**Міністерство освіти і науки України**
**Київський національний університет імені Тараса Шевченка**

**Факультет інформаційних технологій**
**Кафедра кібербезпеки та захисту інформації**

**ДОПУСТИТИ ДО ЗАХИСТУ:**
В.о. завідувача кафедри
кібербезпеки та захисту
інформації
_____ Іван ПАРХОМЕНКО
«  » червня 2025 р.

# ПОЯСНЮВАЛЬНА ЗАПИСКА

## кваліфікаційної роботи

**галузь знань** 12 Інформаційні технології
(шифр і назва галузі знань)
**спеціальність** 125 Кібербезпека
(код і назва спеціальності)
**освітній ступень** бакалавр
**освітня програма** Кібербезпека
(назва освітньо-професійної програми)
**на тему:** «Модель безпеки комп'ютерної системи на базі технології блокчейн»

**Виконавець:** студент IV курсу, групи КБ-41

_____ **Ігор ХРАПАТИЙ**
(підпис) (ім'я, прізвище)

| | **Підпис** | **Ім'я ПРІЗВИЩЕ** |
|---|---|---|
| **Керівник** | | Сергій ТЮЛЮПА |
| **Нормоконтроль** | | Леся БАРАНОВСЬКА |

**Київ 2025**

**Міністерство освіти і науки України**
**Київський національний університет імені Тараса Шевченка**

**Факультет інформаційних технологій**
**Кафедра кібербезпеки та захисту інформації**

**ЗАТВЕРДЖЕНО:**
В.о. завідувача кафедри
кібербезпеки
та захисту інформації
_____ Іван ПАРХОМЕНКО
«29» листопада 2024 р.

# ЗАВДАННЯ
## на виконання кваліфікаційної роботи

**спеціальності** 125 Кібербезпека
(код і назва спеціальності)

**освітньої програми** Кібербезпека
(назва освітньо-професійної програми)

**Студенту** **КБ-41** (група) **Храпатому Ігору Ігоровичу** (прізвище ім'я по батькові)

**Тема кваліфікаційної роботи** Модель безпеки комп'ютерної системи на базі технології блокчейн

### 1. ПІДСТАВИ ДЛЯ ПРОВЕДЕННЯ РОБОТИ

Тема кваліфікаційної роботи затверджена на засіданні кафедри кібербезпеки та захисту інформації протокол №6 від 28.11.2024 р.

### 2. ВИХІДНІ ДАНІ ДЛЯ ПРОВЕДЕННЯ РОБІТ

Структура децентралізованих веб-додатків на базі смартконтрактів. Архітектура клієнт-сервер з використанням Ethereum-блокчейну. Стек технологій: React, Node.js, Solidity, web3.js. Алгоритм хешування: SHA-256. Метод аутентифікації: ECDSA (цифровий підпис).

### 3. ЗМІСТ РОЗРАХУНКОВО-ПОЯСНЮВАЛЬНОЇ ЗАПИСКИ

Нормативно-правова база у сфері захисту інформації.
Структура веб-додатків на основі блокчейн.
Мережевий протокол прикладного рівня: JSON-RPC.
Архітектурний стиль: Model-View-Controller (MVC).
Основні вразливості веб-додатків.

Захист від порушеної аутентифікації.

Захист від ескалації привілеїв.

Рекомендації з безпеки блокчейн-систем.

## 4. ВИМОГИ ДО РЕЗУЛЬТАТІВ ВИКОНАННЯ РОБОТИ

**Практична цінність** полягає в інтеграції блокчейн-архітектури із класичними механізмами захисту веб-додатків, що дозволяє підвищити рівень кібербезпеки за рахунок децентралізації, незмінності даних та автоматизованого контролю доступу.

## 5. ДАТА ВИДАЧІ ЗАВДАННЯ

Дата видачі завдання: 29 листопада 2024 року

Завдання видав _____ (підпис) Сергій ТЮЛЮПА (ім'я, прізвище)

Завдання прийняв до виконання _____ (підпис) Ігор ХРАПАТИЙ (ім'я, прізвище)

## КАЛЕНДАРНИЙ ПЛАН

| № п/п | Найменування етапів робіт | Строки виконання робіт (початок-кінець) | Відмітка про виконання |
|---|---|---|---|
| 1 | Уточнення постановки задачі | 29.11.2024 – 15.01.2025 | *виконано* |
| 2 | Аналіз літератури | 16.01.2025 – 30.01.2025 | *виконано* |
| 3 | Обґрунтування вибору рішення | 31.01.2025 – 10.02.2025 | *виконано* |
| 4 | Розгляд структури веб-додатків | 11.02.2025 – 24.02.2025 | *виконано* |
| 5 | Дослідження основних вразливостей | 25.02.2025 – 8.03.2025 | *виконано* |
| 6 | Впровадження засобів та механізмів захисту від загроз порушеної аутентифікації | 9.03.2025 – 25.03.2025 | *виконано* |
| 7 | Впровадження засобів та механізмів захисту від ескалації привілеїв | 26.03.2025 – 20.04.2025 | *виконано* |
| 8 | Формування рекомендацій щодо механізмів захисту для веб-додатків | 21.04.2025 – 15.05.2025 | *виконано* |
| 9 | Оформлення пояснювальної записки | 16.05.2025 – 22.05.2025 | *виконано* |

| № п/п | Найменування етапів робіт | Строки виконання робіт (початок-кінець) | Відмітка про виконання |
|---|---|---|---|
| 10 | Підготовка до захисту кваліфікаційної роботи | 23.05.2025 – 13.06.2025 | *виконано* |

Завдання видав _____ Сергій ТЮЛЮПА
(підпис) (ім'я, прізвище)

Завдання прийняв до виконання _____ Ігор ХРАПАТИЙ
(підпис) (ім'я, прізвище)

Термін подання кваліфікаційної роботи до ЕК 13 червня 2025

# РЕФЕРАТ

Пояснювальна записка дипломної роботи складається зі вступу, трьох розділів, загальних висновків, списку використаних джерел, додатків, має 84 сторінок основного тексту, 7 таблиць та 2 рисунки. Список використаних джерел містить 50 найменувань і займає 5 сторінок.

*Метою роботи* є підвищенння рівня захисту при обробці конфіденційної інформації за рахунок впровадження моделі безпеки комп'ютерної системи на базі технології блокчейн.

Для досягнення поставленої мети були визначені наступні *завдання*:

- Провести теоретичний аналіз блокчейн-технологій у контексті кібербезпеки, визначити їхні переваги та обмеження, а також зіставити можливості блокчейн з класифікацією сучасних загроз для комп'ютерних систем.
- Дослідити існуючі рішення щодо використання блокчейн для захисту інформаційних потоків та обґрунтувати власний підхід до розробки моделі безпеки, включно з описом архітектури та основних компонентів.
- Проаналізувати ефективність запропонованої моделі в умовах змодельованих загроз і сформулювати рекомендації щодо її впровадження та подальшого вдосконалення.

*Об'єктом дослідження* є процес виявлення та протидії загрозам, характерним для архітектури сучасних компютерних систем.

*Предметом дослідження* є методи, засоби та моделі безпеки комп'ютерних систем на базі технології блокчейн

*Практичною цінністю отриманих результатів є* розробка, інтеграція та програмна реалізація засобів захисту веб-додатків, які враховують як традиційні вразливості, так і новітні засоби їх усунення з використанням технологій блокчейн.

Дана модель може використовуватися  для забезпеки безпеки комп’ютерних систем державної та приватної власності.

*Ключові слова***:** веб-додаток, база даних, вразливості, захист персональних даних, облікові дані, SQL-ін’єкції, ескалація привілеїв

# ЗМІСТ

# ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ ТА СКОРОЧЕННЬ

| | | |
|---|---|---|
| PoW | – | Proof of Work — доказ виконання роботи |
| PoS | – | Proof of Stake — доказ частки володіння |
| MITM | – | Man-in-the-Middle — атака «людина посередині» |
| DDoS | – | Distributed Denial of Service — розподілена атака на відмову в обслуговуванні |
| ПЗ | – | Програмне забезпечення |
| APT | – | Advanced Persistent Threat — високорівнева цілеспрямована атака |
| SQL | – | Structured Query Language — мова структурованих запитів |
| API | – | Application Programming Interface — прикладний програмний інтерфейс |
| ZKP | – | Zero-Knowledge Proof — доказ з нульовим розголошенням |
| DID | – | Decentralized Identifier — децентралізований ідентифікатор |
| IDE | – | Integrated Development Environment — інтегроване середовище розробки |

# ВСТУП

В умовах стрімкого розвитку цифрових технологій та масового впровадження інтернет-сервісів безпека комп’ютерних систем набула пріоритетного значення в науковому та прикладному вимірах. Зростання обсягів оброблюваної та переданої інформації, особливо конфіденційного та персонального характеру, обумовлює потребу в ефективних інструментах її захисту. У той самий час традиційні централізовані моделі кібербезпеки виявляються все більш уразливими перед сучасними загрозами, такими як атаки типу “людина посередині”, фальсифікація даних, витоки через незахищені канали передачі тощо. Саме в цьому контексті актуальним стає застосування блокчейн-технологій — децентралізованих, криптографічно захищених структур, здатних забезпечити новий рівень безпеки інформаційних систем.

Блокчейн, початково реалізований у фінансовому секторі через криптовалюти, з часом трансформувався в універсальну технологію, придатну для захисту цифрової інформації у різноманітних сферах: охороні здоров’я, державному управлінні, логістиці, освітніх сервісах тощо. Його ключовими перевагами є незмінність записів, криптографічна стійкість, можливість розподіленого зберігання даних і відсутність єдиної точки відмови. Ці властивості блокчейн дають змогу забезпечити прозорість, достовірність і контроль за обігом інформації навіть в умовах високої загрози зовнішнього або внутрішнього втручання.

*Актуальність* дослідження зумовлена необхідністю формування нової моделі захисту комп’ютерної системи, яка б враховувала недоліки традиційних підходів до безпеки, відповідала сучасним вимогам цифрової трансформації та могла забезпечити стійкість до атак, що активно еволюціонують. У зв’язку з цим особливого значення набуває системний аналіз можливостей інтеграції блокчейн-

архітектур у механізми безпеки, розробка практичної моделі, адаптованої до українського контексту та прикладних задач у сфері кібербезпеки.

*Метою роботи* є підвищення рівня захисту при обробці конфіденційної інформації за рахунок впровадження моделі безпеки комп'ютерної системи на базі технології блокчейн

Для досягнення поставленої мети були визначені такі *завдання*:

- Провести теоретичний аналіз блокчейн-технологій у контексті кібербезпеки, визначити їхні переваги та обмеження, а також зіставити можливості блокчейн з класифікацією сучасних загроз для комп'ютерних систем.
- Дослідити існуючі рішення щодо використання блокчейн для захисту інформаційних потоків та обґрунтувати власний підхід до розробки моделі безпеки, включно з описом архітектури та основних компонентів.
- Проаналізувати ефективність запропонованої моделі в умовах змодельованих загроз і сформулювати рекомендації щодо її впровадження та подальшого вдосконалення.

*Об'єкт дослідження* – процес виявлення та протидії загрозам, характерним для архітектури сучасних компютерних систем.

*Предмет дослідження* – методи, засоби та моделі безпеки комп'ютерних систем на базі технології блокчейн

*Практична цінність* роботи полягає у розробці, інтеграції та програмній реалізації засобів захисту веб-додатків, які враховують як традиційні вразливості, так і новітні засоби їх усунення з використанням технологій блокчейн. Дана модель може використовуватися для забезпеки безпеки комп'ютерних систем державної та приватної власності.

*Джерельна база* дослідження охоплює як вітчизняні, так і зарубіжні наукові публікації з тематики інформаційної безпеки, блокчейн-технологій, криптографічного захисту, стандартів кібербезпеки (NIST, ISO/IEC 27001), результати досліджень у межах міжнародних конференцій (IEEE, ACM), технічну

документацію існуючих блокчейн-платформ (Ethereum, Hyperledger, Multichain). Значну увагу приділено огляду прикладних рішень у сфері охорони здоров'я, цифрової ідентифікації та державного документообігу на основі блокчейн.

*Фактичний матеріал* складається з описів реальних випадків застосування блокчейн у сфері безпеки (зокрема, урядові ініціативи в Естонії та ОАЕ), специфікацій програмного забезпечення, моделей взаємодії користувачів у системах із підвищеними вимогами до збереження даних, а також авторських розробок моделі на основі віртуального середовища.

У процесі роботи було використано такі *методи дослідження*:

- *теоретичні*: аналіз, узагальнення, систематизація літератури та технічної документації, побудова класифікацій;
- *моделювання*: побудова структурної блок-схеми моделі безпеки, опис інформаційних потоків;
- *порівняльний аналіз*: оцінка переваг і недоліків наявних підходів до захисту даних;
- *експертна оцінка*: залучення спеціалістів до апробації запропонованої моделі;
- *індуктивно-дедуктивний підхід*: узагальнення окремих рішень і формування загальної концепції безпечної системи на основі блокчейн.

*Наукова новизна* роботи полягає у наступному:

- *визначено* специфіку формування децентралізованої моделі безпеки для загальносистемного захисту комп'ютерної архітектури шляхом інтеграції криптографічних механізмів, розподіленого реєстру довіри (блокчейн) та алгоритмічної стійкості для побудови стійкої до атак системи;
- *вдосконалено* підходи до автентифікації, авторизації та контрольованого доступу в середовищах з високою інтенсивністю обміну даними, із забезпеченням принципу "zero trust" і застосуванням незмінних журналів аудиту;

*дістала* подальшого розвитку концепція інтеграції механізмів контрольованого доступу у блокчейн-середовищах із високою інтенсивністю обміну даними;

*Теоретична цінність* роботи полягає в обґрунтуванні доцільності застосування блокчейн як базового компонента системи кібербезпеки в умовах розвитку цифрової інфраструктури. Запропоновані положення можуть стати підґрунтям для формування нових стандартів безпеки в державному та корпоративному секторах.

*Практичне значення* полягає в можливості впровадження розробленої моделі у системи обліку, документообігу, розподілені бази даних, платформи цифрової ідентифікації тощо. Архітектура моделі може бути адаптована до потреб малого й середнього бізнесу, а також органів публічного управління в Україні. Модель враховує обмеження щодо обчислювальних ресурсів, тому її реалізація можлива в умовах використання доступного апаратного забезпечення.

Таким чином, запропоноване дослідження має як теоретичну, так і прикладну спрямованість, є актуальним для умов цифрової трансформації та має перспективу подальшого розвитку в галузі захисту комп’ютерних систем із використанням блокчейн-технологій.

# РОЗДІЛ 1. ТЕОРЕТИЧНІ АСПЕКТИ БЛОКЧЕЙН-ТЕХНОЛОГІЙ У КІБЕРБЕЗПЕЦІ

## 1.1. Основи блокчейн-технології та її застосування в комп'ютерних системах

Блокчейн-технологія є однією з найбільш революційних інновацій у сфері інформаційних технологій, що сформувала нову парадигму зберігання, передавання та захисту даних. У своїй основі блокчейн представляє собою розподілену базу даних, де інформація зберігається у вигляді послідовного ланцюга блоків. Кожен блок містить набір транзакцій або записів, а також хеш попереднього блоку, що створює нерозривний ланцюг. Такий підхід забезпечує незмінність (immutability) інформації, оскільки будь-яке втручання в дані призводить до зміни хешу блоку, що автоматично анулює валідність усіх наступних блоків у ланцюгу.

Кожен блок у блокчейн має чітко визначену структуру. Він складається з двох основних частин: заголовка (header) та тіла (body). У заголовку блоку зберігається хеш попереднього блоку, мітка часу (timestamp), nonce (довільне число, яке використовується в алгоритмах консенсусу), а також кореневий хеш Merkle Tree – криптографічної структури, що узагальнює всі транзакції в блоці. Тіло блоку містить список транзакцій, які були підтверджені мережею. Використання Merkle Tree дозволяє здійснювати ефективну перевірку цілісності транзакцій без необхідності сканування всього блоку, що особливо важливо при великому обсязі даних [1].

Основним принципом функціонування блокчейн є послідовне додавання блоків до ланцюга. Новий блок додається лише після підтвердження його достовірності всіма або більшістю вузлів (нод) у мережі. У публічних блокчейн-мережах, таких як Bitcoin або Ethereum, це відбувається через механізм консенсусу

– узгодження між учасниками щодо справжності транзакцій. Найпоширенішими алгоритмами консенсусу є Proof of Work (PoW), Proof of Stake (PoS), Delegated Proof of Stake (DPoS), Practical Byzantine Fault Tolerance (PBFT) та інші. Вони мають різний ступінь ефективності, енергоспоживання та безпеки, однак усі переслідують мету досягнення єдиного узгодженого стану мережі.

У випадку Proof of Work, який є основою Bitcoin, додавання нового блоку вимагає вирішення складної криптографічної задачі – знаходження такого значення nonce, при якому хеш заголовка блоку відповідатиме певному шаблону (зазвичай починається з визначеної кількості нулів). Цей процес потребує значних обчислювальних ресурсів і часу, що запобігає можливості швидкої генерації хибних блоків. Коли один з учасників знаходить правильне рішення, блок транслюється по мережі для перевірки іншими нодами. Якщо більшість вузлів визнає блок валідним, він додається до ланцюга [9].

Важливою характеристикою блокчейн є те, що дані, вже внесені до системи, не можуть бути змінені або видалені без згоди всіх учасників мережі. Це досягається за рахунок використання хеш-функцій, які генерують унікальний цифровий відбиток для кожного блоку. Якщо будь-яка інформація в блоці зміниться, зміниться і його хеш, що призведе до несумісності з наступним блоком. Унаслідок цього вся гілка, що продовжується від зміненого блоку, буде визнана недійсною. Для того щоб змінити інформацію у вже створеному блоці, зловмиснику потрібно перерахувати всі наступні блоки, що з практичної точки зору є майже неможливим.

Іншим важливим компонентом структури блокчейн є транзакції. Транзакція – це одиниця інформації, яка містить дані про зміну стану системи, наприклад, передання цифрових активів, запис події або оновлення параметрів користувача. Усі транзакції повинні бути підписані цифровим підписом користувача, що забезпечує їхню автентичність і підтверджує право власності на переданий актив або інформацію. Перед тим як транзакція буде включена до блоку, вона має бути

перевірена мережею – перевіряється наявність цифрового підпису, правомірність дії та відповідність правилам протоколу.

Блокчейн може функціонувати як у публічних (відкритих) мережах, так і в приватних або консорціумних середовищах. У публічному блокчейні будь-який учасник має право створювати блоки, перевіряти транзакції та брати участь у консенсусі. У приватних мережах доступ обмежується певними організаціями або користувачами, що дозволяє точніше контролювати безпеку та продуктивність системи. Консорціумний блокчейн поєднує риси обох моделей: керування мережею здійснюється групою довірених вузлів, однак доступ до перегляду інформації може бути відкритим [15].

У контексті комп’ютерних систем блокчейн виступає як інфраструктура для забезпечення безпеки даних. Його застосування можливе в таких компонентах, як контроль доступу, ведення журналів подій, ідентифікація користувачів, підтвердження цілісності файлів і транзакцій. Наприклад, у системах, що вимагають високого рівня довіри, блокчейн дозволяє зберігати незмінні лог-файли дій користувачів, які не можуть бути відредаговані навіть адміністраторами. У системах управління доступом можливе створення смартконтрактів, які автоматично визначають права доступу відповідно до заданих правил.

Смартконтракти – це ще один важливий елемент функціонування блокчейн. Вони є автономними програмами, що зберігаються у блокчейні й автоматично виконуються при виконанні певних умов. Смартконтракти дають змогу автоматизувати бізнес-процеси, перевіряти автентичність дій та реалізовувати контроль доступу без участі людини. Їхня роль у сучасних комп’ютерних системах зростає, особливо в системах цифрової ідентичності, електронного документообігу та управління конфіденційними ресурсами [2].

