhenko, N. M., Ivanichenko, Y. V., & Mazur, N. P. (2025). Technological aspects of implementing intelligent transportation systems in urban infrastructure based on IoT, AI, and cloud technologies. In *Proceedings of the XII All-Ukrainian Scientific and Practical Conference of Young Scientists "Information Technologies – 2025"* (pp. 124-126).
3. Hulak, H. M., Zhyltsov, O. B., Kyrychok, R. V., Korshun, N. V., & Skladannyi, P. M. (2023). *Enterprise information and cyber security*. Borys Grinchenko Kyiv Metropolitan University.
4. Dovzhenko, N., Mazur, N., Skladannyi, P., Kostiuk, Y., & Rzaieva, S. (2024). Integration of IoT and artificial intelligence into intelligent transportation systems. *Cybersecurity: Education, Science, Technique, 2*(26), 430-444. https://doi.org/10.28925/2663-4023.2024.26.708
5. Kostiuk, Y. V., Skladannyi, P. M., Hulak, H. M., Bebeshko, B. T., Khorolska, K. V., & Rzaieva, S. L. (2025). *Information security systems*. Borys Grinchenko Kyiv Metropolitan University.
6. NETSCOUT. (n.d.). *Cyber Threat Horizon: Real-time global threat intelligence*. https://horizon.netscout.com/
7. Forescout. (2025). *2025 threat report: Exploitation grows across IT, IoT and OT*. https://www.forescout.com/blog/2025-threat-report-exploitation-grows-across-it-iot-and-ot/
8. Khedr, A., & Sheeja, S. (2026). Cloud-based congestion-aware data distribution for healthcare IoT using Laplacian kernel clustering and censored weighted queuing. *Neural Computing and Applications, 38*. https://doi.org/10.1007/s00521-026-11854-1
9. Wahyuddin, S., Saikhu, A., & Raharjo, A. (2026). Shapelet transformation of multivariate time series for IoT anomaly detection. *Engineering, Technology & Applied Science Research, 16*, 33549–33556. https://doi.org/10.48084/etasr.17048
10. Dovzhenko, N., Ivanichenko, Y., Skladannyi, P., & Ausheva, N. (2024). Integration of security and fault tolerance of sensor networks based on energy consumption and traffic analysis. *Cybersecurity: Education, Science, Technique, 1*(25), 390-400. https://doi.org/10.28925/2663-4023.2024.25.390400
11. Shah, I., & Tariq, A. (2025). *Building resilient smart cities: AI-driven SOCs and blockchain for IoT cybersecurity*. https://doi.org/10.13140/RG.2.2.13351.25763
12. Sun, Y., Wang, Y., Jiang, G., Cheng, B., & Zhou, H. (2024). Deep learning-based power usage effectiveness optimization for IoT-enabled data center. *Peer-to-Peer Networking and Applications, 17*, 1-18. https://doi.org/10.1007/s12083-024-01663-5
13. Dovzhenko, N., Ivanichenko, Y., & Kostiuk, Y. (2025). Methodology for detection and localization of cyber threats in cloud environments with integrated IoT components based on graph models. *Cybersecurity: Education, Science, Technique, 1*(29), 762-776. https://doi.org/10.28925/2663-4023.2025.29.938
14. Sim, S.-H., & Jeong, Y.-S. (2021). Multi-blockchain-based IoT data processing techniques to ensure the integrity of IoT data in AIoT edge computing environments. *Sensors, 21*(10), 3515. https://doi.org/10.3390/s21103515
15. Abdullah, S., & Assaad, A. (2026). Internet of Things (IoT) and artificial intelligence (AI)-based smart cities management: A review study. *Humanitarian and Natural Sciences Journal, 7*(1), 724-738. https://doi.org/10.53796/hnsj71/45

КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 1 (33), 2026
ISSN 2663 – 4023

Nadiia Dovzhenko
PhD, Associate Professor,
Associate Professor of the Department of Information and
Cyber Security named after Professor Volodymyr Buriachok
Borys Grinchenko Kyiv Metropolitan University, Kyiv, Ukraine
ORCID: 0000-0003-4164-0066
n.dovzhenko@kubg.edu.ua

Yevhen Ivanichenko
PhD, Associate Professor,
Associate Professor of the Department of Computer Science
Borys Grinchenko Kyiv Metropolitan University, Kyiv, Ukraine
ORCID: 0000-0002-6408-443X
y.ivanichenko@kubg.edu.ua

Volodymyr Sokolov
PhD, Associate Professor,
Associate Professor of the Department of Information and
Cyber Security named after Professor Volodymyr Buriachok
Borys Grinchenko Kyiv Metropolitan University, Kyiv, Ukraine
ORCID: 0000-0002-9349-7946
v.sokolov@kubg.edu.ua

ADAPTIVE MODEL OF CYBERTHREAT DETECTION IN IOT SUBSYSTEMS DATE CENTERS

Abstract. The integration of Internet of Things (IoT) technologies, edge/fog computing, and cloud services into modern data centers creates prerequisites for improving monitoring efficiency, infrastructure management automation, continuous telemetry data collection, and adaptive control of cooling systems, power consumption, and network resources within data centers. Alongside these advantages, the number of cyber threats is also increasing due to the expansion of the attack surface, the use of heterogeneous IoT devices, and the complexity of securing distributed infrastructures. This paper investigates the features of implementing IoT components in cloud environments and data centers while considering modern information security threats. Particular attention is paid to DDoS attacks, spoofing attacks, and the compromise of infrastructure nodes. An adaptive cyber threat detection model is proposed, combining statistical network traffic analysis, behavioral analysis of nodes, and graph-based representation of interactions between system components. To assess the state of the infrastructure, an integrated risk indicator is used, taking into account traffic intensity, source entropy, behavioral profile deviation, and interaction graph parameters. The paper also proposes the architecture of an adaptive cyber threat detection system for an IoT-oriented data center, including the IoT layer, the edge/fog preprocessing layer, the analytical cloud layer, the graph correlation module, and the automated cyber incident response layer.

