DOI: https://doi.org/10.36910/6775-2524-0560-2026-64-18
УДК: 004.056.5
Костючко Сергій Миколайович[1], к.т.н., доцент
https://orcid.org/0000-0002-1262-6268
Журавльов Олександр Анатолійович[2], к.т.н., доцент
https://orcid.org/0000-0002-7823-0338
Сурова Наталія Миколаївна[1], к.т.н., доцент
https://orcid.org/0000-0002-7116-0197
Кулакевич Олег Русланович[1], асистент
https://orcid.org/0009-0008-1065-6691
Литвин Вадим Анатолійович[1], магістр
[1]Луцький національний технічний університет, м. Луцьк, Україна
[2] Волинський національний технічний університет, м. Луцьк, Україна
Дослідження проведено на базі центру колективного користування науковим обладнанням «Інженерія даних та цифрова аналітика» Луцького національного технічного університету

МАСШТАБОВАНЕ ВИЯВЛЕННЯ АНОМАЛІЙ У ВЕЛИКИХ ПОТОКАХ МЕРЕЖЕВИХ ДАНИХ НА ОСНОВІ ДИНАМІЧНИХ ГРАФІВ І СПЕКТРАЛЬНИХ ХАРАКТЕРИСТИК

Костючко С. М., Журавльов О. А., Сурова Н. М., Кулакевич О. Р., Литвин В. А. Масштабоване виявлення аномалій у великих потоках мережевих даних на основі динамічних графів і спектральних характеристик. У статті запропоновано метод масштабованого виявлення аномалій у потоках мережевих даних на основі динамічних графів, графових скетчів і спектральних характеристик. Мережеву телеметрію подано як потік ребер, а стан графа – у вигляді матриці скетчу з експоненційним згасанням ваг. Для виявлення структурних змін використано індекс гладкості, що обчислюється без повного спектрального розкладання та забезпечує сталий обсяг пам'яті. Експерименти на синтетичних потоках засвідчили ефективність методу для короткочасних аномалій типу «зірка», однак виявили обмежену чутливість до низькоінтенсивного сканування. Встановлено залежність якості детектування від розміру скетчу, коефіцієнта згасання та тривалості вікна спостереження. Подальші дослідження передбачають побудову ансамблю потокових критеріїв і перевірку методу на реальній телеметрії IPFIX.
Ключові слова: динамічні графи, потокове виявлення аномалій, IPFIX, спектральний аналіз, графовий скетч, виявлення вторгнень, кібербезпека.

Kostiuchko S., Zhuravlov O., Surova N., Kulakevych O., Lytvyn V. Scalable anomaly detection in large network data streams based on dynamic graphs and spectral characteristics. The article proposes a method for scalable anomaly detection in network data streams based on dynamic graphs, graph sketches, and spectral characteristics. Network telemetry is represented as a stream of edges, and the graph state is represented as a sketch matrix with exponential decay of weights. To detect structural changes, a smoothness index is used, which is calculated without full spectral decomposition and provides a constant amount of memory. Experiments on synthetic streams have demonstrated the effectiveness of the method for short-term star-type anomalies, but have revealed limited sensitivity to low-intensity scanning. The dependence of the detection quality on the sketch size, decay coefficient, and duration of the observation window has been established. Further research involves constructing an ensemble of stream criteria and testing the method on real IPFIX telemetry.
Keywords: dynamic graphs, streaming anomaly detection, IPFIX, spectral analysis, graph sketch, intrusion detection, cybersecurity.

Вступ

Моніторинг мережевої інфраструктури ґрунтується на потоковій телеметрії IPFIX/NetFlow, у якій кожний запис описує взаємодію між джерелом і призначенням [16; 19]. Для магістральних сегментів і центрів обробки даних інтенсивність експорту може становити мільйони записів за секунду, що висуває жорсткі вимоги до часу обробки, пам'яті та затримки формування тривоги. Відповідно до NIST CSF 2.0 і NIST SP 800-137, виявлення відхилень має виконуватися безперервно та забезпечувати показники, придатні для реагування [17; 18].