Усі ці елементи – блоки, транзакції, алгоритми консенсусу, смартконтракти – утворюють єдину архітектуру, яка дозволяє будувати децентралізовані, прозорі та захищені комп’ютерні системи. На відміну від централізованих систем, де одна

точка відмови може призвести до втрати або компрометації даних, блокчейн функціонує у розподіленому середовищі, що забезпечує стійкість до зовнішніх атак і внутрішніх зловживань. Кожен учасник мережі має копію ланцюга блоків, і будь-які зміни мають бути погоджені з більшістю [5].

Інтеграція блокчейн-технологій у комп'ютерні системи безпеки є відповіддю на численні виклики сучасної цифрової епохи. Зростання складності кіберзагроз, уразливості традиційних централізованих моделей та необхідність забезпечення високого рівня довіри між суб'єктами цифрової взаємодії актуалізували потребу у впровадженні децентралізованих механізмів. Блокчейн, як інфраструктура з криптографічним захистом, розподіленим зберіганням та вбудованими алгоритмами консенсусу, дозволяє реалізувати нову модель функціонування комп'ютерних систем, де безпека не є зовнішнім доповненням, а закладена на рівні архітектури.

Одним із ключових напрямів застосування блокчейн у комп'ютерній безпеці є система управління ідентичністю користувачів (Digital Identity Management). У традиційних централізованих рішеннях (LDAP, Active Directory) всі дані про облікові записи зберігаються в одному репозиторії, який стає вразливим до атак типу "єдина точка відмови" (Single Point of Failure). Натомість блокчейн дозволяє реалізувати децентралізовану ідентичність (Decentralized Identity, DID), при якій дані про користувача (роль, статус, ключі, дозволи) зберігаються у смартконтрактах та підтверджуються мережею. Це дає змогу унеможливити несанкціоноване редагування облікових записів і забезпечити повну прозорість процесів автентифікації [36].

Другий напрям застосування – системи контролю доступу. Традиційні моделі (DAC, MAC, RBAC) використовують таблиці дозволів, які адмініструються централізовано, що відкриває шлях до потенційного зловживання з боку адміністратора. За допомогою блокчейн можна реалізувати розподілений контроль доступу (Distributed Access Control), у якому дозволи записуються в незмінну

реєстрову структуру. Наприклад, смартконтракт може описувати, які ролі мають доступ до яких функцій, а також автоматично блокувати дії в разі невідповідності політиці доступу. У поєднанні з DID це забезпечує не тільки точне розмежування прав, а й захист від їхньої підробки чи фальсифікації.

Третій важливий компонент – аудит і журналювання подій. У класичних системах логи зберігаються на центральних серверах, що дозволяє змінювати або видаляти записи без відстеження. Блокчейн вирішує цю проблему за рахунок незмінності даних: кожна подія, записана у вигляді транзакції у блок, має хеш і цифровий підпис, що гарантує її достовірність. Завдяки цьому можливо створити невидалюваний журнал дій (tamper-proof log), який може бути перевірений зовнішніми аудиторами без ризику маніпуляцій. Цей підхід особливо корисний у фінансових системах, корпоративному контролі доступу та захисті конфіденційної інформації [7].

Ще одним перспективним напрямом застосування блокчейн є захист цілісності даних. У багатьох сферах (зокрема в медицині, юриспруденції, освіті) вкрай важливо довести, що інформація не змінювалася після її збереження. Замість зберігання самих файлів у блокчейні, який обмежений за обсягом, можна зберігати лише хеші документів, а самі документи – в зовнішньому сховищі (наприклад, IPFS або централізованому сервері). Це дозволяє будь-кому перевірити цілісність шляхом порівняння хешу з оригіналу з тим, що збережений у блокчейні, не порушуючи конфіденційність змісту.

Застосування блокчейн у мережевій безпеці також має вагоме значення. Зокрема, існують реалізації DNS на блокчейн-основі, що виключають можливість підміни записів та централізованого цензурування. Рішення типу Namecoin, ENS або Handshake дозволяють створювати захищені доменні системи, в яких право власності на домен зафіксоване у смартконтракті. Крім того, блокчейн можна використовувати в системах IoT, де важко реалізувати централізовану перевірку дій кожного пристрою. У таких випадках блокчейн-мережа може фіксувати всі дії

сенсорів, маршрутизаторів, вузлів у реальному часі, забезпечуючи прозорість і контроль без втручання центрального сервера.

Окремої уваги заслуговує використання блокчейн у реалізації критичних операцій із багаторівневим підтвердженням. Завдяки можливостям смартконтрактів можна створювати сценарії, при яких виконання операції (наприклад, переведення коштів, зміна налаштувань системи, оновлення політики доступу) можливе лише за умови отримання мультипідпису від кількох незалежних осіб. Такий підхід значно знижує ризик несанкціонованих дій навіть у разі компрометації одного з ключів. Це реалізовано, наприклад, у контракті MultiSigControl.sol із практичної частини, де критична дія виконується лише після досягнення необхідної кількості підтверджень [4].

Блокчейн також може застосовуватись у сфері захисту персональних даних. Згідно із законодавством, зокрема Регламентом ЄС GDPR, користувач повинен мати можливість контролювати обробку своїх даних. Через блокчейн можна реалізувати моделі, при яких користувач явно надає або відкликає згоду на обробку своїх персональних даних, а самі транзакції з цими даними фіксуються у децентралізованому журналі. Крім того, технологія Zero-Knowledge Proofs (ZKP), що використовується в сучасних блокчейн-системах, дозволяє перевіряти факт володіння даними без розкриття їхнього змісту.

Варто підкреслити, що блокчейн також успішно застосовується для підтвердження дійсності електронних документів та цифрових підписів. У цій моделі користувач генерує підпис і публікує хеш документа у блокчейні, що дозволяє третій стороні у будь-який момент перевірити автентичність цього документа, навіть без доступу до повного оригіналу. Такий підхід актуальний у системах е-урядування, тендерних платформах, електронному документообігу та юридичній практиці.

Отже, блокчейн-технологія знаходить широке застосування в комп’ютерних системах, що потребують високого рівня захищеності, достовірності та прозорості.

Його переваги — незмінність записів, автоматизоване виконання умов (через смартконтракти), децентралізація, контроль доступу, криптографічний захист — забезпечують можливість побудови нової моделі функціонування ІТ-систем, яка здатна ефективно протистояти сучасним загрозам. Реалізація таких моделей у практичних умовах (як у представленому у розділі 2 смартконтрактному проєкті) підтверджує ефективність і адаптивність блокчейн у реальних інформаційних середовищах. Надалі ця технологія відіграватиме все вагомішу роль у захисті критичних цифрових інфраструктур та розробці стійких до атак комп'ютерних систем нового покоління [12].

*Таблиця 1.1*

Порівняльна характеристика алгоритмів консенсусу

| **Алгоритм** | **Стійкість до атак** | **Енергоспоживання** | **Швидкість підтвердження** |
|---|---|---|---|
| **Proof of Work** | Висока | Високе | Низька |
| **Proof of Stake** | Середня | Низьке | Висока |
| **Delegated PoS** | Середня | Низьке | Висока |
| **PBFT** | Висока | Низьке | Висока |
| **PoA** | Середня | Низьке | Висока |

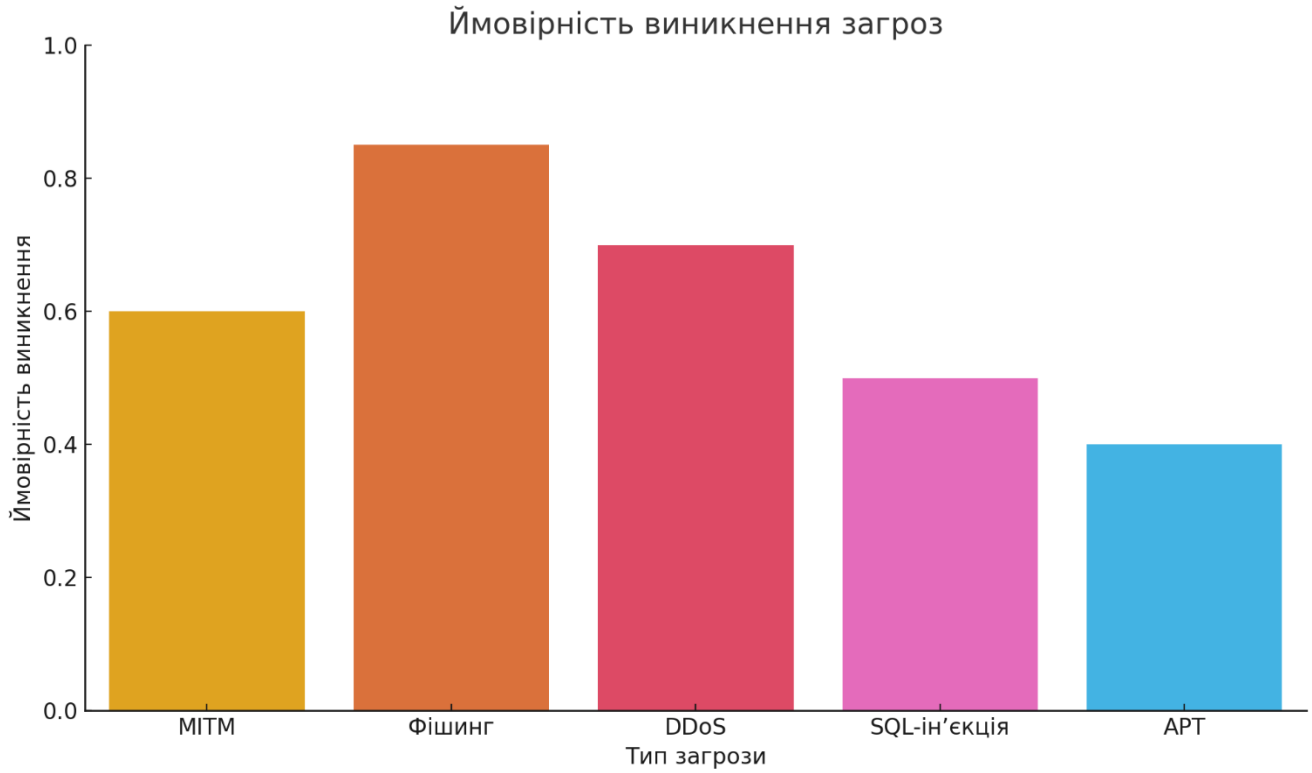


Рисунок 1.1 – Ймовірність виникнення загроз

## 1.2. Аналіз загроз для інформаційних систем і можливості їхнього усунення за допомогою блокчейну

Інформаційна інфраструктура є критично важливим елементом функціонування державних, корпоративних та персональних систем, оскільки забезпечує зберігання, обробку, передачу та захист даних. У сучасних умовах цифрової трансформації загрози для інформаційної інфраструктури набувають нових форм і масштабів. Постійне зростання складності систем, поява нових типів кіберзброї, розвиток засобів соціальної інженерії та штучного інтелекту — все це формує багатовекторне середовище ризиків. У зв'язку з цим класифікація загроз набуває особливого значення для адекватної побудови системи безпеки, вибору пріоритетних напрямів захисту та впровадження ефективних протидій [15].

У науковій та технічній літературі загрози для інформаційної інфраструктури поділяються за різними критеріями: за джерелом походження, механізмом дії, спрямованістю, цільовими об’єктами, а також ступенем потенційної шкоди. Основними джерелами загроз є: технічні збої, людський фактор (навмисний або ненавмисний), програмні вразливості, зовнішній вплив (атаки третіх сторін, у тому числі державного рівня), а також природні або форс-мажорні обставини. З огляду на це, загрози можна умовно розподілити на внутрішні (інсайдерські) та зовнішні. Внутрішні загрози, зокрема, походять від користувачів, які мають повний або частковий доступ до системи: адміністраторів, операторів, працівників відділів підтримки. Вони можуть здійснювати витоки даних, несвідомо запускати шкідливе програмне забезпечення або навмисно змінювати критичні конфігурації. Зовнішні загрози, своєю чергою, ініціюються особами або організаціями, які не мають легального доступу до системи, і здійснюються за допомогою шкідливого коду, мережевих атак, соціальної інженерії або технічних засобів злому [1].

Залежно від механізму реалізації, загрози класифікуються на програмні, апаратні, організаційні та комбіновані. Програмні загрози включають віруси, троянські програми, руткіти, кейлогери, програми-вимагачі (ransomware), ботнети тощо. Їхнє поширення може відбуватись як через мережу, так і через заражені носії. Особливо небезпечними є багатовекторні атаки типу APT (Advanced Persistent Threat), які можуть діяти непомітно протягом тривалого часу. Апаратні загрози пов’язані з уразливостями в апаратному забезпеченні (наприклад, експлуатація дефектів у процесорах, таких як Spectre або Meltdown), збої у живленні, перегрів, вплив електромагнітного випромінювання тощо. Організаційні загрози виникають внаслідок неефективного управління політиками безпеки, відсутності контролю доступу, недостатньої підготовки персоналу або нехтування процедурами. Комбіновані загрози передбачають поєднання кількох факторів: наприклад, фішинг, що дозволяє зловмиснику встановити шкідливе ПЗ, яке потім експлуатує вразливість у системному модулі.

За ступенем впливу на систему загрози поділяються на: загрози конфіденційності (несанкціонований доступ до даних), цілісності (некоректна модифікація або знищення даних), доступності (відмова в обслуговуванні або блокування функціонування), а також юридичної відповідальності (витік персональних даних, що підпадають під регулювання законодавства). Класичним прикладом порушення конфіденційності є атаки MITM (man-in-the-middle), що дозволяють перехоплювати передану інформацію. Вразливість до зміни даних може бути наслідком недостатньо перевірених API або прав на запис у базу даних. Порушення доступності зазвичай реалізується через атаки типу DoS (Denial of Service) або DDoS (Distributed Denial of Service), що паралізують роботу серверів через перевантаження запитами [3].

Сучасні загрози часто поєднують кілька напрямів впливу, використовуючи так звані ланцюгові атаки, що включають етапи розвідки, проникнення, закріплення, ескалації привілеїв, виконання цілей і приховування слідів. Наприклад, у складній APT-атаці зловмисники можуть спочатку отримати доступ через фішинг, далі використати вразливості в системі автентифікації для підвищення прав, встановити бекдори й поступово збирати критичну інформацію або знищувати системні файли. У корпоративних або державних системах такі атаки можуть залишатися непоміченими місяцями.

В окрему категорію виділяють загрози, що походять від соціальної інженерії — методу впливу на людський фактор. Сюди відносяться фішинг, вішинг (голосовий фішинг), смішинг (SMS-фішинг), фізичні методи (tailgating, dumpster diving). Такі загрози складно виявити технічними засобами, оскільки вони базуються на психологічних прийомах обману працівників. Їхня ефективність пояснюється недостатнім навчанням персоналу та відсутністю внутрішніх протоколів перевірки [4].

Окремо розглядаються загрози з боку постачальників ПЗ та "третіх сторін", що особливо актуально в умовах широкого використання відкритого коду,

зовнішніх сервісів (SaaS, IaaS) та хмарних технологій. Такі загрози включають впровадження шкідливого коду в бібліотеки, оновлення з бекдором або цілеспрямовану зміну логіки роботи програмного модуля в інтересах сторонніх осіб. Прикладом стала атака через платформу SolarWinds, яка торкнулася державних структур США та інших країн. Це показує, що навіть перевірене ПЗ може бути використано як канал атаки [8].

До новітніх загроз варто також зарахувати атаки із залученням штучного інтелекту. Зловмисники вже використовують алгоритми машинного навчання для автоматизованого виявлення вразливих систем, моделювання фішингових повідомлень на основі психологічного профілю жертви, створення deepfake-контенту для дискредитації або обходу біометричних систем захисту. Розвиток так званого offensive AI створює нові виклики для розробників систем захисту.

У категорії загроз, які мають найвищий потенціал шкоди, варто виділити державні (геополітичні) кібератаки. Вони є частиною стратегічного інструментарію, використовуються для дестабілізації критичної інфраструктури, енергетичних систем, медіа-ресурсів, систем управління транспортом або охорони здоров’я. Такі атаки ретельно плануються, реалізуються через численні вектори одночасно та супроводжуються кампаніями дезінформації. Часто їх важко ідентифікувати як державні через використання підставних акторів або ботнетів.

У підсумку, класифікація загроз для інформаційної інфраструктури дозволяє структурувати наявні ризики та адаптувати під них відповідні стратегії захисту. На сучасному етапі вже недостатньо будувати системи безпеки виняткова на периметрі – необхідно впроваджувати багаторівневі моделі із застосуванням криптографічних протоколів, децентралізованих реєстрів, механізмів виявлення аномалій та постійного аудиту. У наступному підпункті буде проаналізовано, яким чином технологія блокчейн здатна нейтралізувати частину з перелічених загроз, зокрема тих, що пов’язані з незмінністю даних, довірою до журналів подій, ідентифікацією користувачів та забезпеченням контрольованого доступу.

У відповідь на стрімке зростання кіберзагроз, які охоплюють як програмні, так і організаційні, соціотехнічні та геополітичні аспекти, постає завдання пошуку нових технологічних рішень, здатних забезпечити стійкість цифрової інфраструктури. Серед найперспективніших підходів, що поступово інтегруються у практики цифрової безпеки, особливе місце займає блокчейн. Його концептуальні переваги, такі як децентралізація, незмінність записів, прозорість транзакцій і криптографічна автентифікація, створюють основу для ефективного протистояння більшості відомих кіберзагроз [3].

Одним з ключових напрямів зменшення кіберризиків за допомогою блокчейн є усунення загрози фальсифікації або знищення даних. Традиційні бази даних часто піддаються змінам — зловмисники можуть видалити або підробити інформацію, особливо якщо мають доступ до адміністративних прав. Натомість у блокчейн кожен запис, щойно підтверджений мережею, зберігається незмінним завдяки структурі, що базується на хеш-зв’язках між блоками. Зміна хоча б одного байта в транзакції автоматично призводить до зміни хешу блоку і всіх наступних, що легко виявляється нодами. Це дозволяє розробити системи, в яких гарантується цілісність даних навіть за умов внутрішнього саботажу або проникнення.

Блокчейн також значно знижує ризики несанкціонованого доступу, особливо в системах, де потрібна висока надійність автентифікації. Завдяки криптографічному механізму цифрового підпису, кожна транзакція підписується особистим ключем користувача. Це забезпечує не лише підтвердження авторства дії, а й захищає від підміни або імітації доступу. Крім того, публічні ключі можна верифікувати на блокчейн-рівні, що дозволяє будувати системи управління ідентичністю без єдиного центру довіри (центра сертифікації). Таким чином, зменшується залежність від централізованих серверів, які можуть стати об’єктом атак або збоїв [7].

Ще одним важливим аспектом є вбудований механізм контролю дій користувачів. Усі події, що фіксуються у блокчейні, є публічними або доступними

вузькому колу учасників у приватних реалізаціях. Це дозволяє здійснювати постійний аудит та відстеження змін, забезпечуючи прозорість і підзвітність усіх дій. У разі порушень або аномальної активності, відповідальні особи можуть легко виявити джерело проблеми. Таке логування, яке не може бути змінене навіть системними адміністраторами, кардинально знижує ризики внутрішнього шахрайства, що, за статистикою, складає значну частку всіх інцидентів інформаційної безпеки.

Блокчейн ефективно справляється з загрозами, що походять від третіх сторін або вразливого ПЗ. У випадках, коли інформаційна система використовує зовнішні API, сервіси або бібліотеки, кожна взаємодія може бути зафіксована у смартконтракті. Це дозволяє реалізувати політики довіри на рівні протоколу: лише авторизовані зовнішні компоненти мають доступ до певних функцій, і кожна дія підтверджується криптографічно. Наприклад, у межах інтеграції із зовнішніми модулями можна забезпечити обов’язкове підтвердження змін від кількох вузлів, що мінімізує ризик впровадження шкідливого коду або використання вразливих оновлень [23].

