КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 2 (34), 2026
ISSN 2663 – 4023
DOI 10.28925/2663-4023.2026.34.1336
УДК 004.056.5

Нєдєльніцев Іван В'ячеславович
аспірант кафедри комп'ютерної радіоінженерії та систем технічного захисту інформації
Харківський національний університет радіоелектроніки, Харків, Україна
ORCID:0009-0004-5265-3561
ivan.niedielnitsev@nure.ua

Антіпов Іван Євгенійович
доктор технічних наук, професор, професор кафедри комп'ютерної радіоінженерії та систем технічного захисту інформації
Харківський національний університет радіоелектроніки, Харків, Україна
ORCID:0000-0002-9754-4412
ivan.antipov@nure.ua

МІКРОСЕГМЕНТАЦІЯ IoT-МЕРЕЖ В АРХІТЕКТУРІ НУЛЬОВОЇ ДОВІРИ

Анотація. Масштабування інфраструктур Інтернету речей (IoT) супроводжується появою надлишкової мережевої зв'язності, що розширює поверхню атаки та створює умови для латерального переміщення зловмисника після компрометації окремого вузла. У статті запропоновано автоматизований гібридний метод мікросегментації IoT-мереж, який реалізує принципи архітектури нульової довіри (Zero Trust) шляхом поєднання спектральної кластеризації графа мережі з евристичним прунінгом на основі рольових правил. Мережа моделюється як орієнтований граф з ієрархічними рівнями пристроїв (периферія, агрегація, шлюзи, хмара) та коефіцієнтами критичності вузлів. Розроблено генератор синтетичних топологій із керованим рівнем шуму, який відтворює функціональне ядро зв'язків і стохастичну ентропійну складову за механізмами преференційного приєднання та зональної афінності. Для кількісного оцінювання якості сегментації сформовано систему зважених метрик: зважене зменшення поверхні атаки (wASR), зважений індекс латерального руху (wLMI), частку хибних блокувань (FBR) та коефіцієнт стиснення політики (PCR). Експериментальне дослідження охоплює три масштаби мереж (близько 30, 330 та 950 пристроїв) при інтенсивності шуму від 0 до 5; результати усереднено за трьома незалежними прогонами, наведено 95% довірчі інтервали. Показано, що для великомасштабних мереж метод знижує зважений індекс латерального руху на 72-88% залежно від рівня шуму, утримуючи частку хибних блокувань у межах 1,5-3% при помірному зашумленні, що забезпечує збереження функціональної цілісності системи. Продемонстровано, що синтезовані політики доступу є компактними (коефіцієнт стиснення політики 0,71–0,83 при високому зашумленні), що знижує операційну складність адміністрування безпеки. Визначено обмеження методу для мереж малого масштабу, де розрідженість графа підвищує чутливість до шуму. Окреслено перспективи подальших досліджень: динамічна ресегментація в режимі реального часу, автоматичний вибір кількості сегментів та валідація методу на реальних наборах даних IoT-трафіку.

Ключові слова: архітектура нульової довіри; мікросегментація; Інтернет речей; спектральна кластеризація; політика доступу; латеральне переміщення; поверхня атаки; графова модель мережі.

ВСТУП

Постановка проблеми. Розгортання великих і різнорідних IoT-систем (від розумних домівок до масштабних міських та індустріальних мереж) неминуче створює надлишкові та хаотичні канали зв'язку між вузлами. Така структурна ентропія суттєво розширює поверхню атаки та створює ідеальні умови для горизонтального переміщення зловмисника після компрометації периметра. Горизонтальне переміщення – це техніка, яку використовують зловмисники для навігації мережею та ескалації привілеїв після отримання початкового доступу. Первинна компрометація мережі може відбутися кількома шляхами: через обхід застарілих заходів безпеки, експлуатацію вразливостей програмного забезпечення або

використання легкодоступних IoT-пристроїв, підключених до глобальної мережі (наприклад, IP-камер чи смарт-сенсорів) [1].

На практиці це означає, що зловмисник, отримавши доступ до одного низькопривілейованого периферійного пристрою, може рухатися мережею до критичних вузлів (шлюзів, контролерів або хмарних сервісів), експлуатуючи дозволені, але функціонально зайві маршрути. Відповідно, це призводить до компрометації всієї інфраструктури. У відкритій літературі наразі бракує відтворюваних методик кількісної оцінки ефекту протидії горизонтальному переміщенню саме для зашумлених IoT-мереж, де необхідно зберігати крихкий баланс між безпекою, працездатністю та керованістю політик доступу [2].

Основними архітектурними підходами до протидії цій загрозі є впровадження парадигми Zero Trust, застосування принципу найменших привілеїв (PoLP) та мікросегментація мережі. Модель Zero Trust та PoLP вимагають радикальної мінімізації доступів (залишаючи виключно ті, що необхідні для бізнес-логіки) та запровадження суворої контекстної авторизації, що нівелює можливість вільного переміщення всередині системи [3, 4]. Мікросегментація, як практичний інструмент реалізації Zero Trust, дозволяє розмежовувати трафік на рівні окремих вузлів та мікро-зон, розриваючи транзитивні шляхи атаки для зловмисника.

Дана робота фокусується на автоматизації мікросегментації, оскільки саме архітектурне обмеження зв’язності дає найбільш вимірюваний та превентивний вплив на масштаб потенційної кібератаки. Зважаючи на те, що ручне формування політик доступу для тисяч пристроїв є неможливим завданням, ставиться задача розробки алгоритму автоматичного синтезу політик.

У цій роботі пропонується гібридний метод мікросегментації, що базується на застосуванні спектральної кластеризації графів для виявлення функціональних спільнот та евристичного аналізу для усунення структурних вразливостей мережі. Для оцінки ефективності запропонованого методу розроблено програмний інструментарій, що дозволяє:

– Симулювати топології IoT-мереж різного масштабу з додаванням контрольованого “шуму” у вигляді випадкових зв’язків.
– Автоматично синтезувати політики безпеки на основі виявлених кластерів.
– Кількісно вимірювати результати сегментації за допомогою спеціалізованих метрик:
– wASR (Weighted Attack-Surface Reduction) – зважене зменшення поверхні атаки;
– wLMI (Weighted Lateral Movement Index) – зважений індекс горизонтального переміщення;
– FBR (False Block Rate) – частка хибних блокувань легітимного трафіку;
– PCR (Policy Compression Ratio) – ефективність стиснення правил.

Проведений на основі отриманих топологій експериментальний аналіз доводить здатність алгоритму ефективно “фільтрувати” аномальні зв’язки та кардинально знижувати ризики кібербезпеки при збереженні функціональності IoT-системи.

