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)

БЛОКЧЕЙН-ТЕХНОЛОГІЇ В ЗАБЕЗПЕЧЕННІ ЦІЛІСНОСТІ ДАНИХ

Соловйов Артем

Національний університет «Одеська юридична академія»,
асистент кафедри інформаційних технологій

Цілісність даних є критично важливим аспектом інформаційної безпеки, що гарантує незмінність, точність та достовірність інформації протягом усього її життєвого циклу. У сучасному цифровому світі, де обсяги даних зростають експоненційно, а кіберзагрози стають дедалі складнішими, традиційні методи забезпечення цілісності даних виявляються недостатньо надійними.

Блокчейн-технологія, вперше представлена як основа криптовалюти Bitcoin у 2008 році, пропонує революційний підхід до вирішення проблеми цілісності даних. Завдяки своїй децентралізованій архітектурі, криптографічним механізмам та консенсусним алгоритмам, блокчейн створює незмінний та прозорий реєстр транзакцій, який практично неможливо підробити або модифікувати без виявлення.

Мета дослідження: проаналізувати технічні механізми блокчейн-технології, що забезпечують цілісність даних, та дослідити практичні застосування цих механізмів у сфері кібербезпеки.

Актуальність теми обумовлена зростаючою потребою організацій у надійних механізмах захисту критичних даних від несанкціонованих змін, а також необхідністю створення довірчих систем в умовах відсутності централізованих органів контролю.

1. Технічні основи блокчейн-технології

1.1. Архітектура блокчейну

Блокчейн являє собою розподілену базу даних, що складається з ланцюжка блоків, кожен з яких містить набір транзакцій. Кожен блок включає:

- Заголовок блоку: містить метадані, включаючи хеш попереднього блоку, мітку часу, nonce та корінь дерева Меркла
- Тіло блоку: містить список транзакцій
- Криптографічний хеш: унікальний ідентифікатор блоку, обчислений на основі всіх його даних

Ключовою особливістю є те, що кожен блок містить хеш попереднього блоку, створюючи незламний криптографічний ланцюжок. Будь-яка спроба модифікувати дані в одному блоці призведе до зміни його хешу, що автоматично інвалідує всі наступні блоки.

1.2. Криптографічні механізми забезпечення цілісності

Хеш-функції є фундаментальним інструментом забезпечення цілісності в блокчейні. Найчастіше використовуються SHA-256 (в Bitcoin) та Keccak-256 (в Ethereum). Ці функції мають наступні властивості:

- Детермінованість: однакові вхідні дані завжди дають однаковий хеш
- Односторонність: практично неможливо відновити вхідні дані з хешу
- Ефект лавини: навіть мінімальна зміна вхідних даних кардинально змінює хеш
- Стійкість до колізій: практично неможливо знайти два різні входи з однаковим хешем [1].

2. Механізми забезпечення цілісності даних

2.1. Незмінність історичних записів

Найважливіша властивість блокчейну для цілісності даних - це практична незмінність історичних записів. Якщо зловмисник намагається змінити дані в блоці, який знаходиться на глибині N блоків від кінця ланцюжка:

1. Зміна даних в блоці призводить до зміни його хешу
2. Це вимагає перерахунку хешу наступного блоку, який містить хеш модифікованого блоку
3. Процес каскадно поширюється на всі наступні N блоків
4. Зловмисник повинен перерахувати всі ці блоки швидше, ніж чесні вузли додають нові блоки

При використанні PoW це вимагає контролю над >51% обчислювальної потужності мережі, що економічно недоцільно для великих публічних блокчейнів. Для Bitcoin, наприклад, вартість такої атаки оцінюється в мільярди доларів [2].

3. Практичні застосування в кібербезпеці

3.1. Управління ланцюжками постачання

Блокчейн забезпечує цілісність даних про походження та переміщення товарів:

- IBM Food Trust: відстежує продукти харчування від ферми до магазину, дозволяючи швидко ідентифікувати джерело контамінації
- Everledger: реєструє походження діамантів для боротьби з конфліктними діамантами
- VeChain: перевіряє автентичність розкішних товарів та фармацевтичних препаратів

Криптографічні хеші фізичних товарів реєструються в блокчейні, створюючи незмінний audit trail.