Класичні потокові детектори аналізують частоти окремих пар або локальні статистики, тому низькоінтенсивне сканування, латеральне переміщення, C2-комунікації та розподілені атаки можуть не створювати значного відхилення на рівні одного потоку. Граф взаємодій зберігає реляційну структуру, але повний граф не може бути матеріалізований у режимі необмеженого потоку. Спектральні характеристики здатні реагувати на появу зіркоподібних структур, щільних підграфів і зміну зв'язності, однак стандартне спектральне розкладання не відповідає вимогам реального часу.

Постановка проблеми

Наукова проблема полягає в суперечності між експлуатаційною вимогою сталих витрат ресурсів на одне ребро та детекційною вимогою чутливості до глобальних структурних змін. Потокові алгоритми [8-11] забезпечують масштабованість, але використовують переважно частотні або локальні критерії; спектральні моделі [4-7] працюють із графом як цілим і переважно орієнтовані на пакетне опрацювання.

Метою роботи є розроблення потокового методу SpecStream, у якому динамічний граф стискається в скетч фіксованого розміру, а спектральний зсув оцінюється без обчислення власних значень. Критеріями ефективності є AUC-ROC/AUC-PR, затримка виявлення, пропускна здатність і обсяг стану. Основне припущення полягає в тому, що аномалії, які змінюють розподіл степенів проєкції, спричиняють зростання середньої спектральної частоти сигналу об'єму.

Аналіз останніх досліджень і публікацій

В літературі [1-3] систематизують виявлення аномалій у динамічних графах за традиційними статистичними, матричними, ймовірнісними та глибинними підходами. Спільним висновком є відсутність універсальної моделі, яка одночасно враховує часову еволюцію, глобальну структуру та обмеження потокового середовища.

Спектральна лінія досліджень базується на зміщенні енергії аномальних сигналів у високочастотну область. У [4] запропоновано смугові фільтри на вейвлетах Бета; у [5] гетерофільні ребра інтерпретовано як високочастотний компонент; у [6] використано навчені вейвлети з адаптивним злиттям ознак. Підхід [7] підвищує масштабованість за допомогою поліномів Чебишова, проте передбачає статичний знімок і попереднє обчислення представлень. Отже, діагностична цінність спектральних характеристик доведена, але їх інкрементне застосування до великих потоків залишається недостатньо дослідженим.

Потокові методи мають іншу пріоритетність. MIDAS [8] використовує count-min sketch і критерій χ^2 для виявлення раптових мікрокластерів. AnoEdge/AnoGraph [9] застосовують скетчі вищого порядку для пошуку щільних підматриць. SLADE [10] відстежує дрейф самонавчених вузлових представлень, а Adaptive DecayRank [11] адаптивно оновлює PageRank. Ці методи мають ресурсні гарантії, але не відтворюють повний спектральний профіль і можуть бути нечутливими до структур, які не утворюють повторюваних пар або щільного короткочасного згустку.

Графові моделі для мережевої безпеки узагальнено в [12]. Anomal-E [13] демонструє можливість самонавчання на реберних ознаках без розмітки, а GAT-AD [14] використовує контекст минулої активності. Водночас результати GADBench [15] не підтверджують систематичної переваги спеціалізованих графових нейромереж над простішими ансамблями на великих графах. Це обґрунтовує дослідження компактних інтерпретованих дескрипторів, які не потребують навчання.

Невирішеними залишаються три питання: збереження спектральної чутливості після хеш-проєкції; адаптація часової пам'яті до тривалості інциденту; оцінювання компромісу між якістю, пропускною здатністю та пам'яттю. Запропонований підхід спрямований саме на ці аспекти.