Аналіз останніх досліджень і публікацій. Проблема захисту IoT-інфраструктур вийшла за межі традиційних методів мережевої безпеки через високе різноманіття пристроїв, відсутність стандартизації та обмежені обчислювальні ресурси кінцевих вузлів. У цьому розділі проаналізовано існуючі підходи до сегментації мереж, автоматизації політик безпеки та математичних методів кластеризації, а також визначено невирішені проблеми, на розв’язання яких спрямоване дане дослідження.

А. Парадигма Zero Trust та проблеми мікросегментації в IoT.

Традиційна периметрова модель захисту, заснована на припущенні довіри до внутрішнього сегмента мережі, демонструє обмежену ефективність у середовищах IoT із високим різноманіттям пристроїв та великим масштабом.

У документі NIST SP 800-207 [5] архітектура Zero Trust (ZTA) формалізується як парадигма, в якій мережа за замовчуванням розглядається як потенційно скомпрометована, а доступ до ресурсів надається виключно на основі динамічної оцінки політик, контексту та рівня ризику. Основним положеннями ZTA є відмова від довіри за замовчуванням, безперервна верифікація суб’єктів і пристроїв, застосування принципу найменших привілеїв та логічна мікросегментація ресурсів із контролем доступу на рівні окремих взаємодій. Таким чином, захист переноситься з мережевого периметра на рівень конкретного ресурсу, а рішення щодо доступу приймається індивідуально для кожного запиту.

У роботі “Anatomy of Threats to The Internet of Things“ [6] показано, що відсутність внутрішньої сегментації та ізоляції пристроїв є системною причиною успішних атак у IoT-екосистемах. Автори демонструють, що після первинної компрометації одного вузла (наприклад, через слабку автентифікацію або вразливу прошивку) зловмисник отримує можливість горизонтального (латерального) переміщення в мережі, що суттєво підвищує масштаб інциденту. Така відсутність ізоляції сприяє формуванню ботнетів і реалізації розподілених атак відмови в обслуговуванні (DDoS), оскільки заражені вузли можуть

безперешкодно взаємодіяти в межах єдиного логічного сегмента. Отже, внутрішня сегментація виступає не лише механізмом контролю доступу, а й інструментом обмеження поширення загроз у межах системи.

Водночас, як зазначено у дослідженні "Zero-Trust Hierarchical Management in IoT" [7], пряме застосування класичних підходів мікросегментації в IoT ускладнюється специфікою середовища: великою кількістю пристроїв, їхньою динамічною появою та обмеженими обчислювальними ресурсами. Ручне адміністрування списків контролю доступу або централізовані механізми перевірки стають неможливими в умовах масштабування. У відповідь запропоновано ієрархічну модель управління довірою на основі блокчейну – Amatista, яка поєднує Zero Trust з механізми сегментованого надання даних. Такий підхід забезпечує ізоляцію взаємодій між вузлами, залежну від контексту, без необхідності централізованого контролю кожної транзакції.

Окремо варто відзначити роботу [8], у якій запропоновано автоматизовану мікросегментацію промислових IoT-мереж (IIoT) із застосуванням методів машинного навчання для запобігання латеральному переміщенню, що підтверджує актуальність автоматизації сегментації для індустріальних середовищ.

Отже, можна зробити проміжний висновок, що мікросегментація є критично важливою вимогою для безпеки IoT, проте її ефективна реалізація можлива лише за умов переходу до Zero Trust-парадигми з динамічним, ієрархічно організованим та розподіленим механізмом управління довірою.

B. Автоматизація політик безпеки: MUD та Traffic Analysis.

Сучасні підходи до автоматизації політик безпеки в IoT-мережах можна концептуально поділити на декларативні та поведінкові.

B.1. Декларативний підхід: Manufacturer Usage Description (MUD).

Стандарт RFC 8520 [9] визначає модель Manufacturer Usage Description (MUD) як формалізований механізм опису очікуваної мережевої поведінки IoT-пристрою у вигляді машиночитаного профілю доступу. MUD-файл містить декларативні правила Access Control List (ACL), що визначають дозволені напрямки комунікації, протоколи та адресати, після чого мережевий елемент (наприклад, шлюз або контролер) автоматично генерує відповідні правила фільтрації.

У статті "MUD-Based Behavioral Profiling Security Framework for Software-Defined IoT Networks" [10] показано, що MUD може використовуватися як базовий профіль очікуваної поведінки, інтегрований із SDN-контролером для автоматичного моніторингу відповідності фактичного трафіку задекларованим політикам.

Такий підхід забезпечує:

- автоматизоване розгортання політик;
- централізований контроль через SDN;
- можливість оперативної ізоляції пристрою у разі відхилення від MUD-профілю.

Таким чином, декларативний підхід мінімізує дозволені комунікації, однак його ефективність залежить від наявності коректного MUD-опису для кожного пристрою.

B.2. Поведінковий підхід: автоматична ідентифікація та профілювання.

Альтернативну парадигму представлено в роботі "IoT Sentinel: Automated Device-Type Identification for Security Enforcement in IoT " [11]. Система IoT Sentinel виконує пасивне сканування мережевої поведінки пристрою під час його первинного підключення та класифікує його тип на основі характерних шаблонів трафіку. Після визначення типу пристрою автоматично застосовується відповідний профіль обмеження комунікацій.

Ключовою перевагою цього підходу є незалежність від виробника та можливість застосування до середовищ із великим різноманіттям пристроїв від нових до сильно застарілих. Політики формуються на основі спостережуваної поведінки, що дозволяє підтримувати масштабні різнорідні IoT-мережі. Контроль здійснюється на мережевих контрольних точках (gateway, firewall, SDN), що обмежує латеральне переміщення після потенційної компрометації.

B.3. Поєднання декларативного та поведінкового підходів.

Робота "MUD-Based Behavioral Profiling Security Framework for Software-Defined IoT Networks" [10] демонструє також інтеграцію MUD із поведінковим аналізом трафіку. У запропонованій архітектурі MUD-профіль виступає як еталонна модель нормальної комунікації, а статистичне або ML-профілювання використовується для виявлення відхилень. Таким чином, декларативний підхід задає політику за замовчуванням, тоді як поведінковий забезпечує її адаптивну перевірку та реакцію.

Це дозволяє перейти від статичних ACL до динамічного контекстно-чутливого контролю, що відповідає вимогам масштабних IoT-мереж.

