УДК 004.056:004.89:519.17 DOI: 10.31673/2412-4338.2026.019002

Субач Ігор Юрійович
доктор технічних наук, професор, завідувач кафедри
Інститут спеціального зв'язку та захисту інформації Національного технічного університету України Київський політехнічний інститут імені Ігоря Сікорського, Київ, Україна
ORCID ID: 0000-0002-9344-713X
igor_subach@ukr.net

Фесьоха Віталій Вікторович
доктор філософії, доцент, докторант
Військовий інститут телекомунікацій та інформатизації імені Героїв Крут, Київ, Україна
ORCID ID 0000-0001-6612-1970
vitaliifesokha@gmail.com

Копич Данило Олексійович
аспірант
Інститут спеціального зв'язку та захисту інформації Національного технічного університету України Київський політехнічний інститут імені Ігоря Сікорського, Київ, Україна
ORCID ID: 0009-0005-9809-546X
danyla.kopych@gmail.com

КОНЦЕПЦІЯ ВИЯВЛЕННЯ КІБЕРІНЦИДЕНТІВ В SIEM-СИСТЕМІ НА ОСНОВІ ІНТЕГРАЦІЇ НЕЧІТКИХ ГІПЕРГРАФОВИХ СТРУКТУР І ГЕНЕРАТИВНИХ МОДЕЛЕЙ ШТУЧНОГО ІНТЕЛЕКТУ

Анотація. *У статті представлено концепцію підвищення ефективності виявлення кіберінцидентів у SIEM-системах на основі розроблення концептуальної моделі гібридної архітектури, що поєднує гіперграфові структури даних і генеративний штучний інтелект. Проведено аналіз сучасних методів виявлення загроз у системах аналізу подій безпеки, до яких віднесено класичні рішення на основі кореляційних правил, поведінкові моделі, статистичні методи, машинного та глибокого навчання, графові, гіперграфові та на основі генеративного штучного інтелекту. Визначено їхні переваги, недоліки, характерні обмеження, а також показники ефективності, зокрема точність, гнучкість, інтерпретованість, вимоги до навчальних даних та обчислювальну складність. Проведено системне порівняння відомих підходів, результати якого показали необхідність переходу до гібридних моделей, що поєднують переваги структурних і інтелектуальних методів. Запропоновано концептуальну модель ідентифікації кіберінцидентів в SIEM-системі на основі інтеграції нечітких гіперграфових структур і генеративних моделей штучного інтелекту, де застосовано три взаємопов'язані рівні: структурне представлення даних через нечіткі гіперграфи, генеративний аналіз на основі нейромережевих моделей та пояснювальний модуль XAI (пояснювальний штучний інтелект) для формування інтерпретованого текстового звіту. Розроблений підхід забезпечує виявлення структурних закономірностей у потоках подій, формування прогнозів розвитку можливих атак і відновлення семантичних зв'язків між подіями безпеки. Визначено напрям подальших досліджень, який полягає у розробці нечіткої гіперграфової моделі представлення журналу подій безпеки SIEM-систем. Теоретичний аналіз показує, що запропонована концепція поєднання нечітких гіперграфів і генеративного штучного інтелекту створює необхідні передумови для побудови адаптивних і пояснюваних SIEM-систем нового покоління, здатних до проактивного прогнозування і мінімізації хибних спрацювань.*

Ключові слова: *інформційно-комунікаційна система, кібербезпека, SIEM, кіберінцидент, гіперграф, штучний інтелект.*

Ihor Subach
doctor of technical science, associate professor, head of department
Institute of special communications and information security
National technical university of UkraineIgor Sikorsky Kyiv Polytechnic Institute, Kyiv, Ukraine
ORCID ID: 0000-0002-9344-713X
igor_subach@ukr.net

Vitalii Fesokha
PhD in Information systems and technologies, Associate Professor, Postdoctoral researcher
Kruty Heroes Military Institute of Telecommunications and Information Technologies, Kyiv, Ukraine
ORCID ID 0000-0001-6612-1970
vitaliifesokha@gmail.com

Danylo Kopych
postgraduate student
Institute of special communications and information security
National technical university of UkraineIgor Sikorsky Kyiv Polytechnic Institute, Kyiv, Ukraine
ORCID ID: 0009-0005-9809-546X
danyla.kopych@gmail.com

