КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 1 (29), 2025
ISSN 2663 - 4023
DOI 10.28925/2663-4023.2025.29.938
УДК 004.056:004.77:004.738.5:004.8

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

Іваніченко Євген Вікторович
кандидат технічних наук, доцент,
заступник декана з науково-методичної та навчальної роботи
Київський столичний університет імені Бориса Грінченка Київ, Україна
ORCID ID: 0000-0002-6408-443X
y.ivanichenko@kubg.edu.ua

Костюк Юлія Володимирівна
доцент кафедри інформаційної та кібернетичної безпеки імені професора Володимира Бурячка
Київський столичний університет імені Бориса Грінченка Київ, Україна
ORCID ID: 0000-0001-5423-0985
y.kostiuk@kubg.edu.ua

Петришин Любомир Богданович
доктор технічних наук, професор,
професор кафедри комп'ютерних наук та інформаційних систем
Карпатський національний університет імені Василя Стефаника, Івано-Франківськ, Україна
ORCID ID: 0000-0003-4168-3891
lubomyr.petryshyn@pnu.edu.ua

МЕТОДИКА ВИЯВЛЕННЯ ТА ЛОКАЛІЗАЦІЇ КІБЕРЗАГРОЗ У ХМАРНИХ СЕРЕДОВИЩАХ З ІНТЕГРОВАНИМИ ІОТ-КОМПОНЕНТАМИ НА ОСНОВІ ГРАФОВИХ МОДЕЛЕЙ

Анотація. У роботі запропоновано методику виявлення та локалізації кіберзагроз у хмарних середовищах із інтегрованими IoT-компонентами. Підхід базується на використанні двох взаємодоповнюючих моделей: графа виявлення кіберзагроз (ГВК), який описує багаторівневу структуру атак із урахуванням ризику, затримки та потенціалу поширення, та графа відображення оповіщень кібератак (ГВОК), що моделює часово-причинні залежності між подіями для виявлення складних і комбінованих загроз. ГВОК дозволяє формувати послідовні ланцюги подій на основі телеметрії, логів і поведінкових аномалій, інтегруючи дані з хмарних сервісів та IoT-пристроїв. Завдяки цьому забезпечується можливість не лише ідентифікації окремих інцидентів, але й прогнозування розвитку багатоступеневих атак. Для вибору варіантів реагування застосовано узагальнену метрику оцінювання, яка враховує ефективність локалізації загрози, безперервність надання сервісів та час відновлення довіри до системи. Це дозволяє здійснювати пріоритезацію контрзаходів із мінімізацією впливу на роботу критичних ресурсів. Запропонована методика поєднує класичні та інтелектуальні підходи до аналізу загроз, забезпечує проактивний характер моніторингу та здатність до адаптації в умовах високої динаміки хмарних інфраструктур. Рішення орієнтоване на впровадження у критичних обчислювальних системах, промислових дата-центрах, IoT-мережах та хмарних платформах, де необхідно зберігати баланс між безпекою, продуктивністю й стійкістю інфраструктури.

Ключові слова: хмарне середовище; хмарні сервіси; Інтернет речей (IoT); контрзаходи; кіберінцидент; edge computing; інфраструктура; сенсорні мережі; інформаційна безпека; граф; кіберстійкість; модель; загрози; інтеграція.

ВСТУП

Сучасні інформаційні системи дедалі частіше функціонують на основі хмарних обчислень, що забезпечують масштабованість, гнучкість використання ресурсів та економічну ефективність. Паралельно відбувається інтенсивна інтеграція великої кількості IoT-пристроїв у хмарне середовище, що зумовлює появу нових каналів доступу до даних і критичної інфраструктури організацій. Синергія хмарних сервісів та IoT формує комплексні кіберфізичні системи, здатні опрацьовувати критично важливу інформацію в режимі реального часу й набувати стратегічного значення для бізнесу, науки, медицини та державного управління [1].

Проте така інтеграція породжує нові виклики у сфері кібербезпеки. Хмарні середовища вирізняються динамічною інфраструктурою, у якій віртуальні машини та сервіси можуть створюватися й видалятися в режимі динамічного запиту (on-demand). Пристрої IoT, своєю чергою, часто мають обмежені обчислювальні ресурси та спрощені механізми захисту, що робить їх привабливими цілями для кіберзловмисників. Унаслідок цього загрози можуть поширюватися як через віртуалізовані сервіси хмари, так і через фізичні сенсори та виконавчі пристрої (актуатори), які здійснюють збір і передавання даних [2].

Проблема кіберзахисту в подібних середовищах ускладнюється тим, що класичні підходи до безпеки, зокрема мережеві екрани (фаєрволи) та антивірусні засоби, виявляються недостатніми. Вони не забезпечують комплексного виявлення атак у реальному часі, особливо в умовах багаторівневої інфраструктури, яка поєднує дата-центри, хмарні сервіси, мобільні пристрої та розподілені сенсорні мережі IoT [3].

Метою цієї роботи є розроблення методики виявлення та протидії кіберзагрозам у хмарних середовищах з інтегрованими IoT-пристроями. Запропонована методика має не тільки ідентифікувати потенційні загрози, а й адаптивно формувати контрзаходи з метою збереження працездатності системи. Реалізація підходу повинна гарантувати функціональну стійкість інформаційних систем навіть за умов постійної зміни конфігурацій хмарних ресурсів і значної кількості різнорідних IoT-пристроїв [4].

МЕТОДИКА ВИЯВЛЕННЯ ЗАГРОЗИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Загроза інформаційної безпеки в умовах хмарних обчислень та інтегрованих IoT-пристроїв розглядається як потенційна подія, дія або процес, що може призвести до порушення конфіденційності, цілісності чи доступності даних, а також до компрометації компонентів хмарної інфраструктури або IoT-мереж. Особливістю таких середовищ є висока динамічність: у хмарі сервіси створюються й масштабуються автоматично, тоді як IoT-пристрої формують розподілену сенсорну мережу з великою кількістю точок входу. Це суттєво підвищує ризик виникнення вразливостей, які можуть бути використані кіберзловмисниками для реалізації атак [5].

Виявлення кіберзагроз у подібних системах потребує поєднання традиційних методів (методів порогових значень, статистичних підходів, правилових моделей) з інтелектуальними підходами (машинне навчання, нейронні мережі, аналіз великих даних). На рис.1 наведено класифікацію методів виявлення загроз, актуальних для хмарного середовища з інтеграцією IoT.

У таких системах особливо важливу роль відіграють системи виявлення вторгнень (Intrusion Detection Systems, IDS), адаптовані до гібридної інфраструктури. Вони аналізують не лише мережевий трафік між віртуальними машинами у хмарі, а й

телеметрію від IoT-сенсорів, що часто передають малопотужні зашифровані пакети. Таким чином, зазвичай IDS стають центральним елементом багаторівневої архітектури кіберзахисту [6].