C. Спектральна кластеризація як метод сегментації.

Для задачі групування пристроїв у сегменти доцільно використовувати спектральні методи, що базуються на теорії графів. На відміну від евристичних метричних алгоритмів, спектральна кластеризація

базується на аналізі структури зв'язності графа та вирішує задачу розбиття через спектральні властивості матриці Лапласа. У фундаментальній роботі "A Tutorial on Spectral Clustering" [12] математично обгрунтовано використання власних векторів матриці Лапласа для вирішення задачі мінімального розрізу графу. Зокрема, другий власний вектор (вектор Фідлера) кодує інформацію про оптимальний розріз графів, тоді як використання кількох власних векторів дозволяє переходити до багатокластерного випадку. Це робить спектральний метод стійким до зайвих зв'язків, які часто зустрічаються в неструктурованих IoT-мережах.

У дослідженні "Complex network security using community structure and dynamical analysis: spectral clustering and VEIP-WQU model" [13] спектральна кластеризація використовується для виявлення спільнот у мережах та їх сегментації. Зокрема, показано, що спектральні методи дозволяють виділяти щільно зв'язані підграфи, які можуть розглядатися як окремі функціональні частини. У контексті IoT це відповідає задачі мікросегментації, де метою є мінімізація міжсегментних зв'язків.

Отже, сукупність цих досліджень підтверджує доцільність застосування спектральної кластеризації як інструмента формування сегментів у складних мережах.

Мета статті. Метою статті є розробка та експериментальна оцінка автоматизованого гібридного методу мікросегментації IoT-мереж на основі спектральної кластеризації графа та евристичного прунінгу, що реалізує принципи архітектури нульової довіри та забезпечує кількісно вимірюваний баланс між зниженням ризику латерального переміщення і збереженням функціональної цілісності мережі.

ТЕОРЕТИЧНІ ОСНОВИ ДОСЛІДЖЕННЯ

У цьому розділі описано запропоновану архітектуру системи автоматизованої мікросегментації IoT-мереж. Методологія включає формальну модель системи, алгоритм генерації синтетичних топологій із контрольованою ентропією, дворівневий механізм синтезу політик безпеки та математичний апарат для оцінки ефективності.

А. Модель системи.

IoT-мережа моделюється як орієнтований зважений граф $G = (V, E)$, де V – множина пристроїв (вузлів), а E – множина комунікаційних каналів (ребер).

Кожен вузол характеризується наступними атрибутами:

– Role – визначає функціональне призначення пристрою.
– Level – визначає ієрархічний рівень пристрою в архітектурі мережі.
– Zone – позначає фізичну або логічну приналежність до сегмента (наприклад, кімната, цех, виробнича лінія).
– Criticality – коефіцієнт важливості вузла, що відображає потенційні збитки від його компрометації (використовується для розрахунку зважених метрик безпеки).

Таблиця 1

Ієрархічна модель пристроїв

Рівень (L)	Тип	Приклади ролей	Опис
L1	Edge	– Sensor – Actuator – Camera	Кінцеві пристрої з обмеженими ресурсами. Зазвичай ініціюють потік даних вгору або приймають прості команди.
L2	Aggregation	– Hub – NVR – Controller	Проміжні вузли для агрегації даних, трансляції протоколів та локального управління.
L3	Core	– Gateway	Шлюзи для виходу в зовнішні мережі або маршрутизації між зонами.
L4	Cloud	– Cloud – Server	Хмарні сервіси для глобальної аналітики та зберігання даних.

Множина ребер E поділяється на дві підмножини:

$$E = E_{func} \cup E_{noise} \quad (1)$$

$E =$ де E_{func} – легітимні функціональні зв'язки, необхідні для роботи бізнес-логіки системи, а E_{noise} – паразитні зв'язки, наслідок неправильних конфігурацій або активності зловмисника.

Запропонована модель формалізує IoT-мережу як ієрархічний граф із чітко визначеними ролями та рівнями критичності, що створює фундамент для атомарного аналізу безпеки та побудови політик Zero Trust.

B. Генерація топології та модель шуму.

Для перевірки методу мікросегментації розроблено генератор топологій, що створює графи, наближені до реальних IoT-систем, із можливістю контрольованого зашумлення.

Процес генерації складається з двох етапів:

– Формування функціонального скелета мережі (E_{func}) – генератор створює зв'язки на основі чітко визначених шаблонів взаємодії, що відповідають специфікаціям протоколів (наприклад, $Sensor \rightarrow Hub$ через MQTT, $Camera \rightarrow NVR$ через RTSP). При цьому враховується зональна спорідненість – пристрої підключаються до агрегаторів у своїй зоні з більшим пріоритетом, що мінімізує між-зональний трафік.

– Стохастичне зашумлення (E_{noise}) – додавання випадкових ребер/зв'язків, для моделювання ентропії реального середовища до графу. Імовірність появи ребра залежить від сумісності ролей та параметра масштабування шуму σ :

$$P(u, v) \propto P_{base}(Role_u, Role_v) \times \sigma \quad (2)$$

де $P_{base}(Role_u, Role_v)$ – попередньо визначене значення шуму для конкретної пари вузлів.

Для імітації феномену "Rich get richer", характерного для безмасштабних мереж, генерація шуму використовує механізм пріоритетного з'єднання, коли вузли з високим степенем вхідних зв'язків (наприклад, центральні шлюзи або хаби) мають вищу ймовірність отримати нові паразитні з'єднання.

Алгоритм генерації забезпечує відтворюваність експериментів шляхом створення реалістичних топологій із контрольованою ентропією, що симулюють як функціональну логіку, так і хаотичний шум, характерний для реальних IoT-мереж.

C. Логіка синтезу політик.

Запропонований метод використовує гібридний підхід математики та логіки, що поєднує спектральну кластеризацію, для розділення графу топологіх на кластери, та евристичний прунінг з жорсткими правилами, для покращення того що не враховує кластеризація.

C.1. Спектральна кластеризація.

Спектральна кластеризація це – метод кластеризації, що заснований на концепції зв'язності графів. Цей метод обрано як базовий механізм сегментації через здатність виділяти кластери на основі алгебраїчної зв'язності графу, а не геометричної близькості та можливість знаходити кластери довільної форми, на відміну від кластеризації методом k-середніх.

У зашумленому графі IoT-мережі функціональні групи (наприклад, "Хаб та його сенсори") формують щільні підграфи. Шумові зв'язки, хоч і можуть бути численними, зазвичай є випадковими та "слабкими" з точки зору структури графу. Спектральний алгоритм, працюючи з власними векторами матриці Лапласа, проектує граф у простір, де ці функціональні групи стають лінійно роздільними, а шум ігнорується.

Алгоритм:

– побудова матриці суміжності – формування матриці $A \in \mathbb{R}^{n \times n}$, де $A_{ij} = 1$ якщо існує ребро (i, j).