Теоретичні основи дослідження

1. Формалізація потоку та динамічного графа

Нехай V – множина мережевих вузлів, $|V| = n$. Телеметрія подається як послідовність ребер:

$$S = \langle e^1, e^2, \dots \rangle, \quad e_k = (u_k, v_k, \tau_k), \quad u_k, v_k \in V.$$

Час дискретизується тіками тривалості Δ. Множина B_t містить записи, експортовані в інтервалі $[t\Delta;\ (t+1)\Delta)$. Стан мережевих взаємодій задається матрицею ваг W_t з експоненційним згасанням:

$$W_t = \alpha W_{t-1} + \Delta_t, \quad (\Delta_t)_{\text{uv}} = |\{e \in B_t : e = (u, v)\}|, \quad 0 < \alpha < 1.$$

Ефективна довжина пам'яті дорівнює $\ell eff = (1-\alpha)^{-1}$. Задача полягає у побудові оцінки $z_t \geq 0$ за умов обмеженої пам'яті, амортизованого оновлення $O(1)$ на ребро та контрольованої затримки. Матеріалізація W_t потребує $O(|E|)$ або $O(n^2)$ пам'яті, тому використовується проєкція.

2. Скетч вищого порядку

Вводяться незалежні хеш-функції $\varphi: V \to \{1, \dots, h\}$ для джерел і $\psi: V \to \{1, \dots, h\}$ для призначень. Матриця $M_t \in R^{\text{hxh}}$ агрегує ваги ребер між проєкційними групами:

$$M_t = \Phi^T W_t \Psi = \alpha M_{t-1} + \Phi^T \Delta_t \Psi.$$

Надходження ребра *(u,v)* інкрементує одну комірку $M_t[\varphi(u), \psi(v)]$, тому вартість потокового оновлення є сталою. Загальна маса потоку зберігається точно, проте колізії змішують різні вузли. Для двох незалежних хешів імовірність повної колізії двох пар у тій самій комірці становить $1/h^2$; окрема колізія джерел або призначень має ймовірність $1/h$.

Зі скетчу формується симетрична матриця суміжності двочасткового графа:

$$A_t = [\,0 \;\; M_t\,;\; M_t^{\mathrm{T}} \;\; 0\,], \quad d = [M_t 1\,;\; M_t^{\mathrm{T}} 1], \quad D = diag(d).$$

Нормалізований лапласіан визначається як $L_t = I - D^{-1/2} A_t D^{-1/2}$. Для нульових степенів відповідні елементи $D^{-1/2}$ встановлюються рівними нулю, що усуває ділення на нуль та зберігає коректність для ізольованих проєкційних груп.

3. Спектральний дескриптор та правило рішення

Для сигналу $x \in R^{2h}$ індекс гладкості, або середня спектральна частота, визначається відношенням Релея:

$$\rho_t = (x^{\mathrm{T}} L_t x)/(x^{\mathrm{T}} x) = (\Sigma_k \lambda_k \hat{x}_k^{\,2})/(\Sigma_k \hat{x}_k^{\,2}), \quad 0 \le \rho_t \le 2.$$

Як сигнал використовується вектор степенів $x=d$. Тоді ρ_t обчислюється без власних значень:

$$\rho_t = [\Sigma_{p,\varphi} M_{t,p\varphi}(\sqrt{d_p} - \sqrt{d_{h+\varphi}})^2] \,/\, [\Sigma_k d_k^{\,2}].$$

Обчислювальна складність дескриптора становить $O(h^2)$ на тік, а пам'ять основного стану – $8h^2$ байт для float64. Параметр α визначає часовий масштаб, тоді як h контролює компроміс між колізіями та обчислювальними витратами.

Нестаціонарність компенсується експоненційно зваженою базовою лінією. Для середнього μ_t, дисперсії v_t і коефіцієнта β використовується:

$$z_t = |\rho_t - \mu_{t-1}| \,/\, \sqrt{max(v_{t-1}, \delta)},$$

$$\mu_t = \mu_{t-1} + (1-\beta)(\rho_t - \mu_{t-1}), \quad v_t = \beta[v_{t-1} + (1-\beta)(\rho_t - \mu_{t-1})^2].$$

Оновлення базової лінії пропускається, якщо $z_t \ge \kappa$, щоб зменшити її «отруєння» аномалією. Порогове значення визначається лише на калібрувальній частині нормального потоку; теоретична межа Чебишова використовується як консервативний орієнтир, але не підміняє емпіричне калібрування для нестаціонарних залежних даних.