ANALYSIS OF CURRENT APPROACHES TO DETECTION OF CYBER INCIDENTS IN SIM SYSTEMS AND DIRECTIONS FOR THEIR IMPROVEMENT

Abstract. *The article presents the concept of increasing the efficiency of cyber incident detection in SIEM systems based on the development of a conceptual model of a hybrid architecture that combines hypergraph data structures and generative artificial intelligence. An analysis of modern methods for detecting threats in security event analysis systems is carried out, which include classical solutions based on correlation rules, behavioral models, statistical methods, machine and deep learning, graph, hypergraph and generative artificial intelligence. It is established that classical and statistical methods do not adapt to new types of attacks, and deep learning, although it achieves high accuracy, is inferior in the interpretability of results and resource requirements. A systematic comparison of known approaches is carried out, the results of which showed the need to transition to hybrid models that combine the advantages of structural and intelligent methods. A conceptual model of cyber incident identification in a SIEM system is proposed based on the integration of fuzzy hypergraph structures and generative artificial intelligence models, where three interconnected levels are applied: structural data representation through fuzzy hypergraphs, generative analysis based on neural network models, and an explanatory XAI (Explanatory Artificial Intelligence) module for generating an interpreted text report. The developed approach provides for the detection of structural patterns in event flows, the formation of forecasts of the development of possible attacks, and the restoration of semantic relationships between security events. The direction of further research is determined, which consists in the development of a fuzzy hypergraph model for representing the security event log of SIEM systems. Theoretical analysis shows that the proposed concept of combining fuzzy hypergraphs and generative artificial intelligence creates the necessary prerequisites for building adaptive and explainable new generation SIEM systems capable of proactive prediction and minimizing false positives.*

Keywords: *cybersecurity, SIEM, information and communication system, cyber incident, hypergraph, artificial intelligence.*

1. Вступ

У сучасних системах кібербезпеки спостерігається стрімке зростання обсягу подій, що генеруються інформаційно-комунікаційними системами (ІКС), сервісами та мережевою інфраструктурою. Традиційні SIEM-системи, які переважно спираються на класичні алгоритми аналізу подій та статичні кореляційні правила, виявляються обмеженими за здатністю ефективно обробляти ці потоки даних, своєчасно виявляти складні, багатофакторні та нові типи загроз, а також коректно моделювати й корелювати комплексні міжоб'єктні залежності користувачів, процесів та мережевих вузлів, що призводить до втрати семантики взаємозв'язків серед подій, зниження точності виявлення кіберінцидентів та унеможливлює побудову в умовах швидко еволюціонуючого ландшафту кібератак, а також невизначеності та неповноти даних про них.

2. Постановка проблеми

У зв'язку з цим виникає актуальне наукове завдання щодо розроблення моделей виявлення кіберінцидентів, здатних одночасно забезпечити структурне відображення складних залежностей, врахування невизначеності даних та інтерпретованість результатів аналізу, що потребує переходу до гібридних підходів на основі поєднання структурних і генеративних методів.

3. Аналіз останніх досліджень і публікацій.

Аналіз останніх публікацій [1-3] свідчить про актуальність досліджень можливостей штучного інтелекту (ШІ) та напрямів його використання у сфері кіберзахисту. Проте залишаються низка невирішених низка питань, зокрема: ШІ-системи можуть помилково ідентифікувати нешкідливі дії як

загрози й пропускати реальні кібератаки; величезний обсяг даних перевантажує класичні SIEM-системи, а лінійні методи аналізу часто втрачають логічний зв'язок між розрізненими подіями складної атаки; моделі та методи ШІ швидко розвиваються, однак зловмисники також адаптують свої атаки, використовуючи ті самі або схожі техніки машинного навчання.

4. Мета і задачі дослідження

Метою дослідження є аналіз існуючих підходів до виявлення кіберінцидентів у SIEM-системах, узагальнення їхніх недоліків та визначення шляхів підвищення ефективності роботи цих систем на основі розрозробки та застосування новпоєднання гіперграфових структур і генеративних моделей штучного інтелекту.

5. Результати дослідження

Проведений порівняльний аналіз методологічних підходів [1-5] дозволив виявити фундаментальні компроміси, які неминучі при побудові ефективних SIEM-систем для виявлення кіберінцидентів.