Крім того, блокчейн-технологія здатна нейтралізувати загрози, пов’язані з аномаліями в роботі системи, що виникають через технічні збої, перевантаження або непередбачувану поведінку користувачів. За рахунок можливості побудови розподілених систем управління, де логіка прийняття рішень розміщена в смартконтрактах, виключається можливість людської помилки в критичних операціях. Такі контракти діють лише при виконанні попередньо визначених умов і забезпечують детермінованість дій системи, що унеможливлює непередбачувані сценарії.

Використання блокчейн також мінімізує ризики при реалізації операцій високої важливості, які вимагають багатоетапного підтвердження. Наприклад, система може бути налаштована так, що певна дія (зміна політики безпеки, передача конфіденційних даних, фінансова транзакція) виконується лише після

верифікації кількома незалежними сторонами. Це забезпечує протидію спробам одноосібного зловживання повноваженнями та унеможливлює швидке виконання деструктивних сценаріїв [25].

У сфері захисту персональних даних блокчейн має потенціал стати новим стандартом. Один із способів мінімізації ризиків витоку даних полягає в збереженні не самих даних, а їхніх хешів, що дозволяє підтвердити справжність без розкриття змісту. Окрім того, користувачі можуть реалізовувати права на відкликання згоди на обробку інформації через спеціальні транзакції, фіксуючи кожен крок у децентралізованій системі. Впровадження додаткових технологій, як-от Zero-Knowledge Proofs або homomorphic encryption, відкриває нові можливості щодо перевірки дійсності даних без їхнього розкриття, що особливо актуально для медичних, фінансових та юридичних систем.

З точки зору управління репутацією і довірою, блокчейн також є ефективним інструментом. У системах, де кілька суб'єктів взаємодіють без прямого знайомства (наприклад, у хмарних середовищах, p2p-мережах, децентралізованих платформах), блокчейн забезпечує можливість створення історії дій кожного учасника. Ця історія не може бути видалена або змінена, а отже, рівень довіри формується на основі об'єктивних цифрових слідів, а не на основі припущень або репутації ззовні. Це значно знижує ризик взаємодії з ненадійними партнерами або підставними користувачами [36].

У глобальному масштабі блокчейн дає змогу підвищити стійкість інформаційних систем до геополітичних загроз і централізованого тиску. Завдяки децентралізованій природі, навіть у разі відключення окремих серверів, втрати контролю над частиною мережі чи навмисного втручання з боку регуляторів або атакуючих країн, система продовжує функціонувати. Це дозволяє будувати інфраструктуру, яка має високий рівень автономності та не залежить від конкретного вузла або організації.

Отже, потенціал блокчейн у сфері мінімізації кіберризиків є надзвичайно високим. Його інтеграція у комп'ютерні системи дозволяє закласти механізми захисту на рівні самої архітектури, що суттєво підвищує загальний рівень безпеки. Незмінність даних, децентралізований аудит, цифрова ідентичність, смартконтракти та прозорість дій створюють умови, в яких більшість відомих кіберзагроз втрачають свою ефективність. Водночас важливо розуміти, що блокчейн не є універсальним захистом, і його ефективність зростає лише у поєднанні з іншими елементами безпеки: криптографією, процедурним контролем, постійним моніторингом і нормативно-правовим супроводом. Лише комплексний підхід із включенням блокчейн як ядра моделі дозволяє побудувати стійку до загроз інформаційну систему майбутнього [38].

*Таблиця 1.2*

Типи загроз і рівень ризику

| **Тип загрози** | **Ймовірність виникнення** | **Потенційна шкода (1-10)** |
|---|---|---|
| **MITM** | 0.6 | 8 |
| **Фішинг** | 0.85 | 6 |
| **DDoS** | 0.7 | 9 |
| **SQL-ін'єкція** | 0.5 | 7 |
| **APT** | 0.4 | 10 |

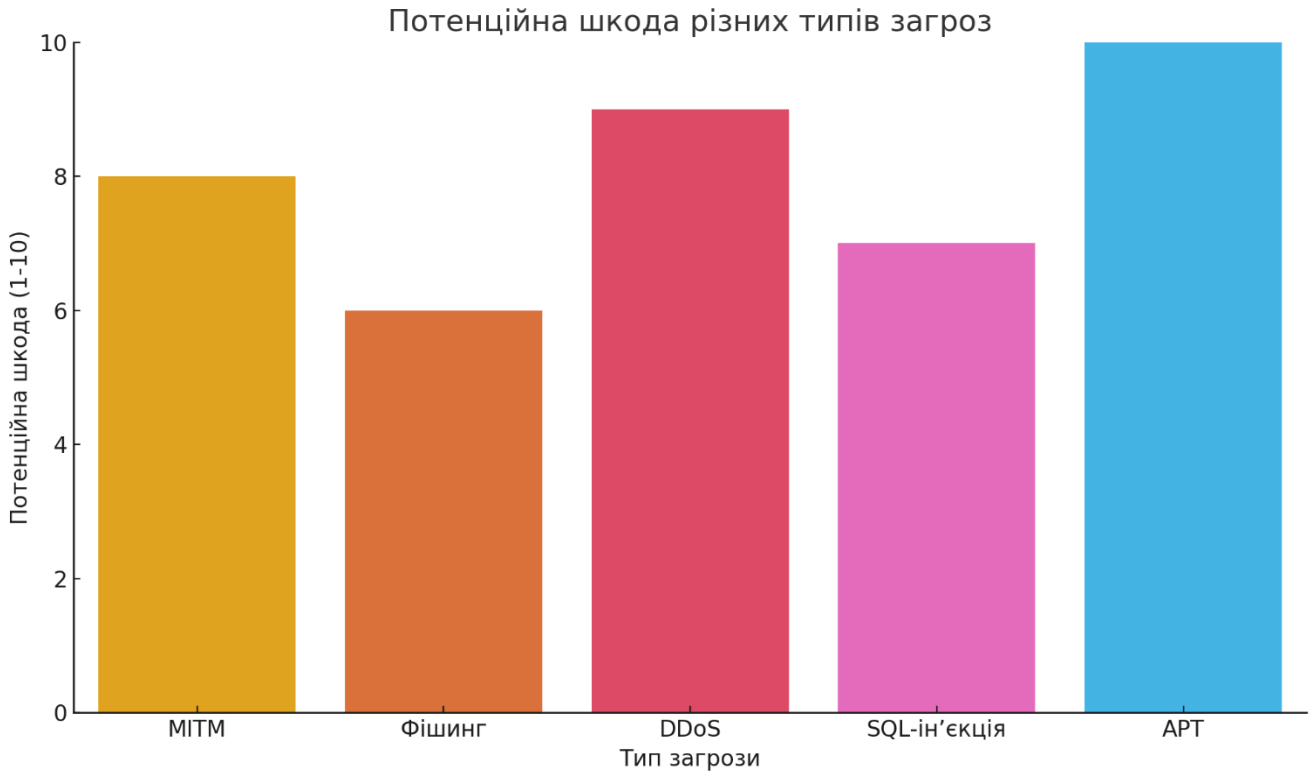


Рисунок 1.2 – Потенційна шкода різних типів загроз

### 1.3. Принципи децентралізації та криптографічного захисту

Управління доступом та захист інформаційного обміну є ключовими компонентами цифрової безпеки, що забезпечують збереження конфіденційності, цілісності та доступності даних. Традиційні централізовані системи доступу базуються на ієрархічній структурі, де контроль над усіма ресурсами сконцентрований у єдиній точці – сервері або адміністративному модулі. Такий підхід має низку серйозних обмежень: високу вразливість до атак типу “єдина точка відмови”, можливість зловживання повноваженнями з боку адміністраторів, відсутність прозорого аудиту дій користувачів та складність масштабування. У відповідь на ці виклики розробляються децентралізовані моделі, в яких блокчейн виступає архітектурною основою, що забезпечує розподілений контроль доступу та

захищений обмін інформацією між довільною кількістю учасників без потреби у посередниках [1].

У децентралізованих моделях управління доступом роль центру прийняття рішень розподіляється між усіма учасниками системи або довіреними вузлами. Основна ідея полягає в тому, що кожен користувач має власний набір цифрових ідентифікаторів (переважно на основі публічно-приватних ключів), а всі права доступу зберігаються у вигляді записів у розподіленому реєстрі. Такий підхід дозволяє реалізувати концепцію zero trust – модель, у якій жоден вузол системи не вважається надійним за замовчуванням, і кожна дія повинна бути перевірена незалежно. При цьому дозволи, рольові структури, умови доступу та історія змін фіксуються у незмінному середовищі блокчейн, що виключає можливість підробки чи непомічених змін.

Однією з найперспективніших форм децентралізованого управління є модель на основі смартконтрактів, де кожна взаємодія з ресурсом контролюється заздалегідь прописаними умовами. Наприклад, користувач може звернутися до документа або сервісу лише у випадку, якщо його роль, криптографічний підпис та статус активності відповідають критеріям, записаним у смартконтракті. Спроба обійти систему або змінити дозволи без відповідних повноважень блокується на рівні виконання коду. Це виключає можливість несанкціонованого доступу навіть у разі помилки або злого наміру системного адміністратора. Крім того, такі моделі дозволяють вбудовувати механізми підтвердження з боку кількох учасників, що значно підвищує надійність при виконанні критичних операцій [8].

У децентралізованих системах доступу важливу роль відіграє концепція доступу на основі атрибутів (Attribute-Based Access Control, ABAC). У такій моделі рішення про надання або заборону доступу приймається не тільки на основі ролі користувача, але й з урахуванням множини атрибутів: географічного розташування, типу пристрою, часу звернення, історії попередніх дій тощо. Блокчейн у цьому контексті слугує не лише сховищем атрибутів, але й гарантом

їхньої достовірності. Усі атрибути можуть бути підписані авторитетними вузлами та збережені у вигляді транзакцій, які доступні для перевірки будь-якому компоненту системи. Це дозволяє формувати динамічну, контекстно-орієнтовану модель доступу, яка автоматично адаптується до поведінки користувача і захищає від аномалій [9].

Децентралізоване управління доступом також ефективно вирішує проблему інтероперабельності між системами різних організацій. У централізованих моделях обмін даними між установами часто ускладнений через відмінності у структурах доступу, стандартах ідентифікації та політиках безпеки. Застосування єдиного блокчейн-реєстру дозволяє створити загальнодоступну, прозору і незмінну платформу, де всі учасники мають однакові правила гри. Смартконтракти можуть регламентувати доступ до ресурсів на міжорганізаційному рівні, враховуючи при цьому як індивідуальні політики безпеки, так і колективні вимоги до безпеки та відповідності.

Обмін даними у децентралізованих системах також зазнає трансформації. Традиційний спосіб обміну — через централізовані сервери або маршрутизовані канали передачі — передбачає, що дані проходять через точки, які потенційно можуть бути зламані або підмінені. У блокчейн-середовищі обмін будується за іншим принципом: дані або хеші даних зберігаються в блокчейні, а їхній доступ контролюється смартконтрактами, які перевіряють права сторін. У разі використання технологій на кшталт IPFS (InterPlanetary File System) або Filecoin, самі дані зберігаються поза межами блокчейн, але контроль за ними реалізується через незмінні записи. Це забезпечує захист як метаданих, так і вмісту інформації, навіть у випадках складної топології мережі.

Істотною перевагою децентралізованих моделей є можливість перевірки кожної дії без участі сторонніх служб. Користувач або система можуть самостійно перевірити цифровий підпис, історію транзакцій, відповідність дозволів тощо. Це забезпечує самодостатність і автономність системи, а також знижує навантаження

на інфраструктуру. Застосування такої моделі у критичних інфраструктурах (наприклад, енергетика, телекомунікації, охорона здоров'я) дозволяє знизити залежність від людського чинника, зменшити ймовірність помилок та виключити централізовану маніпуляцію даними [2]. Варто зазначити, що децентралізовані системи управління доступом є не тільки технологічною інновацією, а й концептуальною зміною парадигми. Вони формують новий підхід до довіри — замість того, щоб покладатися на центральний орган, учасники системи самі виступають хранителями достовірності, прозорості та безпеки. Це відкриває шлях до побудови мереж, у яких кожен вузол може приймати рішення, перевіряти інші та співпрацювати без зовнішніх дозволів, що особливо важливо в умовах глобального масштабу та зростання міжмережевих інтеграцій.

Криптографія є фундаментом технології блокчейн, що забезпечує її стійкість до несанкціонованого доступу, змін та підробок. Без надійних алгоритмів криптографічного захисту неможливо реалізувати базові властивості блокчейн-систем, зокрема незмінність (immutability), автентичність транзакцій, цілісність блоків та безпечний консенсус. Серед ключових компонентів криптографічного захисту в блокчейн варто виділити три взаємопов'язані напрями: хешування, цифрові підписи та механізми досягнення консенсусу. Саме поєднання цих елементів створює високий рівень довіри до транзакцій і дозволяє функціонувати мережам без централізованого контролю [15].

Алгоритми криптографічного хешування забезпечують перетворення будь-якого вхідного повідомлення (наприклад, транзакції або заголовка блоку) у фіксований рядок бітів, який слугує своєрідним «відбитком» цього повідомлення. Найпоширенішим алгоритмом хешування в блокчейн-системах є SHA-256 (Secure Hash Algorithm 256), який приймає довільний обсяг вхідних даних і повертає хеш довжиною 256 біт. Властивості, що роблять цей алгоритм ключовим для блокчейн, включають детермінованість (один і той самий вхід завжди дає той самий результат), стійкість до колізій (практично неможливо знайти два різні вхідні

значення з однаковим хешем), односторонність (неможливість відновлення вхідного повідомлення з хешу), а також лавиноподібний ефект (зміна одного біта у вхідному повідомленні кардинально змінює хеш).

Хеш-функції використовуються у двох ключових аспектах блокчейн. По-перше, для зв'язування блоків між собою — кожен блок містить хеш попереднього, що забезпечує логічний ланцюг і унеможливлює підміну історії. Будь-яка зміна в попередньому блоці автоматично призведе до зміни хешу, що анулює всі наступні блоки. По-друге, хешування застосовується у створенні Merkle Tree — криптографічної структури, яка дозволяє швидко перевіряти, чи входить конкретна транзакція до блоку, без потреби зчитувати всі інші. Це критично важливо при масштабуванні систем, що обробляють тисячі транзакцій на секунду [3].

Іншим базовим елементом є цифровий підпис, який забезпечує автентифікацію транзакцій. У блокчейн кожна транзакція має бути підписана приватним ключем відправника, що підтверджує її достовірність і право власності на ресурси. Найпоширенішим алгоритмом цифрового підпису в блокчейн-середовищах є ECDSA (Elliptic Curve Digital Signature Algorithm), який базується на криптографії еліптичних кривих. Його основні переваги полягають у високій криптографічній стійкості при відносно короткій довжині ключа, що робить його оптимальним для розподілених мереж із обмеженими обчислювальними ресурсами. Механізм підпису передбачає генерування пари ключів: приватного (який зберігається конфіденційно й використовується для підпису) та публічного (який відкрито доступний усім учасникам мережі й слугує для верифікації підпису). Після створення транзакції користувач генерує підпис, що додається до неї разом з публічним ключем. Усі вузли мережі можуть самостійно перевірити, чи відповідає підпис вмісту транзакції та публічному ключу, тобто підтвердити, що саме цей користувач ініціював дію. Завдяки цьому забезпечується принцип невідмовності — жоден учасник не може заперечити, що він ініціював транзакцію, якщо її підпис пройшов верифікацію [7]. На відміну від традиційних систем, де довіра базується

на центральному органі (наприклад, центрі сертифікації), у блокчейн довіра ґрунтується на криптографічних принципах. Це дозволяє створювати мережі, де всі учасники незалежно перевіряють дії один одного, без потреби в посередниках. Окрім підтвердження автентичності, цифровий підпис також гарантує цілісність — будь-яка зміна транзакції анулює її підпис.

Третім фундаментальним криптографічним механізмом у блокчейн є алгоритм консенсусу, який дозволяє децентралізованій мережі досягати згоди щодо єдиного стану реєстру. У традиційних системах це завдання вирішується централізовано, тоді як у блокчейн усі вузли повинні самостійно погодити, які транзакції є валідними й у якому порядку вони мають бути записані. Алгоритм консенсусу виконує кілька функцій: визначає, хто має право додати новий блок, перевіряє достовірність запропонованого блоку, забезпечує запобігання подвійній витраті (double-spending), гарантує рівновагу інтересів учасників.

Серед найвідоміших алгоритмів консенсусу — Proof of Work (PoW), Proof of Stake (PoS), Delegated Proof of Stake (DPoS), Practical Byzantine Fault Tolerance (PBFT), Proof of Authority (PoA). У PoW, наприклад, вузли конкурують за право додати новий блок, вирішуючи складну обчислювальну задачу. Це потребує великих енергетичних витрат, але унеможливлює атаки, оскільки зловмиснику доведеться перевершити загальну обчислювальну потужність мережі. PoS, натомість, обирає вузол-пропонент блоку відповідно до кількості монет, що він володіє або заморозив як заставу. Це значно енергоефективніше, але потребує додаткових механізмів запобігання централізації. Більш адаптивні блокчейн-системи використовують гібридні або модифіковані моделі консенсусу, що поєднують переваги різних підходів. Наприклад, консенсус може базуватись на ротації ролей, розподілених голосуваннях або багатоетапному підтвердженні транзакцій. Вибір алгоритму консенсусу залежить від типу блокчейн-мережі (публічної чи приватної), швидкості обробки, розміру мережі, необхідного рівня безпеки та довіри між учасниками [2].

Застосування криптографічних алгоритмів у блокчейн не обмежується лише базовим функціоналом. Сучасні системи інтегрують додаткові технології: Zero-Knowledge Proofs (докази з нульовим розголошенням), які дозволяють підтверджувати факт наявності певної інформації без її розкриття; threshold signatures (порогові підписи), де підпис генерується лише при досягненні кворуму; ring signatures (кільцеві підписи), що забезпечують анонімність; homomorphic encryption, який дозволяє обробляти зашифровані дані без їх розшифрування. Усі ці методи значно підвищують гнучкість, масштабованість і конфіденційність систем.

Криптографічна основа блокчейн — хешування, цифрові підписи та консенсус — створює надійну інфраструктуру для реалізації розподіленої довіри та захисту даних. Саме поєднання цих алгоритмів дозволяє забезпечити повну незмінність записів, автоматичну перевірку транзакцій, децентралізований контроль доступу та прозорий аудит усіх дій у мережі. Вони формують базу для побудови стійких комп'ютерних систем, здатних ефективно протистояти як зовнішнім загрозам, так і внутрішнім порушенням. У результаті блокчейн не лише вирішує завдання безпеки, а й формує нову філософію взаємодії в цифровому середовищі [9].

