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)

# ПРОБЛЕМИ КІБЕРБЕЗПЕКИ СУЧАСНОГО РИНКУ ВІДЕОІГОР

***Куклінова Тетяна***

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

***Гулієва Анастасія***

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

Сучасний ринок відеоігор є одним із найдинамічніших сегментів цифрової економіки. За останні десять років відеоігри перетворилися з розважального хобі на глобальний технологічний феномен, який поєднує індустрію розваг, цифрові сервіси, штучний інтелект, соціальні мережі та елементи віртуальної економіки. Так, ігрова індустрія сьогодні налічує сотні мільйонів гравців по всьому світу і є ключовим драйвером розвитку цифрового контенту, нових форм віртуальної взаємодії та економічного зростання. Вона охоплює не лише комп'ютерні та мобільні ігри, а й онлайн-платформи, кіберспорт, віртуальні світи та хмарні технології, про що свідчить Рис.1.

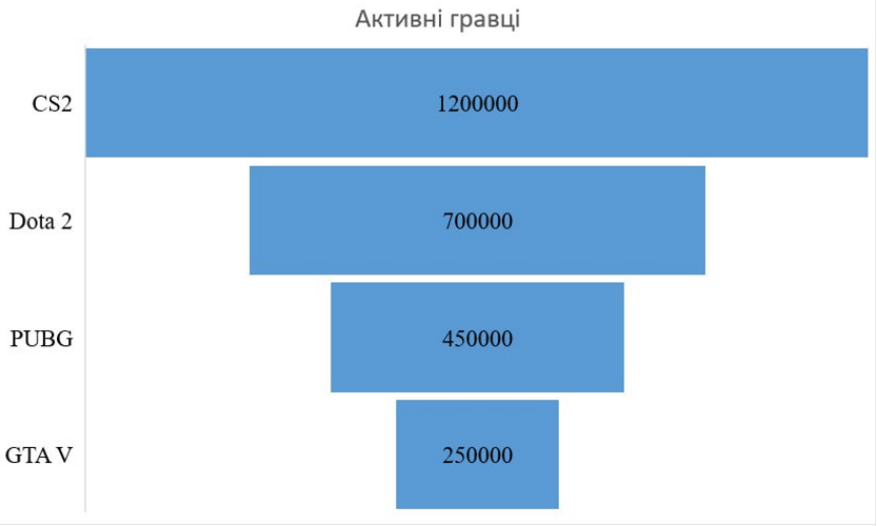


*Рис. 1. Кількість активних гравців популярних ігор (Steam) станом на 01.01.2025 [1]*

Зазначимо, що однією з провідних тенденцій розвитку індустрії є поширення хмарного геймінгу та стрімінгових сервісів, що дозволяють запускати ігри без потреби у потужному обладнанні, а традиційна модель володіння іграми поступово замінюється підпискою на доступ до великої бібліотеки контенту. Паралельно зростає використання штучного інтелекту для створення реалістичної поведінки персонажів та персоналізації ігрового досвіду. Розробники активно інтегрують технології доповненої та віртуальної реальності, розвивають жанр соціальних онлайн-ігор, де формується спільний простір для взаємодії мільйонів користувачів.

Також важливим напрямом трансформації ринку є формування внутрішньої цифрової економіки відеоігор. Її основою стали мікротранзакції, внутрішньоігрові покупки та використання віртуальних валют. У деяких іграх створюються повноцінні економічні системи, де гравці купують або продають предмети, персонажів чи акаунти. Цей процес посилюється із розвитком блокчейн-технологій, що дозволяють створювати та передавати унікальні цифрові об'єкти з доказом власності. Проте такий напрям потребує регулювання, оскільки межує з реальними фінансовими операціями та може спричиняти кіберзлочинність.

Але популярні мережеві ігри також стають основною ціллю кіберзлочинців. Так, у грі Counter-Strike 2 щотижня фіксуються масові випадки викрадення акаунтів через фішингові сайти, що імітують Steam Login. Також поширене шахрайство зі скінами, які мають реальну ринкову вартість, перетворює гру на інструмент тіньового обміну цифрових активів. Аналогічна ситуація спостерігається в Dota 2, де кіберзловмисники використовують бот-мережі для викрадення акаунтів із високим рейтингом MMR та поширюють шкідливе програмне забезпечення під виглядом скриптів. Популярним методом атак залишається соціальна інженерія, коли шахраї виманюють дані входу, обіцяючи «прокачування персонажа» або вигідний обмін [1] (Рис.2).