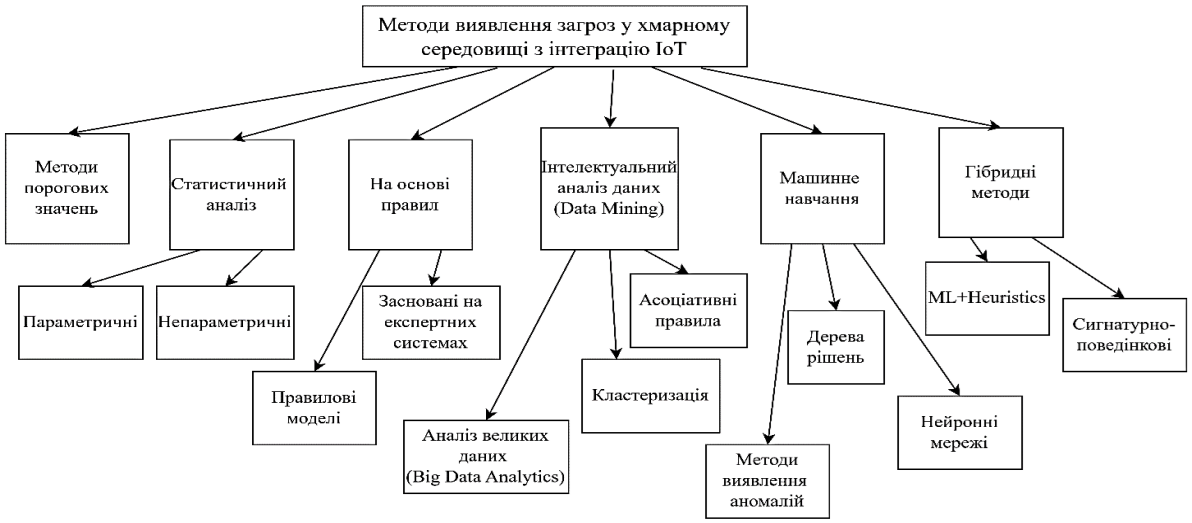

Рис. 1. Класифікація методів виявлення загроз у хмарних середовищах з інтеграцією IoT

Запропонована методика логічно поділяється на такі модулі:

- Модуль збору трафіку і статистики — фіксує трафік з віртуальних машин та контейнерів у хмарному середовищі, а також з сенсорних IoT-пристроїв. Для IoT-мереж важливо враховувати специфіку протоколів, таких як MQTT, CoAP чи Zigbee. На цьому рівні застосовуються методи порогових значень і базовий статистичний аналіз;
- Модуль навчання — будує модель виявлення кіберзагроз на основі графів вразливостей і історичних даних. У випадку IoT ця модель включає профілі поведінки пристроїв, їх типовий обсяг трафіку та часові закономірності. Зазвичай використовуються методи машинного навчання, нейронні мережі та аналіз великих даних;
- Модуль виявлення кіберзагроз — здійснює кореляцію подій між різними рівнями: хмара — IoT — користувацькі сервіси. Наприклад, аномалія у поведінці датчика температури може поєднуватися з несанкціонованим доступом до віртуальної машини, вказуючи на комбіновану атаку. Зазначений модуль ґрунтується на правилових моделях та методах Data Mining;
- Модуль оповіщення та контрзаходів — формує повідомлення про атаку та ініціює дії захисту (ізоляція віртуальної машини, блокування IoT-пристрою, зміна топології хмарної мережі). Для ефективності на цьому рівні застосовуються гібридні методи, що поєднують евристичні та сигнатурно-поведінкові підходи.

Як показано на рис. 1, методика охоплює повний спектр методів – від класичних до інтелектуальних і гібридних. Це дозволяє не лише виявляти окремі інциденти, але й прогнозувати багатоступеневі атаки, які комбінують вектори уразливостей у IoT-пристроях і віртуалізованих ресурсах хмари. Запропонований підхід забезпечує проактивний характер кіберзахисту, коли система не просто реагує на атаку, а й передбачає її розвиток [7].

МОДУЛЬНА МОДЕЛЬ ВИЯВЛЕННЯ КІБЕРЗАГРОЗ У ХМАРНОМУ СЕРЕДОВИЩІ З ІНТЕГРОВАНИМИ IOT-КОМПОНЕНТАМИ

Для комплексного кіберзахисту у хмарній інфраструктурі з інтегрованими IoT-компонентами необхідно розробити багаторівневу модель, яка інтегрує аналіз мережевого трафіку, поведінки пристроїв та стану віртуальних ресурсів. Якщо класифікація методів виявлення (рис. 1) описує загальні підходи, то модульна модель (рис. 2) конкретизує їх практичну реалізацію.