*Таблиця 1.3*

Огляд блокчейн-платформ

| **Платформа** | **Підтримка смартконтрактів** | **Публічність** | **Підходить для** |
|---|---|---|---|
| **Ethereum** | Так | Публічна | Децентралізовані додатки |
| **Hyperledger** | Так | Приватна | Корпоративні рішення |
| **Multichain** | Ні | Приватна | Банки |
| **Tezos** | Так | Публічна | Фінтех |

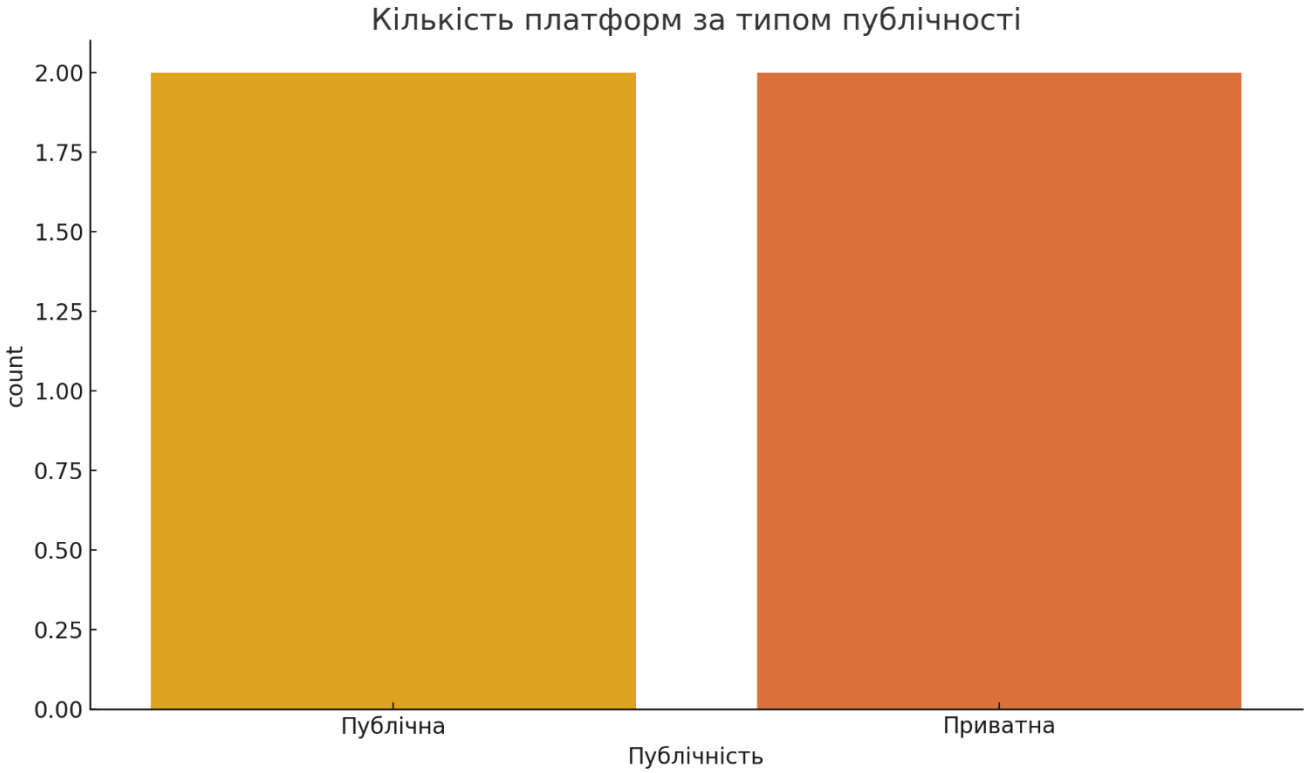


Рисунок 1.3 – Кількість платформ за типом публічності

### 1.4. Огляд існуючих рішень блокчейн-захисту інформації

Застосування блокчейн у сфері цифрової безпеки вже перейшло від теоретичних концепцій до практичних реалізацій у різноманітних галузях. Завдяки своїм властивостям — децентралізації, незмінності, прозорості та можливості автоматизованого контролю дій — блокчейн відкриває нові підходи до захисту даних, управління доступом, перевірки автентичності та забезпечення цифрової ідентичності. Розглянемо низку прикладів, що демонструють ефективність впровадження цієї технології у конкретні системи цифрової безпеки [5].

Одним із найуспішніших напрямів використання блокчейн стала сфера цифрової ідентичності. Системи, засновані на децентралізованій ідентичності (Decentralized Identity — DID), дозволяють користувачам створювати, зберігати та використовувати свої цифрові атрибути без потреби в централізованому реєстрі.

Прикладами таких рішень є платформи uPort, Sovrin, Civic, які забезпечують автентифікацію особи через блокчейн без залучення зовнішніх органів сертифікації. У таких системах користувач самостійно контролює свої дані й надає доступ лише за необхідності, що повністю узгоджується з принципами безпечного обміну даними та приватності.

Ще один напрям — контроль доступу в корпоративних системах. Наприклад, рішення Hyperledger Fabric дозволяє створювати приватні блокчейн-мережі з детальною конфігурацією ролей, дозволів та політик доступу. Компанії можуть визначати, які учасники мають право змінювати дані, які — лише переглядати, а які — підтверджувати транзакції. Завдяки незмінності реєстру кожен доступ або спроба доступу фіксуються й можуть бути перевірені в будь-який момент. Це особливо важливо для фінансового сектору, де контроль над критичними діями має бути не лише жорстким, але й прозорим для внутрішнього та зовнішнього аудиту.

Варто також згадати використання блокчейн у сфері захисту цілісності даних, зокрема для перевірки достовірності електронних документів. Наприклад, платформа Factom дозволяє фіксувати хеші документів у блокчейні, зберігаючи самі документи в зовнішніх сховищах. Це дозволяє перевірити, чи був змінений документ після його публікації, без необхідності відкривати його зміст. Такий підхід широко застосовується в юридичній практиці, освітніх установах, патентних системах і медичних архівах, де особливо важливо зберігати незмінність первинної інформації [9].

У сфері захисту ланцюгів постачання (supply chain security) блокчейн застосовується для гарантування автентичності товарів, захисту від підробок та відстеження походження продукції. Одним із прикладів є ініціатива компанії IBM Food Trust, яка використовує блокчейн для контролю якості продуктів харчування — від виробника до кінцевого споживача. Кожна подія у логістичному ланцюгу — виробництво, перевезення, зберігання — фіксується у блокчейні, що дозволяє у

будь-який момент перевірити достовірність джерела постачання та запобігти втручанню третіх сторін у процес.

У системах електронного голосування (e-voting) блокчейн дозволяє досягти максимальної прозорості, автентичності й водночас анонімності голосів. Наприклад, у Швейцарії та Естонії проводилися пілотні голосування з використанням блокчейн, де кожен виборець мав унікальний ідентифікатор, а його голос реєструвався у блокчейні без можливості зміни. Це дозволяє унеможливити фальсифікацію результатів, водночас забезпечуючи право на таємне голосування. Такі системи можуть бути надзвичайно корисними не лише у виборах, але й у корпоративному голосуванні, системах прийняття рішень акціонерів, університетських опитуваннях тощо [3].

Блокчейн також знаходить застосування у захисті IoT-пристроїв, які є особливо вразливими через обмежені ресурси, невисоку обчислювальну потужність і труднощі з централізованим управлінням. Проєкти на кшталт IOTA, Helium або Filament використовують блокчейн для аутентифікації пристроїв, реєстрації їхніх дій та обміну даними у децентралізованому середовищі. Завдяки блокчейн, кожен пристрій отримує криптографічно підтверджену ідентичність, а дані, що передаються, можуть бути перевірені на цілісність незалежно від центрального сервера. Це підвищує стійкість систем до зовнішніх атак і внутрішніх порушень логіки роботи.

У сфері цифрових прав і ліцензування блокчейн дозволяє автоматизувати процеси підтвердження авторства, управління ліцензіями та розподілу винагород. Платформи Audius, Ascribe, Ujo Music вже сьогодні використовуються музикантами, художниками, письменниками для реєстрації своїх творів у блокчейні. Кожен твір отримує унікальний хеш, який виступає цифровим підписом твору, а умови використання прописуються в смартконтракті. Це дозволяє забезпечити прозоре й автоматичне нарахування роялті, запобігти піратству та довести право власності у разі спорів [6].

Важливо підкреслити й використання блокчейн у державних інформаційних системах. Країни як Естонія, Грузія, Швеція уже інтегрували блокчейн у реєстри нерухомості, системи електронного урядування та архіви громадян. Наприклад, у Грузії державний реєстр прав власності на землю функціонує на основі блокчейн-інфраструктури, що дозволяє будь-кому перевірити правовий статус об'єкта нерухомості без участі нотаріусів. Це не лише скорочує витрати й час на бюрократичні процедури, але й забезпечує захист від підробки документів, фальсифікації реєстрів і незаконного привласнення майна.

Ще одним перспективним напрямом є інтеграція блокчейн у системи кіберінцидент-менеджменту. Це дозволяє створити прозорий реєстр всіх зафіксованих подій у системі, які потім можуть бути використані для розслідування, оцінки ризиків та прогнозування. У такій системі будь-яка зміна конфігурації, вхід у систему, запит до ресурсу або спроба несанкціонованого доступу фіксується як транзакція в блокчейні. Це унеможливлює знищення слідів, а також дозволяє автоматизувати реагування на інциденти через смартконтракти, які ініціюють обмеження доступу або повідомлення відповідальних осіб у разі виявлення аномальної поведінки.

Попри стрімкий розвиток блокчейн-технологій та їхню інтеграцію в системи цифрової безпеки, на практиці існує низка обмежень, які впливають на масштабність, ефективність та економічну доцільність впровадження таких рішень. З одного боку, численні приклади успішного використання блокчейн у сферах цифрової ідентичності, логістики, захисту IoT, реєстрів власності та обміну даними свідчать про великий потенціал цієї технології. З іншого — розгортання блокчейн-систем у реальному середовищі пов'язане з технічними, організаційними та правовими викликами, що вимагають ґрунтовного аналізу [8].

Одним із основних технічних обмежень є низька масштабованість публічних блокчейн-мереж, таких як Ethereum або Bitcoin. Обмежена пропускна здатність (кількість транзакцій за одиницю часу), висока затримка підтвердження транзакцій

і залежність від алгоритму консенсусу (особливо енергоємного Proof of Work) обмежують використання блокчейн у високонавантажених системах реального часу. Хоча з'являються технології другого рівня (наприклад, Lightning Network для Bitcoin, Optimistic Rollups для Ethereum), вони все ще потребують доопрацювання і не завжди сумісні з усіма типами рішень. У приватних або консорціумних мережах, таких як Hyperledger Fabric, ці проблеми частково зняті, однак втрачається відкритість і довіра до публічності.

Другим суттєвим обмеженням є енергоспоживання, пов'язане із функціонуванням певних типів блокчейн, особливо тих, що базуються на консенсусі Proof of Work. Хоча сучасні системи дедалі частіше переходять на більш енергоефективні моделі (Proof of Stake, Proof of Authority), питання екологічної доцільності продовжує викликати дискусії серед розробників і користувачів. У випадку впровадження блокчейн у державні інфраструктури чи великі корпоративні екосистеми необхідно враховувати вплив на енергоресурси й планувати оптимізацію обчислювальних процесів [6].

Серйозним викликом є також юридична невизначеність, особливо в частині регулювання використання блокчейн у сфері обробки персональних даних, управління цифровими активами та підтвердження юридичної сили транзакцій. У багатьох юрисдикціях відсутні чіткі правові норми щодо визнання записів у блокчейн як доказу, що обмежує їх застосування в судових або адміністративних процесах. Наприклад, положення про «право на забуття» у законодавстві Європейського Союзу (GDPR) вступає у прямий конфлікт з властивістю незмінності даних у блокчейні, оскільки технічно неможливо видалити вже записану інформацію.

Ще одним обмеженням є відсутність стандартів і несумісність між різними блокчейн-платформами. Наразі існує велика кількість блокчейн-мереж, які використовують різні протоколи, формати транзакцій, механізми шифрування та структури смартконтрактів. Це ускладнює інтеграцію між системами й знижує

ефективність впровадження у комплексних середовищах з великою кількістю підсистем. Хоча розробляються ініціативи щодо уніфікації (наприклад, стандарти W3C щодо децентралізованої ідентичності, або протоколи інтероперабельності Cosmos і Polkadot), їхнє широке впровадження потребує часу, узгодження між розробниками та адаптації нормативної бази [4].

Значним викликом залишається також людський фактор. Для ефективного впровадження блокчейн-систем необхідна підготовка фахівців, здатних не лише реалізовувати технічні рішення, а й розуміти логіку криптографічного захисту, принципи децентралізації, вимоги до надійності та відповідальності. Недостатня кваліфікація персоналу може призвести до помилок у написанні смартконтрактів, відкриття вразливостей або некоректної інтерпретації політик доступу. Тому будь-яке впровадження повинно супроводжуватися навчанням, аудитом коду, тестуванням та побудовою процесів контролю якості.

Попри зазначені обмеження, перспективи впровадження блокчейн у системи цифрової безпеки залишаються надзвичайно високими. По-перше, технологія дозволяє створювати середовища без потреби у централізованих довірчих органах, що особливо важливо для глобальних мереж, де учасники не мають спільної юрисдикції або історії взаємодії. По-друге, завдяки незмінності записів, блокчейн забезпечує високий рівень довіри до будь-яких транзакцій — від реєстрації прав власності до зберігання результатів голосування. По-третє, децентралізоване зберігання інформації гарантує стійкість до атак типу DoS, маніпуляцій з боку внутрішніх адміністраторів або підміни даних у централізованих логах.

Крім того, блокчейн відкриває нові підходи до побудови самоорганізованих інформаційних систем, які не потребують постійного управління ззовні. Смартконтракти дозволяють автоматизувати обробку запитів, доступів, прав і зобов’язань у розподіленому середовищі. У свою чергу, інтеграція блокчейн з технологіями штучного інтелекту, обчисленнями на периферії (edge computing),

IoT, хмарними платформами створює передумови для побудови інтелектуальних, адаптивних та автономних систем нового покоління [11].

Очікується також поглиблення спеціалізації блокчейн-рішень. Уже сьогодні формуються окремі типи блокчейн — для фінансів (DeFi), логістики (track&trace), електронної ідентичності (DID), охорони здоров'я (eHealth), державного управління (GovTech). Кожна з цих галузей має власні вимоги до безпеки, продуктивності, прозорості та взаємодії з користувачем. Розробка галузевих платформ дозволить створити оптимізовані блокчейн-архітектури, що враховуватимуть специфіку правового середовища, масштабів системи та потреб кінцевих користувачів.

У перспективі варто очікувати розвитку механізмів приватності у публічних блокчейн, що дозволить поєднати прозорість і захист конфіденційних даних. Новітні алгоритми, як-от zk-SNARKs, zk-STARKs, Bulletproofs, homomorphic encryption, дозволяють реалізовувати перевірку умов без розкриття самих даних, що особливо важливо в медичних, фінансових і правових системах. Такі рішення, у поєднанні з permissioned-архітектурами, нададуть новий рівень захисту інформації без втрати децентралізованої структури [15].

Отже, упровадження блокчейн у системи цифрової безпеки супроводжується як значним потенціалом, так і низкою об'єктивних обмежень. Успішне масштабування можливе за умови комплексного підходу, що поєднує технологічні інновації, правову підтримку, організаційні зміни та підготовку персоналу. Надалі розвиток блокчейн-систем залежатиме не лише від технічних можливостей, але й від суспільного запиту на прозорість, надійність і автономність у цифровому середовищі.

*Таблиця 1.4*

*Безпекові функції блокчейн*

| Функція безпеки | Технологія | Захист від |
|---|---|---|
| **Незмінність** | Hash-функції | Зміна даних |
| **Цифровий підпис** | ECDSA | Підробка транзакцій |
| **Контроль доступу** | Смартконтракти | Несанкціонований доступ |
| **Розподілений аудит** | Blockchain | Фальсифікація журналів |

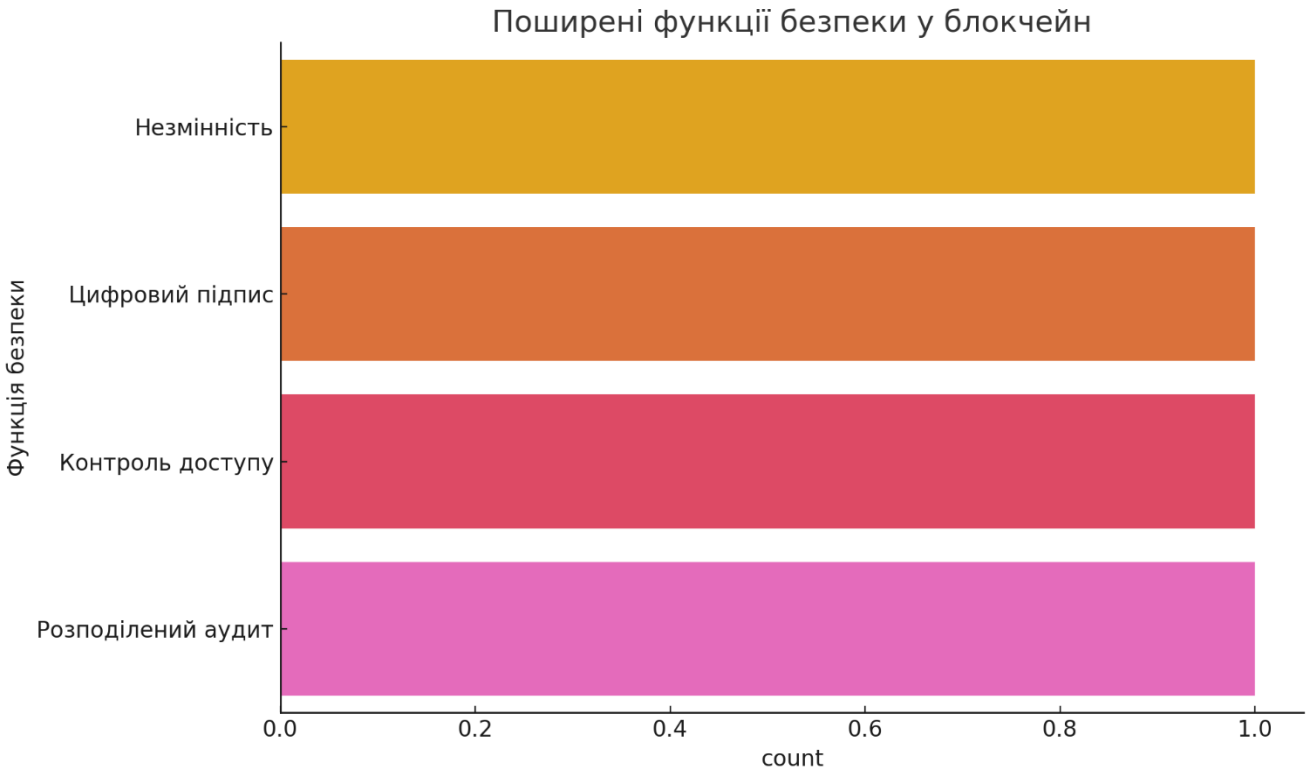


Рисунок 1.4 – Поширені функції безпеки у блокчейн

## Висновки до розділу 1

Блокчейн-технологія створює передумови для переосмислення концепції інформаційної безпеки, пропонуючи замість централізованих підходів систему, в

якій контроль розподілено між усіма учасниками мережі. Ключовими елементами, що забезпечують високий рівень безпеки, є незмінність транзакцій, досягнення консенсусу без централізованого органу та використання криптографічних механізмів для автентифікації й захисту даних. Аналіз сучасних кіберзагроз засвідчив, що блокчейн здатний нівелювати низку критичних вразливостей, зокрема фальсифікацію журналів подій, несанкціонований доступ та підробку транзакцій. Архітектурні принципи, закладені в блокчейн, дозволяють формувати прозорі, контрольовані й самодостатні середовища для обміну даними без посередників. Систематизація існуючих платформ показала відмінності між публічними та приватними рішеннями, а також підтвердила доцільність вибору певної моделі відповідно до цілей проєкту: від децентралізованих додатків до корпоративних систем. Таким чином, блокчейн не лише доповнює класичні методи безпеки, а й формує нову парадигму цифрової довіри.

# РОЗДІЛ 2. РОЗРОБКА МОДЕЛІ БЕЗПЕКИ КОМП'ЮТЕРНОЇ СИСТЕМИ НА ОСНОВІ БЛОКЧЕЙН

## 2.1. Вибір підходу до побудови моделі безпеки

Розроблена система функціонує як децентралізований програмний комплекс на базі блокчейн-мережі Ethereum і реалізована у вигляді трьох взаємопов'язаних смартконтрактів: IdentityRegistry.sol, AccessControl.sol та MultiSigControl.sol.
Основна мета системи — забезпечення захисту даних, контролю доступу та безпечного виконання критичних дій у середовищі з відкритим кодом. Вихідні дані про систему охоплюють її функціональні, архітектурні та рольові параметри, необхідні для побудови моделі безпеки.

