НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ «ОДЕСЬКА ЮРИДИЧНА АКАДЕМІЯ»

ФАКУЛЬТЕТ КІБЕРБЕЗПЕКИ ТА ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

28 листопада 2025 року

КІБЕРБЕЗПЕКА В СУЧАСНОМУ СВІТІ: АКТУАЛЬНІ ВИКЛИКИ

МАТЕРІАЛИ VI МІЖНАРОДНОЇ НАУКОВО-ПРАКТИЧНОЇ КОНФЕРЕНЦІЇ

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Національний університет «Одеська юридична академія»
Факультет кібербезпеки та інформаційних технологій
Кафедра кібербезпеки

КІБЕРБЕЗПЕКА В СУЧАСНОМУ СВІТІ: АКТУАЛЬНІ ВИКЛИКИ

МАТЕРІАЛИ VI МІЖНАРОДНОЇ НАУКОВО-ПРАКТИЧНОЇ КОНФЕРЕНЦІЇ

28 листопада 2025 року, м. Одеса

Одеса, 2025

MINISTRY OF EDUCATION AND SCIENCE OF UKRAINE
National University «Odesa Law Academy»
Faculty of Cybersecurity and Information Technologies
Department of Cybersecurity

CYBERSECURITY IN TODAY'S WORLD: ACTUAL CHALLENGES

MATERIALS OF THE VI INTERNATIONAL SCIENTIFIC AND PRACTICAL CONFERENCE

November 28, 2025, Odesa

Odesa, 2025

УДК 004.056

Відповідальній редактор:

О. В. Дикий, декан факультету кібербезпеки та інформаційних технологій, кандидат юридичних наук, доцент

Матеріали видано в авторській редакції.
Повну відповідальність за достовірність та якість поданого матеріалу несуть учасники конференції, їхні наукові керівники, які рекомендували ці матеріали до друку.

Рекомендовано до друку
Вченою радою Національного університету
«Одеська юридична академія»
(протокол №3 від 29.11.2025 р.)

Матеріали Міжнародної науково-практичної конференції «Кібербезпека в сучасному світі: актуальні виклики» (м. Одеса, 28 листопада 2025 р.). Одеса, 2025. 287 с.

У конференції взяли участь студенти, аспіранти, молоді вчені, викладачі та науковці. Конференція проводиться на базі Національного університету «Одеська юридична академія».

UDC 004.056

Editor-in-chief:

O. V. Dykyi, Dean of the Faculty of Cybersecurity and Information Technologies,
Candidate of Law, Associate Professor

The materials were published in the author's edition.
Full responsibility for the reliability and quality of the submitted material
bears the participants of the conference, their scientific supervisors,
who recommended these materials for publication.

Recommended for printing
by the Academic Council of the National University
«Odesa Law Academy»
(Minutes No. 3 dated 11/29/2025)

Materials of the International Scientific and Practical Conference «Cybersecurity in the Modern World: Current Challenges» (Odessa, November 28, 2025). Odesa, 2025. 287 p.

The conference was attended by students, postgraduates, young scientists, teachers and researchers. The conference is held at the National University «Odesa Law Academy».

VI Міжнародна науково-практична конференція

«Кібербезпека в сучасному світі: актуальні виклики»

28 листопада 2025 року

ТЕМАТИЧНІ НАПРЯМКИ КОНФЕРЕНЦІЇ:

Секція 1. Алгоритмічні та технічні аспекти кібербезпеки

Секція 2. Штучний інтелект та інформаційні технології

Секція 3. Управлінські, соціальні та психологічні аспекти взаємодії з кіберпростором

Секція 4. Нормативно-правові засади кібербезпеки та захисту інформації

E-mail: kiberprostirconf@gmail.com (Для питань та тез)

VI International Scientific and Practical Conference

«Cybersecurity in today's world: actual challenges»

28 November 2025 year

THEMATIC DIRECTIONS OF THE CONFERENCE:

Section 1. Algorithmic and technical aspects of cybersecurity

Section 2. Artificial intelligence and information technologies

Section 3. Management, social and psychological aspects of interaction with cyberspace

Section 4. Regulatory and legal principles of cybersecurity and information protection

E-mail: kiberprostirconf@gmail.com (Для питань та тез)

Однак справжній цифровий суверенітет не може бути забезпечений, поки управління даними залишається у постачальників. Формальне перенесення зберігання даних в ЦОД, територіально розташованих в країнах ЄС, не усуває юридичних ризиків і проблеми безпеки даних, створюючи лише видимість контролю. Справжній суверенітет даних може бути досягнутий лише при використанні власної європейської інфраструктури, доповненої використанням шифрування даних на стороні клієнта, використанням відкритого програмного забезпечення і моделей нульової довіри. Тільки такий комплекс заходів дозволить гарантувати захист даних і створити повноцінне суверенне хмара.