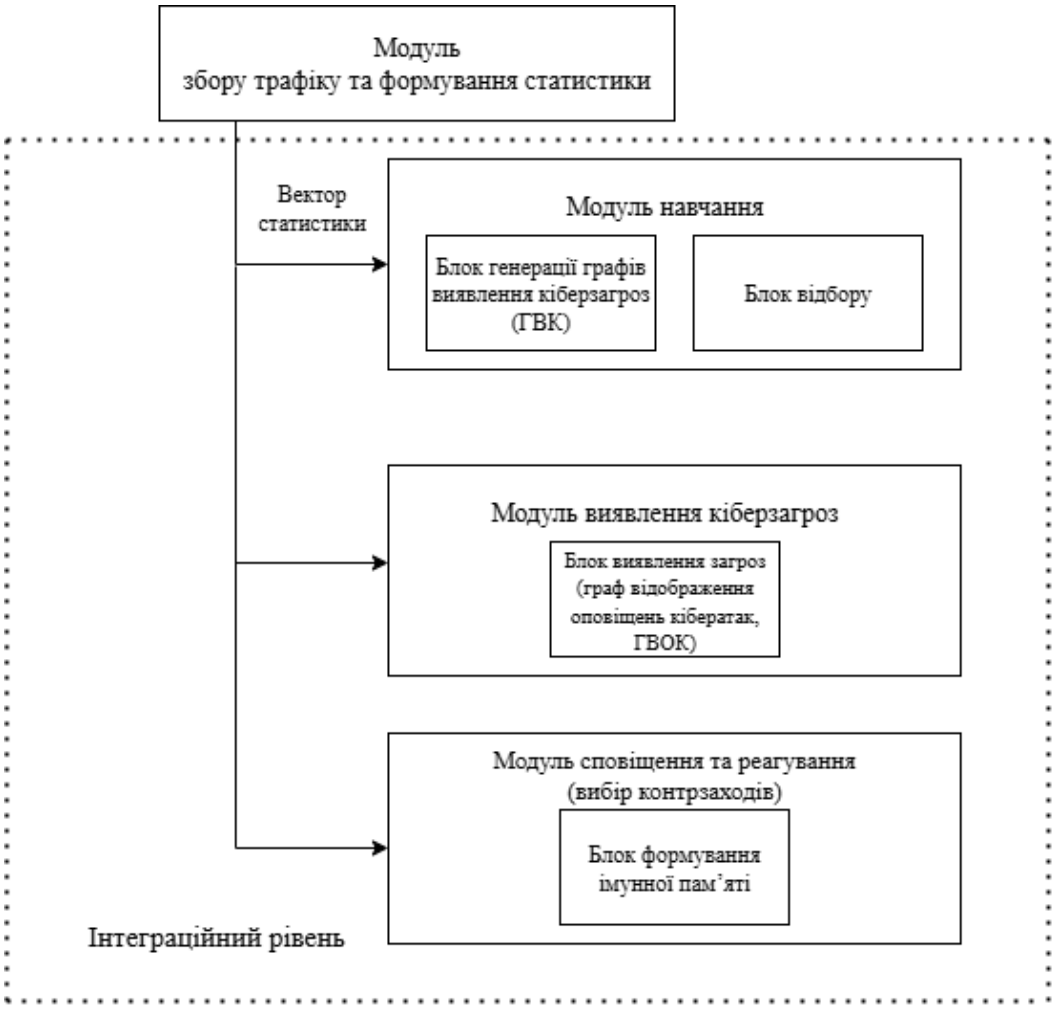

Рис. 2. Модульна модель виявлення кіберзагроз у хмарному середовищі з інтегрованими IoT-компонентами

Модуль збору трафіку та формування статистики відповідає за перехоплення та агрегування мережевого трафіку на ключових вузлах інфраструктури. Для хмарного середовища це включає обмін даними між віртуальними машинами, контейнерами та гібридними сервісами (SaaS, PaaS, IaaS).

Для IoT-пристроїв враховуються специфічні протоколи передачі — MQTT, CoAP, Zigbee, BLE, які характеризуються малими пакетами та низьким енергоспоживанням. Зібрані дані структуруються у вектори статистики, що відображають параметри потоків (швидкість, затримку, розмір пакетів, відхилення від базового рівня). Таким чином формується первинний набір даних для подальшого аналізу.

Завданням наступного *модуля навчання* є побудова графа виявлення кіберзагроз (ГВК). Для хмарної частини він відображає взаємозв'язки між віртуальними машинами, контейнерами та сервісами, показуючи потенційні «шляхи атаки».

Для IoT-пристроїв додаються шаблони їхньої поведінки — періодичність передавання даних, рівень споживання енергії, стабільність зв'язку. У складі модуля функціонує блок генерації графа та блок відбору, який виконує селекцію ознак і відсіювання «шумових» даних. Використовуючи алгоритми машинного навчання (нейронні мережі, дерева рішень, методи кластеризації), формується профіль «нормальної поведінки», від якого відстежуються відхилення.

На етапі *модуля виявлення кіберзагроз* відбувається кореляція між подіями у хмарі та в IoT-сегменті. Аномально високий трафік з датчика відеоспостереження у поєднанні з підозрілими змінами у хмарному контейнері може вказувати на DDoS-атаку або несанкціоноване використання ресурсів.

Для аналізу застосовується граф відображення оповіщень кібератак (ГВОК), який дозволяє простежити ланцюжки взаємопов'язаних інцидентів. Крім того, блок формування імунної пам'яті накопичує інформацію про попередні атаки й формує «бібліотеку» сценаріїв, які використовуються під час повторних або подібних загроз. Це підвищує адаптивність та знижує час реагування.

У хмарному сегменті модуль сповіщення та реагування призначений для вибору та ініціації контрзаходів сприяє ізоляції віртуальної машини, міграції контейнера на інший вузол чи зміні топології маршрутизації трафіку. В IoT-мережах застосовуються блокування підозрілих сенсорів, переведення пристроїв у «білий список» або реконфігурація шлюзів [8]. Важливо, що рішення приймаються адаптивно, залежно від сценарію атаки, виявленого у попередньому модулі.

Інтеграційний рівень координує обмін даними між хмарною інфраструктурою та сенсорними IoT-мережами, забезпечує уніфікацію форматів логів і телеметрії, розподілений збір даних з edge-пристроїв, а також балансування навантаження між аналітичними модулями у хмарі та на периферії (edge/fog computing). Завдяки цьому досягається масштабованість і можливість обробки подій у реальному часі [9].

Варто зауважити, що описана модульна модель дозволяє здійснювати моніторинг і виявлення загроз одночасно у двох взаємопов'язаних сегментах — віртуалізованій хмарі та розподілених мережах IoT-пристроїв. Вона інтегрує класичні методи виявлення з інтелектуальними підходами й забезпечує проактивний захист, здатний не лише фіксувати атаки, але й прогнозувати їх подальший розвиток [10].

ГРАФ ВИЯВЛЕННЯ КІБЕРЗАГРОЗ У ХМАРНОМУ СЕРЕДОВИЩІ З ІНТЕГРОВАНИМИ IOT-КОМПОНЕНТАМИ

Граф виявлення кіберзагроз (ГВК) у хмарних та IoT інфраструктурах слугує формалізованою моделлю, яка допомагає описати взаємозв'язки між вразливостями, активами та потенційними сценаріями атак (рис. 3).

Варто зазначити, що у хмарних середовищах вершинами графа виступають віртуальні машини, контейнери, сервіси зберігання та мережеві сегменти. У IoT-мережах це — сенсори, шлюзи, контролери та мобільні пристрої [11]. Таким чином, граф здатен відобразити багаторівневу структуру, у якій поєднано логічні ресурси хмари та фізичні точки доступу IoT.

Формально ГВК описується наступним чином, як орієнтований граф:

$$G_{\text{гвк}} = (V, E, W), \quad (1)$$

де V — множина вершин, що представляє вразливості та об'єкти інфраструктури; E — множина спрямованих ребер, що моделює можливі переходи з однієї стадії атаки до іншої; W — система вагових коефіцієнтів, яка характеризує ризик, складність виявлення та критичність переходу.

Щодо вершин, то вони зазвичай можуть бути трьох типів, а саме: V_1 — вузли вразливостей хмарних сервісів (наприклад, помилки у конфігурації контейнерів, відсутність оновлень віртуальної машини); V_2 — вузли вразливостей IoT-пристроїв (незахищені протоколи, використання дефолтних паролів, переповнення буферів); V_3 — вузли результатів використання вразливостей (наприклад, захоплення привілеїв, компрометація сенсора чи зловживання API хмари).

Для кожного ребра $e \in E$ визначаються метрики:

- R (Risk Score) — інтегральний показник небезпеки переходу, який розраховується на основі ймовірності експлуатації та потенційного впливу;
- L (Latency Impact) — показник затримки або деградації продуктивності, яку може викликати експлуатація уразливості (важливо для IoT у реальному часі);
- P (Propagation Factor) — коефіцієнт поширюваності атаки, що показує, наскільки швидко компрометація одного вузла може призвести до ураження сусідніх елементів (наприклад, «ефект доміно» у сенсорній мережі).

Таким чином, вагова функція для ребра може бути описана як:

$$W(e) = \alpha R + \beta L + \gamma P, \quad (2)$$

де α, β, γ — коефіцієнти ваги, які визначають пріоритети для конкретного середовища.

Використовуючи ГВК, можна побудувати сценарії багатоступеневих атак, які починаються з IoT-пристрою і закінчуються компрометацією хмарного сервісу, або навпаки — коли проникнення у віртуальну машину стає відправною точкою для зараження IoT-шлюзів[12].