4. Критерій ефективності

$$max\ AUC(z,y), \text{за умов } 8h^2 \le B,\ c_{up} d + \gamma h^2/\bar{m} \le cmax,\ L \le Lmax.$$

Критерій доповнюється AUC-PR, оскільки частка аномальних тіків мала. Оптимізація параметрів виконується на валідаційних потоках, а остаточні показники – на незалежних тестових реалізаціях.

Результати дослідження

Для усунення залежності від одного зерна генератора застосовано три незалежні множини: калібрувальну, валідаційну та тестову. Параметри h і α обиралися на шести валідаційних реалізаціях; остаточне оцінювання виконано на восьми незалежних тестових потоках. Кожний тест містив 1900 тіків, 30 000 хостів і в середньому близько 700 ребер/тік. Перші 500 тіків використовувалися лише для ініціалізації та калібрування. У кожний потік внесено по п'ять епізодів класу A (коротка зіркоподібна перебудова без зміни загального обсягу) та класу B (розподілене горизонтальне сканування без повторюваних пар).

Порівняння виконано з об'ємним EWMA-критерієм. Він є контрольним, а не повною реалізацією опублікованих MIDAS/AnoGraph; тому висновки стосуються саме реалізованого базового детектора. Для кожної метрики наведено середнє та 95 % довірчий інтервал за незалежними тестовими реалізаціями. Параметри експерименту подано в таблиці 1.

Таблиця 1 – Параметри повторного експерименту

Параметр	Значення	Призначення
Розмір скетчу h	32, 64, 128	валідаційна сітка
Згасання α	0,90; 0,95	часова пам'ять
Згасання β	0,9995	адаптація базової лінії
Кількість тестів	8 незалежних зерен	оцінка варіативності
Метрики	AUC-ROC, AUC-PR, Мребер/с	якість і ресурси

Найкращу середню валідаційну якість отримано для h = 128, α = 0,90 і β = 0,9995. SpecStream стабільно виявляв короткі зіркоподібні зміни: AUC-A становив 0,936 ± 0,033. Перевага за AUC-PR

є істотнішою, ніж за AUC-ROC, що важливо для незбалансованого потоку. Водночас показники класу B характеризуються великим довірчим інтервалом: результат залежить від того, наскільки конкретна хеш-проєкція змінює розподіл степенів, що можемо спостерігати в таблиці 2.

Таблиця 2 – Результати експериментального оцінювання потокових детекторів аномалій

Метод	AUC-A	PR-A	AUC-B	PR-B	Мребер/с	Стан
SpecStream	0,936 ± 0,033	0,442 ± 0,009	0,624 ± 0,210	0,483 ± 0,133	9,19 ± 0,35	128 кБ
Volume-EWMA	0,764 ± 0,026	0,072 ± 0,010	0,707 ± 0,031	0,535 ± 0,038	1549 ± 34	<1 кБ

Об'ємний критерій є значно швидшим, але його PR-A низький, оскільки в класі A загальна кількість ребер навмисно не змінювалася. Для класу B він іноді реагував на флуктуації інтенсивності, що підвищувало AUC, але не забезпечувало структурної інтерпретації. Таким чином, пропускну здатність простого статистичного критерію не можна безпосередньо трактувати як перевагу в детекційній здатності.

Результати підтверджують основну гіпотезу лише для аномалій, що змінюють степені проєкційних груп. Метод не є універсальним: розподілене сканування з унікальними парами може залишатися слабко помітним. Великий інтервал AUC-B свідчить про залежність від колізій хешування та потребу в ансамблі незалежних скетчів.

Вибір h має виконуватися разом з інтенсивністю m̄. Замість жорсткої умови $\bar{m} \gtrsim h^2$ доцільно контролювати відношення $h^2/\bar{m}$: його зростання підвищує розрідженість матриці та вартість обчислення. Значення $h = 128$ дало кращу якість у цьому експерименті, але потребувало 128 кБ основного стану та знизило пропускну здатність. Для сенсорів із жорсткішими ресурсними обмеженнями доцільним є $h = 64$ із очікуваною втратою чутливості.

