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)

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

показує, що стабільність якості виявлення залежить від різноманітності навчальних даних, коректної валідації й контролю умов застосування [3].

AI-вузол у системі виконує дві взаємодоповнювальні функції: (1) побудова перцептивних «відбитків» (embeddings/хешів) для масштабованого пошуку схожих копій (у тому числі змінених або фрагментованих), (2) оцінка ймовірності синтетичного походження або маніпуляції (детектори фейків, аналіз артефактів, узгодженість метаданих). Така комбінація зменшує залежність від одного індикатора та підвищує відтворюваність результатів перевірки [2,3].

Компонент глибинного watermarking розглядається як механізм маркування, здатний зберігати витягуваність водяного знака після типових перетворень (JPEG/HEVC-компресія, масштабування, кадрування) та частини навмисних атак. Оглядові дослідження підкреслюють, що нейромережеві схеми можуть підвищити робастність і водночас зберегти непомітність, але потребують строгого тестування на різних класах атак і контролю помилок першого/другого роду [4].

Перцептивне хешування доповнює watermarking: навіть якщо знак знищено або істотно спотворено, схожість за перцептивним хешем дозволяє знаходити похідні копії та прив'язувати їх до первинного еталона. В оглядах з перцептивного хешування акцентується компроміс між чутливістю до підробок і стійкістю до допустимих перетворень, а також необхідність ефективної індексації (LSH/ANN) для пошуку в великих колекціях [5].

Узагальнену відповідність типових атак і практичних контрзаходів, які можуть реалізовуватися в AI-підсиленій системі підтвердження авторства, наведено у табл. 1.

Таблиця 1. Узагальнення загроз і контрзаходів для підтвердження авторства мультимедіа. Джерело: авторська розробка.

Загроза (приклад)	**AI/технічний контрзахід**	**Артефакт доказовості**
Підміна авторства / підробка первинних даних	Watermark + перцептивний відбиток; реєстрація хешів	Хеш еталона, watermark-ID, запис реєстрації
Deepfake/синтетична генерація, семантична підміна	Детектори маніпуляцій + порівняння embeddings	Скоринг, різниця embeddings, протокол перевірки
Компресія/масштабування/ кадрування, повторне кодування	Робастне витягування watermark; стійкі хеші	Результат витягування, стійкий хеш, журнал
Стирання watermark, adversarial збурення	Ансамбль детекторів; тест на стійкість; пороги	Метрики/пороги, підтвердження стійкості
Масове копіювання/репости, часткові фрагменти	ANN/LSH пошук за відбитками; виявлення фрагментів	Список збігів, оцінка схожості, джерела

Як видно з табл. 1, для реальних сценаріїв необхідне багатоканальне підтвердження: одночасне використання watermarking, перцептивних відбитків та протоколювання результатів перевірки. Це дозволяє зменшити вплив доменних зсувів для детекторів і зберегти відтворюваність процедури навіть тоді, коли один з каналів частково деградує.

На рис. 1 подано узагальнену архітектуру AI-підсиленої системи захисту авторських прав на мультимедійні дані, у якій поєднуються зазначені механізми.

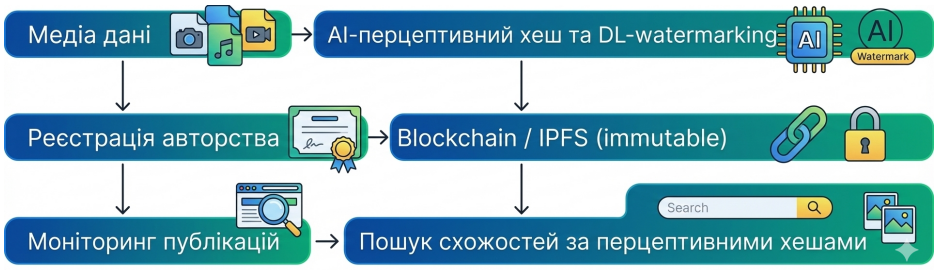

Рис. 1. Архітектура AI-підсиленого захисту авторських прав на мультимедійні дані. Джерело: авторська розробка.

Отже, застосування ШІ в системах захисту авторських прав на мультимедіа доцільно розглядати не як «єдиний детектор», а як складову багатокомпонентного конвеєра, де результат підтверджується незалежними каналами: watermark, перцептивними відбитками та протоколюванням перевірок. Така побудова підвищує стійкість до еволюції генеративних моделей, забезпечує відтворюваність та формує основу для технічно коректного доведення авторства й цілісності у кіберпросторі [1-5].