Важливим елементом є те, що ГВК дозволяє не лише відобразити вже відомі вразливості, а й прогнозувати потенційні вектори атак. Для цього застосовуються методи кореляції оповіщень та аналітика поведінки пристроїв: наприклад, раптове збільшення енергоспоживання сенсора у поєднанні з аномаліями у віртуальному контейнері може сигналізувати про приховану атаку типу lateral movement.

У результаті, ГВК стає динамічною моделлю, яка постійно оновлюється за рахунок нових даних з IoT-пристроїв і хмарних логів [13]. Це забезпечує адаптивність системи захисту, а також можливість раннього виявлення складних комбінованих атак.

На основі побудованого графа виявлення кіберзагроз (рис. 3) функцію ваги переходу між вузлами, що враховує ризик експлуатації, вплив на затримку в системі та потенціал поширення атаки. Формалізація ваги ребра $W(e)$ розраховується за формулою (1), де вагові коефіцієнти $\alpha = 0.5, \beta = 0.3, \gamma = 0.2$ відповідають пріоритетам середовища, в якому ризик є домінуючим чинником, затримка має помірну вагу, а здатність атаки до поширення оцінюється як менш критична.

ISSN 2663 - 4023

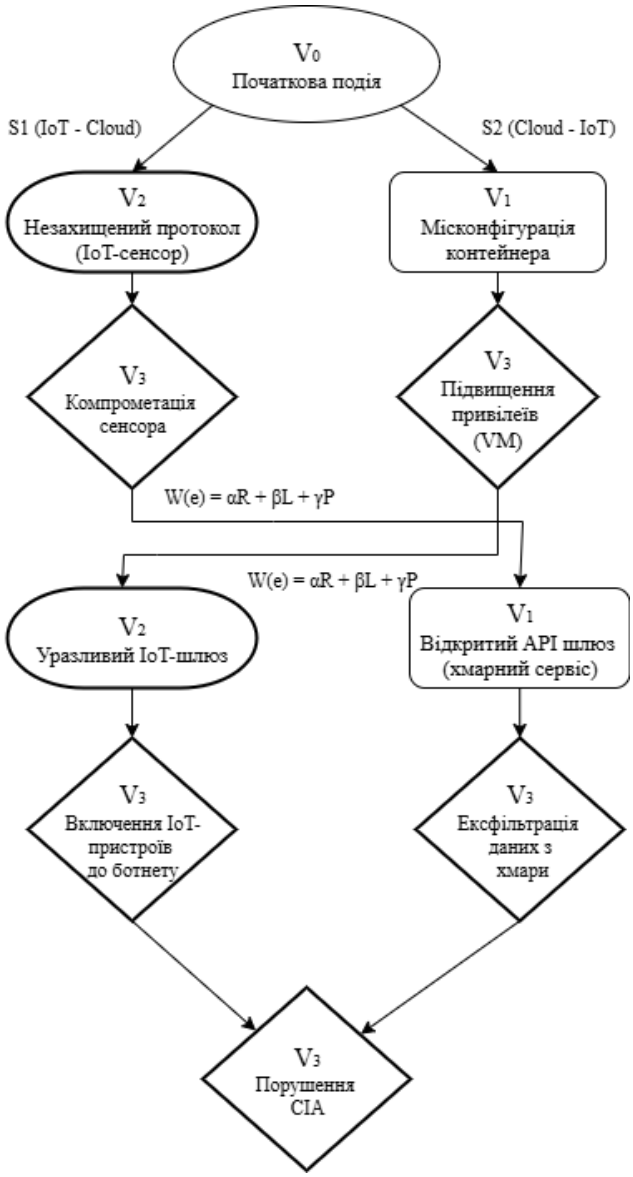

Рис. 3. Приклад графа виявлення кіберзагроз (ГВК) у хмарному середовищі з інтегрованими IoT-компонентами

Такий розподіл ваг відображає характерні особливості хмарній інфраструктурі з інтегрованими IoT-компонентами, що поєднують високу чутливість до затримок у реальному часі з обмеженим каскадуванням загроз — від базових вразливостей сенсорного рівня до комплексних сценаріїв експлуатації, які охоплюють граничні шлюзи та хмарні сервіси [14]. Розрахунок значень $W(e)$ наведено у табл. 1.

Таблиця 1

Значення метрик і розраховані ваги W(e) для сценаріїв атак

Сценарій	R	L	P	W(e)
1	0.2	0.1	0.3	0.20
2	0.4	0.2	0.5	0.37
3	0.6	0.4	0.6	0.54
4	0.7	0.5	0.7	0.66
5	0.9	0.7	0.8	0.84

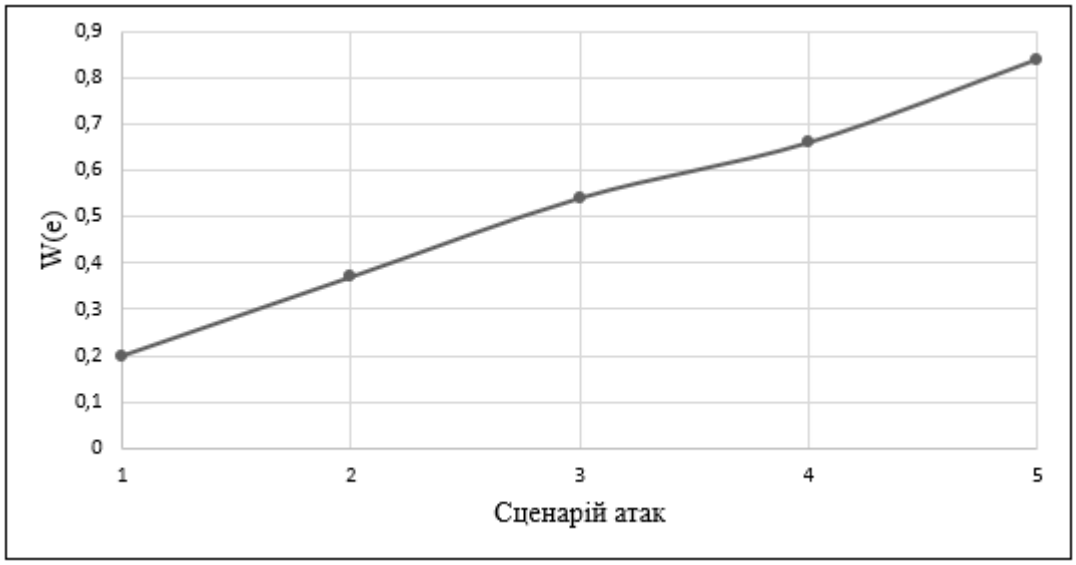

Рис.4. Залежність ваги переходу W(e) від сценарію атаки в хмарному середовищі з інтегрованими IoT-компонентами

Результати розрахунків представлено на Рис.4, і показують монотонне зростання ваги переходу зі збільшенням значень ризику, затримки та поширюваності (R, L і P). Тому можна стверджувати, що запропонована модель дозволяє кількісно оцінювати небезпечність переходів між вузлами ГВК залежно від складності сценарію атаки.