Оцінювання має такі обмеження: використано синтетичні потоки; реалізація виконана однопотоково на Python/NumPy; фактична пам'ять процесу перевищує $8h^2$ через тимчасові масиви; поріг не гарантує сталого FPR у разі різкого дрейфу нормального трафіку. Тому наведені показники характеризують обчислювальний прототип, а не готовий промисловий IDS.

Висновки

Запропоновано метод SpecStream для потокового оцінювання спектральних змін у динамічному графі мережевих взаємодій. Заміна повного графа скетчем $h \times h$ та обчислення відношення Релея без спектрального розкладання забезпечують $O(1)$ оновлення на ребро, $O(h^2)$ оброблення тіка та фіксований основний стан.

Повторний експеримент із незалежними калібрувальними, валідаційними й тестовими реалізаціями показав AUC 0,936 ± 0,033 для коротких структурних аномалій за пропускної здатності 9,19 ± 0,35 млн ребер/с. Для розподіленого горизонтального сканування якість є нестабільною, що визначає межу застосовності одного спектрального дескриптора. Подальші дослідження мають охоплювати ансамблі незалежних скетчів, адаптивні пороги, реальну IPFIX-телеметрію та порівняння з відтвореними реалізаціями MIDAS, AnoGraph і SLADE.

Список бібліографічного опису

1. Екле, О. А., та Еберле, В. (2024). Виявлення аномалій у динамічних графах: комплексний огляд. Праці ACM з виявлення знань у даних, 18(8), стаття 192, 1-44. https://doi.org/10.1145/3669906
2. Цяо, Х., Тун, Х., Ань, Б., Кінг, І., Аггарвал, К., та Пан, Г. (2025). Глибинне виявлення аномалій у графах: огляд і нові перспективи. Праці IEEE з інженерії знань і даних, 37(9), 5106-5126. https://doi.org/10.1109/TKDE.2025.3581578
3. Ян, Л., Шателен, К., та Адам, С. (2024). Навчання представлень динамічних графів за допомогою нейронних мереж: огляд. Відкритий доступ IEEE, 12, 43460-43484. https://doi.org/10.1109/ACCESS.2024.3378111
4. Тан, Ц., Лі, Ц., Гао, Ц., та Лі, Ц. (2022). Переосмислення графових нейронних мереж для виявлення аномалій. У матеріалах 39-ї Міжнародної конференції з машинного навчання (Збірник праць з досліджень у галузі машинного навчання, т. 162, с. 21076-21089). PMLR. https://proceedings.mlr.press/v162/tang22b.html
5. Гао, Ю., Ван, С., Хе, С., Лю, Ц., Фен, Х., та Чжан, Ю. (2023). Урахування гетерофілії у виявленні аномалій у графах: погляд із позиції спектра графа. У матеріалах Вебконференції ACM 2023 (с. 1528-1538). ACM. https://doi.org/10.1145/3543507.3583268
6. Чжен, Ц., Ян, Ц., Чжан, Т., Цао, Л., Цзян, Б., Фань, С., У, С.-М., та Чжу, С. (2025). Динамічне спектральне виявлення аномалій у графах. Праці конференції AAAI зі штучного інтелекту, 39(12), 13410-13418. https://doi.org/10.1609/aaai.v39i12.33464
7. Лю, Ю., Сє, Ц., Чень, Ю., Цзінь, С., Чжен, Т., Чун, Б., та Хе, Т. (2026). Зменшення нерівномірності гомофілії у виявленні аномалій у графах: масштабований та адаптивний підхід. У матеріалах Вебконференції ACM 2026. ACM. https://doi.org/10.1145/3774904.3792454