Очевидно (див. табл. 1), що жоден окремо взятий метод не забезпечує оптимальний баланс між усіма критичними вимогами. Рух від простих до складних методів не є лінійним, а радше процесом постійного балансування між точністю, гнучкістю, обчислювальною вартістю, вимогами до даних та пояснюваністю. Кожен наступний крок у цій еволюції – це не безумовний прогрес, а свідома гра на компромісах: виграш у гнучкості й здатності працювати з новими загрозами неминуче оплачується зростанням складності, ресурсних витрат і втратою прозорості для аналітиків.

Таблиця 1

Порівняльні характеристики основних підходів до виявлення кіберінцидентів

Метод / Підхід	Гнуч-кість	Точність	Вимоги до даних	Складність обчислень	Інтерпре-тованість	Навчання	APT (атаки)
Rule-based	Низька	Середня	Низькі	Низька	Висока	–	Низька
Статистичні	Середня	Низька	Середні	Низька	Середня	Мін.	Середня
ML	Висока	Висока	Високі	Середня	Середня	Значне	Висока
DL	Висока	Дуже вис.	Дуже вис.	Висока	Сер.-Вис.	Інтенсивне	Висока
GNN	Висока	Висока	Середні	Висока	Середня	Складне	Висока
HGNN	Дуже вис.	Дуже вис.	Середні	Дуже вис.	Низька	Складне	Дуже вис.
GenAI	Висока	Висока	Варіативні	Дуже вис.	Низька	Значне	Дуже вис.

Кількісну оцінку співвідношення цих параметрів, яка виконувалась на основі узагальнення результатів аналізу сучасних досліджень у галузі виявлення кіберінцидентів та систем виявлення вторгнень, а також на основі метрик ефективності, що традиційно використовуються для оцінювання систем кібербезпеки [4–9], наведено у таблиці 2.

Таблиця 2

Порівняння гнучкості, складності та точності

Методи	Гнучкість	Складність	Точність	Балансність
Rule-based	(1/5)	(1/5)	(3/5)	Жорстко
Statistical	(2/5)	(2/5)	(2/5)	Обидві низькі
ML	(4/5)	(3/5)	(4/5)	Баланс
DL	(4/5)	(4/5)	(5/5)	Чорна скринька
Graph	(4/5)	(3/5)	(4/5)	Баланс
Hypergraph	(5/5)	(5/5)	(4/5)	Крайній Баланс
Gen-AI	(4/5)	(4/5)	(4/5)	Галюцинації

Для забезпечення можливості порівняння різних підходів використано нормовану експертно-аналітичну шкалу від 1 до 5, де значення відображають відносний рівень прояву відповідної

характеристики: 1 – дуже низький рівень або мінімальна відповідність критерію; 2 – низький рівень; 3 – середній рівень; 4 – високий рівень; 5 – дуже високий рівень.

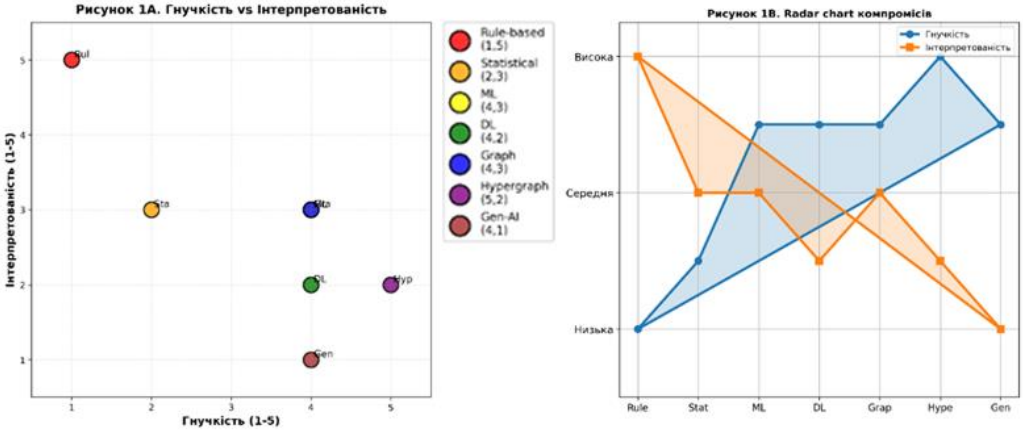

Рис. 1. Компроміс між гнучкістю та інтерпретованістю

Гнучкість не тотожна точності, і підвищення одного параметра не гарантує зростання іншого. Найбільш практичними для реальних SOC є гібридні методи, які пропонують збалансований компроміс без критичної втрати прозорості. Зокрема, Hypergraph-підходи виступають перспективним напрямом для сценаріїв з особливо складними APT-атаками, тоді як DL і Gen-AI доцільно застосовувати обережно, як аналітичні модулі другого рівня, а не як єдине джерело істини.