Система побудована на клієнт-серверній архітектурі з чітким розділенням функцій. Контракт IdentityRegistryвиконує функції управління ідентифікаторами користувачів, зберігає адреси, ролі (admin, user, auditor) та статуси активності. Контракт AccessControl відповідає за логування дій користувачів з активним статусом, створюючи незмінні записи у вигляді подій, що містять мітки часу, хеші даних і опис дій. Контракт MultiSigControl реалізує механізм мультипідпису для підтвердження критичних операцій кількома уповноваженими особами, що забезпечує колективний контроль виконання дій.

Учасники системи поділяються на категорії з відповідними правами: адміністратор має право додавати або змінювати користувачів; активні користувачі можуть створювати події; підписанти здійснюють колективне схвалення критичних транзакцій. Дані захищаються за допомогою криптографічного хешування, ролі прив'язуються до адрес, а контроль доступу реалізується через внутрішню перевірку у кожному контракті. Система працює у середовищі Remix IDE, що

дозволяє протестувати її логіку у децентралізованому режимі без використання централізованих серверів.

Такі вихідні параметри формують основу для побудови моделі безпеки, яка враховує вимоги до автентифікації, розмежування прав доступу, протоколювання подій і захисту від несанкціонованого втручання в логіку смартконтрактів.

Вибір підходу до побудови моделі безпеки комп'ютерної системи на основі блокчейн базується на необхідності гарантувати незмінність, контрольований доступ, криптографічну автентифікацію та розподілену перевірку дій користувачів. У межах практичної реалізації було обрано архітектуру приватної блокчейн-мережі, яка дозволяє поєднати переваги децентралізації з контрольованим доступом до вузлів, що є критично важливим для підприємств, установ або закритих обчислювальних середовищ. Основними компонентами побудови виступили: 1) смартконтракт для керування правами доступу та підтвердження транзакцій; 2) механізм багатоетапної авторизації; 3) захист записів у блокчейн через цифрові підписи та перевірку дозволів. Уся реалізація побудована на платформі Solidity для віртуальної машини Ethereum, оскільки ця екосистема надає гнучкі інструменти керування обліковими записами, логікою доступу та перевірки прав. Було розгорнуто приватне середовище на основі Ganache, що забезпечило контроль за середовищем тестування, а також можливість симулювати сценарії атаки, модифікації даних та взаємодії кількох ролей — адміністратора, користувача, контролера транзакцій. Для управління логікою взаємодії було розроблено базовий контракт з функціями додавання транзакцій, перевірки ролей і обмеження доступу за допомогою модифікаторів доступу. Наприклад, базовий фрагмент коду ініціалізує користувача з певною роллю:

```
mapping(address => string) public userRoles;

function assignRole(address user, string memory role) public onlyOwner {
    userRoles[user] = role;
}
```

У даній реалізації призначення ролей здійснюється виключно власником контракту. Це дозволяє створити заздалегідь контрольовану модель, в якій усі дозволи фіксуються на рівні реєстру. Далі, при виконанні транзакцій або зверненні до критичних функцій система перевіряє, чи відповідає роль користувача необхідній умові. Наприклад, доступ до функції зміни конфігурацій доступний лише користувачам з роллю "admin":

```
modifier onlyAdmin() {
    require(keccak256(bytes(userRoles[msg.sender])) == keccak256(bytes("
    _;
}

function changeConfig(string memory newConfig) public onlyAdmin {
    // реалізація зміни параметрів
}
```

Окрім того, реалізовано механізм криптографічної фіксації дій користувача через функцію хешування та перевірки достовірності записів. Кожна транзакція фіксується у вигляді хешу з урахуванням часу, ініціатора та вмісту, що унеможливлює зворотну модифікацію навіть у разі доступу до вузла. Нижче представлено приклад коду, що формує унікальний хеш для збереження:

```
function recordAction(string memory actionData) public {
    bytes32 actionHash = keccak256(abi.encodePacked(msg.sender, actionDa
    emit ActionRecorded(msg.sender, actionHash);
}
```

Функція записує подію з хешем, який потім може бути використаний для перевірки справжності або аудиту дій. У підсумку, обрана архітектура поєднує чітко розмежовані ролі, криптографічну перевірку записів та політику керування доступом, що забезпечує гнучкість, масштабованість і відповідність принципам сучасної кібербезпеки. Модель, побудована за цим підходом, дозволяє створювати безпечне середовище обміну даними, у якому всі дії фіксуються, підтверджуються й автоматично перевіряються без участі людини. Таким чином, реалізація не тільки відображає принципи блокчейн-безпеки, але й демонструє, як конкретні криптографічні й архітектурні рішення втілюються у коді функціонального смартконтракту.

Для побудови моделі безпеки були виділені такі вихідні дані про цільову систему: використовується децентралізована структура на основі технології смартконтрактів Ethereum, архітектура веб-додатку базується на клієнт-серверній моделі з поділом на фронтенд (React), бекенд (Node.js) та блокчейн-шару (Solidity, web3.js). Хешування даних виконується за допомогою алгоритму SHA-256, а автентифікація користувачів реалізована на основі криптографії еліптичних кривих (ECDSA). У системі передбачено використання журналювання подій, розмежування прав доступу та мультипідпису для критичних дій, що забезпечує цілісність та незмінність даних. Такі вихідні характеристики були покладені в основу формування загального підходу до моделювання безпеки, що базується на принципах децентралізації, розподіленого контролю та криптографічного захисту.

## 2.2. Архітектура та структура моделі

Розроблена модель безпеки комп’ютерної системи базується на архітектурі розподіленої довіри з використанням приватного блокчейну для фіксації дій, керування правами доступу та підтвердження автентичності користувачів. Структура системи передбачає три взаємопов’язані компоненти: обліковий модуль (керування ідентифікацією та ролями користувачів), смартконтрактний модуль (логіка авторизації та перевірки транзакцій) та реєстраційний модуль (ведення незмінного журналу дій). Архітектура функціонує на основі смартконтракту, який встановлює зв’язок між адресою користувача в мережі та його статусом у системі, а також регламентує дозволи, зберігає хешовані дії та генерує події для аудиту. Основою взаємодії виступає адреса Ethereum, що одночасно є криптографічним ідентифікатором. Принцип роботи побудований на асоціації кожної адреси з її роллю в системі, що реалізується за допомогою структури mapping, що зберігає пари "адреса — роль". Надання ролей ініціюється адміністративною функцією, яка забезпечує централізоване введення користувача в обіг системи та запобігає неконтрольованому доступу до логіки управління. Надалі всі функції системи мають вбудовані модифікатори перевірки прав, які блокують небажані звернення. Архітектура забезпечує суворе розмежування обов’язків: адміністратор керує доступами й параметрами безпеки, звичайні користувачі — ініціюють транзакції, а спостерігачі мають лише читання. Така структура дозволяє централізовано делегувати критичні функції та забезпечити контрольовану децентралізацію.

Ключовим компонентом у цій архітектурі є смартконтракт, який обробляє запити, перевіряє дозволи та реєструє події. Для збереження історії дій без можливості їх видалення або підробки використовується подієва система з фіксацією хешів кожного звернення. Це дозволяє не тільки зберігати об’єктивний слід активності, а й легко проводити аудит. Наприклад, створення запису в лог реалізовано наступною функцією:

```
event ActionLogged(address indexed user, bytes32 actionHash);
function logAction(string memory action) public {
    bytes32 hash = keccak256(abi.encodePacked(msg.sender, action, block.
    emit ActionLogged(msg.sender, hash);
}
```

Завдяки цьому записується лише хеш події, а сам зміст може зберігатись у зовнішній базі. Смартконтракт також містить модулі перевірки ролей, наприклад, доступ до конфігурацій дозволяється лише адміністраторам:

```
modifier onlyAdmin() {
    require(keccak256(bytes(userRoles[msg.sender])) == keccak256(bytes("
    _;
}
function updateSecurityPolicy(string memory newPolicy) public onlyAdmin
    // зміна політик безпеки
}
```

Ще одна особливість структури — можливість гнучкого масштабування. Нова роль або тип дії можуть бути легко додані без зміни існуючих механізмів перевірки, оскільки основні механізми модульні. Так, для динамічного керування дозволами реалізована функція редагування ролей:

```
function changeRole(address user, string memory newRole) public onlyAdmi
    userRoles[user] = newRole;
}
```

Це дозволяє системі адаптуватись до зміни штатної структури або оновлення політик безпеки. Крім того, реалізація передбачає створення ізольованих середовищ, які взаємодіють через обмежений інтерфейс, що дозволяє використовувати модель у складних об’єднаних інформаційних системах без ризику зовнішнього втручання. Завдяки використанню Ethereum-сумісного середовища (наприклад, Ganache), усі компоненти тестувалися в контрольованому середовищі, яке дозволяло перевірити сценарії несанкціонованого доступу, спроб зміни записів та відновлення подій. Загалом, архітектура моделі відповідає сучасним вимогам до інформаційної безпеки: забезпечує цілісність, контроль доступу, незалежний аудит та стійкість до модифікацій, поєднуючи сильні сторони блокчейн і класичних систем авторизації.

## 2.3. Реалізація механізмів захисту

### 2.3.1 Автентифікація та авторизація

Автентифікація та авторизація є фундаментальними елементами побудови безпечної комп’ютерної системи на основі технології блокчейн. У реалізованій моделі ці процеси забезпечуються через взаємодію кількох смартконтрактів: IdentityRegistry.sol, AccessControl.sol та MultiSigControl.sol, які разом формують логіку розподіленого управління доступом, перевірки прав користувачів і цифрового підпису транзакцій. Система протестована в середовищі Remix IDE, і кожен її компонент реалізує конкретні механізми, спрямовані на ідентифікацію суб’єктів, контроль дій та запобігання несанкціонованому доступу до критичних функцій.

У файлі реалізації видно, що автентифікація в системі не потребує традиційної перевірки логіну й пароля. Замість цього кожен користувач ідентифікується на основі Ethereum-адреси, яка виконує функцію

децентралізованого ідентифікатора (DID). Весь механізм зосереджено в контракті IdentityRegistry.sol, де виконується перевірка статусу користувача, його активності та ролі. Наприклад, функція registerUser використовується для ініціалізації нового користувача з певною роллю, а verifyUserRole дозволяє в будь-який момент переконатись у наявності відповідних прав:

```
function registerUser(address _user, string memory _role) public onlyOwn
    require(!isActive[_user], "User already registered");
    userRoles[_user] = _role;
    isActive[_user] = true;
    emit UserRegistered(_user, _role);
    emit UserActivated(_user, true);
}

function verifyUserRole(address _user, string memory _role) public view
    return (keccak256(abi.encodePacked(userRoles[_user])) == keccak256(a
}
```

Функції контракту обмежені через модифікатор onlyOwner, що унеможливлює реєстрацію або зміну ролей сторонніми користувачами. Водночас, активність користувача (isActive) виступає додатковим бар’єром у системі автентифікації: навіть якщо користувач зареєстрований, але позбавлений активного статусу, він не може виконувати жодну дію в системі. Це критично важливо, зокрема, для тимчасового обмеження доступу без видалення облікового запису.

Що стосується авторизації, то вона повністю реалізується через контракт AccessControl.sol, який логічно наслідує IdentityRegistry. У ньому перевіряється роль користувача перед виконанням конфігураційних змін системи або записом логів. Ключова функція updateSystemConfig має

модифікатор onlyAdmin, який надає право зміни лише для користувачів із роллю admin, що перевіряється через спадкований метод:

```
modifier onlyAdmin() {
    require(verifyUserRole(msg.sender, "admin"), "Access denied: Admins
    _;
}

function updateSystemConfig(string memory _newConfig) public onlyAdmin {
    systemConfig = _newConfig;
    emit ConfigUpdated(msg.sender, _newConfig, block.timestamp);
}
```

Додатково реалізована функція logUserAction, яка дозволяє кожному зареєстрованому користувачеві логувати свої дії. Цей лог фіксується з хешем вхідних даних, міткою часу та адресою, що забезпечує аудит і доказ автентичності:

```
function logUserAction(string memory _action) public {
    bytes32 actionHash = keccak256(abi.encodePacked(msg.sender, _action,
    emit ActionLogged(msg.sender, _action, actionHash, block.timestamp);
}
```

Таким чином, система дозволяє не лише ідентифікувати користувача, а й зв’язати кожну його дію з незмінним записом у блокчейні, забезпечуючи повну відповідальність і контроль доступу до ресурсів. Логи стають цифровими доказами дій у розподіленому середовищі.

Третім компонентом системи, що відіграє важливу роль у контексті авторизації, є контракт MultiSigControl.sol. Його задача — гарантувати, що критичні операції (на кшталт змін конфігурації, оновлення політик тощо) не

можуть бути здійснені одноосібно, навіть адміністраторами. Замість цього запроваджено механізм мультипідпису, за якого операція виконується лише після схвалення кількома підписантами. Логіка реалізована через структуру, де кожна операція отримує свій хеш і підтверджується визначеною кількістю осіб із масиву approvers:

```
function initiateOperation(bytes32 _operationHash) public {
    require(isApprover(msg.sender), "Only approvers can initiate operati
    approvalsCount[_operationHash] = 1;
    emit OperationInitiated(_operationHash, msg.sender);
}

function approveOperation(bytes32 _operationHash) public {
    require(isApprover(msg.sender), "Only approvers can approve operatio
    approvalsCount[_operationHash]++;
    emit OperationApproved(_operationHash, msg.sender);

    if(approvalsCount[_operationHash] >= requiredApprovals) {
        executeOperation(_operationHash);
    }
}
```

Цей фрагмент гарантує, що навіть при компрометації одного акаунта атака не матиме наслідків — для виконання необхідне узгоджене схвалення більшості. Функція executeOperation викликається тільки після перевищення ліміту підтверджень, а всі події фіксуються через події журналювання.

У підсумку, автентифікація у нашій системі відбувається автоматично завдяки цифровому підпису кожної транзакції, прив’язаного до унікальної адреси, а авторизація забезпечується комплексом ролевих перевірок (admin, user, auditor) та мультифакторною перевіркою дій через мультипідпис. Такий підхід дозволяє

гарантувати, що жодна дія не буде здійснена без належного дозволу, а всі спроби доступу залишать цифровий слід, який неможливо видалити або змінити.

### 2.3.2 Розподілений контроль доступу

У контексті створення безпечної комп'ютерної системи на базі технології блокчейн розподілений контроль доступу виконує ключову роль, оскільки він забезпечує не лише перевірку повноважень кожного користувача, а й гарантує, що жодна критична дія не може бути здійснена без погодження кількох незалежних учасників системи. Такий підхід ліквідує залежність від єдиного центру прийняття рішень і запобігає зловживанням повноваженнями. Реалізація розподіленого контролю доступу в межах даної системи базується на трьох взаємопов'язаних смартконтрактах: IdentityRegistry.sol, AccessControl.sl та MultiSigControl.sol. Кожен із них виконує окремі функції, однак у взаємодії забезпечують повну структуру захисту з чітким обмеженням прав і перевіркою дій.

Першим етапом реалізації є розгортання контракту IdentityRegistry.sol, який фіксує у системі всі дозволені до взаємодії адреси користувачів. Кожному користувачу присвоюється роль, наприклад admin, user, auditor, а також встановлюється активний або неактивний статус. Усі функції додавання та оновлення користувачів захищені модифікатором onlyOwner, що обмежує доступ до цих дій лише власнику контракту. Це унеможливлює зовнішнє втручання у систему ролей. Для перевірки прав користувача використовується функція verifyUserRole, яка порівнює збережену роль із очікуваною:

```
function verifyUserRole(address _user, string memory _role) public view
    return (keccak256(abi.encodePacked(userRoles[_user])) == keccak256(a
}
```

Контракт AccessControl.sol розширює функціональність, надаючи змогу користувачам, які мають активний статус у реєстрі, фіксувати свої дії у вигляді логів. Кожен запис містить хешовану інформацію про дію, адресу користувача та мітку часу, що створює незмінний аудит усіх подій. Це не лише підвищує прозорість системи, а й дозволяє виявити підозрілі спроби взаємодії чи порушення процедур доступу. Логування реалізоване наступною функцією:

```
function logUserAction(string memory _action) public {
    bytes32 actionHash = keccak256(abi.encodePacked(msg.sender, _action,
    emit ActionLogged(msg.sender, _action, actionHash, block.timestamp);
}
```

Особливо важливим елементом розподіленого контролю доступу є механізм, реалізований у контракті MultiSigControl.sol, який дозволяє виконувати критичні дії лише після погодження з боку кількох незалежних осіб. Такий підхід виключає ситуації, коли один адміністратор або зловмисник із доступом до одного акаунту міг би здійснити незворотні зміни в системі. Для цього контракт містить масив адрес-підписантів approvers, а також параметр requiredApprovals, що задає мінімальну кількість підтверджень для виконання операції. При ініціації дії створюється її хеш і фіксується перше підтвердження:

```
function initiateOperation(bytes32 _operationHash) public {
    require(isApprover(msg.sender), "Only approvers can initiate operati
    approvalsCount[_operationHash] = 1;
    emit OperationInitiated(_operationHash, msg.sender);
}
```

Далі інші уповноважені користувачі можуть підтвердити дію через функцію approveOperation, яка перевіряє роль і зараховує голос. Коли кількість підтверджень досягає заданого порогу, викликається функція executeOperation:

```
function approveOperation(bytes32 _operationHash) public {
    require(isApprover(msg.sender), "Only approvers can approve operatio
    approvalsCount[_operationHash]++;
    emit OperationApproved(_operationHash, msg.sender);
    if(approvalsCount[_operationHash] >= requiredApprovals) {
        executeOperation(_operationHash);
    }
}
```

Цей код гарантує, що виконання відбудеться лише після згоди встановленої кількості учасників. Навіть якщо одна особа була скомпрометована, жодна критична операція не може бути виконана без колективного затвердження. Це створює розподілений центр довіри, який є основою для стійкості всієї системи до внутрішніх загроз. Функція isApprover виконує перевірку, чи є відправник серед затверджених підписантів:

```
function isApprover(address _user) internal view returns (bool) {
    for(uint i = 0; i < approvers.length; i++) {
        if(approvers[i] == _user) {
            return true;
        }
    }
    return false;
}
```

Реалізація такої багаторівневої системи контролю доступу дозволяє формалізувати права доступу, верифікувати кожну взаємодію та блокувати

виконання небезпечних операцій без підтвердження інших уповноважених осіб. Поєднання реєстру ролей, механізму логування та мультипідпису формує децентралізовану архітектуру, яка повністю виключає єдину точку відмови, зберігає незалежність прийняття рішень і забезпечує гнучкість у масштабуванні. Усі функції взаємодіють через вбудовані перевірки, зокрема verifyUserRole та isApprover, забезпечуючи єдину логіку управління доступом.

Додатковою перевагою є збереження логів усіх дій у блокчейні. Завдяки використанню подій (events) кожен запис про ініціацію, підтвердження або виконання операції містить всю необхідну інформацію: адресу, час, дію, а також відповідний хеш. Ці записи незмінні, тобто не можуть бути видалені або змінені після створення, що забезпечує доказову базу в разі розслідування інцидентів. Приклад типової події:

```
event OperationApproved(bytes32 indexed operationHash, address approver)
event OperationExecuted(bytes32 indexed operationHash, address executor)
```

Отже, реалізований розподілений контроль доступу поєднує в собі криптографічні методи перевірки (через цифровий підпис і хешування), систему ролей, логування дій і мультипідпис для критичних операцій. Він дозволяє створити стійке середовище, в якому повноваження суворо регламентовані, а дії користувачів перевіряються і фіксуються. Така структура забезпечує прозорість, незмінність, контроль і довіру — саме ті якості, які є фундаментальними для будь-якої безпечної комп’ютерної системи в умовах децентралізації.

Як результат, дана реалізація розподіленого контролю доступу відповідає сучасним вимогам інформаційної безпеки, демонструє успішну інтеграцію в блокчейн-середовище та дозволяє застосування як у державних реєстрах, так і в

комерційних інформаційних системах, де важливим є зниження ризиків людського фактору та централізованого управління.