8. Бхатія, С., Лю, Ж., Хуї, Б., Юн, М., Шин, К., та Фалутсос, К. (2022). Виявлення аномалій у потоках ребер у реальному часі. Праці ACM з виявлення знань у даних, 16(4), стаття 75, 1-22. https://doi.org/10.1145/3494564
9. Бхатія, С., Вадхва, М., Кавагучі, К., Шах, Н., Ю, П. С., та Хуї, Б. (2023). Виявлення аномалій у потокових графах на основі скетчів. У матеріалах 29-ї конференції ACM SIGKDD з виявлення знань і добування даних (с. 93-104). ACM. https://doi.org/10.1145/3580305.3599504
10. Лі, Ц., Кім, С., та Шин, К. (2024). SLADE: виявлення динамічних аномалій у потоках ребер без міток засобами самокерованого навчання. У матеріалах 30-ї конференції ACM SIGKDD з виявлення знань і добування даних (с. 1506-1517). ACM. https://doi.org/10.1145/3637528.3671845
11. Екле, О. А., Еберле, В., та Крістофер, Ц. (2025). Adaptive DecayRank: виявлення аномалій у динамічних графах у реальному часі з байєсівським оновленням PageRank. Прикладні науки, 15(6), 3360. https://doi.org/10.3390/app15063360
12. Біло, Т., Ель-Мадхун, Н., Аль-Ага, К., та Зуауї, А. (2023). Графові нейронні мережі для виявлення вторгнень: огляд. Відкритий доступ IEEE, 11, 49114-49139. https://doi.org/10.1109/ACCESS.2023.3275789
13. Кавілл, Е., Ло, В. В., Лаєгі, С., та Портман, М. (2022). Anomal-E: самокерована система виявлення мережевих вторгнень на основі графових нейронних мереж. Системи, засновані на знаннях, 258, 110030. https://doi.org/10.1016/j.knosys.2022.110030
14. Латіф-Мартінес, Х., Суарес-Варела, Ц., Кабельос-Апарісіо, А., та Барлет-Рос, П. (2025). GAT-AD: мережі графової уваги для контекстного виявлення аномалій у моніторингу мереж. Комп'ютери та промислова інженерія, 200, 110830. https://doi.org/10.1016/j.cie.2024.110830
15. Тан, Ц., Хуа, Ф., Гао, Ц., Чжао, П., та Лі, Ц. (2023). GADBench: повторний аналіз і порівняльне оцінювання контрольованого виявлення аномалій у графах. Досягнення в системах оброблення нейронної інформації, 36, 29628-29653.
16. Клез, Б., Треммелл, Б., та Ейткен, П. (ред.). (2013). Специфікація протоколу експорту інформації про IP-потоки для обміну даними про потоки (RFC 7011). Інженерна рада Інтернету. https://doi.org/10.17487/RFC7011
17. Національний інститут стандартів і технологій США. (2024). Концептуальна основа кібербезпеки NIST, версія 2.0 (NIST CSWP 29). https://doi.org/10.6028/NIST.CSWP.29
18. Демпсі, К., та ін. (2011). Безперервний моніторинг інформаційної безпеки федеральних інформаційних систем та організацій (NIST SP 800-137). Національний інститут стандартів і технологій США. https://doi.org/10.6028/NIST.SP.800-137
19. Клез, Б. (ред.). (2004). Експорт службової інформації Cisco Systems NetFlow версії 9 (RFC 3954). Інженерна рада Інтернету. https://doi.org/10.17487/RFC3954