– розрахунок Лапласіана – обчислення симетричної нормалізованої матриці Лапласа:

$$L_{sym} = I - D^{-\frac{1}{2}} A D^{-\frac{1}{2}} \quad (3)$$

де D – діагональна матриця степенів вершин $D_{ij} = \sum_j A_{ij}$, I – одинична матриця.

– Спектральна декомпозиція – знаходження k найменших власних векторів, що відповідають найменшим власним числам L_{sym}. Ці вектори формують матрицю ознак $U \in \mathbb{R}^{n \times k}$. Другий власний вектор (вектор Фідлера) містить інформацію про оптимальний розріз графу.

– Кластеризація – рядки матриці U кластеризуються алгоритмом k-середнього, розбиваючи множину V на кластери $\{C_1, \ldots, C_k\}$.

– Формування політики-кандидата – зв'язок (u, v) попередньо дозволяється, якщо u та v належать до одного кластера $C_u = C_v$ або якщо один із вузлів має дозволену роль Gateway або Cloud, що забезпечує зв'язність інфраструктури.

Таким чином, спектральна кластеризація виступає в ролі математичного фільтра, що автоматично відокремлює функціональні зв'язки від шуму без необхідності ручного налаштування правил, забезпечуючи масштабованість методу.

С.2. Евристичний прунінг.

Результат кластеризації є математично обґрунтованим, все ж має деякі логічні вразливості (наприклад, дозволений зв'язок між двома сенсорами в одному кластері / зоні), які можна покращити. Для того щоб прибрати подібні зайві зв'язки застосовується фільтрація на основі правил.

Нехай *L(u)* – рівень вузла *u*, а *R(u)* – роль вузла *u*. Ребро *(u, v)* видаляється з політики, якщо виконується хоча б одна з умов:

– $L(u) = L(v) = 1$ – обидва вузли мають однаковий рівень та є вузлами нижчого, першого рівня. Сенсори та камери не повинні спілкуватися між собою, це є горизонтальною ізоляцією;

– $|L(u) - L(v)| > 1$ та існує $u \rightarrow w \rightarrow v$ – якщо різниця між рівнями більша за одиницю, але при цьому в графі існує шлях від вузла *u* без "стрибків" до вузла *v*. Це змушує трафік проходити через точки контролю такі як хаби або контроллери.

– $L(u) > L(v)$ та $R(v) \neq Actuator$ – заборонено надсилання керуючих команд до пристроїв, що не підтримують вхідне управління, такі як сенсори або камери. Приймати команди можуть лише актуатори.

– $L(u) < 3$ та $R(v) = Cloud$ – блокування прямого доступу пристроїв рівня першого та другого до зовнішніх мереж (Cloud) в обхід шлюзу.

Правила прунінгу забезпечують необхідну відповідність бізнес-логіці та мінімізацію поверхні атаки, блокуючи специфічні вектори, які неможливо виявити чисто математичними методами.

Таким чином, розроблена методологія поєднує теорію графів з евристичним аналізом для створення автоматизованої, стійкої до шуму системи мікросегментації, здатної адаптуватися до масштабу та складності сучасних IoT-екосистем.

МЕТОДИКА ДОСЛІДЖЕННЯ

Для кількісної верифікації запропонованого методу мікросегментації сформовано систему критеріїв, що охоплює три виміри: рівень захищеності, функціональну цілісність та операційну ефективність.

А. Ключові метрики дослідження.

А.1. Зважене зменшення поверхні атаки (wASR).

Кількісна оцінка ефективності сегментації вимагає спеціалізованих метрик. У основоположній роботі "An Attack Surface Metric"[14] було введено однойменну метрику – поверхня атаки (Attack Surface), в якій запропоновано вимірювати небезпеку системи через сукупність доступних методів та каналів даних. Для кращої наочності покращення безпеки системи при наявності зміни, має сенс вимірювати зменшення цього показника, шляхом розрахунку відношення нового значення поверхня атаки системи до того що було перед внесеними змінами. Таким чином можна продемонструвати, що система стала більш або менш захищеною внаслідок зроблених дій.

Традиційна метрика Attack Surface Reduction (ASR) надає просту кількісну оцінку зменшення периметра атаки проте має суттєвий недолік бо не враховує важливість каналів між різними типами вузлів у системі. Компрометація шлюзу несе значно більші ризики, ніж доступ до периферійного сенсора, що робить класичний ASR нерепрезентативним для оцінки реального впливу на безпеку.

З огляду на обмеження базової метрики, у дослідженні запроваджено зважену версію *wASR*, яка враховує критичність вузлів. Це дозволяє оцінити не просто кількість заблокованих шляхів, а реальне зниження сумарного ризику для інфраструктури.

Математична модель метрики виглядає наступним чином:

$$wASR = 1 - \frac{\sum_{(u,v)\in E_{policy}} Crit(v)}{\sum_{(u,v)\in E_{total}} Crit(v)} \quad (4)$$

де:

– E_{total} – множина всіх спостережуваних фізичних та логічних зв'язків у мережі до сегментації (включаючи ентропійну складову).

– E_{policy} – підмножина зв'язків, дозволених синтезованою політикою.

– $Crit(v) \in [0, 1]$ – коефіцієнт критичності вузла-приймача v.

Фізичний зміст *wASR* полягає у відображенні ступеня мінімізації вектора атак саме на критичні активи. Значення, що наближається до одиниці, свідчить про ефективну ізоляцію найважливіших компонентів системи, навіть якщо загальна кількість дозволених з'єднань залишається значною.

Перевагою такого підходу є фокусування на впливі ризику, хоча це і додає складності у визначенні коректних ваг критичності для кожного типу пристроїв.

А.2. Зважений індекс латерального руху (wLMI).

Індекс латерального руху *LMI* базується на теорії графів досяжності та визначає середню частку вузлів мережі, до яких зловмисник може отримати доступ, скомпрометувавши один довільний пристрій. Ця метрика добре характеризує топологічну зв'язність графу атаки. Проте, аналогічно до *ASR*, класичний *LMI* ігнорує цінність активів. Ситуація, коли зловмисник отримує доступ до 10 сенсорів, і ситуація, коли він отримує доступ до 10 контролерів управління, дадуть однакове значення *LMI*, хоча наслідки будуть кардинально різними.

Для усунення цього недоліку було обрано зважену метрику *wLMI*, яка оцінює не кількість досяжних вузлів, а сумарну "вартість" активів під загрозою.

Формально метрика розраховується як:

$$wLMI = \frac{1}{|V|}\sum_{u\in V}\frac{\sum_{v\in Reach(u,\,E_{policy})} Crit(v)}{\sum_{v\in V} Crit(v) \;-\; Crit(u)} \tag{5}$$

Тут $Reach(u,\, E_{policy})$ представляє множину всіх вузлів, до яких існує шлях від u. Знаменник формули нормалізує значення відносно сумарної критичності всіх вузлів мережі, крім стартового вузла u.