Рисунок 1 демонструє компроміс між гнучкістю та інтерпретованістю. Традиційні методи високо інтерпретовані, але є негнучкими, тоді як сучасні підходи досягають високої адаптивності за рахунок зниження прозорості.

Рисунок 2 ілюструє компроміс між точністю виявлення та обчислювальною складністю. Глибоке навчання досягає максимальної точності (5/5), але вимагає значних ресурсів (4/5), тоді як гібридні методи (Graph/Hypergraph) знаходяться в оптимальній зоні для практичного впровадження.

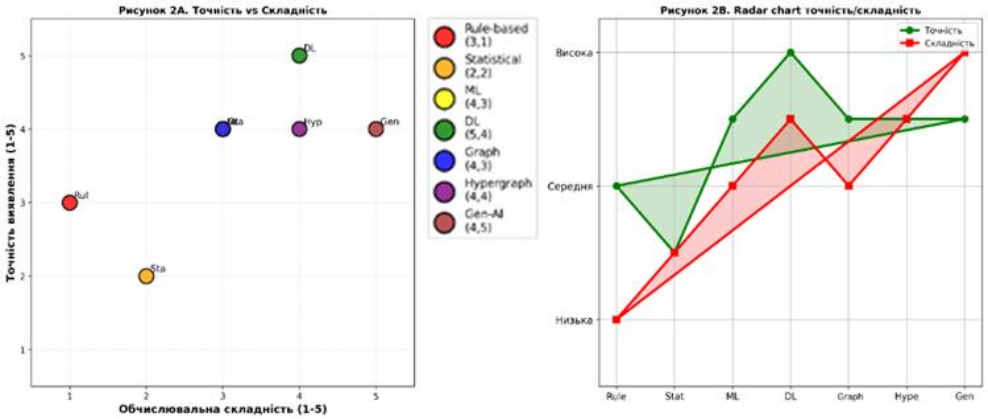

Рис. 2. Компроміс між точністю виявлення та обчислювальною складністю

Таблиця порівняння демонструє, що ефективне виявлення кіберінцидентів/кібератак в SIEM-системах потребує гібридного підходу, де: Rule-based методи – базовий захист; Statistical методи – виявлення базових аномалій; ML методи – адаптивна детекція на кореляціях; Graph/GNN – моделювання multi-entity зв'язків; Hypergraph – складна багатоетапна APT детекція; Generative AI – прогнозування загроз та генерація сценаріїв.

Отже, проведений аналіз можливостей та обмежень сучасних SIEM-систем свідчить про певне вичерпання потенціалу класичних методів для протидії APT-атакам. Подальший розвиток технологій виявлення кіберінцидентів лежить у площині переходу від аналізу ізольованих подій до моделювання складної топології кібератак та генеративного передбачення загроз.

Можливості традиційних графових моделей є недостатніми для опису багатовимірних зв’язків у сучасних ІКС. Кібератаки рідко є простою послідовністю дій «точка-точка». Вони охоплюють одночасну взаємодію багатьох сутностей (користувач, IP-адреса, процес, файл, політика доступу тощо). Тому, перспективним напрямом є застосування гіперграфових моделей, де одне гіперребро може з’єднувати довільну кількість вершин, що дозволяє: зберегти семантичний контекст, де одна дія

впливає на групу активів; знаходити неявні зв'язки між розрізненими подіями, які губляться при лінійному аналізі або стандартній граф-аналітиці; враховувати невизначеність та неповноту даних у подіях шляхом використання нечітких гіперграфів, що знижує рівень хибних спрацювань.

У сою чергу, роль ШІ у SIEM-системах трансформується з виявлення до класифікації, генерації та прогнозування кіберінцидентів. Використання генеративного ШІ дозволяє вирішити проблему дефіциту розмічених даних про рідкісні кібератаки. Ключові напрями застосування: генерація синтетичних, але реалістичних сценаріїв кібератак для тренування детекторів, що дозволяє виявляти загрози, які ще не зустрічалися в реальному середовищі; моделювання можливих шляхів розвитку кібератаки на основі поточної конфігурації мережі, перетворюючи кіберзахист з реактивного на проактивний; формування гіпотез для пошуку вразливостей, аналізуючи відхилення від нормальних структурних патернів у гіперграфі.