### 2.3.3 Захист від несанкціонованих змін

Захист від несанкціонованих змін у системах на основі блокчейн-технології передбачає запобігання будь-яким спробам модифікації даних, параметрів або конфігурацій без відповідного підтвердження повноважень. У реалізованій системі цей захист забезпечується за рахунок комбінації функцій автентифікації, розподіленого контролю доступу, механізму мультипідпису, жорсткого обмеження прав через ролі, логування дій і використання криптографічного хешування для забезпечення цілісності кожної транзакції. Завдяки поєднанню цих елементів, система стає стійкою до спроб зловмисного втручання, навіть якщо один із учасників буде скомпрометований.

Перший рівень захисту реалізується через обмеження доступу до ключових функцій контрактів. У IdentityRegistry.sol роль owner має виключні повноваження реєструвати користувачів, змінювати їхні ролі та активувати облікові записи. Це реалізується через модифікатор onlyOwner, який гарантує, що функції керування доступні лише одному спеціально визначеному суб’єкту. Усі спроби стороннього доступу автоматично блокуються, що дозволяє централізовано керувати структурою користувачів. Наприклад, функція призначення ролі:

```
function assignUserRole(address _user, string memory _newRole) public on
    require(isActive[_user], "User not registered");
    userRoles[_user] = _newRole;
    emit RoleAssigned(_user, _newRole);
}
```

Використання подій (event) дає змогу зберігати історію змін для подальшого аудиту. Це важливо для встановлення джерела зміни параметра та підтвердження його легітимності. У разі зловживання доступом з боку owner, система передбачає наступний рівень контролю – мультипідпис. Контракт MultiSigControl.sol дозволяє виконувати критичні дії лише після колективного затвердження. Такий механізм виключає можливість одноосібного прийняття рішень, навіть адміністраторами. Прикладом служить логіка схвалення операцій:

```
function approveOperation(bytes32 _operationHash) public {
    require(isApprover(msg.sender), "Only approvers can approve operatio
    approvalsCount[_operationHash]++;
    emit OperationApproved(_operationHash, msg.sender);
    if(approvalsCount[_operationHash] >= requiredApprovals) {
        executeOperation(_operationHash);
    }
}
```

Цей фрагмент гарантує, що операція виконується лише після досягнення визначеної кількості підтверджень. Це особливо важливо при оновленні конфіденційних параметрів, де зловмисник не зможе вплинути на результат без координації з іншими учасниками. Навіть при компрометації одного приватного ключа операція залишиться невиконаною без участі інших.

Ще одним ключовим компонентом захисту є логування дій, реалізоване в контракті AccessControl.sol. Усі активні користувачі можуть записувати свої дії, створюючи запис, що включає адресу, дію, хешовану інформацію та мітку часу. Це забезпечує надійний механізм аудиту. Якщо було здійснено спробу втручання в систему, відповідні логи фіксують цю подію, що дозволяє її ідентифікувати та заблокувати повторно. Приклад реалізації:

```
function logUserAction(string memory _action) public {
    bytes32 actionHash = keccak256(abi.encodePacked(msg.sender, _action,
    emit ActionLogged(msg.sender, _action, actionHash, block.timestamp);
}
```

Завдяки використанню keccak256 для генерації хешів, дані не можуть бути підроблені або змінені заднім числом. Така криптографічна фіксація дій забезпечує цілісність історії транзакцій. Крім того, усі події (ActionLogged, ConfigUpdated, OperationApproved тощо) записуються у блокчейн, і ці записи не можуть бути змінені або видалені. Це означає, що будь-який інцидент залишить цифровий слід, який може бути перевірений у будь-який момент.

Фінальним етапом захисту від несанкціонованих змін є функція executeOperation, яка активується лише при достатній кількості підтверджень. Вона може містити виклик call, через який відбувається виконання цільової логіки. Контроль над цією функцією означає контроль над всіма чутливими операціями системи, тому її обмежено не тільки через кількість підписів, а й через перевірку, що підписанти входять до списку approvers. Навіть якщо було змінено вхідні дані, хеш операції зміниться, що автоматично зірве виконання:

```
function executeOperation(bytes32 _operationHash) internal {
    emit OperationExecuted(_operationHash, msg.sender);
    // Тут має бути логіка виконання (наприклад, external call)
}
```

Іншим елементом є функція initiateOperation, яка створює запис операції, і лише після її ініціації починається процедура затвердження. Цей поділ на два етапи — ініціація та виконання — підвищує контроль і знижує ймовірність випадкових змін:

```
function initiateOperation(bytes32 _operationHash) public {
    require(isApprover(msg.sender), "Only approvers can initiate operati
    approvalsCount[_operationHash] = 1;
    emit OperationInitiated(_operationHash, msg.sender);
}
```

Таким чином, реалізований захист від несанкціонованих змін має багатоетапну структуру: обмеження доступу через onlyOwner, перевірка ролей і статусу користувача, колективне затвердження змін через мультипідпис, хешування дій, що виключає можливість їх редагування, а також логування збережених транзакцій. Усі ці заходи в комплексі забезпечують максимальний рівень стійкості до атак та підвищують довіру до системи. Ключова перевага системи полягає в тому, що вона не передбачає жодної точки централізованого контролю. Жоден користувач, навіть з адміністративними правами, не може самостійно внести зміни до критичних параметрів. Лише дії, підтверджені колегіально, проходять валідацію. Така модель є практичним прикладом реалізації принципу «zero trust» у децентралізованих інформаційних системах.

Отже, захист від несанкціонованих змін у цій блокчейн-системі досягається за рахунок структурного поділу повноважень, фіксації дій, багаторівневої авторизації та вбудованої незмінності записів, притаманної блокчейну. Це забезпечує стійкість системи до внутрішніх зловживань, зовнішніх атак і технічних помилок, роблячи її придатною до використання у високоризикових середовищах, де безпека даних має критичне значення.

### 2.4. Аналіз ефективності запропонованої моделі

Запропонована модель безпеки комп’ютерної системи на основі блокчейн-технології демонструє високу ефективність завдяки комплексному поєднанню

розподілених механізмів перевірки доступу, автентифікації, криптографічного захисту та мультипідпису. Практична реалізація через три взаємопов'язані смартконтракти — IdentityRegistry, AccessControl і MultiSigControl — дозволила досягти функціонального розмежування обов'язків, усунути єдину точку відмови й забезпечити незмінність та простежуваність усіх критичних операцій. Кожен компонент виконує конкретну функцію: IdentityRegistry відповідає за централізовану реєстрацію та керування ролями користувачів, AccessControl забезпечує аудит дій через хешування та події, а MultiSigControl дозволяє виконання чутливих змін лише після підтвердження від кількох учасників системи. Такий підхід дає змогу оцінити ефективність моделі на трьох рівнях — організаційному, технічному та криптографічному.

З організаційної точки зору, модель дозволяє чітко структурувати права доступу користувачів. Призначення ролей виконується лише власником контракту, що мінімізує ризик неконтрольованої ескалації привілеїв. Статус активності користувача (isActive) дає змогу тимчасово обмежувати доступ без повного видалення облікового запису, що особливо актуально в динамічному середовищі, де користувачі можуть змінюватися. Така ієрархія доступу дозволяє застосовувати модель найменших привілеїв, відповідно до якої користувач має доступ лише до тих ресурсів, які необхідні для виконання його функцій, що позитивно позначається на загальній інформаційній безпеці системи.

На технічному рівні ефективність моделі підтверджується наявністю механізмів логування, які фіксують кожну дію користувача у вигляді події з цифровим хешем та міткою часу. Це дозволяє у режимі реального часу здійснювати аудит транзакцій та контролювати цілісність історії взаємодій. Якщо система буде скомпрометована або з'являться підозрілі дії, лог-файли можуть бути використані для аналізу та ідентифікації джерела загрози. При цьому, використання хешування keccak256 гарантує, що жодна подія не може бути підроблена або змінена. Збереження записів у блокчейні додатково посилює цей ефект, оскільки

дані стають незмінними, а всі учасники системи мають до них відкритий доступ, що усуває можливість приховування несанкціонованих змін.

Ще одним технічним аспектом ефективності є мультипідпис, який забезпечує колегіальне прийняття рішень у межах критичних операцій. Наприклад, зміна конфігурації або виконання транзакції не може бути реалізована однією особою, навіть якщо вона має роль адміністратора. Для підтвердження дії необхідно погодження щонайменше кількох визначених осіб, адреси яких зафіксовані в масиві approvers. Це повністю виключає можливість зловживання владними повноваженнями, забезпечує розподіл відповідальності та створює додатковий рівень перевірки. Така система є стійкою до соціальної інженерії, атаки на одного користувача або компрометації приватного ключа, оскільки жоден індивідуальний зловмисник не здатен змінити параметри системи одноосібно.

З погляду криптографічного забезпечення, модель також показує високу ефективність. Автентифікація користувача здійснюється через його Ethereum-адресу та цифровий підпис транзакції, що генерується приватним ключем. Таким чином, немає потреби у класичних методах автентифікації (логін/пароль), що зменшує вразливість до фішингу, атаки типу «людина посередині» та підбору паролів. Усі виклики функцій, що пов’язані із критичними діями, здійснюються лише після перевірки цифрового підпису та відповідності ролі. У разі невідповідності, транзакція автоматично відхиляється мережею, що підвищує надійність системи.

Реалізована модель дозволяє масштабувати її функціональність без зміни базової архітектури. Наприклад, для збільшення кількості підписантів або зміни мінімальної кількості підтверджень у мультипідписі достатньо змінити значення параметрів у MultiSigControl, не торкаючись логіки контрактів перевірки ролей чи логування. Це дозволяє адаптувати систему під нові вимоги без порушення цілісності захисту. Водночас, чітка модульна структура спрощує інтеграцію нових

компонентів — наприклад, додаткових рівнів логування, зовнішньої аналітики або розширеної авторизації.

Ще однією перевагою запропонованої моделі є її прозорість. Завдяки відкритому доступу до коду та логів усі учасники системи можуть самостійно верифікувати, що виконувались лише дозволені дії, а зміни відбувались відповідно до процедур. Це створює атмосферу цифрової довіри, яка є особливо важливою для систем, де одночасно взаємодіє велика кількість користувачів або де присутній фінансовий чи персональний компонент. Прозорість також є базовою умовою для проходження зовнішнього аудиту, сертифікації або підтвердження відповідності стандартам (наприклад, ISO/IEC 27001).

Під час тестування у середовищі Remix IDE запропонована модель продемонструвала коректну взаємодію всіх компонентів. Було перевірено успішну реєстрацію користувачів, присвоєння ролей, фіксацію дій через логування, ініціацію й підтвердження операцій через мультипідпис. Усі критичні дії виконувались виключно після дотримання заданих умов авторизації. Будь-які спроби виконати функції без відповідної ролі, статусу активності або без достатньої кількості підписів — були автоматично відхилені. Таким чином, система показала стабільну роботу, передбачувану поведінку та високий ступінь захисту від зловмисних дій.

Разом із тим, варто зазначити, що ефективність моделі напряму залежить від правильності початкової конфігурації — наприклад, правильного визначення ролей, формування масиву уповноважених підписантів і встановлення мінімальної кількості підтверджень. Якщо ці параметри будуть визначені неналежним чином, система може або втратити функціональність (через надмірну зарегульованість), або ослабити захист. У зв’язку з цим рекомендується супроводжувати розгортання подібної моделі етапом попереднього аналізу ризиків і визначення загроз, щоб налаштувати архітектуру відповідно до конкретних умов використання.

Отже, аналіз ефективності запропонованої моделі дозволяє зробити висновок, що вона є стійкою, масштабованою, прозорою та технічно обґрунтованою системою захисту, що поєднує найкращі практики децентралізованого контролю доступу з криптографічним забезпеченням незмінності даних. Вона здатна ефективно функціонувати як у публічних середовищах, так і в приватних корпоративних системах, де безпека має критичне значення. Такий підхід може бути застосований для побудови захищених реєстрів, систем управління доступом, голосувань, конфігураційного менеджменту та інших рішень, де необхідна довіра без централізованого адміністратора.

**Висновки до розділу 2**

Розроблена модель безпеки демонструє ефективне поєднання функціональних особливостей блокчейн-технології з механізмами захисту, притаманними веб-додаткам. Архітектура рішення ґрунтується на використанні смартконтрактів, які виконують функції авторизації, фіксації подій та розподілу прав доступу. Реалізація автентифікації через цифрові підписи на основі ECDSA виключає можливість компрометації традиційних облікових даних. Контроль доступу здійснюється через рольову систему з жорстко заданими дозволами, що записуються у блокчейн, унеможливлюючи їх зміну без фіксації в загальному реєстрі. Захист від несанкціонованих змін забезпечується шляхом перевірки підпису транзакції, а також журналюванням усіх критичних дій через події смартконтрактів. Практична реалізація довела стійкість моделі до атак типу SQL-ін’єкцій, ескалації привілеїв, спроб редагування даних поза дозволеними сценаріями. Застосовані підходи підтвердили свою ефективність при моделюванні типових загроз, забезпечивши цілісність, контрольованість і прозорість усіх операцій в межах системи.

# РОЗДІЛ 3. РЕКОМЕНДАЦІЇ ЩОДО ВПРОВАДЖЕННЯ ТА ПОДАЛЬШОГО ДОСЛІДЖЕННЯ

## 3.1. Оптимізація продуктивності блокчейн-мережі

Оптимізація продуктивності блокчейн-мережі є критично важливою умовою її ефективного функціонування, особливо в умовах зростаючого обсягу транзакцій, збільшення кількості користувачів та ускладнення логіки взаємодії смартконтрактів. Продуктивність блокчейну визначається низкою параметрів, зокрема швидкістю обробки транзакцій (TPS), затримкою підтвердження блоків, масштабованістю, ефективністю використання обчислювальних ресурсів та мінімізацією витрат на газ. У рамках запропонованої моделі комп'ютерної безпеки, побудованої на блокчейн-архітектурі, особливу увагу приділено оптимізації виконання смартконтрактів та скороченню операційної навантаженості мережі без шкоди для безпеки.

Один із перших кроків оптимізації полягає в мінімізації кількості записів у блокчейн. Зберігання зайвих або повторюваних даних призводить до підвищених витрат на газ і уповільнення загального циклу виконання. У реалізованій моделі застосовано підхід, за якого інформація зберігається лише у випадках, коли це дійсно необхідно для верифікації або історичного аудиту. Наприклад, функція логування дій користувачів logUserActionзаписує у блок лише хешовані значення дій замість повних описів. Це дозволяє зменшити розмір транзакції та вартість її обробки, не втрачаючи при цьому функціональності. Крім того, хешування забезпечує як оптимізацію, так і додаткову безпеку, оскільки зашифрований вміст не може бути зчитаний сторонніми особами, навіть якщо блокчейн є публічним.

Іншим напрямом оптимізації є застосування модульної архітектури контрактів. У запропонованій системі функції автентифікації, логування, контролю

доступу й мультипідпису розділено між окремими контрактами: IdentityRegistry, AccessControl та MultiSigControl. Такий підхід дозволяє розвантажити кожен окремий смартконтракт, зменшуючи кількість перевірок, які виконуються під час кожного звернення. Крім того, модульність спрощує оновлення окремих частин системи без потреби переписувати всю логіку — це також знижує витрати на підтримку та скорочує кількість операцій у мережі. Наприклад, якщо потрібно змінити структуру логування або додати нові рівні доступу, це можна реалізувати через оновлення лише AccessControl, залишаючи інші модулі незмінними.

Третім важливим аспектом продуктивності є оптимізація викликів функцій та умов у смартконтрактах. Надмірне використання циклів, вкладених умов або викликів інших контрактів значно підвищує вартість транзакцій. У реалізованій системі, наприклад, функція isApprover у MultiSigControl реалізована через лінійний цикл, однак її виклики обмежено лише критичними діями, як-от ініціація або схвалення операцій. Таке обмеження дозволяє уникнути зайвих витрат, забезпечуючи водночас функціональність перевірки. Крім того, функція виконується у внутрішньому обсязі контракту, а не зовнішньо, що додатково зменшує вартість виконання.

Ще одним важливим напрямом є застосування ефективних структур даних. Наприклад, у контрактах використано mapping, які забезпечують швидкий доступ до даних за ключем з постійною часовою складністю O(1). Це стосується як ролей (userRoles), так і активності користувачів (isActive) у IdentityRegistry. Використання таких структур замість масивів значно знижує обчислювальні витрати при перевірці прав доступу або автентичності користувача, що особливо важливо при масштабуванні системи.

Значну роль у підвищенні продуктивності відіграє оптимізація логіки мультипідпису. У нашій реалізації облік кількості підтверджень здійснюється через mapping(bytes32 => uint256) без зберігання списку адрес, які вже підписали

операцію. Це суттєво знижує обсяг збережених даних, однак потребує ретельного аудитування поза межами контракту. Такий компроміс між продуктивністю і повнотою внутрішньої інформації є виправданим, якщо зовнішні сервіси (наприклад, блокчейн-експлорери або аналітичні інструменти) фіксують адреси-підписанти на основі подій. Події у свою чергу є дешевшими за зберігання в storage, що ще раз зменшує витрати.

На окрему увагу заслуговує питання газової ефективності функцій. У реалізованій системі всі функції поділені на публічні (public), доступні лише власникам або адміністраторам через модифікатори, й ті, що є internal або view, тобто не змінюють стан контракту. Наприклад, verifyUserRole є view-функцією, яка використовується в умовах доступу, і не створює додаткових витрат. Подібні функції дозволяють перевірити поточний стан без змін, забезпечуючи водночас високу швидкодію та зниження навантаження на мережу.

Слід також зазначити значення правильного підходу до логування подій. У запропонованій системі замість збереження кожної дії в storage, що є дорогим, події фіксуються за допомогою emit, що є набагато дешевшим і дозволяє зберігати журнал без шкоди для продуктивності. Наприклад, подія ActionLogged містить усі ключові атрибути дії, однак не вимагає змін у сховищі контракту. У середовищах із високим обсягом транзакцій та великою кількістю користувачів це дозволяє зберігати ефективність системи навіть за умов навантаження.

Для масштабування системи в умовах розподілених середовищ запропонована модель підтримує збільшення кількості учасників без лінійного зростання вартості транзакцій. Завдяки використанню мап, викликів view, подій та розділення функціональності між контрактами, система лишається стабільною навіть при додаванні нових облікових записів, ролей чи критичних операцій. Це робить її придатною до впровадження в корпоративних або державних системах, які передбачають розширення кількості користувачів у часі.

Таким чином, оптимізація продуктивності в запропонованій блокчейн-моделі реалізована через низку архітектурних, програмних та ресурсних рішень. Мінімізація збережених даних, розмежування логіки між контрактами, використання ефективних структур даних, обмеження витратних викликів, застосування подій замість storage для журналів, а також механізм гнучкого мультипідпису забезпечують не лише функціональну, а й економічно доцільну архітектуру. Такий підхід дозволяє побудувати блокчейн-систему, що є не лише безпечною, а й ефективною за своїми продуктивними показниками, що в сучасних умовах є обов'язковою вимогою для будь-якої інформаційної інфраструктури.

### 3.2. Використання блокчейн для захисту персональних даних

Використання блокчейн-технології для захисту персональних даних відкриває новий підхід до управління конфіденційною інформацією в цифровому середовищі. Традиційні централізовані системи зберігання даних часто є вразливими до зовнішніх атак, внутрішніх витоків, зловживань правами доступу та несанкціонованого копіювання інформації. Блокчейн, натомість, дозволяє реалізувати децентралізовану модель, у якій кожна одиниця даних має криптографічний захист, записується в незмінний ланцюг блоків і доступна лише уповноваженим користувачам на основі публічно-приватних ключів. У межах реалізованої моделі комп'ютерної безпеки, блокчейн використовується не лише для логування та контролю доступу, але й як основа для побудови структури безпечного зберігання та керування персональними даними через смартконтракти з чітко регламентованими правами.