Список використаних джерел

1. OpenCloud. US law in European data centres? The CLOUD Act makes it possible. [Електронний ресурс]. URL: https://opencloud.eu/en/the-cloud-act-makes-it-possible (дата звернення: 10.11.2025).
2. Art. 48 GDPR: Transfers or disclosures not authorised by Union law. [Електронний ресурс]. URL: https://gdpr-info.eu/art-48-gdpr/ (дата звернення: 10.11.2025).
3. Навігація в майбутньому цифрового суверенітету. Omdia Market Radar: Sovereign Cloud 2025. [Електронний ресурс]. URL: https://discover.vultr.com/omdia-sovereign-cloud-2025 (дата звернення: 11.11.2025).
4. Чанишев Р.І. Федеративна європейська інфраструктура даних Gaia-X як інструмент технологічного суверенітету Європи: досвід для України. *Системи та технології*. 2022. №2 (64). С. 48-55. DOI https://doi.org/10.32782/2521-6643-2022.2-64.6/.
5. European Cloud services operate in a largely fragmented environment that poses major challenges in terms of complexity, performance and security [Електронний ресурс]. URL: https://surl.li/kwwbph (дата звернення: 11.11.2025).

Ключові слова: sovereign cloud, цифровий суверенітет, юрисдикція даних, гіперскейлери, моделі можливих реалізацій концепції «суверенної хмари», досвід побудови суверенного хмарного сервісу в ЄС.
Keywords: sovereign cloud, digital sovereignty, data jurisdiction, hyperscalers, models of possible implementations of the “sovereign cloud” concept, experience in building a sovereign cloud service in the EU.

ГРАФОВІ МОДЕЛІ ДЛЯ ВАЛІДАЦІЇ ВРАЗЛИВОСТЕЙ

Денисюк Владислав

Національний технічний університет «Харківський Політехнічний Інститут», аспірант кафедри кібербезпеки

Традиційні методи виявлення та валідації вразливостей – статичний аналіз, динамічне тестування, сканування забезпечують лише локальний погляд на безпеку інформаційної системи. Вони визначають наявність

окремих вразливостей, але не здатні врахувати складні залежності між компонентами, шляхи потенційної експлуатації та каскадний вплив на інші елементи інфраструктури.

У сучасних гібридних та розподілених системах критичним стає **не лише знайти вразливість**, а й **оцінити, як вона може бути використана у ланцюгу атаки**, яким чином взаємодіє з іншими загрозами та чи може спричинити компрометацію системи на вищому рівні. Графові моделі, графи атак, графи залежностей, поведінкові графи дозволяють побудувати комплексне представлення структури системи, її взаємозв'язків, потенційних шляхів експлуатації та ризиків. Вони дають змогу перейти від точкової валідації вразливостей до **системного, структурного та прогнозного аналізу**, що підвищує ефективність валідації [1].

Попри наявність окремих підходів до моделювання шляхів атак, досі бракує адаптивних інтегрованих методів, які одночасно враховували б топологію системи, взаємозв'язки між її компонентами, характеристики вразливостей, ймовірність їх експлуатації та можливості машинного навчання для прогнозування ризику. Це створює потребу у розробці графових моделей, здатних забезпечити ефективну валідацію вразливостей шляхом поєднання аналізу статичних залежностей із урахуванням динамічної поведінки інформаційної системи.

Метою роботи є обґрунтування використання графових моделей для валідації вразливостей у сучасних інформаційних системах, включно з побудовою графів атак, графів залежностей та застосуванням графових методів машинного навчання для оцінки ризику й прогнозування експлуатації.

Графова модель валідації вразливостей може бути формально описана як орієнтований граф:

$$G = (V, E) \qquad (1)$$

де V – це множина вузлів, що відповідають станам системи, компонентам, конфігураціям або вразливостям, а E – це множина орієнтованих ребер, які описують можливі переходи між станами, залежності між компонентами або кроки потенційної атаки. Таким чином, граф надає структурне уявлення про те, як одна вразливість або зміна стану може впливати на інші елементи інформаційної системи. Кожен вузол $v \in V$може мати власні властивості, які характеризують рівень небезпеки чи важливості елемента. Для формального опису їх можна представити у вигляді функції ознак:

$$f(v) \in R^k \qquad (2)$$

де k – це кількість параметрів, наприклад складність експлуатації, критичність компонента або рівень привілеїв, який може бути отриманий при успішній атаці. Ребра графа описують не лише сам факт залежності між вузлами, але й силу або значущість цього зв'язку, що формалізується наступною ваговою функцією:

$$w: E \to R \geq 0 \qquad (3)$$

У сукупності ці елементи дозволяють досліджувати як статичні властивості системи, так і її динамічну поведінку, моделюючи можливі сценарії розвитку атаки та визначаючи критичні точки, в яких необхідна валідація. Для випадків, коли граф використовується у моделях машинного навчання, застосовується спрощене представлення через матрицю суміжності:

$$A = [a_{ij}] \qquad (4)$$

Де a_{ij} = 1 , якщо між вузлами існує зв'язок, та 0 у протилежному разі. Ознаки вузлів описуються матрицею:

$$X \in R^{Vk} \qquad (5)$$

що використовується як вхід для алгоритмів, здатних враховувати структуру графа при оцінці ризику [2]. Таке формальне представлення дозволяє описати вразливості не як ізольовані об'єкти, а як частини складної системи з численними залежностями, що суттєво підвищує точність і корисність валідації. Графові моделі забезпечують можливість визначати найкоротші шляхи атаки, оцінювати каскадні ефекти та розуміти, як змінюється ризик при додаванні або усуненні певної вразливості. Завдяки цьому вони створюють основу для побудови адаптивних і масштабованих систем валідації, здатних ефективно реагувати на сучасні типи загроз [3]. У цьому контексті графові згорткові мережі (GCN) дозволяють моделі враховувати інформацію сусідніх вузлів, а методи на кшталт GraphSAGE забезпечують ефективність у великій інфраструктурі завдяки семплінгу локальних підграфів. Мережі з механізмами уваги, такі як GAT, здатні визначати найважливіші зв'язки для оцінки ризику та пріоритизації. На відміну від традиційних табличних моделей машинного навчання, які оперують переважно числовими показниками на зразок CVSS, CWE чи KEV, графові методи беруть до уваги структуру зв'язків між компонентами, що робить їх суттєво точнішими та більш придатними для реальних інформаційних систем.

Висновок: у роботі обґрунтовано важливість застосування графових моделей для валідації вразливостей у сучасних інформаційних системах. Графи атак і залежностей дозволяють моделювати комплексні шляхи експлуатації та визначати структурно критичні вразливості. Перспективи подальших досліджень передбачають розробку гібридних моделей, які поєднують графові методи машинного навчання, а також застосування графових нейронних мереж для прогнозування zero-day вразливостей. Подальший розвиток цієї тематики може охоплювати інтеграцію графових моделей у системи типу SIEM та SOAR, а також створення механізмів автоматизованої побудови графів у масштабних інфраструктурах. Важливим напрямом є й формування практичних індикаторів компрометації, побудованих на основі шляхів атаки, що забезпечує більш глибоке та контекстне виявлення загроз.

Список використаної літератури:

1. Angel, D. Protection of Medical Information Systems Against Cyber Attacks: A Graph Theoretical Approach. Wireless Personal Communications, 126, pp. 3455-3464 (2022).
2. A Compact Vulnerability Knowledge Graph for Risk Assessment / J. Yin et al. ACM Transactions on Knowledge Discovery from Data. 2024.
3. Saulaiman M. N.-E., Kozlovszky M., Csilling A. Graph-Based Automation of Threat Analysis and Risk Assessment for Automotive Security. Information. 2025. Vol. 16, no. 6. P. 449.

Ключові слова: графи атак; графи залежностей; валідація вразливостей; графові методи машинного навчання; кібербезпека; моделювання атак; оцінка ризику; експлуатованість; структурний аналіз систем.
Keywords: attack graphs; dependency graphs; vulnerability validation; graph-based machine learning methods; cybersecurity; attack modeling; risk assessment; exploitability; structural system analysis.

AI-ПІДСИЛЕНА ВЕРИФІКАЦІЯ АВТОРСТВА МУЛЬТИМЕДІЙНИХ ДАНИХ В УМОВАХ ГЕНЕРАТИВНОГО ШІ

Овчинников Микола

асистент кафедри кібербезпеки Національного університету «Одеська юридична академія»

Стрімкий розвиток генеративних моделей (GAN, дифузійні моделі) суттєво знизив поріг створення синтетичних зображень, відео та аудіо, що практично не відрізняються від реальних. Це підсилює ризики підміни авторства, масового піратського копіювання, а також формування фальсифікованих доказів у кіберінцидентах. Аналітичні огляди deepfake-атак підкреслюють, що змагальність між генераторами й детекторами призводить до швидкого «старіння» ознак і потребує комбінованих підходів до перевірки достовірності медіа [1,2].

Для задач захисту інтелектуальної власності на мультимедійні дані доцільно переходити від разових перевірок до системної доказовості: фіксації первинного походження, контролю версій, відстеження похідних копій та формування технічно коректного ланцюга збереження (chain of custody). У межах дисертаційної тематики пропонується інформаційна система, що поєднує AI-аналіз контенту, робастне маркування та незмінний журнал подій як основу для доведення авторства та цілісності.

Сучасні атаки на медіа здатні одночасно змінювати семантику (підміна облич, голосу, контексту), маскувати сліди обробки (перекомпресія, ресемплінг, повторне кодування) та обходити детектори через зсув домену або спеціально підібрані збурення. Систематичний огляд методів детекції

ЗМІСТ