ГРАФ ВІДОБРАЖЕННЯ ОПОВІЩЕНЬ КІБЕРАТАК У ХМАРНОМУ СЕРЕДОВИЩІ З ІНТЕГРОВАНИМИ ІОТ-КОМПОНЕНТАМИ

Граф відображення оповіщень кібератак (ГВОК) є механізмом формалізації та кореляції подій безпеки, що надходять із різнорідних джерел: логів хмарних сервісів, журналів віртуалізованих середовищ та телеметрії IoT-пристроїв (рис.5).

На відміну від класичних систем, у хмарному середовищі з інтегрованими IoT-компонентами події розподілені як у логічному просторі (віртуальні машини, контейнери, API), так і у фізичному (сенсори, шлюзи, мобільні пристрої) [15].

Формально ГВОК описується як орієнтований граф, наступним чином:

$$G_{\text{гвок}} = (A, E, P, M), \quad (3)$$

де A — множина оповіщень, що містять дані про аномалії у хмарі та IoT; E — множина спрямованих ребер, що відображають причинно-часові зв'язки між подіями; P — множина маршрутів, які моделюють сценарії проходження кібератак; M — метрики, що характеризують якість і пріоритетність оповіщень.

Кожне оповіщення $a \in A$ є структурованим повідомленням, яке включає IP-адресу або ідентифікатор віртуального ресурсу (у випадку хмари) чи MAC-адресу сенсора (у випадку IoT), часову мітку події, тип загрози (аномалія трафіку, несанкціонований доступ, спроба експлуатації вразливості) та рівень критичності.

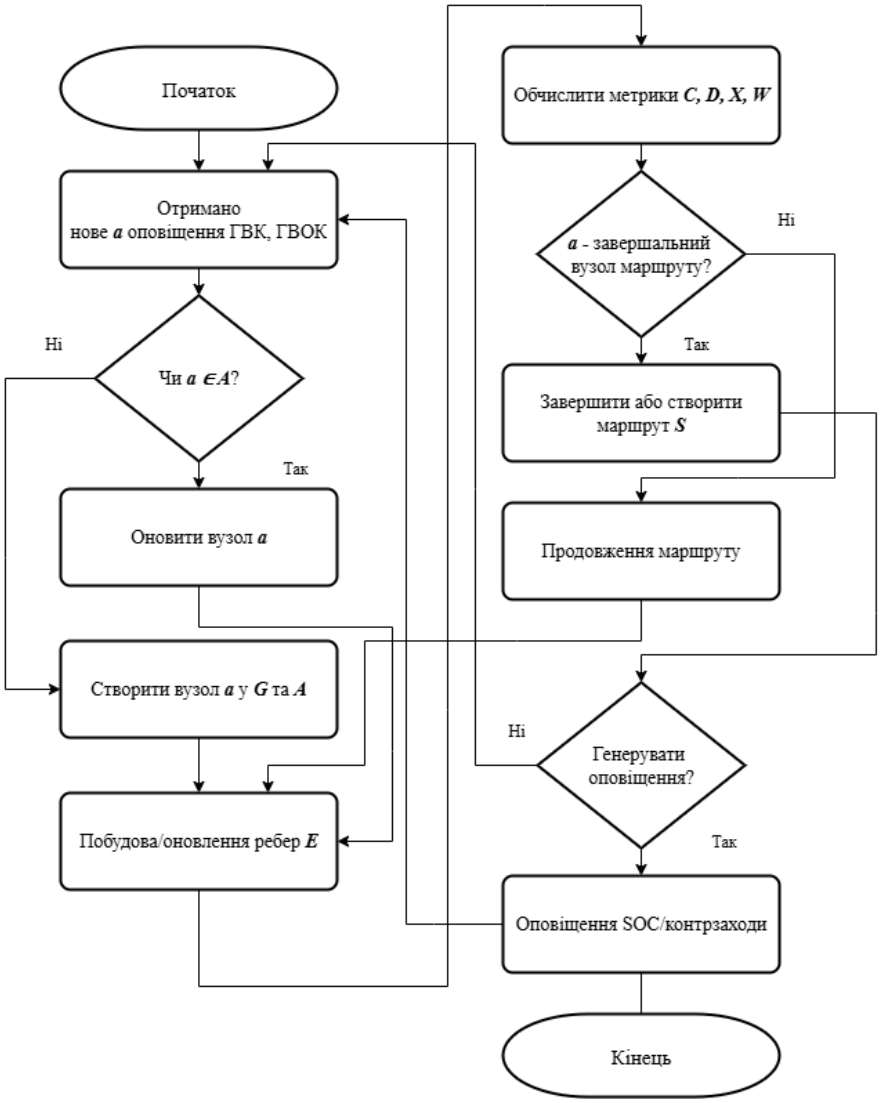

Рис. 5. Алгоритм відображення оповіщень кібератак у хмарному середовищі з інтегрованими IoT-компонентами

Особливістю ГВОК у хмарних системах з інтегрованими IoT-компонентами є те, що ребра E відображають не лише часову послідовність подій, але й кореляцію між різними доменами: наприклад, збій у сенсорі температури може співпадати з підозрілою активністю у контейнері, який отримує дані від цього сенсора.

Для більш глибокого аналізу вводяться такі метрики:

- C (Confidence) — ймовірність того, що оповіщення дійсно відображає атаку, а не хибне спрацювання;
- D (Propagation Delay) — часовий інтервал між двома оповіщеннями, що формують ланцюжок атаки (важливий для IoT, де атаки можуть розгортатися поступово);
- X (Cross-Domain Correlation) — коефіцієнт кореляції подій між хмарним та IoT-сегментами (чим вище значення, тим більша ймовірність комплексної атаки).

Таким чином, маршрут $S_i \subset P$ у ГВОК може виглядати як ланцюг:

$$S_i = \{aIoT1 \rightarrow aIoT2 \rightarrow aCloud1 \rightarrow aCloud2\}, \quad (4)$$

де атака починається з компрометації IoT-пристрою, потім поширюється на шлюз і зрештою зачіпає хмарні сервіси.

Важливою властивістю ГВОК є його здатність виявляти комбіновані атаки. Наприклад:

- масове сканування IoT-пристроїв у мережі;
- подальше зараження частини сенсорів;
- використання їх як «точок входу» для доступу до приватної хмари;
- ексфільтрація даних з віртуальної машини.

Завдяки виявленню таких маршрутів у ГВОК система отримує змогу прогнозувати можливий розвиток атаки ще до того, як вона досягне критично важливих вузлів.

ВИБІР КОНТРЗАХОДІВ У ХМАРНОМУ СЕРЕДОВИЩІ З ІНТЕГРОВАНИМИ IOT-КОМПОНЕНТАМИ

Після того як система визначила можливий маршрут проходження кібератаки, необхідно обрати оптимальні контрзаходи, які одночасно будуть ефективними проти загрози та мінімізуватимуть вплив на продуктивність середовища.