З іншого боку, критичною проблемою впровадження Deep Learning є ефект «чорної скриньки». Для довіри до системи необхідно розвивати методи Explainable AI (XAI), адаптовані для кібербезпеки: візуалізація підграфа атаки, що показує конкретні вузли та зв'язки, які стали причиною тривоги; використання ШІ для генерації текстового опису інциденту зрозумілою мовою, що значно пришвидшує роботу аналітика.

Відповідно до наведеного, пропонується гібридна архітектура аналізу подій, що поєднує їх структурне моделювання на основі гіперграфів та генеративний аналіз із використанням великих мовних моделей (дивись рисунок 4).

Запропонована система виявлення кіберінцидентів реалізує гібридну архітектуру аналізу подій безпеки, що інтегрує структурні методи моделювання взаємозв'язків між подіями та інтелектуальні методи семантичної інтерпретації. Архітектура системи орієнтована на оброблення журналів подій SIEM-системи та складається з трьох взаємопов'язаних функціональних рівнів: рівня структурного представлення подій, рівня виявлення інцидентів та рівня семантичної інтерпретації і прогнозування.

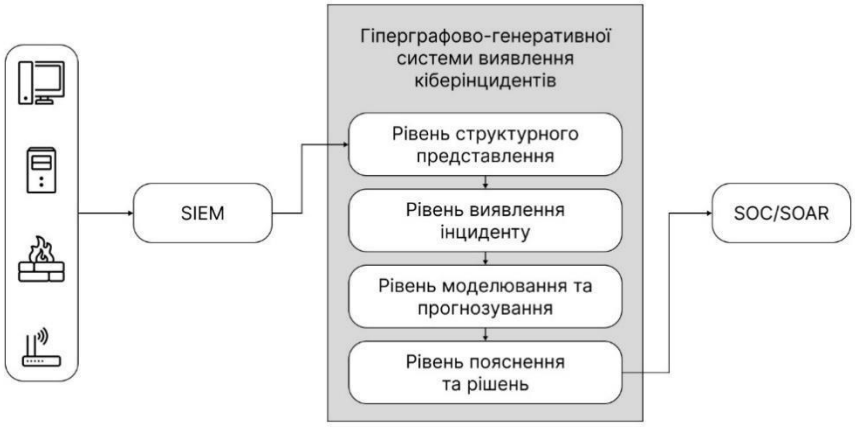

Рис. 4. Архітектура гіперграфово-генеративної системи виявлення кіберінцидентів

На рівні структурного представлення система перетворює потік подій безпеки на структурну модель у вигляді нечіткого гіперграфа. У цій моделі вершини відповідають сутностям ІКС (користувачам, вузлам мережі, процесам, файлам тощо), тоді як гіперребра відображають події безпеки, що пов'язують декілька сутностей одночасно. Такий підхід дозволяє зберігати семантичний контекст подій та відображати складні багатосутнісні взаємодії між елементами системи, що, у свою чергу, забезпечує цілісне подання семантичного контексту складних кібератак/кіберінцидентів.

Нехай нечіткий гіперграф описується кортежем:

$$H_{Fuzzy} = (V, \varepsilon, \mu), \quad (1)$$

де V – множина вершин, що відповідають сутностям інформаційно-комунікаційної системи; ε – множина нечітких гіперребер, кожне з яких представляє окрему подію безпеки, що пов'язує підмножину вершин; $\mu: \varepsilon \to [0,1]$ – функція, яка відображає ступінь належності події безпеки до кіберінциденту та формується на основі інтеграції декількох часткових характеристик події (критичність, аномальність, репутаційні атрибути джерела тощо).

Такий підхід забезпечує можливість: зберігати складні багатовимірні залежності між подіями та сутностями; враховувати невизначеність, неповноту й суперечливість даних; виконувати подальший аналіз на рівні підграфів гіперграфа подій, що відповідають потенційним сценаріям атак.

На рівні виявлення кіберінциденту здійснюється аналіз структурних властивостей побудованого гіперграфа з метою виявлення аномальних підструктур. Кіберінцидент у цьому випадку

інтерпретується як підграф нечіткого гіперграфа подій, топологічні характеристики якого відповідають певним патернам атак або перевищують визначений поріг ризику. Для цього використовуються операції аналізу гіперграфів, зокрема пошук зв'язних компонент, виділення щільних підструктур та оцінювання агрегованої міри ризику та ін.