References

1. Ekle, O. A., & Eberle, W. (2024). Anomaly detection in dynamic graphs: A comprehensive survey. ACM Transactions on Knowledge Discovery from Data, 18(8), Article 192, 1-44. https://doi.org/10.1145/3669906
2. Qiao, H., Tong, H., An, B., King, I., Aggarwal, C., & Pang, G. (2025). Deep graph anomaly detection: A survey and new perspectives. IEEE Transactions on Knowledge and Data Engineering, 37(9), 5106-5126. https://doi.org/10.1109/TKDE.2025.3581578
3. Yang, L., Chatelain, C., & Adam, S. (2024). Dynamic graph representation learning with neural networks: A survey. IEEE Access, 12, 43460-43484. https://doi.org/10.1109/ACCESS.2024.3378111
4. Tang, J., Li, J., Gao, Z., & Li, J. (2022). Rethinking graph neural networks for anomaly detection. In Proceedings of the 39th International Conference on Machine Learning (Proceedings of Machine Learning Research, Vol. 162, pp. 21076-21089). PMLR. https://proceedings.mlr.press/v162/tang22b.html
5. Gao, Y., Wang, X., He, X., Liu, Z., Feng, H., & Zhang, Y. (2023). Addressing heterophily in graph anomaly detection: A perspective of graph spectrum. In Proceedings of the ACM Web Conference 2023 (pp. 1528-1538). ACM. https://doi.org/10.1145/3543507.3583268
6. Zheng, J., Yang, C., Zhang, T., Cao, L., Jiang, B., Fan, X., Wu, X.-M., & Zhu, X. (2025). Dynamic spectral graph anomaly detection. Proceedings of the AAAI Conference on Artificial Intelligence, 39(12), 13410-13418. https://doi.org/10.1609/aaai.v39i12.33464
7. Liu, Y., Xie, Q., Chen, Y., Jin, X., Zheng, T., Chong, B., & He, T. (2026). Mitigating homophily disparity in graph anomaly detection: A scalable and adaptive approach. In Proceedings of the ACM Web Conference 2026. ACM. https://doi.org/10.1145/3774904.3792454
8. Bhatia, S., Liu, R., Hooi, B., Yoon, M., Shin, K., & Faloutsos, C. (2022). Real-time anomaly detection in edge streams. ACM Transactions on Knowledge Discovery from Data, 16(4), Article 75, 1-22. https://doi.org/10.1145/3494564
9. Bhatia, S., Wadhwa, M., Kawaguchi, K., Shah, N., Yu, P. S., & Hooi, B. (2023). Sketch-based anomaly detection in streaming graphs. In Proceedings of the 29th ACM SIGKDD Conference (pp. 93-104). ACM. https://doi.org/10.1145/3580305.3599504
10. Lee, J., Kim, S., & Shin, K. (2024). SLADE: Detecting dynamic anomalies in edge streams without labels via self-supervised learning. In Proceedings of the 30th ACM SIGKDD Conference (pp. 1506-1517). ACM. https://doi.org/10.1145/3637528.3671845
11. Ekle, O. A., Eberle, W., & Christopher, J. (2025). Adaptive DecayRank: Real-time anomaly detection in dynamic graphs with Bayesian PageRank updates. Applied Sciences, 15(6), 3360. https://doi.org/10.3390/app15063360
12. Bilot, T., El Madhoun, N., Al Agha, K., & Zouaoui, A. (2023). Graph neural networks for intrusion detection: A survey. IEEE Access, 11, 49114-49139. https://doi.org/10.1109/ACCESS.2023.3275789
13. Caville, E., Lo, W. W., Layeghy, S., & Portmann, M. (2022). Anomal-E: A self-supervised network intrusion detection system based on graph neural networks. Knowledge-Based Systems, 258, 110030. https://doi.org/10.1016/j.knosys.2022.110030

14. Latif-Martínez, H., Suárez-Varela, J., Cabellos-Aparicio, A., & Barlet-Ros, P. (2025). GAT-AD: Graph attention networks for contextual anomaly detection in network monitoring. Computers & Industrial Engineering, 200, 110830. https://doi.org/10.1016/j.cie.2024.110830
15. Tang, J., Hua, F., Gao, Z., Zhao, P., & Li, J. (2023). GADBench: Revisiting and benchmarking supervised graph anomaly detection. Advances in Neural Information Processing Systems, 36, 29628-29653.
16. Claise, B., Trammell, B., & Aitken, P. (Eds.). (2013). Specification of the IP Flow Information Export (IPFIX) protocol for the exchange of flow information (RFC 7011). IETF. https://doi.org/10.17487/RFC7011
17. National Institute of Standards and Technology. (2024). The NIST Cybersecurity Framework (CSF) 2.0 (NIST CSWP 29). https://doi.org/10.6028/NIST.CSWP.29
18. Dempsey, K., et al. (2011). Information security continuous monitoring (ISCM) for federal information systems and organizations (NIST SP 800-137). NIST. https://doi.org/10.6028/NIST.SP.800-137
19. Claise, B. (Ed.). (2004). Cisco Systems NetFlow Services Export Version 9 (RFC 3954). IETF. https://doi.org/10.17487/RFC3954

Історія статті:
Отримано: 05.08.2026 Доопрацьовано: 20.09.2026 Прийнято до друку: 23.09.2026 Опубліковано: 29.09.2026