У випадку хмарної інфраструктури з інтегрованими IoT-компонентами завдання ускладнюється через розподілений характер системи: контрзаходи можуть стосуватися як віртуалізованих ресурсів у хмарі, так і сенсорних пристроїв на периферії [16].

Контрзаходи для хмарного середовища можуть включати ізоляцію або тимчасове вимкнення віртуальної машини, що демонструє підозрілу активність, міграцію контейнерів на «чисті» вузли для запобігання поширенню атак, перебудову маршрутизації трафіку у SDN-середовищі (Software-Defined Networking) або динамічне посилення політик доступу до API або сховищ даних.

Контрзаходи для IoT-сегменту можуть містити наступні кроки: блокування або переведення в «режим карантину» сенсорів із підозрілою поведінкою, оновлення прошивки та примусове перезавантаження IoT-пристроїв, сегментація IoT-мережі, щоб зменшити ймовірність поширення атаки або пріоритезація «білого списку» довірених пристроїв[17].

Для обґрунтованого вибору контрзаходів доцільно використовувати мультикритеріальну оцінку, яка враховує не лише вартість чи інтрузивність заходу, але й специфіку розподілених систем. Для цього доцільно описати наступні метрики:

- (Operational Overhead) — додаткові витрати ресурсів на реалізацію контрзаходу (наприклад, міграція контейнера потребує обчислювальних і мережевих ресурсів);
- SCI (Service Continuity Index) — показник впливу контрзаходу на безперервність роботи сервісу; чим вищий SCI, тим менше ймовірність переривання критичних сервісів;
- CE (Containment Efficiency) — коефіцієнт, що відображає, наскільки ефективно контрзахід локалізує атаку в обмеженому сегменті;
- TRT (Trust Recovery Time) — час, необхідний для відновлення повної функціональності системи після застосування контрзаходу.

Комплексний показник вибору контрзаходу можна описати наступним чином:

$$Y = \frac{\alpha \cdot \mathrm{CE} + \beta \cdot \mathrm{SCI}}{\gamma \cdot \mathrm{O} + \delta \cdot \mathrm{TRT}}, \quad (5)$$

де α,β,γ,δ — коефіцієнти ваги, що визначають пріоритети конкретного середовища (наприклад, для промислового IoT важливішим є мінімальний TRT, тоді як у фінансових хмарах ключовим фактором може виступати SCI).

У випадку виявлення DDoS-атаки через IoT-камери система може:

- відключити або ізолювати групу пристроїв (високий CE, низький SCI, бо вплине на сервіс відеомоніторингу);
- перенаправити трафік на віртуальні фільтри у хмарі (середній CE, високий SCI, більший O).

Вибір оптимального варіанту залежить від обчисленого показника Y.

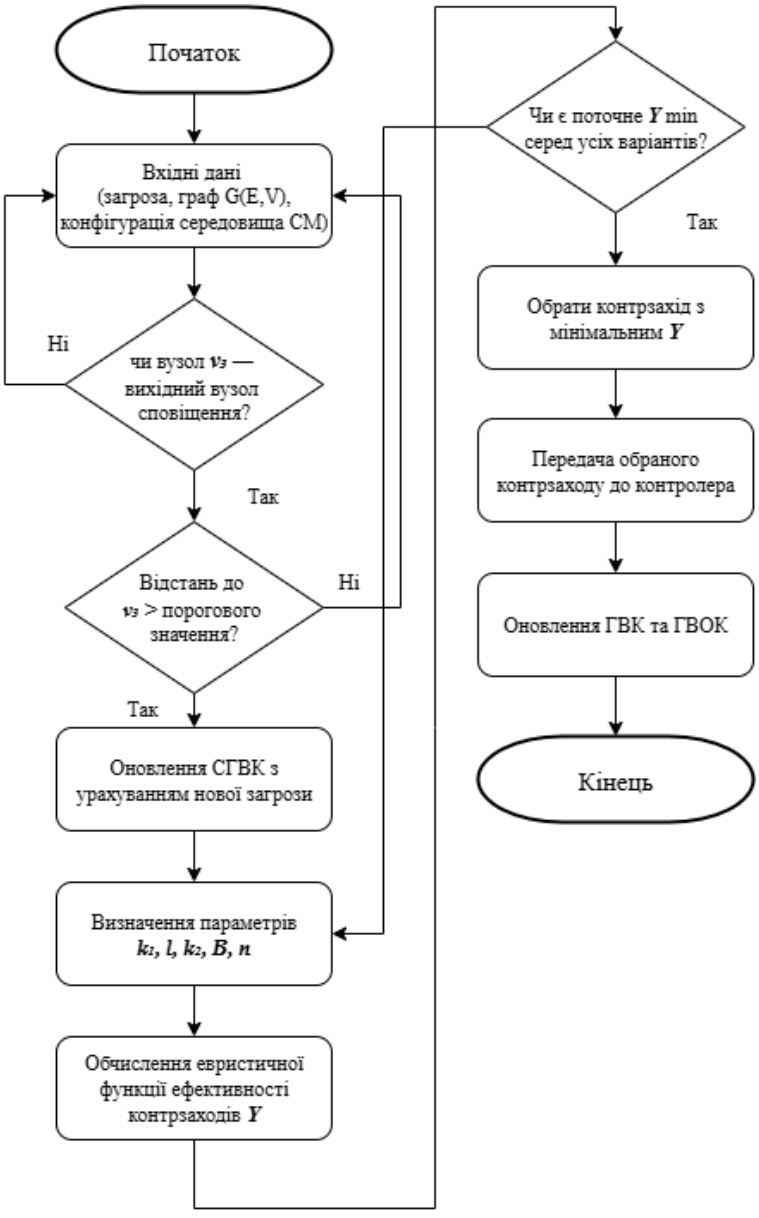

Рис.6. Алгоритм визначення контрзаходів отриманої загрози

Таким чином, процес вибору контрзаходів у хмарному середовищі з інтегрованими IoT-компонентами базується на балансі між ефективністю локалізації атаки та збереженням безперервності роботи сервісів [18]. Це дозволяє формувати адаптивну стратегію кіберзахисту, яка динамічно змінюється залежно від характеру атаки і критичності уражених компонентів.

ВИСНОВКИ ТА ПЕРСПЕКТИВИ ПОДАЛЬШИХ ДОСЛІДЖЕНЬ

У статті запропоновано оптимізовану методику виявлення та локалізації кіберзагроз у хмарних середовищах з інтегрованими IoT-компонентами, яка ґрунтується на застосуванні графових моделей — графа виявлення кіберзагроз (ГВК) та графа відображення оповіщень кібератак (ГВОК). Методика передбачає моделювання сценаріїв поширення загроз із використанням формалізованих переходів між вузлами інфраструктури, а також реалізацію мультикритеріального підходу до вибору контрзаходів із врахуванням показників ризику, продуктивності та ефективності локалізації.

