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)

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

справедливість ігрового процесу, запобігаючи маніпуляціям з віртуальними активами, які можуть бути продані за реальні гроші. Дослідження показують, що ефективність таких підходів зростає при інтеграції з хмарними сервісами, де дані зберігаються в зашифрованому вигляді, зменшуючи ризики масових витоків, як це спостерігалося в інцидентах з великими платформами [1].

На противагу цьому, в офлайн-іграх методи кібербезпеки зосереджені на локальному рівні, де ключовими є системи цифрового управління правами (DRM), такі як Denuvo чи Steam DRM, які запобігають піратству шляхом перевірки ліцензій та блокування несанкціонованих копій. Ці системи часто включають офлайн-аутентифікацію, де гра періодично перевіряє цілісність файлів за допомогою хеш-функцій, щоб виявити модифікації чи вбудоване шкідливе ПЗ. Крім того, для захисту від вірусів у завантажених модифікаціях застосовуються вбудовані антивірусні модулі або рекомендації щодо використання зовнішнього ПЗ для сканування файлів перед установкою. У порівнянні з онлайн-іграми, тут менше уваги приділяється мережевим загрозам, але акцент робиться на запобіганні локальним вразливостям, таким як ін'єкції коду в збережені файли чи експлойти в одиночних режимах. Дослідження підкреслюють, що офлайн-ігри менш вразливі до масових атак, але ризики зростають при використанні піратських версій, де шкідливе ПЗ може бути замасковане під гру [2].

Порівнюючи методи в онлайн та офлайн іграх, можна відзначити, що в онлайн-середовищі переважають динамічні системи моніторингу, такі як AI-виявлення аномалій для боротьби з читами та ботами, тоді як в офлайн-іграх статичні перевірки, як хешування файлів, забезпечують базовий захист. Онлайн-ігри часто інтегрують VPN-рекомендації для маскування IP-адрес гравців, запобігаючи доксінгу чи светінгу, чого не потребують офлайн-ігри, де загрози обмежуються локальним пристроєм. Однак спільним для обох є використання сильних паролів та оновлень ПЗ для закриття вразливостей. Актуальні дослідження вказують на те, що гібридні ігри, які поєднують онлайн та офлайн елементи, вимагають комбінованих методів, де локальний DRM доповнюється мережевим шифруванням для захисту збережень у хмарі. Це дозволяє мінімізувати ризики, пов'язані з переходом між режимами, і підвищує загальну стійкість системи [3].

Відмінності у методах кібербезпеки наведено в таблиці 1.

У контексті офлайн-ігор методи кібербезпеки еволюціонували від простих ключів активації до складних систем, таких як вбудовані античити в одиночних кампаніях, які перевіряють модифікації на сумісність та безпеку. Наприклад, ігри на зразок тих, що використовують Unity чи Unreal Engine, інтегрують локальні скрипти для виявлення змін у коді, запобігаючи ін'єкціям шкідливого вмісту. Порівняно з онлайн, де загрози динамічні та вимагають постійного моніторингу, офлайн-методи більш пасивні, але ефективні для

збереження інтелектуальної власності. Дослідження зазначають, що в офлайн-режимах ризики часто пов'язані з користувацькими помилками, такими як завантаження з ненадійних джерел, тому рекомендації включають використання офіційних магазинів та регулярні оновлення. Це підкреслює необхідність освітніх елементів навіть у локальних іграх, де гравці можуть не усвідомлювати загроз [4].

Таблиця 1 – Аналіз методів кібербезпеки за середовищем ігор

Аспект захисту	Онлайн-ігри	Офлайн-ігри
Основні загрози	DDoS-атаки, фішинг, витоки даних, читери	Піратство, шкідливе ПЗ в модифікаціях, локальні експлойти
Ключові методи	MFA, firewalls, AI-моніторинг трафіку, шифрування даних	DRM-системи, хеш-перевірки файлів, антивірусні сканери
Рівень складності	Високий (мережевий, реального часу)	Середній (локальний, статичний)
Ефективність	Залежить від серверної інфраструктури, висока при інтеграції з хмарою	Висока для запобігання копіюванню, але нижча проти користувацьких помилок

