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)

АЛГОРИТМІЧНІ ПІДХОДИ ДО ПІДТВЕРДЖЕННЯ АВТОРСТВА ТА ЦІЛІСНОСТІ МУЛЬТИМЕДІЙНИХ ДАНИХ

Овчинников Микола

асистент кафедри кібербезпеки Національного університету «Одеська юридична академія»

Захист інтелектуальної власності на мультимедійні дані у кіберпросторі ускладнюється тим, що контент легко копіюється й модифікується, а типові перетворення (компресія, перекодування, зміна роздільності, кадрування) можуть знищувати або спотворювати ознаки авторства. Для правовласника важливі не лише виявлення копій, а й доказовість результатів: відтворюваний ланцюжок обробки, контроль цілісності артефактів та можливість аудиту, що напряму пов'язано з алгоритмічними та технічними аспектами кібербезпеки. [2,5]

У межах досліджень розробляється підхід до інформаційної системи, що поєднує робастне водяне маркування, перцептивне хешування/фінгерпринти та незмінний журнал подій (permissioned blockchain або WORM-лог). Комбінація цих компонентів зменшує ризик «однієї точки відмови»: водяний знак забезпечує вбудовану атрибуцію, перцептивні ознаки підтримують масштабований пошук, а журнал підвищує незаперечність і прозорість процедури перевірки. [1,3,2]

Алгоритмічний конвеєр включає нормалізацію контенту (уніфікація параметрів кодування, стабілізація яскравості/контрасту; для відео – ключові кадри; для аудіо – спектральні «відбитки»), формування стійкого опису об'єкта (перцептивний хеш та додаткові ознаки), а також вбудування водяного знаку у частотній області (DCT/DWT) з адаптивним добором сили вбудування. Для доказовості результати (ідентифікатор контенту, хеші, параметри маркування, часові мітки) підписуються та реєструються у незмінному журналі разом із протоколами перевірок. [3,4]

Загрозна модель охоплює стирання/спотворення маркування, геометричні перетворення, часткове використання (колажі, ремікси), а також атаки на доказовість (підробка журналів, компрометація ключів). Протидія реалізується багатоканально: поєднанням робастного маркування, незалежних ознак схожості, криптографічного підпису та контрольованого доступу (ролі, MFA, принцип найменших привілеїв). Оцінювання ефективності пропонується проводити через ймовірність детекції знаку після перетворень, точність пошуку (precision/recall) і помилки прийняття рішень (FAR/FRR) для порогів схожості; узагальнення наведено у табл. 1 і на рис. 1. [1,3]

Практична реалізація контуру вимагає узгодження параметрів між модулями: для водяних знаків — вибір домену вбудування (DCT/DWT), сили сигналу та секретного ключа; для перцептивних ознак — нормалізація,

квантування й побудова індексів близькості. У результаті формується компактний «відбиток» контенту, придатний для індексації та аудиту без розкриття первинних даних, а також забезпечується трасованість операцій у межах життєвого циклу мультимедійного об'єкта [1].

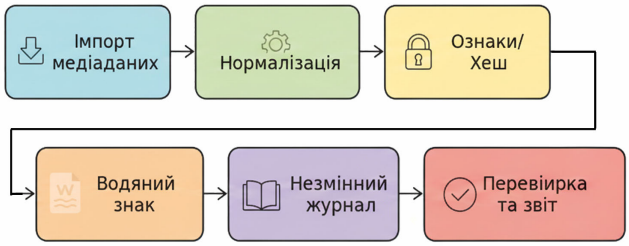

Рис. 1. Узагальнена схема алгоритмічного контуру.

Схема на рис. 1 відображає «ланцюжок довіри»: кожен етап формує артефакти (хеші, параметри маркування, часові мітки, підписи), які зберігаються разом із посиланням на медіаоб'єкт. Важливо, що ці артефакти мають бути достатніми не лише для підтвердження факту перевірки, а й для її повторення іншою стороною за тим самим протоколом (версії алгоритмів, пороги рішень, параметри препроцесингу). Такий підхід забезпечує відтворюваність процедури верифікації, дозволяє локалізувати етап, на якому виникла аномалія (наприклад, деградація водяного знака після перекодування або «дрейф» перцептивних ознак після генеративної модифікації), і підвищує доказовість результатів під час інцидентного аналізу або експертизи. Додатковою перевагою є можливість формування узгодженого «пакета доказів» для взаємодії з платформами чи судовими інстанціями: посилання на джерело, таймлайн подій, результати витягування маркера та метрики схожості. За умови незмінного журналювання (WORM/permissioned-реєстр) зменшується ризик підміни або ретроспективного редагування даних перевірки, що критично для процедур, де потрібна простежуваність та аудит дій користувачів [2, 5].

Наведене у таблиці 1 узагальнення дозволяє формалізувати відповідність «атака — контрзахід — метрика/критерій» та використовувати ці показники для налаштування порогів схожості й регламентів перевірки у практичних сценаріях (пошук копій, доведення авторства, аудит змін) [1, 3, 4].

Запропонований комплекс дає змогу будувати відтворюваний «пакет доказів» (артефакти, параметри, метрики, посилання на записи журналу) та підвищує стійкість захисту прав на мультимедійні дані в умовах типових кіберзагроз. Перспективними напрямами є підвищення стійкості до генеративних модифікацій (deepfake), оптимізація пошуку у великих колекціях (ANN-індекси) та формалізація ризик-орієнтованих показників ефективності впровадження.

Таблиця 1. Загрози та технічні контрзаходи (узагальнено). Джерело: авторська розробка.