Формально кіберінцидент можна інтерпретувати як зв'язний підграф $H_{sub} \subseteq H_{Fuzzy}$, для якого агрегована міра ризику перевищує визначений поріг:

$$\mu_{Incident}(H_{sub}) = \ T_{agg}(\{e \in H_{sub}\}) \geq \alpha, \quad (2)$$

де T_{agg} – оператор агрегації значень функції належності $\mu(e)$; α – порогове значення для прийняття рішення щодо виявлення кіберінциденту.

Зауважимо, що у порівнянні з класичними підходами, запропоноване подання кіберінциденту дозволяє більш ефективно відображати причинно-наслідкові зв'язки між розрізненими подіями безпеки.

Третій рівень моделювання, прогнозування та пояснення реалізує семантичну інтерпретацію виявлених аномальних структур та прогнозування можливого розвитку кібератаки. На цьому рівні застосовується велика мовна модель (ВММ), яка аналізує топологію аномального підграфа разом із контекстною інформацією з бази знань кібербезпеки (тактики, техніки та процедури атак, відомі сценарії кібератак, доменно-специфічні правила) та формує пояснюваний текстовий опис інциденту, а також рекомендації щодо реагування на нього.

Даний рівень запропонованої архітектури спрямований на подолання двох критичних проблем сучасних ШІ-підходів у кібербезпеці – дефіциту розмічених даних про рідкісні атаки та низьку інтерпретованість рішень. Для цього вводиться модуль семантичної інтерпретації та прогнозування G_{Exp}, який здійснює генеративний аналіз виділених аномальних підграфів та забезпечує пояснювану підтримку прийняття рішень.

Модуль G_{Exp} представляється кортежем:

$$G_{Exp} = \langle M_{Gen}, K, S_{prop} \rangle, \quad (3)$$

де M_{Gen} – ВММ, призначена для семантичної інтерпретації структурних патернів у гіперграфі, а також для генерації текстових пояснень та гіпотез щодо розвитку атаки; K – зовнішня база знань, яка включає формалізовані тактики, техніки та процедури атак, відомі сценарії кібератак та доменно-специфічні правила, що являють собою формалізовані обмеження предметної області, які визначають допустимі або аномальні конфігурації вершин і гіперребер у гіперграфі подій та використовуються для ідентифікації підграфів, що можуть відповідати сценаріям кібератак; S_{prop} – механізм симуляції поширення загрози, що дозволяє оцінювати можливі траєкторії розвитку атаки в інфраструктурі та визначати найбільш критичні активи.

Функціонально рівень виконує три основні задачі: на основі топології аномального підграфа ідентифікує потенційно пропущені ланки в ланцюжку атаки, порівнюючи спостережуваний патерн із відомими сценаріями в базі знань K; використовуючи S_{prop}, проєктує виявлений патерн та згенеровані гіпотези на модель інфраструктури та оцінює ймовірні сценарії подальшого поширення загрози; генеративна модель M_{Gen} формує текстовий звіт, який містить опис виявленого кіберінциденту, ключові події й сутності, можливі пропущені етапи, прогнозовані наслідки та рекомендовані дії з реагування.

На основі результатів структурного аналізу на рівні нечіткого гіперграфа та семантичної інтерпретації ситуації модулем G_{Exp} система формує множину рішень D, що відображає можливі дії реагування на виявлені кіберінциденти.

Таким чином, запропонована архітектура забезпечує поєднання структурного аналізу подій безпеки з інтелектуальною інтерпретацією результатів, що дозволяє підвищити ефективність виявлення складних багатоетапних атак та зменшити когнітивне навантаження на аналітиків центрів операцій безпеки.

Як базову основу використано модель ідентифікації кіберінцидентів, запропоновану в роботі [10], яка формально описується кортежем:

$$MF = \langle KF, O, RF, C \rangle, \quad (4)$$

де KF – нечіткий класифікатор; O – множина ознак; RF – множина нечітких правил; C – кіберінцидент.

Проте, дана модель забезпечує інтерпретованість прийняття рішень, але використовує векторне представлення ознак та правило-орієнтовану логіку, що обмежує здатність відображати складні багатосутнісні залежності у випадку багатокрокових APT-атак та сценаріїв з неповними даними.