Низьке значення *wLMI* свідчить про високий рівень ізоляції мережі, де інцидент безпеки локалізується в межах одного сегмента. Це значно ускладнює або унеможливлює ескалацію привілеїв до рівня ядра мережі (Gateway/Cloud), що є головною метою мікросегментації.

Недоліком цієї метрики є висока обчислювальна складність ($O(N^3)$ для повного розрахунку транзитивного замикання), проте вона надає найбільш точну картину залишкового ризику.

А.3. Частота помилкових блокувань (FBR).

У контексті систем виявлення вторгнень та фаєрволів *FBR* визначає ймовірність помилкового блокування легітимної активності. Це ключова метрика для оцінки придатності системи. Значення *FBR* безпосередньо вказує на відсоток функціоналу, який буде втрачено при впровадженні політик безпеки. Для промислових систем прийнятним вважається значення, що наближається до нуля (*FBR < 0.05*), оскільки вищі показники свідчать про значну деградацію сервісу.

Головним недоліком у контексті даного дослідження є складність визначення "легітимності" в умовах відсутності розмічених даних. Тому для цього використовується адаптована версія метрики *FBR*, яка спирається на синтетичну "істину", закладену при генерації топології для можливості розрахунку, та оцінки ефективності.

Математична модель:

$$FBR = \frac{\left|E_{GT} \setminus E_{policy}\right|}{|E_{GT}|} \tag{6}$$

де:

– E_{GT} – еталонна множина зв'язків, визначена специфікаціями протоколів та архітектурою системи.
– E_{policy} – підмножина зв'язків, дозволених синтезованою політикою.

А.4. Коефіцієнт стиснення політики (PCR).

Важливим критерієм є складність отриманих політик безпеки в результаті роботи алгоритму. Абсолютна кількість правил у списку контролю доступу дозволяє оцінити навантаження на систему, але не дає уявлення про ефективність фільтрації відносно розміру мережі. 1000 правил може бути багато для малої мережі, але мало для великої.

Саме тому для більшої репрезентативності оцінки ефективності було обрано відносний показник *PCR*, який характеризує ступінь зменшення ентропії.

Математична модель:

$$PCR = \frac{|E_{policy}|}{|E_{total}|} \tag{7}$$

Завдяки цьому значенню можна зрозуміти здатність алгоритму відсікати надлишкові та небезпечні з'єднання. В умовах високої зашумленості топології низьке значення *PCR* свідчить про ефективну фільтрацію аномалій та оптимізацію використання апаратних ресурсів комутаторів.

Сформована система метрик забезпечує комплексну оцінку ефективності, уникаючи однобічного фокусування виключно на показниках захищеності. Обраний набір критеріїв (*wASR, wLMI, FBR, PCR*)

дозволяє кількісно виміряти баланс між безпекою та функціональністю, а також провести експерименти, в яких якісно оцінити запропонований метод.

РЕЗУЛЬТАТИ ДОСЛІДЖЕННЯ

Для перевірки ефективності запропонованого методу було проведено серію експериментів, моделюючи IoT-мережі різного масштабу з контрольованим рівнем ентропії топології (шумом). Метою експериментів є оцінка компромісу між безпекою (зниження LMI) та функціональною цілісністю (мінімізація FBR).

А. Експериментальна установка.

Експерименти проводилися на трьох масштабах мереж:

– Мала мережа: модель розумного будинку або невеликої лабораторії приблизно 30 пристроїв.
– Середня: модель розумного офісу або будівлі, з приблизно 330 пристроями у мережі.
– Велика: модель розумного міста або автоматизованого виробництва, з орієнтовно 950 пристроями.

Для кожного масштабу інтенсивність шуму σ варіювалась від 0.0 – ідеальна топологія, до 5.0 – екстремально зашумлена, де кількість паразитних зв'язків у 5 разів перевищує норму.

Для забезпечення статистичної достовірності та відтворюваності кожен сценарій виконувався з трьома різними значеннями seed (100, 200, 300), а результати усереднювалися. Затінені області на рисунках відповідають 95% довірчим інтервалам за прогонами.

В. Зважене зменшення поверхні атаки (wASR).

Основним показником ефективності політик безпеки, отриманих в процесі експериментів, є їхня здатність мінімізувати доступні вектори атак без шкоди для легітимних операцій. Метрика *wASR* відображає відносну частку заблокованих зв'язків, зважену на критичність відповідно до типів зв'язку, до яких обмежується доступ.

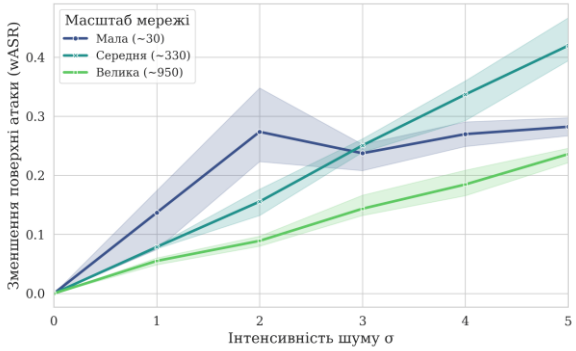

Рис. 1. Зважене зменшення поверхні атаки (wASR) відносно шуму

На рис. 1 наведено залежність показника wASR від інтенсивності топологічного шуму σ для мереж різного масштабу. Цей графік ілюструє, яку частку "шумових" або потенційно небезпечних зв'язків алгоритму вдалося ідентифікувати та відсікти.

З отриманих результатів можна виділити такі закономірності:

– Для мереж середнього та великого масштабу спостерігається стабільне лінійне зростання wASR із підвищенням рівня шуму. Це свідчить про те, що алгоритм успішно розпізнає надлишкові зв'язки як аномальні та ізолює їх. Зокрема, при $\sigma = 5$ для середньої мережі вдається досягти зменшення поверхні атаки на рівні 0.42 (42%), що є суттєвим показником покращення безпеки.
– Малі мережі демонструють цікаву динаміку: при низьких значеннях шуму ($\sigma = 2$) вони показують вищий рівень фільтрації порівняно з іншими масштабами. Однак після досягнення рівня $\sigma = 3$ показник стабілізується в межах 0.24 – 0.28. Це може говорити про те, що у малих графах алгоритм швидше досягає межі роздільної здатності між функціональними зв'язками та шумом.
– При високих рівнях зашумлення $\sigma > 3$крива середньої мережі продовжує зростати, випереджаючи показники малих мереж (0.34 при σ = 4 та 0.42 при σ = 5), тоді як велика мережа зростає стабільно, залишаючись у дослідженому діапазоні нижче малої. Це вказує на кращу спроможність спектральної кластеризації до узагальнення структури мережі, коли кількість випадкових зв'язків значно перевищує кількість легітимних.