Keywords: IoT, sensor, data center, cloud environment, cybersecurity, DDoS attacks, spoofing, edge computing, graph analysis, risk assessment, compromise.

REFERENCES (TRANSLATED AND TRANSLITERATED)

1. Dovzhenko, N., Ivanichenko, Y., Ausheva, N., Shevchuk, Y., & Lukovskyi, T. (2025). Study of data center architectures with integration of IoT components to ensure energy efficiency and cyber resilience. *Cybersecurity: Education, Science, Technique*, *4*(28), 547-564. https://doi.org/10.28925/2663-4023.2025.28.835
2. Dovzhenko, N. M., Ivanichenko, Y. V., & Mazur, N. P. (2025). Technological aspects of implementing intelligent transportation systems in urban infrastructure based on IoT, AI, and cloud technologies. In *Proceedings of the XII All-Ukrainian Scientific and Practical Conference of Young Scientists "Information Technologies – 2025"* (pp. 124-126).
3. Hulak, H. M., Zhyltsov, O. B., Kyrychok, R. V., Korshun, N. V., & Skladannyi, P. M. (2023). *Enterprise information and cyber security*. Borys Grinchenko Kyiv Metropolitan University.

4. Dovzhenko, N., Mazur, N., Skladannyi, P., Kostiuk, Y., & Rzaieva, S. (2024). Integration of IoT and artificial intelligence into intelligent transportation systems. *Cybersecurity: Education, Science, Technique, 2*(26), 430-444. https://doi.org/10.28925/2663-4023.2024.26.708
5. Kostiuk, Y. V., Skladannyi, P. M., Hulak, H. M., Bebeshko, B. T., Khorolska, K. V., & Rzaieva, S. L. (2025). *Information security systems*. Borys Grinchenko Kyiv Metropolitan University.
6. NETSCOUT. (n.d.). *Cyber Threat Horizon: Real-time global threat intelligence*. https://horizon.netscout.com/
7. Forescout. (2025). *2025 threat report: Exploitation grows across IT, IoT and OT*. https://www.forescout.com/blog/2025-threat-report-exploitation-grows-across-it-iot-and-ot/
8. Khedr, A., & Sheeja, S. (2026). Cloud-based congestion-aware data distribution for healthcare IoT using Laplacian kernel clustering and censored weighted queuing. *Neural Computing and Applications, 38*. https://doi.org/10.1007/s00521-026-11854-1
9. Wahyuddin, S., Saikhu, A., & Raharjo, A. (2026). Shapelet transformation of multivariate time series for IoT anomaly detection. *Engineering, Technology & Applied Science Research, 16*, 33549–33556. https://doi.org/10.48084/etasr.17048
10. Dovzhenko, N., Ivanichenko, Y., Skladannyi, P., & Ausheva, N. (2024). Integration of security and fault tolerance of sensor networks based on energy consumption and traffic analysis. *Cybersecurity: Education, Science, Technique, 1*(25), 390-400. https://doi.org/10.28925/2663-4023.2024.25.390400
11. Shah, I., & Tariq, A. (2025). *Building resilient smart cities: AI-driven SOCs and blockchain for IoT cybersecurity*. https://doi.org/10.13140/RG.2.2.13351.25763
12. Sun, Y., Wang, Y., Jiang, G., Cheng, B., & Zhou, H. (2024). Deep learning-based power usage effectiveness optimization for IoT-enabled data center. *Peer-to-Peer Networking and Applications, 17*, 1-18. https://doi.org/10.1007/s12083-024-01663-5
13. Dovzhenko, N., Ivanichenko, Y., & Kostiuk, Y. (2025). Methodology for detection and localization of cyber threats in cloud environments with integrated IoT components based on graph models. *Cybersecurity: Education, Science, Technique, 1*(29), 762-776. https://doi.org/10.28925/2663-4023.2025.29.938
14. Sim, S.-H., & Jeong, Y.-S. (2021). Multi-blockchain-based IoT data processing techniques to ensure the integrity of IoT data in AIoT edge computing environments. *Sensors, 21*(10), 3515. https://doi.org/10.3390/s21103515
15. Abdullah, S., & Assaad, A. (2026). Internet of Things (IoT) and artificial intelligence (AI)-based smart cities management: A review study. *Humanitarian and Natural Sciences Journal, 7*(1), 724-738. https://doi.org/10.53796/hnsj71/45

Отримано редакцією журналу / Received: 28.02.26
Прорецензовано / Revised: 03.03.26
Схвалено до друку / Accepted: 25.06.26