Список використаних джерел:

1. Tolosana R. et al. Deepfakes and beyond: A survey of face manipulation and fake detection. Information Fusion. 2020;64:131-148. doi:10.1016/j.inffus.2020.06.014.
2. Verdoliva L. Media Forensics and DeepFakes: An Overview. IEEE J. Sel. Top. Signal Process. 2020;14(5):910-932. doi:10.1109/JSTSP.2020.3002101.
3. Rana M.S. et al. Deepfake Detection: A Systematic Literature Review. IEEE Access. 2022;10:25494-25513. doi:10.1109/ACCESS.2022.3154404.
4. Hosny K.M. et al. Digital image watermarking using deep learning: A survey. Computer Science Review. 2024;53:100662. doi:10.1016/j.cosrev.2024.100662.
5. Du L., Ho A.T.S., Cong R. Perceptual hashing for image authentication: A survey. Signal Process.: Image Commun. 2020;81:115713. doi:10.1016/j.image.2019.115713.

Ключові слова: генеративний ШІ, deepfake, мультимедійні дані, цифрове водяне маркування, перцептивне хешування, верифікація авторства, контент-автентифікація, ланцюг доказовості.

Keywords: generative AI, deepfake, multimedia data, digital watermarking, perceptual hashing, authorship verification, content authentication, evidential chain.

Науковий керівник: к.т.н., доцент Ахмаметьєва Г.В.

ЗМІСТ

Секція 1. АЛГОРИТМІЧНІ ТА ТЕХНІЧНІ АСПЕКТИ КІБЕРБЕЗПЕКИ... 10

ІНФОРМАЦІЙНА БЕЗПЕКА ДЕРЖАВИ У СОЦІАЛЬНИХ МЕРЕЖАХ: ВИКЛИКИ ТА ЗАГРОЗИ СУЧАСНОГО ЕТАПУ 10
Дикий Олег

A REVIEW ON MANY-VALUED LOGIC: A NOVEL PARADIGM FOR INFORMATION SECURITY 12
Aboobacker P

МЕТОДИ ТА РИЗИКИ ПОБУДОВИ СИСТЕМ З END-TO-END ШИФРУВАННЯМ 15
Вінковська Ірина
Чебаненко Олег

A 10-BIT S-BOX GENERATED BY FEISTEL CONSTRUCTION FROM CELLULAR AUTOMATA 217
Thomas Prévost
Bruno Martin

СИСТЕМИ РАНЖУВАННЯ ТА АНАЛІЗУ ІНФОРМАЦІЇ ПРИ ПРОТИДІЇ КІБЕРЗЛОЧИНАМ 26
Кухаренко Сергій
Сидорчук Владислав

БЕЗПЕКА ANDROID-ЗАСТОСУНКІВ НА KOTLIN ТА JETPACK COMPOSE 29
Манаков Сергій

КОНЦЕПЦІЯ ТА РОЗГОРТАННЯ ВИСОКОІНТЕРАКТИВНОГО ХАНІПОТУ НА НА ОСНОВІ ЕМУЛЯЦІЇ ЛЕГІТИМНОГО ВЕБСЕРВЕРА (NGINX) 29
Бойко Віктор

МІЖНАБОРНЕ ТЕСТУВАННЯ МЕТОДУ KNN+TF-IDF У ЗАДАЧІ ВИЯВЛЕННЯ ІН'ЄКЦІЙНИХ АТАК У ВЕБ-ЗАПИТАХ 34
Коробейнікова Тетяна
Кравчук Назар

ПРОБЛЕМИ КІБЕРБЕЗПЕКИ СУЧАСНОГО РИНКУ ВІДЕОІГОР 37
Куклінова Тетяна
Гулієва Анастасія

ВИКОРИСТАННЯ OPENDATA UKRAINE В ЦІЛЯХ OSINT 40
Бойко Віктор
Дручик Софія

ЛОКАЛЬНИЙ МЕНЕДЖЕР ПАРОЛІВ ІЗ ГЕНЕРУВАННЯМ ДЛЯ МОБІЛЬНИХ ПРИСТРОЇВ 40
Тимошенко Лідія
Вакуліна Сана
Волобуєва Ірина