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)

КОНТРОЛЬ ЦІЛІСНОСТІ БАЗИ ДАНИХ ЗА ДОПОМОГОЮ БЛОКЧЕЙНІВ

Бойко Віктор

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

Панчук Ганна

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

Найважливішою умовою для новітніх інформаційних систем є дотримання достовірності даних, якщо цілісність масивів буде порушена, присутня велика можливість втратити точність даних, ускладнити процедури точності даних, аналізу та мати фінансові втрати. Такі стандарти як, запис всіх операцій, обчислення контрольних сум, резервування, є дієвими, коли присутня повна довіра до людей, які керують системою та відсутні будь які ризики з довірою [1].

Метод блокчейну, у свою чергу, дає інший підхід, який гарантує недоторканість інформації. Його суть полягає у формуванні послідовного реєстру транзакцій, де кожен блок містить у собі хеш попереднього. Через такий спосіб, спроба змінити остаточну інформацію дуже важко та одразу виявляється, оскільки порушується взаємозв'язок усіх елементів цього ланцюга [2].

Блокчейн є переліком блоків, де кожен містить у собі інформацію та хеш попереднього блоку. Для забезпечення надійності та незмінності інформації застосовується такий алгоритм :

- Хешування записів – кожне внесення змін або додавання елемента до бази даних супроводжується генеруванням хешу.
- Формування блоку – сформований набір хешів об'єднується в один блок. Об'єднаний блок отримує тимчасову мітку, а саме ідентифікатор користувача, який здійснив дію, яка, у свою чергу, посилається на попередній блок у ланцюгу.
- Запис у блокчейн-реєстр – Виконується пересилання створеного блоку до розподіленого або гібридного блокчейн-мережі, яка зберігається окрема від первинної бази даних.
- Підтвердження – система повторно обчислює хеші для поточних даних і звіряє їх з тими, що були зафіксовані у блокчейні. У разі виявлення невідповідностей відбувається фіксація порушення цілісності. [3, 4]

Перевагами такої системи є:

- Гарантія незмінності записів – після того, як користувач затвердив блок у ланцюга, будь-яка спроба модифікації буде виявлено акт втручання.

– Розподілений механізм контролю – відбувається мінімізація загроз будь-яких маніпуляцій, це відбувається через відсутність єдиного центру зберігання даних.

– Мінімальне використання ресурсів – система може працювати як додатковий рівень поверх існуючих систем керування базами даних, це не вимагає значні обчислювальні ресурси.

– Спрощене впровадження – можлива реалізація через стандартизовані програмні інтерфейси без потреби створення повноцінного публічного блокчейну.

– Прозорість аудиту – кожен запис даних може бути незалежно перевірений сторонами [2, 4].

Створимо порівняльну таблицю, яка надасть нам бачення ефективності порівняно з традиційними методами контролю, та проставимо бали від 0 до 5, де 0 – найнижча оцінка, 5 – найвища.

Таблиця 1 Порівняння методів контролю

Метод контролю	Виявлення втручання	Рівень захисту	Прозорість аудиту	Вимоги ресурсів
Блокчейн	5	5	4	3
Журналювання транзакцій	4	3	3	4
Контроль сум	2	3	3	2
Резервне копіювання	4	3	2	5

Отже, можемо побачити, що блокчейн забезпечує найвищий рівень захисту при низькому споживання ресурсів [3, 1].

Подальші напрями розвитку охоплюють поєднання технологій блокчейну зі штучним інтелектом для автоматичного виявлення аномалій у транзакціях, а також з квантово-стійкими алгоритмами шифрування, які можуть гарантувати безпеку в умовах квантових обчислень [3].

Одним із перспективних рішень є також створення хмарних блокчейн-сервісів, що надають змогу організаціям інтегрувати контроль цілісності у свої бази даних без великих витрат.

Одним із прикладів є застосування контролю цілісності бази даних за допомогою блокчейнів у сфері фінансів. Він може бути застосований для підтвердження достовірності транзакцій у бухгалтерських реєстрах. Кожна фінансова операція отримує свій запис у блокчейні та має свою унікальну мітку. Якщо хтось спробує змінити, додати або вилучити запис у базі даних, відповідний хеш не збігатиметься з початковими даними в реєстрі, що дозволяє миттєво виявити спробу шахрайства [1, 5].

Впровадження блокчейнів для контролю цілісності баз даних забезпечує найвищий рівень захисту при мінімальних ресурсних витратах. Даний підхід дає змогу виявляти спроби втручання даних у реальному часі та створює надійну основу для побудови довірених цифрових систем. Застосування такого методу є значним у сферах, де критично важливим є збереження автентичності записів, наприклад банківської, юридичної, методичної сфер.

Список використаних джерел:

1. Кузьменко О. В. Методи забезпечення цілісності інформації в розподілених базах даних. – К.: НТУУ КПІ, 2020.
2. Соловйов А. В. *Криптографічні методи захисту інформації*. – Харків: Університет внутрішніх справ, 2018.
3. Antonopoulos A. M. *Mastering Blockchain*. – O'Reilly Media, 2021.
4. Chen L., Xu L., Shah N., Gao Z., Lu Y., Shi W. On Security Analysis of Proof-of-Work and Proof-of-Stake in Blockchain. – IEEE Transactions, 2019.
5. Nakamoto S. Bitcoin: A Peer-to-Peer Electronic Cash System. – 2008.

Ключові слова: Блокчейн, Контроль цілісності, База даних, Розподілений реєстр, Хешування, Незмінність записів, Прозорість аудиту, Виявлення втручання.
Keywords: Blockchain, Integrity Control, Database, Distributed Ledger, Hashing, Immutability of Records, Audit Transparency, Tampering Detection.

ОГЛЯД ЕВОЛЮЦІЇ АРХІТЕКТУРИ ІГРОВИХ РУШІЇВ

Толокнов Анатолій
асистент кафедри інформаційних технологій
Національного університету «Одеська юридична академія»

Ігрові рушії становлять технологічну основу сучасної індустрії відеоігор, надаючи розробникам комплексні інструменти для побудови інтерактивних віртуальних просторів. Протягом останніх років архітектурна організація ігрових рушіїв зазнала суттєвих перетворень, переходячи від монолітних структур до модульних, високоефективних систем [1]. Провідні представники галузі, Unity та Unreal Engine, продовжують встановлювати індустріальні стандарти, проте паралельно з'являються спеціалізовані платформи, розроблені для специфічних жанрів та технічних вимог.

Архітектурний розвиток ігрових рушіїв пройшов тривалий шлях від елементарних двовимірних систем до комплексних багатокомпонентних платформ. Традиційна об'єктно-орієнтована архітектура, що тривалий час домінувала в галузі, поступово замінюється більш ефективними підходами, зокрема Entity Component System (ECS) [2]. Архітектура ECS представляє

ЗМІСТ