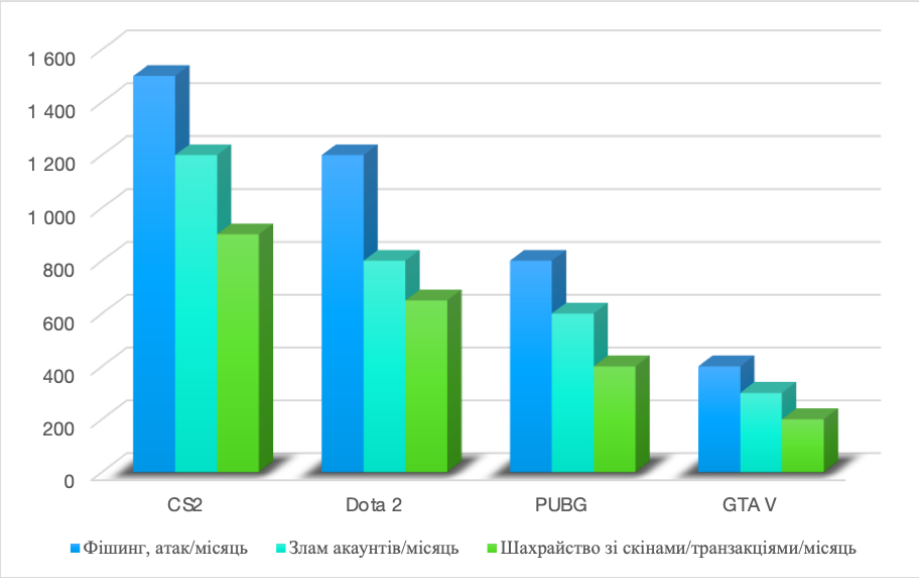


*Рис. 2 Статистика кіберзагроз у популярних іграх Steam у 2024рр.[1]*

Швидке зростання галузі супроводжується значним збільшенням кіберзагроз. Щодня здійснюються тисячі зламів облікових записів, викрадень даних користувачів, фінансових махінацій та хакерських атак на ігрові сервери. Масового характеру набули атаки типу DDoS, які призводять до відмови серверів у роботі [2]. Злочинці використовують автоматизовані інструменти для підбору паролів, що дозволяє захоплювати акаунти, які часто пов'язані з банківськими картками або іншими платіжними даними [3].

Особливої уваги потребує захист неповнолітніх користувачів. Велика частина аудиторії відеоігор – підлітки та молодь, що робить їх вразливими до маніпуляцій, онлайн-булінгу, грумінгу та шахрайства.

Серйозною загрозою є також розповсюдження шкідливого програмного забезпечення під виглядом модів, читів або безкоштовних доповнень. Після встановлення такі програми виявляються вірусами, що викрадають персональні дані або надають хакеру дистанційний доступ до комп'ютера користувача. Уразливості можуть міститися навіть в офіційних ігрових клієнтах через недосконале тестування безпеки, особливо у багатокористувацьких іграх із великим мережевим навантаженням.

Підкреслюється, що, особлива увага має бути приділена аспектам кібербезпеки, які є критично важливими для захисту персональних даних користувачів та цілісності платформи Необхідно передбачити інтеграцію систем захисту, регулярне тестування на вразливості та оперативне реагування на інци-денти. Окрім технічних засобів, слід впроваджувати політики інформаційної безпеки для користувачів і персоналу. [4].

Отже, розв'язання проблем кібербезпеки вимагає комплексного підходу: застосування багатофакторної автентифікації, регулярні оновлення програмного забезпечення, захист серверів від DDoS-атак, моніторинг підозрілої активності, а також навчання користувачів основам кібергігієни. Ігрові компанії повинні впроваджувати принцип «безпека за задумом», передбачаючи проєктування систем з урахуванням захисту з самого початку розробки. Водночас її розвиток супроводжується зростанням кіберзагроз, що створює ризики для мільйонів користувачів і компаній. Подальший поступ ринку можливий лише за умови поєднання технологічних інновацій із підвищеною увагою до кібербезпеки, етичних стандартів обробки даних та міжнародної співпраці у сфері цифрового захисту.

**Список використанних джерел:**

1. SteamDB. Counter-Strike 2. URL: https://steamdb.info/app/730/
2. Imperva. Comprehensive digital security. URL: https://www.imperva.com/blog/understanding-cyber-threats-in-gaming/?utm_source
3. Cloudflare. DDoS-огляди та аналітика. URL: https://blog.cloudflare.com/ddos-threat-report-for-2025-q1/?utm_source=chatgpt.com/
4. Куклінова Т.В., Чепурна О.Є., Куклінова С.І. Проєктне управління розробкою веб порталу для цифрових спільнот геймерів: ризики, ресурси та результативність. Цифрова економіка та економічна безпека. 2025. Випуск 3(18). URL: https://dees.iei.od.ua/index.php/journal/article/view/740 DOI: https://doi.org/10.32782/dees.18-40

**Ключові слова:** ігрова індустрія, gamedev, ринок відеоігор, кібербезпека
**Keywords:** gaming industry, gamedev, video game market, cybersecurity

# ЗМІСТ