Запропонований підхід забезпечує проактивний характер моніторингу та реагування в умовах гібридних середовищ, дозволяючи динамічно адаптувати засоби захисту до поточних умов інфраструктури. Формалізація ваги переходу між вузлами у вигляді $W(e) = \alpha R + \beta L + \gamma P$, а також інтегральна метрика Y для пріоритезації контрзаходів, надають можливість кількісної оцінки маршрутів атаки та прогнозування їхнього потенційного впливу на безперервність функціонування сервісів.

Перспективи подальших досліджень полягають у динамічному підлаштуванні вагових коефіцієнтів у моделі $W(e)$ відповідно до типу атак і контексту конкретного середовища, оптимізації метрики Y з урахуванням параметрів SLA та ризик-орієнтованих сценаріїв, а також у розширенні графових моделей для охоплення міждоменної взаємодії в edge/fog-архітектурах. Окрему увагу доцільно приділити інтеграції алгоритмів глибинного навчання для автоматичного профілювання нових IoT-пристроїв та аномальної поведінки, а також розробці інструментів візуалізації динамічних ГВК/ГВОК у режимі реального часу для покращення інформованості операторів безпеки та зниження часу реакції на складні загрози.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Hulak, H. M., Zhyltsov, O. B., Kyrychok, R. V., Korshun, N. V., & Skladannyi, P. M. (2023). *Enterprise information and cyber security* [Textbook]. Kyiv: Borys Grinchenko Kyiv Metropolitan University.
2. Sáez-de-Cámara, X., Flores, J. L., Arellano, C., Urbieta, A., & Zurutuza, U. (2023). Clustered federated learning architecture for network anomaly detection in large scale heterogeneous IoT networks. *Computers & Security, 131*, 103299. https://doi.org/10.1016/j.cose.2023.103299
3. Kostiuk, Y., Dovzhenko, N., Mazur, N., Skladannyi, P., & Rzaieva, S. (2025). Методика захисту GRID-середовища від шкідливого коду під час виконання обчислювальних завдань [Methodology for protecting GRID environment from malicious code during computational tasks]. *Cybersecurity: Education, Science, Technique, 3*(27), 22–40. https://doi.org/10.28925/2663-4023.2025.27.710
4. Amarnath, L., Shah, P., Chandramouli, H., & Arun, S. (2019). Trustworthy cloud services for IoT security: Triple integration of security, privacy and reputation. *International Journal of Engineering and Advanced Technology, 8*, 3280–3283. https://doi.org/10.35940/ijeat.F9536.088619
5. Yang, Y.-M., Chang, K.-C., & Luo, J.-N. (2025). Hybrid neural network-based intrusion detection system: Leveraging LightGBM and MobileNetV2 for IoT security. *Symmetry, 17*(3), 314. https://doi.org/10.3390/sym17030314
6. Dovzhenko, N., Mazur, N., Skladannyi, P., Kostiuk, Y., & Rzaieva, S. (2024). Інтеграція IoT та штучного інтелекту в інтелектуальні транспортні системи [Integration of IoT and artificial intelligence into intelligent transport systems]. *Cybersecurity: Education, Science, Technique, 2*(26), 430–444. https://doi.org/10.28925/2663-4023.2024.26.708
7. Popovska, H., Dimovski, T., & Popovski, F. (2024). The role of cloud providers in IoT services. *International Journal of Computer Science and Information Technology, 16*, 85–95. https://doi.org/10.5121/ijcsit.2024.16407
8. Gulfam, U. H., Iqra, Y., Muhammad, A., Tehseen, M., Khan, M., Ines, J., & Habib, H. (2025). Energy-efficient deep learning-based intrusion detection system for edge computing: A novel DNN-KDQ model. *Journal of Cloud Computing, 14*. https://doi.org/10.1186/s13677-025-00762-9

9. Kostiuk, Y. V., Skladannyi, P. M., Bebeshko, B. T., Khorolska, K. V., Rzaieva, S. L., & Vorokhob, M. V. (2025). *Information and communication systems security* [Textbook]. Kyiv: Borys Grinchenko Kyiv Metropolitan University.
10. Engr, Z., Mushtaher, U., Ahsan, H. M., Aribah, M., Syed, H., & Chaman, B. (2025). AI-driven cybersecurity for IoT-cloud ecosystems. *Physical Education Health and Social Sciences, 3*, 63–76. https://doi.org/10.5281/zenodo.17079810
11. Dovzhenko, N., Ivanichenko, Y., Skladannyi, P., & Ausheva, N. (2024). Інтеграція безпеки та відмовостійкості сенсорних мереж на основі аналізу енергоспоживання та трафіку [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
12. Mallidi, S. K. R., & Ramisetty, R. R. (2025). A multi-level intrusion detection system for industrial IoT using bowerbird courtship-inspired feature selection and hybrid data balancing. *Discover Computing, 28*, 109. https://doi.org/10.1007/s10791-025-09632-z
13. Prasad, A., Alenazy, W., Ahmad, N., Ali, G., Abdallah, H., & Ahmad, S. (2025). Optimizing IoT intrusion detection with cosine similarity-based dataset balancing and hybrid deep learning. *Scientific Reports, 15*. https://doi.org/10.1038/s41598-025-15631-3
14. Barabash, O., Ausheva, N., Skladannyi, P., Ivanichenko, Y., & Dovzhenko, N. (2024). Технічні аспекти побудови відмовостійкої інфраструктури сенсорної мережі [Technical aspects of building a fault-tolerant sensor network infrastructure]. *Cybersecurity: Education, Science, Technique, 4*(24), 185–195. https://doi.org/10.28925/2663-4023.2024.24.185195
15. Kostiuk, Y. V., Skladannyi, P. M., Hulak, H. M., Bebeshko, B. T., Khorolska, K. V., & Rzaieva, S. L. (2025). *Information security systems* [Textbook]. Kyiv: Borys Grinchenko Kyiv Metropolitan University.
16. Rampone, G., Ivaniv, T., & Rampone, S. (2025). A hybrid federated learning framework for privacy-preserving near-real-time intrusion detection in IoT environments. *Electronics, 14*(7), 1430. https://doi.org/10.3390/electronics14071430
17. Kikissagbe, B. R., & Adda, M. (2024). Machine learning-based intrusion detection methods in IoT systems: A comprehensive review. *Electronics, 13*(18), 3601. https://doi.org/10.3390/electronics13183601
18. Wang, Y., Han, Z., Du, Y., Li, J., & He, X. (2025). BS-GAT: A network intrusion detection system based on graph neural network for edge computing. *Cybersecurity, 8*. https://doi.org/10.1186/s42400-024-00296-8

КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 1 (29), 2025
ISSN 2663 - 4023

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

Yevhen Ivanichenko
PhD, Associate Professor, Deputy Dean for Scientific-Methodological and Educational Work
Borys Grinchenko Kyiv Metropolitan University Kyiv, Ukraine
ORCID ID: 0000-0002-6408-443X
y.ivanichenko@kubg.edu.ua