Аналізуючи ефективність методів, в онлайн-іграх серйозні ігри для навчання кібербезпеки, такі як симуляції хакерських атак, показують високу залученість гравців, дозволяючи практикувати захист у віртуальному середовищі без реальних ризиків. Ці методи включають гейміфікацію, де елементи, як бали за правильні дії, мотивують до вивчення концепцій шифрування чи мереж. У офлайн-іграх подібні підходи рідкісні, але можуть проявлятися в освітніх модулях, інтегрованих у гру, для навчання базовим принципам безпеки. Порівняння демонструє, що онлайн-методи більш інтерактивні та адаптивні, тоді як офлайн фокусуються на статичному захисті. Актуальні огляди підкреслюють, що інтеграція гейміфікації підвищує ефективність навчання в обох типах, зменшуючи людський фактор як слабку ланку [5].

Розглядаючи еволюцію методів, в онлайн-іграх все частіше застосовуються AI-системи для виявлення аномальної поведінки, такі як автоматизовані боти чи читери, що аналізують патерни дій гравців у реальному часі. Це контрастує з офлайн, де AI може використовуватися для локальної перевірки файлів, але без мережевого компоненту. Порівняльні дослідження показують, що онлайн-ігри вимагають більш ресурсоємних методів через глобальну взаємодію, тоді як офлайн дозволяють економію ресурсів за рахунок локалізації. Однак у гібридних моделях, як у іграх з опціональним онлайн, методи комбінуються, забезпечуючи гнучкість. Це підкреслює тенденцію до уніфікації підходів для підвищення загальної безпеки індустрії [6].

У висновковій частині аналізу варто зазначити, що порівняльний підхід до методів кібербезпеки в онлайн та офлайн іграх розкриває необхідність балансу між технологічними інноваціями та освітою користувачів, аби мінімізувати ризики в еволюціонуючій цифровій екосистемі.

Список використаних джерел

1. Leder M., Sharadin G. Why Attackers Target the Gaming Industry. Imperva. URL: https://www.imperva.com/blog/cyber-attacks-gaming-industry/ (дата звернення: 30.10.2025).
2. The 10 biggest online gaming risks and how to avoid them. Kaspersky Lab. URL: https://www.kaspersky.com/resource-center/threats/top-10-online-gaming-risks (дата звернення: 30.10.2025).
3. Chattopadhyay S., Tiwari M., Tiwari T., Kapila D. Role of Cyber security in Gaming technology. 2023 3rd International Conference on Advance Computing and Innovative Technologies in Engineering (ICACITE). 2023. PP. 446-451. DOI: 10.1109/ICACITE57410.2023.10182589
4. Nanjundan P., Chinnasami S., Saravanan V., Ramachandran M. Contrasting the impact of online games and offline games: A comparative analysis. Contemporaneity of English Language and Literature in the Robotized Millennium. 2024. №2(4). PP. 28-36. DOI: 10.46632/cellrm/2/4/4
5. Coenraad M., et al. Experiencing Cybersecurity One Game at a Time: A Systematic Review of Cybersecurity Digital Games. Simulation & Gaming. 2024. №51(5). PP. 586-611. DOI: https://doi.org/10.1177/1046878120933312
6. Ng C. Y., Hasan M. K. B. Cybersecurity serious games development: A systematic review. Computers & Security. 2025. №150. DOI: https://doi.org/10.1016/j.cose.2024.104307

Ключові слова: кібербезпека, онлайн-ігри, офлайн-ігри, DDoS-атаки, фішинг, витоки даних, багатофакторна аутентифікація, цифрове управління правами, шифрування даних, AI-моніторинг, піратство, шкідливе програмне забезпечення.
Keywords: cybersecurity, online games, offline games, DDoS attacks, phishing, data leaks, multi-factor authentication, digital rights management, data encryption, AI monitoring, piracy, malware.

СИСТЕМА ВИЯВЛЕННЯ ВИТОКІВ ПЕРСОНАЛЬНИХ ДАНИХ

Бойко Віктор

кандидат технічних наук, доцент кафедри кібербезпеки Національного університету «Одеська юридична академія»

Вередін Діана

студентка 4-го курсу факультету кібербезпеки та інформаційних технологій Національного університету «Одеська юридична академія»

Зростання цифровізації суспільства призвело до підвищення цінності персональних даних, як активів. Використання інформаційних технологій, хмарних сервісів та віддаленого доступу до даних створює нові ризики та

ЗМІСТ