3.2. Управління цифровими ідентичностями

Децентралізовані системи ідентичності використовують блокчейн для:

- Створення самосуверенних цифрових ідентичностей, контрольованих користувачем
- Захисту від підробки документів та крадіжки особистих даних
- Забезпечення цілісності верифікаційних даних (освітніх сертифікатів, дипломів, ліцензій)

Приклади: Civic, uPort, Sovrin Foundation.

3.3. Захист цілісності логів та аудитів

Критичні системні логи можуть зберігатися в блокчейні або анкоритися до блокчейну через регулярне публікування хешів:

- Унеможливлює видалення або модифікацію логів зловмисниками після компрометації системи
- Забезпечує судову значимість логів для форензичного аналізу
- Дозволяє виявити момент компрометації шляхом порівняння локальних логів з блокчейн-записами

3.4. Безпека IoT-пристроїв

Блокчейн може вирішити проблеми безпеки Інтернету речей:

- Firmware integrity: хеші затверджених версій firmware зберігаються в блокчейні, пристрої перевіряють цілісність перед оновленням
- Децентралізована автентифікація: пристрої можуть автентифікуватися один перед одним без централізованого сервера
- Незмінний журнал взаємодій: всі комунікації між IoT-пристроями записуються, дозволяючи виявити аномальну поведінку

3.5. Захист інтелектуальної власності

Блокчейн надає timestamp-сервіс для доказу існування документів в певний момент часу:

- Автори можуть анкорити хеші своїх творів в блокчейн, створюючи незаперечний доказ авторства
- Патентні відомства можуть використовувати блокчейн для реєстрації заявок
- Цифрові активи (NFT) підтверджують автентичність та власність цифрових об'єктів

4. Обмеження та виклики

4.1. Масштабованість

Публічні блокчейни мають обмежену пропускну здатність:

- Bitcoin: ~7 транзакцій/секунду
- Ethereum: ~15-30 транзакцій/секунду

Це неприйнятно для додатків, що вимагають високої швидкості обробки. Рішення включають:

- Layer-2 протоколи
- Sharding - розподіл блокчейну на паралельні ланцюжки
- Sidechains та state channels

4.2. Конфіденційність

Прозорість блокчейну може конфліктувати з вимогами конфіденційності. Рішення:

- Zero-knowledge proofs: дозволяють доводити істинність тверджень без розкриття даних
- Приватні блокчейни з контрольованим доступом
- Анкорінг: зберігання лише хешів конфіденційних даних в публічному блокчейні

4.3. Енергоспоживання

PoW-блокчейни споживають величезну кількість електроенергії. Альтернативи:

- Перехід на PoS
- Використання відновлюваних джерел енергії
- Вибір більш ефективних консенсусних механізмів для корпоративних застосувань [3].

Блокчейн-технологія представляє парадигмальний зсув у підходах до забезпечення цілісності даних. Завдяки комбінації криптографічних механізмів, децентралізованої архітектури та консенсусних алгоритмів, блокчейн створює практично незмінний реєстр, який не залежить від довіри до централізованих органів.

Блокчейн не є універсальним рішенням для всіх проблем цілісності даних, але для застосувань, що вимагають децентралізованої довіри, незмінності та прозорості, він представляє одну з найбільш перспективних технологій сучасної кібербезпеки.

Список використаних джерел:

1.Buterin,V.Ethereum White Paper. 2014. URL: https://ethereum.org/en/whitepaper/.
2. Crosby, M. et al. BlockChain Technology: Beyond Bitcoin. Applied Innovation Review. 2016. Issue
2. URL: https://scet.berkeley.edu/wp-content/uploads/AIR-2016-Blockchain.pdf.
3. Zyskind, G., Nathan, O. Decentralizing Privacy: Using Blockchain to Protect Personal Data. IEEE Security and Privacy Workshops. 2015. URL: https://ieeexplore.ieee.org/document/7163223

Ключові слова: Блокчейн, цілісність даних, криптографія, хеш-функції, консенсусні алгоритми, децентралізація, кібербезпека.

Keywords: Blockchain, data integrity, cryptography, hash functions, consensus algorithms, decentralization, cybersecurity.

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