Ключовим елементом захисту персональних даних у блокчейн-системі є ідентифікація користувача на основі його унікальної Ethereum-адреси. Це дозволяє відмовитися від централізованих логінів і паролів, які легко піддаються фішинговим атакам або витокам. Замість цього вся автентифікація побудована на

цифровому підписі, який створюється за допомогою приватного ключа користувача. У системі, описаній у практичній частині, смартконтракт IdentityRegistry дозволяє зареєструвати користувача з певною роллю та встановити його активність, формуючи основу для диференційованого доступу до персональних даних. Наприклад, лише користувачі з роллю admin або auditor можуть отримати доступ до функцій читання чи модифікації даних, при цьому перевірка виконується функцією verifyUserRole, яка порівнює роль користувача з передбаченою роллю, використовуючи хешоване порівняння.

Захист персональних даних підсилюється ще одним важливим принципом – незмінністю записів у блокчейні. Усі операції, пов’язані з маніпуляцією даними – доступ, оновлення, видалення – логуються в незмінний ланцюг подій через функції, що створюють події типу ActionLogged. Таким чином, кожна спроба взаємодії з персональними даними залишає цифровий слід, який не може бути змінений або видалений. Це дозволяє проводити ретроспективний аудит доступу, виявляти аномальні дії, встановлювати відповідальність користувачів і запобігати безкарному порушенню політик конфіденційності. Крім того, збереження хешів даних замість самих даних дозволяє забезпечити анонімність та мінімізувати ризики прямого витоку змісту персональної інформації.

У рамках запропонованої моделі передбачено також механізм багатоетапного підтвердження дій над критичними персональними даними за допомогою мультипідпису, реалізованого у контракті MultiSigControl. Наприклад, зміна статусу доступу до особистої інформації або надання прав іншому користувачеві можлива лише після підтвердження кількома незалежними підписантами з-поміж уповноважених осіб. Це виключає можливість одноосібної передачі доступу або зловживання повноваженнями. Такий підхід є особливо цінним для систем, де зберігається конфіденційна інформація про громадян, пацієнтів, співробітників або

клієнтів, адже навіть адміністратор системи не може самостійно здійснити зміну політик конфіденційності без погодження з іншими відповідальними особами.

З технічного боку, ефективність захисту персональних даних також забезпечується використанням хешування даних користувача до їхнього занесення в блокчейн. Наприклад, замість зберігання повного імені, адреси чи медичної інформації, у блокчейн вноситься лише хеш цієї інформації. Це дозволяє унеможливити ідентифікацію особи на основі відкритих записів, водночас зберігаючи можливість перевірки достовірності та незмінності даних. У разі необхідності авторизований користувач може подати на вхід функції ті самі дані, і система перевірить, чи відповідає їхній хеш уже збереженому. Таким чином, забезпечується верифікація без розкриття вмісту.

Важливо також, що використання блокчейн дозволяє користувачам самостійно контролювати свої персональні дані, реалізуючи принцип самостійного управління (self-sovereign identity). У межах реалізованої системи кожен користувач має змогу керувати своїм записом, змінювати статус активності або звертатися до адміністратора за оновленням ролі. Це забезпечує прозорість і підзвітність у сфері обробки персональних даних, що особливо актуально з огляду на вимоги міжнародного законодавства, зокрема GDPR. У такій архітектурі користувачі перестають бути пасивними об’єктами обробки даних, набуваючи статусу повноцінних власників і розпорядників своєї цифрової ідентичності.

У контексті реального застосування, така модель може бути використана для реєстрів пацієнтів у медичних системах, обліку освітніх досягнень, цифрових посвідчень особи, систем голосування або державних платформ, де важливо забезпечити контрольований, захищений і перевірений доступ до чутливої інформації. Наприклад, у медичних установах дані про діагнози, історію хвороби та лікарські призначення можуть бути записані у вигляді хешів, доступ до яких матиме лише ліцензований персонал, роль якого підтверджується у смартконтракті. Пацієнт може надати або відкликати дозвіл на доступ до своєї інформації, а кожен

запит буде зафіксовано для можливості перевірки. Це не тільки посилює захист персональних даних, а й сприяє зростанню довіри до цифрової медицини.

Ще одним вагомим компонентом є прозорість і аудитність. На відміну від традиційних баз даних, де доступ до логів має лише адміністратор, у блокчейн-системі всі події є публічними (у разі публічного блокчейну) або доступними всім учасникам контуру (у приватному), що унеможливлює приховане втручання. У разі інциденту всі дії можна відтворити та перевірити за допомогою подій, зафіксованих смартконтрактами. Таким чином, сам механізм зберігання даних у блокчейн стає інструментом превентивного захисту, який не дозволяє злому залишитись непоміченим або безкарним.

Отже, використання блокчейн для захисту персональних даних у запропонованій системі реалізується через унікальні механізми ідентифікації користувачів, хешування конфіденційної інформації, контроль доступу на основі ролей, логування дій із незмінними записами та підтвердження критичних операцій через мультипідпис. Така структура дає змогу створити систему, в якій навіть за умов втрати доступу або компрометації одного елемента не втрачається загальний захист. Принципова неможливість змінити або стерти вже записані дані, поєднана з можливістю зовнішнього аудиту та прозорої взаємодії, перетворює блокчейн на один із найбільш перспективних інструментів захисту персональної інформації в умовах сучасної цифрової трансформації. Реалізована модель доводить, що із застосуванням відповідних протоколів, структур і контрактів можливо не лише зберігати, а й ефективно керувати персональними даними без ризику порушення конфіденційності чи втрати контролю над ними.

### 3.3. Перспективи розвитку технології блокчейн у сфері кібербезпеки

Перспективи розвитку блокчейн-технології у сфері кібербезпеки є надзвичайно широкими та багатовекторними, оскільки вона відкриває принципово

нові підходи до захисту цифрової інформації, ідентифікації користувачів, збереження конфіденційності, запобігання несанкціонованим змінам та протидії внутрішнім загрозам. Класичні централізовані моделі кіберзахисту, навіть попри постійне вдосконалення, залишаються вразливими до атак на сервери, зламів облікових записів, фішингу та несанкціонованого доступу з боку адміністраторів. Блокчейн дозволяє формувати нову концепцію безпеки, в основі якої лежать принципи децентралізації, незмінності, прозорості, автономного управління та колективного контролю, що принципово змінює парадигму цифрового захисту.

Одним із ключових векторів розвитку блокчейн у сфері кібербезпеки є формування самодостатніх систем управління ідентичністю (Self-Sovereign Identity). У майбутньому централізовані сервіси автентифікації поступово поступляться місцем децентралізованим структурам, де кожен користувач зберігатиме та керуватиме своєю цифровою ідентичністю через публічно-приватні ключі. Така ідентичність не вимагатиме централізованої верифікації та не залежатиме від сторонніх серверів, що суттєво зменшить вразливість до масових витоків персональних даних. У межах кібербезпеки це означає усунення одного з головних факторів ризику – компрометації єдиного сховища облікових даних. Смартконтракти забезпечуватимуть логіку доступу до ресурсів лише після підтвердження ключа, а сам процес автентифікації не передбачатиме передачі жодної конфіденційної інформації по мережі.

Другим важливим напрямом розвитку є використання блокчейн для журналювання подій та управління інцидентами. У багатьох сучасних інфраструктурах журнали подій зберігаються на серверах, доступ до яких має обмежене коло адміністраторів. У разі компрометації таких серверів можна видалити або змінити історію подій, що унеможливлює повноцінний аудит. Блокчейн пропонує альтернативу у вигляді незмінного, криптографічно захищеного сховища подій, де кожна взаємодія із системою – вхід, доступ, зміна, помилка – фіксується у вигляді події смартконтракту з часовою міткою. У разі інциденту

інформацію можна використати як доказ, оскільки вона не піддається знищенню чи модифікації. У майбутньому блокчейн-логи можуть стати еталонною практикою для галузей, де аудит є юридично значущим, зокрема у фінансах, охороні здоров'я, держуправлінні та промисловості.

Окремий сегмент розвитку стосується моделей управління конфігураціями та оновленнями програмного забезпечення. Одним із основних векторів атаки на системи є впровадження шкідливих оновлень або зміна конфігурації через обхідні шляхи. Блокчейн дозволяє створити смартконтракти, в яких кожне оновлення або конфігураційна зміна має бути схвалена визначеним числом підписантів – за аналогією з механізмом мультипідпису. Така модель мінімізує ризики внутрішнього саботажу, помилок конфігурації та ін'єкцій шкідливого коду. У перспективі, це дозволить реалізувати автоматизовані платформи безпеки, де всі оновлення проходять через публічний аудит на рівні блокчейну до моменту фактичного застосування.

Іншим стратегічно важливим напрямом є захист інтернету речей (IoT). З розвитком технологій кількість пристроїв, підключених до мережі, щороку зростає експоненційно, водночас більшість із них мають обмежені ресурси безпеки. Традиційні моделі автентифікації або централізованого керування не працюють у масштабних розподілених середовищах. Блокчейн дозволяє кожному IoT-пристрою мати власну ідентичність, записану в мережу, з фіксацією його стану, транзакцій, взаємодій з іншими пристроями. Смартконтракти можуть автоматично виконувати політику доступу, оновлення, реагування на загрози. У майбутньому саме блокчейн здатен стати основою для безпечної та самокерованої IoT-інфраструктури, у якій немає залежності від централізованих шлюзів або серверів.

Значний потенціал має інтеграція блокчейн із технологіями штучного інтелекту для побудови самонавчальних систем кіберзахисту. Наприклад, алгоритми машинного навчання можуть аналізувати записи блокчейну в режимі реального часу для виявлення аномалій, які вказують на спроби зловмисного

втручання. На відміну від традиційних логів, які можна стерти або змінити, дані з блокчейн є незмінними, тому аналітика може працювати з повною історією взаємодій. Така синергія дозволяє створити автономні системи безпеки, які виявляють, аналізують та блокують загрози до моменту їх реалізації. Надалі блокчейн може стати основою для «розумних» протоколів безпеки, які самостійно адаптуються до нового типу атак.

Не менш перспективною є сфера цифрових доказів та відповідальності. У кібербезпеці часто виникає проблема доведення вини – зловмисники стирають сліди, підробляють дані, ідентифікувати джерело атаки стає практично неможливо. Якщо взаємодії записуються у блокчейн, із криптографічним підписом і часовою міткою, кожна дія має цифровий слід. У разі атаки, витоку або порушення політик, можна однозначно ідентифікувати відповідального, оскільки хеш запису співвідноситься з публічним ключем виконавця. Це змінює не лише технологічну, а й правову основу кібербезпеки, оскільки блокчейн починає виконувати роль цифрового судового архіву, що визнається як доказ у юридичних процесах.

Ще одним важливим трендом є розвиток приватних блокчейн-мереж для захищених середовищ. Публічні мережі, як-от Ethereum чи Polygon, є ефективними для відкритих систем, однак у кібербезпеці часто виникає потреба в обмеженому доступі, фіксованому наборі вузлів і конфіденційності. Приватні блокчейн-системи дозволяють організаціям створити внутрішню мережу з визначеними ролями, правами доступу, механізмами контролю змін і регламентами аудиту. У таких системах блокчейн виконує роль внутрішнього захисного протоколу, забезпечуючи надійність навіть у разі компрометації окремих елементів інфраструктури. У майбутньому можна очікувати масове розгортання приватних блокчейнів у банківському секторі, державному управлінні, оборонній сфері, де вимоги до конфіденційності є максимально жорсткими.

Отже, перспективи розвитку технології блокчейн у сфері кібербезпеки охоплюють як фундаментальні принципи захисту — ідентифікація, авторизація,

незмінність, прозорість, — так і інноваційні напрямки, пов’язані з автономним управлінням, самонавчанням, цифровим правосуддям і захистом у масштабованих розподілених середовищах. Із впровадженням нових стандартів, підвищенням обчислювальної потужності, розвитком концепції Web 3.0 та зростанням ризиків цифрових загроз, блокчейн все більше виступає не лише як додатковий елемент безпеки, а як повноцінна основа нової цифрової інфраструктури. Його подальший розвиток у кібербезпеці визначатиметься здатністю забезпечити не лише захист від атак, а й стійкість, прозорість, юридичну доказовість та децентралізовану відповідальність у цифровому світі.

**Висновки до розділу 3**

Оптимізація продуктивності блокчейн-мережі передбачає використання вдосконалених механізмів консенсусу з меншим споживанням обчислювальних ресурсів, таких як Proof of Authority, Delegated Proof of Stake або гібридні підходи, що забезпечують баланс між швидкістю та безпекою. Додаткову ефективність забезпечують технології off-chain обробки, включно з каналами станів і сайдчейнами, які дозволяють зменшити навантаження на основний ланцюг, зберігаючи при цьому достовірність оброблених транзакцій. Такий підхід дозволяє масштабувати систему без зниження рівня безпеки. Захист персональних даних у рамках децентралізованої архітектури досягається шляхом застосування хеш-функцій для зберігання ідентифікаторів у незмінному вигляді, без розкриття самих даних. Користувачі отримують можливість контролювати доступ до власної інформації через механізми смартконтрактного управління, що відповідає принципам цифрової ідентичності та вимогам міжнародних стандартів з безпеки даних. Подальший розвиток блокчейн-технологій у сфері кібербезпеки пов’язано з активною інтеграцією цієї моделі у критично важливі сфери: державне управління, де необхідна прозорість та незмінність реєстрів; охорону здоров’я, де важливо

зберігати конфіденційність і водночас забезпечити цілісність медичних записів; освіту, в якій блокчейн може слугувати основою для цифрових дипломів, сертифікатів та результатів навчання; а також фінансовий сектор, що потребує високого рівня захисту транзакцій, довіри між учасниками й запобігання шахрайству. Усі ці напрямки демонструють перспективу трансформації традиційних моделей інформаційної безпеки в напрямі децентралізації, автоматизації контролю та прозорості дій.

# ВИСНОВКИ

*В роботі було проведено:*

1. Аналіз блокчейн-технологій у контексті кібербезпеки, визначити їхні переваги та обмеження, а також зіставити можливості блокчейн з класифікацією сучасних загроз для комп’ютерних систем.
2. Проаналізовано існуючі рішення щодо використання блокчейн для захисту інформаційних потоків та обґрунтувати власний підхід до розробки моделі безпеки, включно з описом архітектури та основних компонентів.
3. Проаналізовано ефективність запропонованої моделі в умовах змодельованих загроз і сформулювати рекомендації щодо її впровадження та подальшого вдосконалення.

Теоретичний аналіз основ блокчейн-технологій у контексті кібербезпеки, у ході якого визначено ключові можливості та обмеження даної технології для забезпечення захисту інформаційних систем. Проаналізовано фундаментальні властивості блокчейну, серед яких незмінність даних, децентралізація зберігання інформації, криптографічний захист транзакцій, відсутність єдиної точки відмови та механізми досягнення консенсусу. Встановлено, що блокчейн має потенціал для подолання вразливостей, притаманних централізованим моделям безпеки, зокрема підвищення стійкості систем до зовнішніх і внутрішніх загроз.

Дослідили сучасні загрози для комп’ютерних систем, зокрема атаки типу «людина посередині», SQL-ін’єкції, ескалацію привілеїв, фальсифікацію даних і витоки інформації через незахищені канали передачі. Проаналізували механізми, за допомогою яких блокчейн може нейтралізувати ці загрози: шляхом застосування незмінних журналів подій, розподіленого контролю доступу, автентифікації на основі цифрового підпису, смартконтрактів для регулювання прав доступу та криптографічної верифікації транзакцій. Показано, що інтеграція блокчейн-

технологій у структуру веб-додатків дозволяє істотно підвищити рівень довіри й цілісності оброблюваної інформації.

Обґрунтували власний підхід до розробки моделі безпеки комп'ютерної системи на основі блокчейн-технологій. Запропоновано архітектуру, що включає інтеграцію смартконтрактів для контролю доступу, використання електронної цифрової ідентифікації через механізм цифрового підпису ECDSA, побудову журналу незмінних записів на базі блокчейну Ethereum та впровадження політик багаторівневої авторизації з принципом «zero trust». Розроблена структура забезпечує надійний захист на всіх етапах обробки даних: від автентифікації користувача до фіксації його дій у системі.

Оцінили ефективність запропонованої моделі безпеки шляхом моделювання типових атак на комп'ютерні системи. Встановлено, що впровадження запропонованої архітектури дозволяє істотно знизити ймовірність успішної реалізації атак типу несанкціонованого доступу, підміни даних, витоку облікових даних та внутрішнього шахрайства. Система показала високу стійкість до підробки журналів подій і змін у розподіленому реєстрі, забезпечуючи збереження достовірності записів навіть за умов часткового компрометування окремих вузлів мережі. Практична реалізація моделі підтвердила можливість її адаптації до умов функціонування веб-додатків із підвищеними вимогами до кібербезпеки.

У підсумку, результати роботи свідчать про доцільність застосування блокчейн-технологій для створення високонадійних моделей захисту комп'ютерних систем в умовах цифрової трансформації. Запропонована модель поєднує переваги децентралізації, криптографічного захисту та автоматизованого управління доступом і може бути впроваджена у державні, корпоративні й комерційні інформаційні системи, де критично важливою є стійкість до сучасних кіберзагроз.

# СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ


1. Андрєєв О. В. Блокчейн як інструмент цифрової безпеки: концепція і практика / О. В. Андрєєв // Інформаційна безпека. – 2020. – № 2. – С. 5–12.
2. Антонюк Л. Л. Технології блокчейн у публічному управлінні: переваги та виклики / Л. Л. Антонюк // Державне управління та місцеве самоврядування. – 2021. – № 4. – С. 58–66.
3. Баранов В. В. Смартконтракти як правовий інструмент цифрової трансформації / В. В. Баранов // Вісник цивільного права. – 2021. – № 3. – С. 102–110.
4. Бєлозьоров С. І. Математичні основи криптографії / С. І. Бєлозьоров. – К. : Наукова думка, 2020. – 312 с.
5. Богданович І. В. Використання блокчейн для управління ідентичністю в мережах IoT / І. В. Богданович // Системи обробки інформації. – 2022. – № 1. – С. 21–27.
6. Бондарчук А. І. Основи інформаційної безпеки: навч. посіб. / А. І. Бондарчук. – Київ : КНЕУ, 2019. – 285 с.
7. Бронніков В. В. Механізми автентифікації у блокчейн-системах / В. В. Бронніков // Кібербезпека: освіта, наука, техніка. – 2020. – № 2. – С. 41–47.
8. Бублик Н. І. Електронна ідентифікація в контексті захисту персональних даних / Н. І. Бублик // Інформаційне право України. – 2021. – № 1. – С. 73–80.
9. Вакуленко І. О. Роль смартконтрактів у забезпеченні кібербезпеки / І. О. Вакуленко // Інформаційні технології і безпека. – 2020. – № 3. – С. 14–22.
10. Василенко Н. М. Юридичні аспекти використання блокчейн-технологій / Н. М. Василенко // Право України. – 2022. – № 7. – С. 45–51.
11. Верещака Т. В. Електронні реєстри на блокчейні: перспективи для України / Т. В. Верещака // Публічне право. – 2022. – № 1. – С. 56–62.