З огляду на це запропоновано удосконалену гібридну модель виявлення кіберінцидентів у середовищі SIEM (5), що поєднує нечітке гіперграфове представлення журналів подій із генеративним модулем їхньої семантичної інтерпретації.

$$M_{SIEM} = \langle E, H_{Fuzzy}, O_{per}, G_{Exp}, D \rangle, \quad (5)$$

де $E = \{e_i\}$ – множина вхідних подій; H_{Fuzzy} – модуль відображення потоків подій у динамічний нечіткий гіперграф; O_{per} – множина операцій над нечіткими гіперграфами, що реалізує алгоритмічні процедури виявлення аномальних структур; G_{Exp} – модуль семантичної інтерпретації та прогнозування на основі генеративного штучного інтелекту; D – множина рішень щодо інцидентів (виявлення, класифікація, пріоритезація, рекомендації щодо реагування).

6. Висновки та перспективи подальших досліджень

Встановлено, що однією з ключових причин зниження ефективності існуючих SIEM-систем є втрата семантичного контексту при лінійному або парному аналізі подій.

Обґрунтовано доцільність використання нечітких гіперграфових моделей в якості математичного апарату для представлення журналів подій безпеки.

Запропоновано концепцію інтеграції нечітких гіперграфових моделей подій із BMM для аналізу подій безпеки в SIEM-системах.

Розроблено концептуальну модель гібридної архітектури SIEM, яка інтегрує три взаємопов'язані рівні: структурне представлення потоків подій у вигляді динамічного нечіткого гіперграфа; алгоритмічний аналіз аномальних структур і топологічних патернів атак; генеративний модуль семантичної інтерпретації та прогнозування розвитку кіберінцидентів.

Перспективи подальших досліджень пов'язані з: розробленням методів побудови нечіткого гіперграфа подій безпекиі та методів пошуку аномальних підграфів, що відповідають сценаріям складних багатоетапних атак, а також інтеграцією гіперграфових моделей із BMM для семантичного аналізу та прогнозування розвитку кіберінцидентів.

Внесок авторів Ігор Субач – концептуалізація дослідження, постановка задачі, участь у формуванні висновків дослідження; Віталій Фесьоха – проведення системного та порівняльного аналізу сучасних підходів до виявлення кіберінцидентів, інтерпретація отриманих результатів, участь у формуванні висновків дослідження; Данило Копич – збір і аналіз джерел, підготовка огляду літератури, розроблення та обґрунтуванні концепції виявлення кіберінцидентів, формалізація моделі.

Декларація про штучний інтелект

Інструменти штучного інтелекту використовувалися для мовно-стилістичного редагування тексту та не впливали на науковий зміст, результати та висновки дослідження..

Конфлікт інтересів

Автори заявляють про відсутність конфлікту інтересів та підтверджують, що під час підготовки цієї роботи не існувало жодних комерційних, фінансових чи інших взаємовідносин, які могли б бути розцінені як такі, що здатні вплинути на результати дослідження або їх інтерпретацію. Робота виконана відповідно до принципів академічної доброчесності, етичних норм проведення наукових досліджень та вимог редакційної політики щодо запобігання конфлікту інтересів.

Список використаної літератури

1. Pulyala, S. R. (2024). From detection to prediction: AI-powered SIEM for proactive threat hunting and risk mitigation. Turkish Journal of Computer and Mathematics Education, 15(1), 34-43.

2. Paidy, P. (2025). Unified Threat Detection Platform with AI, SIEM, and XDR. International Journal of Artificial Intelligence, Data Science, and Machine Learning, 6(1), 95-104. https://doi.org/10.63282/3050-9262.IJAIDSML-V6I1P111.

3. Marri, R., Varanasi, S., & Kalidindi Chaitanya, S. V. (2024). Integrating Next-Generation SIEM with Data Lakes and AI: Advancing Threat Detection and Response . Journal of Artificial Intelligence General Science (JAIGS) ISSN:3006-4023, 3(1), 446–465. https://doi.org/10.60087/jaigs.v3i1.263.

4. Subach, I. Y., Kubrak, V. O., Mykytiuk, A. V., Korotaiev, S. O. (2020). Zero-day polymorphic cyberattacks detection using fuzzy inference system. Austrian Journal of Technical and Natural Sciences, 5–6, 8–13.