Підсумовуючи, можна стверджувати, що значення *wASR* корелює з масштабом мережі: чим складнішою є топологія, тим вищий потенціал для автоматизованого зменшення поверхні атаки. Це

дозволяє ефективно впроваджувати концепцію Zero Trust, динамічно адаптуючи суворість політик до рівня зайвих зв'язків в мережі.

C. Стійкість до топологічних шумів.

При покращенні безпеки мережі критично важливим фактором є збереження її функціональності. Адже можна зробити систему "абсолютно безпечною", зменшивши поверхню атаки до нуля, при цьому вона повністю перестане працювати та виконувати поставлені перед нею задачі. Тому дуже важливим є баланс між безпекою та функціонуванням мережі. Саме це співвідношення зображене на рис. 2, де False Block Rate це відсоток легітимних функціональних зв'язків, які були помилково заблоковані політикою.

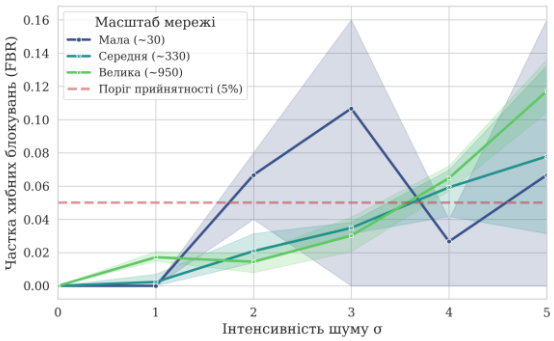

Рис. 2. Стійкість до топологічних шумів

На рис. 2 наведено залежність FBR від рівня шуму. Пунктиром позначено рівень "допустимих втрат", тобто прийнятний FBR, що дорівнює 5% від усіх функціональних зв'язків.

З графіка чітко видно що для мереж великого масштабу алгоритм демонструє високу стійкість та прогнозоване зростання разом з рівнем шуму. При рівні шуму $\sigma = 2$(коли близько 53% зв'язків є шумовими), показник FBR у середньому становить 1.5%. Це підтверджує гіпотезу, що спектральна кластеризація працює ефективніше на великих графах, де статистичні патерни є більш вираженими.

Проте застосування політик для малої мережі призводить до нестабільних результатів. Через малу кількість вузлів та зв'язків між ними, на малих значеннях шуму, алгоритм спектральної кластеризації працює гірше та гірше відрізняє легітимні зв'язки з шумом. Тому при рівні шуму $\sigma = 2$ відсоток FBR вже виходить за рамки прийнятних блокувань (у середньому 6.7%).

Відповідно можна сказати, що метод є найбільш ефективним для великих корпоративних та індустріальних IoT середовищ, де він зберігає понад 98% функціональності навіть при значному зашумлені топології. Натомість для малих мереж ручне налаштування може бути більш доцільними.

D. Зважений індекс латерального руху (wLMI).

Ключовою метрикою безпеки є важений індекс латерального руху (Weighted Lateral Movement Index), який відображає зважену ймовірність досягнення критичних вузлів з будь-якого скомпрометованого вузла.

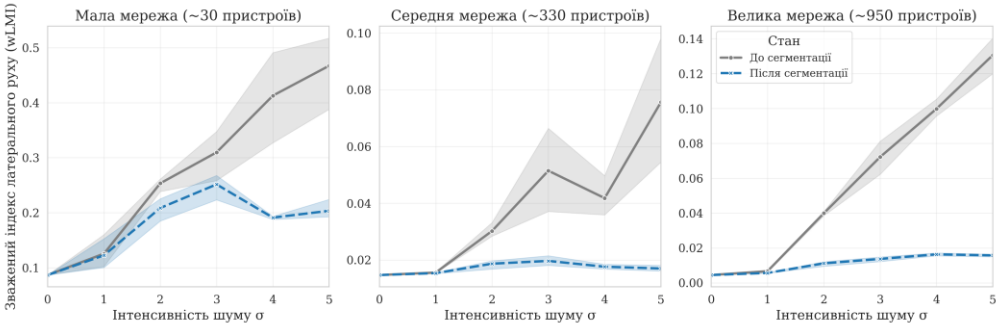

Рис. 3. Вплив мікросегментації на індекс wLMI

На рис. 3. Зображено залежність *wLMI* до (Baseline) та після (Segmented) застосування мікросегментації від значення шуму для різних масштабів. Тобто чітко видно зміни ризику горизонтального переміщення мережею.

З отриманих графіків видно, що ефективність мікросегментації дуже корелює з кількістю зв'язків, а відповідно і масштабом мережі.

Для малих мереж при малих значеннях шуму зниження *wLMI* є помірним, оскільки топологічна "відстань" між вузлами є малою за визначенням. Проте варто відмітити що зі збільшенням шуму, та кількості зв'язків відповідно, ефективність також починає зростати та різниця між значеннями *wLMI* помітно зменшуються.

Для мереж середнього та великого масштабу, де кількість зв'язків більша за замовчуванням, ефект від застосування мікросегментації, стає помітним на менших значеннях шуму та стабільно стримує зростання ризику горизонтального переміщення, утримуючи *wLMI* на низькому рівні навіть при значному зашумленні топології.

До прикладу, для великої мережі при рівні шуму $\sigma = 2$ алгоритм забезпечує зниження ризику горизонтального переміщення на 71.9% за зваженим індексом wLMI (а при $\sigma \geq 3$ – на 81-88%). Це означає, що синтезована політика успішно локалізує атаки в межах однієї зони, ізолюючи критичні вузли такі як Шлюз та Контроллер від скомпрометованих сенсорів.

Е. Коефіцієнт стиснення політики (PCR).

Окрім метрик безпеки, критичним параметром для впровадження систем Zero Trust є операційна ефективність. Зі збільшенням мережі та рівня шуму зростає і кількість зв'язків (ребер графа топології), а як наслідок і політик, тому варто оцінити здатність запропонованого алгоритму фільтрувати зайві правила. Для цього була введена метрика Policy Compression Ratio (PCR), яка є співвідношенням кількості правил у політиці до загальної кількості ребер у графі:

$$PCR = \frac{E_{policy}}{E_{total}} \tag{8}$$

PCR має демонструвати, що при зростанні шуму відсоток дозволених зв'язків зменшується.