Yuliia Kostiuk
PhD in Computer Science
Associate Professor of the Department of Information and Cybernetic Security
named after Professor Volodymyr Buriachok
Borys Grinchenko Kyiv Metropolitan University, Kyiv, Ukraine
ORCID ID: 0000-0001-5423-0985
y.kostiuk@kubg.edu.ua

Liubomyr Petryshyn
Doctor of Technical Sciences, Professor,
Professor of the Department of Computer Science and Information Systems
Vasyl Stefanyk Carpathian National University, Ivano-Frankivsk, Ukraine
ORCID ID: 0000-0003-4168-3891
lubomyr.petryshyn@pnu.edu.ua

GRAPH-BASED METHODOLOGY FOR DETECTION AND LOCALIZATION OF CYBER THREATS IN CLOUD ENVIRONMENTS WITH INTEGRATED IOT COMPONENTS

Abstract. This paper proposes a methodology for detecting and localizing cyber threats in cloud environments integrated with IoT components. The approach relies on two complementary models: the Cyber-Threat Detection Graph (CTDG), which captures the multi-layered structure of attacks while accounting for risk, latency, and propagation potential; and the Cyberattack Alert Mapping Graph (CAMG), which models temporal–causal dependencies among events to reveal complex and combined threats. CAMG enables the construction of sequential event chains from telemetry, logs, and behavioral anomalies, integrating data from cloud services and IoT devices. This makes it possible not only to identify individual incidents but also to forecast the evolution of multi-stage attacks. To select response options, a generalized evaluation metric is applied that considers the effectiveness of threat localization, service continuity, and the time required to restore system trust. This supports the prioritization of countermeasures while minimizing the impact on critical resources. The proposed methodology blends classical and intelligent threat-analysis techniques, provides proactive monitoring, and remains adaptable under the high dynamism of cloud infrastructures. The solution targets deployment in mission-critical computing systems, industrial data centers, IoT networks, and cloud platforms, where maintaining a balance among security, performance, and infrastructure resilience is essential.

Keywords: cloud environment; cloud services; Internet of Things (IoT); countermeasures; cyber incident; edge computing; infrastructure; sensor networks; information security; graph; cyber resilience; model; threats; integration.

REFERENCES (TRANSLATED AND TRANSLITERATED)

1. Hulak, H. M., Zhyltsov, O. B., Kyrychok, R. V., Korshun, N. V., & Skladannyi, P. M. (2023). *Enterprise information and cyber security* [Textbook]. Kyiv: Borys Grinchenko Kyiv Metropolitan University.
2. Sáez-de-Cámara, X., Flores, J. L., Arellano, C., Urbieta, A., & Zurutuza, U. (2023). Clustered federated learning architecture for network anomaly detection in large scale heterogeneous IoT networks. *Computers & Security, 131*, 103299. https://doi.org/10.1016/j.cose.2023.103299
3. Kostiuk, Y., Dovzhenko, N., Mazur, N., Skladannyi, P., & Rzaieva, S. (2025). Methodology for protecting GRID environment from malicious code during computational tasks. *Cybersecurity: Education, Science, Technique, 3*(27), 22–40. https://doi.org/10.28925/2663-4023.2025.27.710
4. Amarnath, L., Shah, P., Chandramouli, H., & Arun, S. (2019). Trustworthy cloud services for IoT security: Triple integration of security, privacy and reputation. *International Journal of Engineering and Advanced Technology, 8*, 3280–3283. https://doi.org/10.35940/ijeat.F9536.088619
5. Yang, Y.-M., Chang, K.-C., & Luo, J.-N. (2025). Hybrid neural network-based intrusion detection system: Leveraging LightGBM and MobileNetV2 for IoT security. *Symmetry, 17*(3), 314. https://doi.org/10.3390/sym17030314
6. Dovzhenko, N., Mazur, N., Skladannyi, P., Kostiuk, Y., & Rzaieva, S. (2024). Integration of IoT and artificial intelligence into intelligent transport systems. *Cybersecurity: Education, Science, Technique, 2*(26), 430–444. https://doi.org/10.28925/2663-4023.2024.26.708
7. Popovska, H., Dimovski, T., & Popovski, F. (2024). The role of cloud providers in IoT services. *International Journal of Computer Science and Information Technology, 16*, 85–95. https://doi.org/10.5121/ijcsit.2024.16407
8. Gulfam, U. H., Iqra, Y., Muhammad, A., Tehseen, M., Khan, M., Ines, J., & Habib, H. (2025). Energy-efficient deep learning-based intrusion detection system for edge computing: A novel DNN-KDQ model. *Journal of Cloud Computing, 14*. https://doi.org/10.1186/s13677-025-00762-9
9. Kostiuk, Y. V., Skladannyi, P. M., Bebeshko, B. T., Khorolska, K. V., Rzaieva, S. L., & Vorokhob, M. V. (2025). *Information and communication systems security* [Textbook]. Kyiv: Borys Grinchenko Kyiv Metropolitan University.
10. Engr, Z., Mushtaher, U., Ahsan, H. M., Aribah, M., Syed, H., & Chaman, B. (2025). AI-driven cybersecurity for IoT-cloud ecosystems. *Physical Education Health and Social Sciences, 3*, 63–76. https://doi.org/10.5281/zenodo.17079810
11. 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
12. Mallidi, S. K. R., & Ramisetty, R. R. (2025). A multi-level intrusion detection system for industrial IoT using bowerbird courtship-inspired feature selection and hybrid data balancing. *Discover Computing, 28*, 109. https://doi.org/10.1007/s10791-025-09632-z
13. Prasad, A., Alenazy, W., Ahmad, N., Ali, G., Abdallah, H., & Ahmad, S. (2025). Optimizing IoT intrusion detection with cosine similarity-based dataset balancing and hybrid deep learning. *Scientific Reports, 15*. https://doi.org/10.1038/s41598-025-15631-3
14. Barabash, O., Ausheva, N., Skladannyi, P., Ivanichenko, Y., & Dovzhenko, N. (2024). Technical aspects of building a fault-tolerant sensor network infrastructure. *Cybersecurity: Education, Science, Technique, 4*(24), 185–195. https://doi.org/10.28925/2663-4023.2024.24.185195
15. Kostiuk, Y. V., Skladannyi, P. M., Hulak, H. M., Bebeshko, B. T., Khorolska, K. V., & Rzaieva, S. L. (2025). *Information security systems* [Textbook]. Kyiv: Borys Grinchenko Kyiv Metropolitan University.
16. Rampone, G., Ivaniv, T., & Rampone, S. (2025). A hybrid federated learning framework for privacy-preserving near-real-time intrusion detection in IoT environments. *Electronics, 14*(7), 1430. https://doi.org/10.3390/electronics14071430
17. Kikissagbe, B. R., & Adda, M. (2024). Machine learning-based intrusion detection methods in IoT systems: A comprehensive review. *Electronics, 13*(18), 3601. https://doi.org/10.3390/electronics13183601
18. Wang, Y., Han, Z., Du, Y., Li, J., & He, X. (2025). BS-GAT: A network intrusion detection system based on graph neural network for edge computing. *Cybersecurity, 8*. https://doi.org/10.1186/s42400-024-00296-8