5. Sarker, I. H., Janicke, H., Ferrag, M. A., & Abuadbba, A. (2024). Multi-aspect rule-based AI: Methods, taxonomy, challenges and directions toward automation, intelligence and transparent cybersecurity modeling for critical infrastructures. Internet of Things, 101110. https://doi.org/10.1016/j.iot.2024.101110.

6. Liu, K., Wang, F., Ding, Z., Liang, S., Yu, Z., & Zhou, Y. (2022). A review of knowledge graph application scenarios in cyber security. arXiv preprint arXiv:2204.04769.

7. Lourenço, B., Adão, P., Ferreira, J. F., Marques, M. M., & Vaz, C. (2025). Structuring Security: A Survey of Cybersecurity Ontologies, Semantic Log Processing, and LLMs Application. arXiv preprint arXiv:2510.16610.

8. Cotti, L., Drago, I., Rula, A., Bianchini, D., & Cerutti, F. (2025). OntoLogX: Ontology-Guided Knowledge Graph Extraction from Cybersecurity Logs with Large Language Models. arXiv preprint arXiv:2510.01409.

9. Kalakoti, R., Vaarandi, R., Bahsi, H., & Nõmm, S. (2025). Evaluating explainable AI for deep learning-based network intrusion detection system alert classification. arXiv preprint arXiv:2506.07882.

10. Субач, І., & Кубрак, В. (2023). Модель ідентифікації кіберінцидентів SIEM-системою для захисту інформаційно-комунікаційних систем. Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка», 4(20), 81–92. https://doi.org/10.28925/2663-4023.2023.20.8192

References

1. Pulyala, S. R. (2024). From detection to prediction: AI-powered SIEM for proactive threat hunting and risk mitigation. Turkish Journal of Computer and Mathematics Education, 15(1), 34-43.

2. Paidy, P. (2025). Unified Threat Detection Platform with AI, SIEM, and XDR. International Journal of Artificial Intelligence, Data Science, and Machine Learning, 6(1), 95-104. https://doi.org/10.63282/3050-9262.IJAIDSML-V6I1P111.

3. Marri, R., Varanasi, S., & Kalidindi Chaitanya, S. V. (2024). Integrating Next-Generation SIEM with Data Lakes and AI: Advancing Threat Detection and Response . Journal of Artificial Intelligence General Science (JAIGS) ISSN:3006-4023, 3(1), 446–465. https://doi.org/10.60087/jaigs.v3i1.263.

4. Subach, I. Y., Kubrak, V. O., Mykytiuk, A. V., Korotaiev, S. O. (2020). Zero-day polymorphic cyberattacks detection using fuzzy inference system. Austrian Journal of Technical and Natural Sciences, 5–6, 8–13.

5. Sarker, I. H., Janicke, H., Ferrag, M. A., & Abuadbba, A. (2024). Multi-aspect rule-based AI: Methods, taxonomy, challenges and directions toward automation, intelligence and transparent cybersecurity modeling for critical infrastructures. Internet of Things, 101110. https://doi.org/10.1016/j.iot.2024.101110.

6. Liu, K., Wang, F., Ding, Z., Liang, S., Yu, Z., & Zhou, Y. (2022). A review of knowledge graph application scenarios in cyber security. arXiv preprint arXiv:2204.04769.

7. Lourenço, B., Adão, P., Ferreira, J. F., Marques, M. M., & Vaz, C. (2025). Structuring Security: A Survey of Cybersecurity Ontologies, Semantic Log Processing, and LLMs Application. arXiv preprint arXiv:2510.16610.

8. Cotti, L., Drago, I., Rula, A., Bianchini, D., & Cerutti, F. (2025). OntoLogX: Ontology-Guided Knowledge Graph Extraction from Cybersecurity Logs with Large Language Models. arXiv preprint arXiv:2510.01409.

9. Kalakoti, R., Vaarandi, R., Bahsi, H., & Nõmm, S. (2025). Evaluating explainable AI for deep learning-based network intrusion detection system alert classification. arXiv preprint arXiv:2506.07882.

10. Subach, I., & Kubrak, V. (2023). Model of cyber incident identification by SIEM for protection of information and communication systems. Electronic Professional Scientific Journal «Cybersecurity: Education, Science, Technique», 4(20), 81–92. https://doi.org/10.28925/2663-4023.2023.20.8192

Надійшла до редакції: 11.11.25
Прийнята до друку: 17.03.26
Опубліковано: 30.03.26