Загроза	Атака	Контрзахід	Метрика/критерій
Стирання маркування	Компресія, фільтрація, перекодування	Робастне вбудування у DCT/DWT; адаптивна сила	Pdet після перетворень
Геометричні зміни	Кадрування, поворот, ресайз	Нормалізація; синхронізуючі шаблони/інваріантні ознаки	Стійкість до Δмасштабу/Δкута
Часткове використання	Колаж, ремікс, підміна фрагментів	Перцептивні ознаки + пошук за близькістю; сегментація	Precision/Recall (пошук)
Підробка доказів	Зміна журналів, компрометація ключів	Незмінний журнал + підпис; контроль доступу (ролі, MFA)	Аудит, незаперечність

Для компонента робастного маркування доцільно застосовувати частотні методи (DCT/DWT) із адаптивним вибором сили вбудування, що підвищує стійкість до компресії та фільтрації при мінімальній помітності. Параметри маркування (ключ, домен, коефіцієнт) фіксуються у доказовому пакеті та підписуються, а ефективність оцінюється за метриками непомітності (PSNR/SSIM) і ймовірності детекції після перетворень (Pdet). [1]

Перцептивне хешування та мультимодальні «фінгерпринти» забезпечують пошук збігів у великих колекціях за принципом близькості, а не біт-в-біт. Для зменшення помилкових спрацювань комбінуються кілька типів ознак, а пороги добираються за результатами валідації (ROC/EER) з контролем FAR/FRR; підозрілі збіги підтверджуються повторною перевіркою наявності водяного знака. [3,4]

Незмінний журнал подій реалізується як WORM-сховище або permissioned blockchain із хеш-ланцюжком та деревами Меркла для підтвердження цілісності. У журналі зберігаються хеші, перцептивні відбитки та метадані (без розміщення медіаданих), що підвищує конфіденційність. Захист посилюється керуванням ключами, рольовим доступом і MFA; метрики верифікації можуть передаватися до SIEM/SOAR для інцидентних сповіщень. [2,5].

Список використаних джерел:

1. Mekhfioui M., El Bazi N., Laayati O., et al. Optimized Digital Watermarking for Robust Information Security in Embedded Systems. Information. 2025;16(4):322. https://doi.org/10.3390/info16040322.
2. Qureshi A., Megías Jiménez D. Blockchain-Based Multimedia Content Protection: Review and Open Challenges. Applied Sciences. 2021;11(1):1. https://doi.org/10.3390/app11010001.
3. Du L., Ho A.T.S., Cong R. Perceptual hashing for image authentication: A survey. Signal Processing: Image Communication. 2020;81:115713. https://doi.org/10.1016/j.image.2019.115713.

4. Xing H., Wang Y., Xia L., He M. Image perceptual hashing for content authentication based on Watson's visual model and locally linear embedding. Journal of Real-Time Image Processing. 2023;20:7. https://doi.org/10.1007/s11554-023-01269-9.
5. Xiao X., He X., Zhang Y., et al. Blockchain-based reliable image copyright protection. IET Blockchain. 2023;3(4):222–237. https://doi.org/10.1049/blc2.12027.

Ключові слова: кібербезпека, інтелектуальна власність, мультимедійні дані, цифровий водяний знак, перцептивний хеш, блокчейн, форензіка.
Keywords: cybersecurity, intellectual property, multimedia data, digital watermark, perceptual hash, blockchain, forensics.

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

ПОРІВНЯЛЬНИЙ АНАЛІЗ МЕТОДІВ КІБЕРБЕЗПЕКИ В ОНЛАЙН ТА ОФЛАЙН ІГРАХ

Скідан Владислав
аспірант кафедри кібербезпеки Національного університету «Одеська юридична академія»

У сфері комп'ютерних ігор кібербезпека набуває все більшого значення через стрімкий розвиток технологій та зростання аудиторії гравців, які взаємодіють з віртуальними середовищами. Онлайн-ігри, що передбачають постійне підключення до мереж, стикаються з широким спектром загроз, таких як DDoS-атаки, фішинг та витоки даних, тоді як офлайн-ігри, орієнтовані на локальне виконання, більше схильні до ризиків, пов'язаних з піратством, шкідливим програмним забезпеченням у модифікаціях чи несанкціонованим доступом до локальних файлів. Порівняльний аналіз методів кібербезпеки в цих двох типах ігор дозволяє виявити спільні та відмінні підходи до захисту, підкреслюючи необхідність адаптації стратегій до специфіки середовища. Зокрема, в онлайн-іграх акцент робиться на мережевому рівні захисту, тоді як в офлайн-іграх переважають локальні механізми аутентифікації та контролю цілісності файлів.

У онлайн-іграх методи кібербезпеки часто включають багатошарові системи захисту, такі як шифрування даних для запобігання витокам інформації, багатофакторну аутентифікацію для захисту акаунтів гравців та системи виявлення ботів і читів, які використовують фаєрволи та CAPTCHA для блокування автоматизованих атак. Наприклад, DDoS-атаки, що перевантажують сервери та призводять до простоїв, вимагають впровадження спеціалізованих інструментів моніторингу трафіку, які аналізують аномалії в реальному часі та автоматично перенаправляють шкідливий трафік. Крім того, для боротьби з соціальною інженерією, такою як фішинг через ігрові чати, застосовуються освітні кампанії та автоматизовані фільтри контенту, що сканують повідомлення на наявність шкідливих посилань. Ці методи не лише захищають дані гравців, але й забезпечують

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