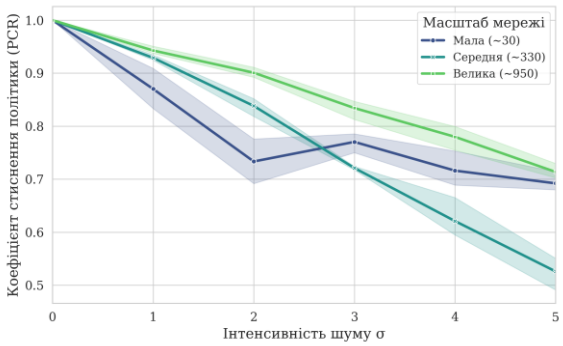

Рис. 4. Коефіцієнт стиснення політики

З графіку на рис. 4 видно, що у мережах де відсутній шум ($\sigma = 0$), $PCR = 1$. Це свідчить про те, що алгоритм коректно ідентифікує всі існуючі зв'язки як легітимні, не створюючи помилкових блокувань.

При зростанні рівня шуму, коефіцієнт *PCR* знижується. Для мережі великого масштабу при $\sigma = 3$ значення $PCR = 0.83$. Це означає, що алгоритм автоматично класифікує та відсікає ~17% зв'язків як аномальні або надлишкові.

Відповідно можна зробити висновок, що запропонований алгоритм працює коректно та покращує співвідношення сигнал/шум у політиках безпеки, автоматично усуваючи зайві підключення без втручання оператора.

ВИСНОВКИ ТА ПЕРСПЕКТИВИ ПОДАЛЬШИХ ДОСЛІДЖЕНЬ

У цій роботі запропоновано та досліджено автоматизований гібридний метод мікросегментації для масштабних IoT-мереж, спрямований на реалізацію архітектури Zero Trust та протидію горизонтальному переміщенню зловмисників. Поєднання спектральної кластеризації з евристичним прунінгом дозволило ефективно розділити мережу на ізольовані зони, автоматично відфільтровуючи аномальні та надлишкові зв'язки без потреби ручного налаштування списків контролю доступу.

Результати експериментального моделювання на топологіях різного масштабу підтверджують високу результативність запропонованого підходу. Для великомасштабних мереж алгоритм продемонстрував стійкість до значного топологічного шуму. Навіть за умов високого рівня шуму (зайвих зв'язків) індекс горизонтального переміщення (*wLMI*) було знижено на 72-88% залежно від рівня шуму,

що свідчить про радикальне зменшення поверхні атаки (*wASR*) та надійну ізоляцію критичних вузлів інфраструктури (шлюзів, контролерів) від потенційно скомпрометованих периферійних пристроїв.

Критично важливим здобутком є збереження функціональної цілісності системи: для мереж великого та середнього масштабу частка хибних блокувань (*FBR*) для значень $\sigma \leq 3$ не перевищує 5%, що має задовольняти вимоги коректного функціонування більшості промислових або мереж розумних міст. Водночас дослідження виявило обмеження алгоритму для мереж малого масштабу, де через природну розрідженість графа метод є більш чутливим до шуму, що призводить до погіршення функціональності мережі через непередбачуваність відсотку хибних блокувань.

Окрім підвищення рівня захищеності, запропонований метод знижує операційну складність адміністрування безпеки. Значення метрики стиснення політики (*PCR*) доводять, що алгоритм здатний генерувати компактні та оптимізовані правила фільтрації (ACL), тим самим полегшуючи підтримку системи та оптимізуючи навантаження на мережеве обладнання. У подальших дослідженнях перспективним напрямом є інтеграція даного алгоритму з системами аналізу мережевого трафіку для динамічної перебудови політик мікросегментації в режимі реального часу залежно від поточного стану загроз.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. MITRE. (2025). *Lateral movement, tactic TA0008 (Enterprise).* MITRE ATT&CK. Retrieved August 16, 2026, from https://attack.mitre.org/tactics/TA0008/
2. Osman, A., Wasicek, A., Köpsell, S., & Strufe, T. (2020). Transparent microsegmentation in smart home IoT networks. In *3rd USENIX Workshop on Hot Topics in Edge Computing (HotEdge '20)*. USENIX Association. https://www.usenix.org/conference/hotedge20/presentation/osman
3. Saltzer, J. H., & Schroeder, M. D. (1975). The protection of information in computer systems. *Proceedings of the IEEE, 63*(9), 1278–1308. https://doi.org/10.1109/PROC.1975.9939
4. Smiliotopoulos, C., Kambourakis, G., & Kolias, C. (2024). Detecting lateral movement: A systematic survey. *Heliyon, 10*(4), e26317. https://doi.org/10.1016/j.heliyon.2024.e26317
5. Rose, S., Borchert, O., Mitchell, S., & Connelly, S. (2020). *Zero trust architecture* (NIST Special Publication 800-207). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-207
6. Makhdoom, I., Abolhasan, M., Lipman, J., Liu, R. P., & Ni, W. (2019). Anatomy of threats to the Internet of Things. *IEEE Communications Surveys & Tutorials, 21*(2), 1636–1675. https://doi.org/10.1109/COMST.2018.2874978
7. Samaniego, M., & Deters, R. (2018). Zero-trust hierarchical management in IoT. In *2018 IEEE International Congress on Internet of Things (ICIOT)* (pp. 88–95). https://doi.org/10.1109/ICIOT.2018.00019
8. Arifeen, M., Petrovski, A., & Petrovski, S. (2021). Automated microsegmentation for lateral movement prevention in Industrial Internet of Things (IIoT). In *2021 14th International Conference on Security of Information and Networks (SIN)* (pp. 1–6). https://doi.org/10.1109/SIN54109.2021.9699232
9. Lear, E., Droms, R., & Romascanu, D. (2019). *Manufacturer usage description specification* (RFC 8520). RFC Editor. https://doi.org/10.17487/RFC8520
10. Krishnan, P., Jain, K., Buyya, R., Vijayakumar, P., Nayyar, A., Bilal, M., & Song, H. (2022). MUD-based behavioral profiling security framework for software-defined IoT networks. *IEEE Internet of Things Journal, 9*(9), 6611–6622. https://doi.org/10.1109/JIOT.2021.3113577
11. Miettinen, M., Marchal, S., Hafeez, I., Asokan, N., Sadeghi, A.-R., & Tarkoma, S. (2017). IoT SENTINEL: Automated device-type identification for security enforcement in IoT. In *2017 IEEE 37th International Conference on Distributed Computing Systems (ICDCS)* (pp. 2177–2184). https://doi.org/10.1109/ICDCS.2017.283
12. von Luxburg, U. (2007). A tutorial on spectral clustering. *Statistics and Computing, 17*(4), 395–416. https://doi.org/10.1007/s11222-007-9033-z
13. Jouyban, M., & Hosseini, S. (2025). Complex network security using community structure and dynamical analysis: Spectral clustering and VEIP-WQU model. *Applied Network Science, 10*, 24. https://doi.org/10.1007/s41109-025-00717-8
14. Manadhata, P. K., & Wing, J. M. (2011). An attack surface metric. *IEEE Transactions on Software Engineering, 37*(3), 371–386. https://doi.org/10.1109/TSE.2010.60

КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 2 (34), 2026
ISSN 2663 – 4023

Ivan Niedielnitsev
PhD Student, Department of Computer Radio Engineering and Technical Information Protection
Kharkiv National University of Radio Electronics, Kharkiv, Ukraine
ORCID:0009-0004-5265-3561
ivan.niedielnitsev@nure.ua

Ivan Antipov
Doctor of Technical Sciences, Professor, Professor of the Department of Computer Radio Engineering and Technical Information Protection
Kharkiv National University of Radio Electronics, Kharkiv, Ukraine
ORCID:0000-0002-9754-4412
ivan.antipov@nure.ua

MICRO-SEGMENTATION OF IOT NETWORKS IN THE ZERO TRUST ARCHITECTURE

Abstract. The scaling of Internet of Things (IoT) infrastructures is accompanied by redundant network connectivity that expands the attack surface and enables lateral movement of an adversary after a single node has been compromised. The article proposes an automated hybrid method for micro-segmentation of IoT networks that implements the principles of the Zero Trust architecture by combining spectral clustering of the network graph with heuristic role-based pruning. The network is modeled as a directed graph with hierarchical device levels (edge, aggregation, gateway, cloud) and node criticality coefficients. A synthetic topology generator with a controlled noise level has been developed; it reproduces the functional core of connections and a stochastic entropy component using preferential attachment and zone affinity mechanisms. To quantify the quality of segmentation, a system of weighted metrics has been formed: weighted Attack Surface Reduction (wASR), weighted Lateral Movement Index (wLMI), False Block Rate (FBR), and Policy Compression Ratio (PCR). The experimental study covers three network scales (about 30, 330, and 950 devices) with noise intensity from 0 to 5; the results are averaged over three runs, and 95% confidence intervals are provided. It is shown that for large-scale networks the method reduces the weighted lateral movement index by 72-88% depending on the noise level, while keeping the false block rate within 1.5-3% at noise levels up to 3, which preserves the functional integrity of the system. The synthesized access policies are compact (policy compression ratio of 0.71-0.83 under high noise), which reduces the operational complexity of security administration. The limitations of the method for small networks, where graph sparsity increases sensitivity to noise, are identified. Prospects for further research are outlined: dynamic re-segmentation in real time, automatic selection of the number of segments, and validation on real IoT traffic datasets.

Keywords: Zero Trust architecture; micro-segmentation; Internet of Things; spectral clustering; access policy; lateral movement; attack surface; network graph model.

REFERENCES (TRANSLATED AND TRANSLITERATED)

1. MITRE. (2025). *Lateral movement, tactic TA0008 (Enterprise).* MITRE ATT&CK. Retrieved August 16, 2026, from https://attack.mitre.org/tactics/TA0008/
2. Osman, A., Wasicek, A., Köpsell, S., & Strufe, T. (2020). Transparent microsegmentation in smart home IoT networks. In *3rd USENIX Workshop on Hot Topics in Edge Computing (HotEdge '20)*. USENIX Association. https://www.usenix.org/conference/hotedge20/presentation/osman
3. Saltzer, J. H., & Schroeder, M. D. (1975). The protection of information in computer systems. *Proceedings of the IEEE, 63*(9), 1278-1308. https://doi.org/10.1109/PROC.1975.9939
4. Smiliotopoulos, C., Kambourakis, G., & Kolias, C. (2024). Detecting lateral movement: A systematic survey. *Heliyon, 10*(4), e26317. https://doi.org/10.1016/j.heliyon.2024.e26317
5. Rose, S., Borchert, O., Mitchell, S., & Connelly, S. (2020). *Zero trust architecture* (NIST Special Publication 800-207). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-207
6. Makhdoom, I., Abolhasan, M., Lipman, J., Liu, R. P., & Ni, W. (2019). Anatomy of threats to the Internet of Things. *IEEE Communications Surveys & Tutorials, 21*(2), 1636-1675. https://doi.org/10.1109/COMST.2018.2874978

7. Samaniego, M., & Deters, R. (2018). Zero-trust hierarchical management in IoT. In *2018 IEEE International Congress on Internet of Things (ICIOT)* (pp. 88-95). https://doi.org/10.1109/ICIOT.2018.00019
8. Arifeen, M., Petrovski, A., & Petrovski, S. (2021). Automated microsegmentation for lateral movement prevention in Industrial Internet of Things (IIoT). In *2021 14th International Conference on Security of Information and Networks (SIN)* (pp. 1-6). https://doi.org/10.1109/SIN54109.2021.9699232
9. Lear, E., Droms, R., & Romascanu, D. (2019). *Manufacturer usage description specification* (RFC 8520). RFC Editor. https://doi.org/10.17487/RFC8520
10. Krishnan, P., Jain, K., Buyya, R., Vijayakumar, P., Nayyar, A., Bilal, M., & Song, H. (2022). MUD-based behavioral profiling security framework for software-defined IoT networks. *IEEE Internet of Things Journal, 9*(9), 6611-6622. https://doi.org/10.1109/JIOT.2021.3113577
11. Miettinen, M., Marchal, S., Hafeez, I., Asokan, N., Sadeghi, A.-R., & Tarkoma, S. (2017). IoT SENTINEL: Automated device-type identification for security enforcement in IoT. In *2017 IEEE 37th International Conference on Distributed Computing Systems (ICDCS)* (pp. 2177-2184). https://doi.org/10.1109/ICDCS.2017.283
12. von Luxburg, U. (2007). A tutorial on spectral clustering. *Statistics and Computing, 17*(4), 395-416. https://doi.org/10.1007/s11222-007-9033-z
13. Jouyban, M., & Hosseini, S. (2025). Complex network security using community structure and dynamical analysis: Spectral clustering and VEIP-WQU model. *Applied Network Science, 10,* 24. https://doi.org/10.1007/s41109-025-00717-8
14. Manadhata, P. K., & Wing, J. M. (2011). An attack surface metric. *IEEE Transactions on Software Engineering, 37*(3), 371-386. https://doi.org/10.1109/TSE.2010.60

Отримано редакцією журналу / Received: 04.02.26
Прорецензовано / Revised: 16.02.26
Схвалено до друку / Accepted: 24.09.26