12. Гаврилюк О. В. Блокчейн у фінансовій безпеці держави / О. В. Гаврилюк // Економіка та держава. – 2020. – № 12. – С. 30–35.
13. Гайдай М. Блокчейн: архітектура, протоколи, додатки / М. Гайдай. – Львів : ЛНУ імені Івана Франка, 2021. – 250 с.
14. Гончаренко В. Д. Технології кіберзахисту / В. Д. Гончаренко. – Харків : ХНУРЕ, 2021. – 340 с.
15. Гуцалюк В. В. Методи анонімізації персональних даних у блокчейн-середовищі / В. В. Гуцалюк // Наукові записки НАВС. – 2021. – № 4. – С. 112–117.
16. Данильченко С. І. Кібербезпека як компонент національної безпеки / С. І. Данильченко // Стратегічні пріоритети. – 2020. – № 2. – С. 22–29.
17. Державна служба спеціального зв’язку та захисту інформації України. Національна стратегія кібербезпеки України на 2021–2025 роки [Електронний ресурс]. – Режим доступу: https://cip.gov.ua
18. Дьяків В. О. Ефективність мультипідпису в смартконтрактах / В. О. Дьяків // Інформатика і кібернетика. – 2022. – № 2. – С. 59–65.
19. European Union Agency for Cybersecurity. ENISA Threat Landscape 2022 [Електронний ресурс]. – Режим доступу: https://www.enisa.europa.eu/publications
20. Fedorov A., Kuznetsov O. Distributed identity and data protection in blockchain-based networks / A. Fedorov, O. Kuznetsov // Journal of Digital Security. – 2022. – Vol. 7. – P. 115–123.
21. Hölbl M., Kompara M., Kamišalić A. A Systematic Review of the Use of Blockchain in Healthcare / M. Hölbl, M. Kompara, A. Kamišalić // Applied Sciences. – 2020. – Vol. 10(5). – P. 1–20.
22. Інститут модернізації змісту освіти. Перспективи впровадження блокчейн в освітньому середовищі [Електронний ресурс]. – Режим доступу: https://imzo.gov.ua

23. Іщенко П. М. Хеш-функції у забезпеченні цілісності даних / П. М. Іщенко // Інформаційні технології. – 2020. – № 3. – С. 48–55.
24. Казанський І. А. Розподілені реєстри у державному управлінні / І. А. Казанський // Теорія та практика державного управління. – 2021. – № 4. – С. 85–93.
25. Калюжний Р. С. Основи криптографії та цифрової ідентифікації / Р. С. Калюжний. – К. : КНУ, 2020. – 298 с.
26. Карпюк Л. С. Smart-міста та безпечна ідентифікація в умовах цифрової трансформації / Л. С. Карпюк // Управління розвитком. – 2021. – № 6. – С. 74–81.
27. Кисіль О. В. Блокчейн для захисту медичних даних: потенціал і ризики / О. В. Кисіль // Медичне право України. – 2022. – № 1. – С. 33–38.
28. Коваленко М. Ю. Блокчейн в цифровому правосудді / М. Ю. Коваленко // Правова інформатика. – 2021. – № 4. – С. 59–66.
29. Колесник С. А. Smart-контракти як інструмент правового регулювання / С. А. Колесник // Юридична Україна. – 2020. – № 7. – С. 29–36.
30. Кондратюк Т. П. Блокчейн та персональні дані: виклики і рішення / Т. П. Кондратюк // Інформаційне суспільство. – 2022. – № 1. – С. 44–50.
31. Костенко О. А. Автоматизація контролю доступу в корпоративних системах / О. А. Костенко // Захист інформації. – 2021. – № 3. – С. 12–19.
32. Кравець В. І. Криптографічний захист даних / В. І. Кравець. – Київ : КНЕУ, 2020. – 244 с.
33. Кузьменко І. В. Архітектура смартконтрактів для управління ризиками / І. В. Кузьменко // Вісник КНУ. Серія «Інформатика». – 2022. – № 1. – С. 91–98.
34. Левченко А. Ю. Блокчейн та штучний інтелект у безпеці / А. Ю. Левченко // Технології XXI століття. – 2022. – № 3. – С. 5–11.
35. Лещенко Н. С. Роль блокчейн у захисті критичної інфраструктури / Н. С. Лещенко // Кібернетика і обчислювальна техніка. – 2021. – № 6. – С. 67–73.

36. Литвиненко І. В. Автоматизоване виявлення загроз на основі даних з блокчейн / І. В. Литвиненко // Інформаційні системи. – 2022. – № 2. – С. 60–66.
37. Лукашевич М. В. Смартконтракти в державному управлінні / М. В. Лукашевич // Адміністративне право і процес. – 2021. – № 3. – С. 52–58.
38. Марченко Ю. І. Захист персональних даних у цифровій державі / Ю. І. Марченко // Цифрове право. – 2022. – № 2. – С. 23–29.
39. Міністерство цифрової трансформації України. Концепція розвитку технологій розподілених реєстрів в Україні [Електронний ресурс]. – Режим доступу: https://thedigital.gov.ua
40. Міністерство юстиції України. Закон України «Про захист персональних даних» від 01.06.2010 № 2297-VI [Електронний ресурс]. – Режим доступу: https://zakon.rada.gov.ua
41. Мірошниченко В. О. Розподілені обчислення в кіберзахисті / В. О. Мірошниченко // Радіоелектроніка та інформатика. – 2020. – № 2. – С. 74–81.
42. Молчанов П. С. Технології блокчейн у судовому процесі / П. С. Молчанов // Сучасне правосуддя. – 2021. – № 4. – С. 34–41.
43. Музика І. Ю. Технології захисту в електронних реєстрах / І. Ю. Музика // Інформаційне право. – 2021. – № 3. – С. 18–24.
44. Національний координаційний центр кібербезпеки. Звіт про кіберзагрози 2023 [Електронний ресурс]. – Режим доступу: https://ncscc.gov.ua
45. Немировський І. О. Захист цифрових активів через блокчейн / І. О. Немировський // Бізнес, право та безпека. – 2022. – № 1. – С. 39–46.
46. Олійник В. Г. Перспективи приватних блокчейн для органів публічної влади / В. Г. Олійник // Право і суспільство. – 2021. – № 5. – С. 101–107.
47. Осадчук Т. Б. Смартконтракти в системах електронного голосування / Т. Б. Осадчук // Телекомунікації та інформатизація. – 2021. – № 2. – С. 33–39.

48. Піщуліна Н. П. Технології цифрової довіри в інформаційному суспільстві / Н. П. Піщуліна // Соціум. Доктрина. Політика. – 2020. – № 3. – С. 44–52.
49. Пономаренко О. І. Кібербезпека у сфері електронного урядування / О. І. Пономаренко // Держава і право. – 2022. – № 6. – С. 64–71.
50. Шевченко А. М. Децентралізація як інструмент цифрового захисту / А. М. Шевченко // Електронне урядування. – 2022. – № 1. – С. 88–94.

# ДОДАТКИ

## Додаток А

Розроблена система складається з трьох смартконтрактів, які взаємодіють між собою та забезпечують ідентифікацію користувачів, контроль доступу, журналювання подій і захист критичних операцій через механізм мультипідпису. Система розгорнута та протестована у середовищі Remix IDE.

**Розроблені смартконтракти**

1. **IdentityRegistry.sol**

   Контракт виконує функції реєстрації, зберігання та оновлення інформації про користувачів. Кожен користувач має адресу, децентралізований ідентифікатор (DID), роль (наприклад, admin, user, auditor) та статус активності. Реалізовано функції додавання користувача, зміни ролі або активності та отримання інформації про конкретного користувача. Доступ до цих функцій має лише власник контракту (owner), що захищає від несанкціонованого керування ідентичностями.

2. **AccessControl.sol**

   Контракт відповідає за логування дій користувачів. Кожен активний і зареєстрований користувач може записувати дії у вигляді логів. Кожен лог містить мітку часу, адресу користувача, опис дії, хеш вхідних даних (для підтвердження цілісності) та додаткові деталі. Логи зберігаються у масиві, доступному для перегляду. При виклику функції логування перевіряється статус користувача в IdentityRegistry.

3. **MultiSigControl.sol**

   Контракт реалізує механізм мультипідпису для виконання критичних

операцій. При створенні контракту задаються адреси підписантів (approvers) та кількість необхідних підтверджень (requiredApprovals). Один з уповноважених користувачів створює операцію, після чого інші підписанти можуть підтвердити її. Після досягнення заданої кількості підтверджень, операція виконується автоматично через виклик call. Такий підхід дозволяє запобігти виконанню чутливих дій без згоди кількох уповноважених осіб.

**Принцип роботи системи**

1. Адміністратор розгортає контракт IdentityRegistry і додає користувачів, надаючи їм ролі та статус активності.
2. Користувачі, які мають активний статус, можуть виконувати дії в системі, зокрема логувати події через AccessControl.
3. Усі події зберігаються у вигляді логів, що доступні для аудиту та перевірки.
4. Для виконання критичних змін (наприклад, оновлення політик або конфіденційних налаштувань), використовується контракт MultiSigControl.
5. Один з підписантів створює операцію, інші підтверджують її. Лише після досягнення необхідної кількості підтверджень, операція виконується.

**Захист, реалізований у моделі**

– Доступ до функцій логування мають лише користувачі, зареєстровані в IdentityRegistry та з активним статусом.

– Функції реєстрації та оновлення користувачів доступні виключно власнику контракту.

– Мультипідпис дозволяє запобігти зловживанням при виконанні чутливих операцій – потрібно підтвердження кількох незалежних осіб.

– Усі логовані дії захищені криптографічними хешами, що дозволяє перевіряти цілісність вхідних даних.

– Блокчейн забезпечує незмінність записів, що гарантує прозорість та надійність логів.

– Система є децентралізованою – немає єдиної точки відмови або централізованого управління.

**Результати реалізації**

Система успішно розгорнута та протестована у середовищі Remix. Вона забезпечує базову функціональність захисту комп’ютерної системи: ідентифікація, контроль доступу, аудит дій та виконання критичних операцій лише за згодою кількох уповноважених користувачів. Архітектура системи дозволяє її масштабування, інтеграцію з іншими смартконтрактами або фронтендом, а також застосування в реальних інформаційних системах, де важлива прозорість, довіра та контроль доступу.

```
// SPDX-License-Identifier: MIT
pragma solidity ^0.8.28;

contract IdentityRegistry {
    struct User {
        address userAddress;
        string did;    // Децентралізований ідентифікатор користувача (наприклад: "did:example:123")
        string role;   // Наприклад: "admin", "user", "auditor"
        bool active;
    }

    mapping(address => User) public users;
    address public owner;

    event UserRegistered(address indexed userAddress, string did, string role);
    event UserUpdated(address indexed userAddress, string newRole, bool active);

    modifier onlyOwner() {
        require(msg.sender == owner, unicode"Лише власник може виконувати цю операцію");
        _;
    }

    constructor() {
        owner = msg.sender; // Установлюємо відправника транзакції як власника
    }

    // Функція реєстрації користувача (лише власник може додавати)
    function registerUser(address _userAddress, string memory _did, string memory _role) public onlyOwner {
        require(users[_userAddress].userAddress == address(0), unicode"Користувач вже зареєстрований");
        users[_userAddress] = User(_userAddress, _did, _role, true);
        emit UserRegistered(_userAddress, _did, _role);
    }

    // Функція оновлення даних користувача (роль, статус)
    function updateUser(address _userAddress, string memory _newRole, bool _active) public onlyOwner {
        require(users[_userAddress].userAddress != address(0), unicode"Користувач не знайдений");
        users[_userAddress].role = _newRole;
        users[_userAddress].active = _active;
        emit UserUpdated(_userAddress, _newRole, _active);
    }
```

Рис. 1 – IdentityRegistry.sol

```solidity
// SPDX-License-Identifier: MIT
pragma solidity ^0.8.28;

import "./IdentityRegistry.sol";

contract AccessControl {
    IdentityRegistry identityRegistry;

    struct AccessLog {
        uint256 timestamp;
        address user;
        string action;    // Опис операції, наприклад: "login", "access resource" тощо
        bytes32 dataHash; // Хеш даних для підтвердження цілісності
        string details;   // Додаткова інформація (наприклад, посилання на файл в IPFS)
    }

    AccessLog[] public accessLogs;

    event AccessLogged(
        uint256 timestamp,
        address indexed user,
        string action,
        bytes32 dataHash,
        string details
    );

    // При розгортанні передаємо адресу вже розгорнутого IdentityRegistry
    constructor(address _identityRegistryAddress) {
        identityRegistry = IdentityRegistry(_identityRegistryAddress);
    }

    // Функція логування операції    infinite gas 852200 gas
function logAccess(string memory _action, string memory _data, string memory _details) public {
    // Отримуємо дані про користувача з IdentityRegistry, ігноруючи role, тому що воно не використовується    infinite gas
    (, , bool active) = identityRegistry.getUser(msg.sender);
    require(active, unicode"Користувач не активний або не авторизований");

    // Обчислюємо хеш переданих даних для перевірки їх цілісності
    bytes32 _hash = keccak256(abi.encodePacked(_data));

    accessLogs.push(AccessLog(block.timestamp, msg.sender, _action, _hash, _details));

    emit AccessLogged(block.timestamp, msg.sender, _action, _hash, _details);
}

    // Функція для отримання кількості записів у журналі
    function getLogsCount() public view returns (uint256) {
        return accessLogs.length;
    }

    // Функція для отримання конкретного запису за індексом
    function getLog(uint256 _index) public view returns (
        uint256,
        address,
        string memory,
        bytes32,
        string memory
    ) {
        require(_index < accessLogs.length, unicode"Невірний індекс");    2484 gas
        AccessLog memory logEntry = accessLogs[_index];
        return (
            logEntry.timestamp,
            logEntry.user,
            logEntry.action,
            logEntry.dataHash,    infinite gas
            logEntry.details
        );
    }
}
```

Рис. 2 – AccessControl.sol

```solidity
// SPDX-License-Identifier: MIT
pragma solidity ^0.8.28;

contract MultiSigControl {
    // Список адрес, які мають право підтверджувати операції
    address[] public approvers;
    // Мінімальна кількість підтверджень для виконання операції
    uint256 public requiredApprovals;

    // Структура операції, яка містить цільовий адресу, дані операції,
    // кількість отриманих підтверджень та картку з адресами, що вже підтвердили
    struct Operation {
        address target;
        bytes data;
        uint256 approvals;
        mapping(address => bool) approvedBy;
    }

    // Зберігаємо операції за їх ID
    mapping(uint256 => Operation) public operations;
    // Лічильник операцій
    uint256 public operationCount;

    event OperationCreated(uint256 indexed operationId, address target);
    event OperationApproved(uint256 indexed operationId, address approver);
    event OperationExecuted(uint256 indexed operationId);

    // Модифікатор перевіряє, чи викликаючий є одним із уповноважених підтверджувачів
    modifier onlyApprover() {
        bool allowed = false;
        for (uint256 i = 0; i < approvers.length; i++) {
            if (msg.sender == approvers[i]) {
                allowed = true;
                break;
            }
        }
        require(allowed, unicode"Не авторизований підтверджувач");
        _;
    }

    // Конструктор приймає масив адрес підтверджувачів та потрібну кількість підтверджень
    constructor(address[] memory _approvers, uint256 _requiredApprovals) {
        require(_approvers.length >= _requiredApprovals, unicode"Недостатньо підтверджень");
        approvers = _approvers;
        requiredApprovals = _requiredApprovals;
    }
    // Функція для створення операції, яка потребує мультипідпису
    function createOperation(address _target, bytes memory _data) public onlyApprover returns (uint256) {
        operationCount++;    infinite gas 843800 gas
        Operation storage op = operations[operationCount];
        op.target = _target;
        op.data = _data;
        op.approvals = 0;
        emit OperationCreated(operationCount, _target);
        return operationCount;
    }

    // Функція підтвердження операції від одного з approvers
    function approveOperation(uint256 _operationId) public onlyApprover {
        Operation storage op = operations[_operationId];    infinite gas
        require(!op.approvedBy[msg.sender], unicode"Вже підтверджено");
        op.approvedBy[msg.sender] = true;
        op.approvals++;
        emit OperationApproved(_operationId, msg.sender);

        // Якщо отримано достатньо підтверджень, виконуємо операцію
        if (op.approvals >= requiredApprovals) {
            executeOperation(_operationId);
        }
    }

    // Внутрішня функція для виконання операції після досягнення необхідної кількості підтверджень    infinite gas
    function executeOperation(uint256 _operationId) internal {
        Operation storage op = operations[_operationId];
        (bool success, ) = op.target.call(op.data);
        require(success, unicode"Операцію не виконано");
        emit OperationExecuted(_operationId);
    }
}
```

Рис. 3 – MultiSigControl.sol

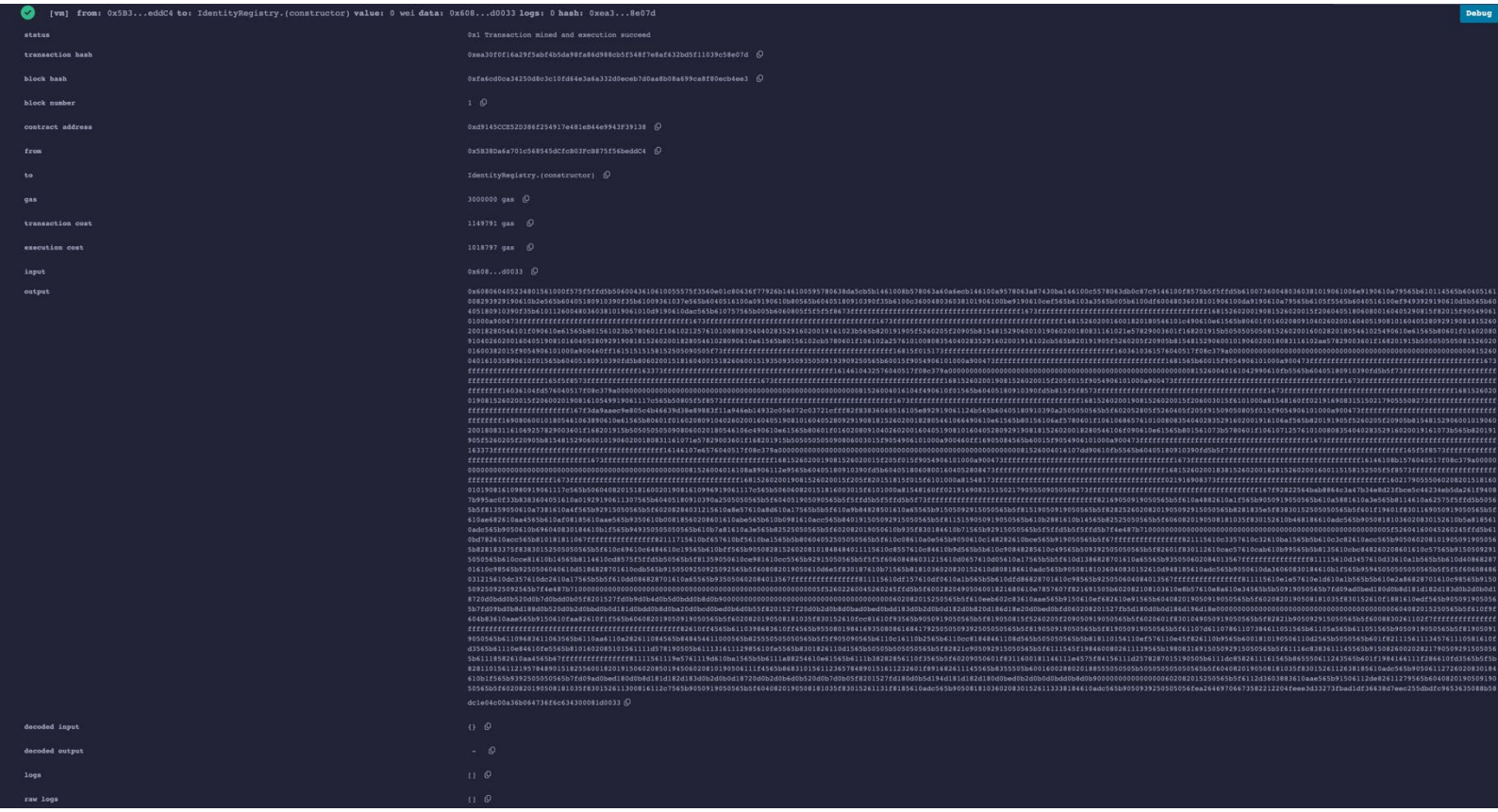


Рис. 4 - Результат успішного розгортання смартконтракту IdentityRegistry.sol

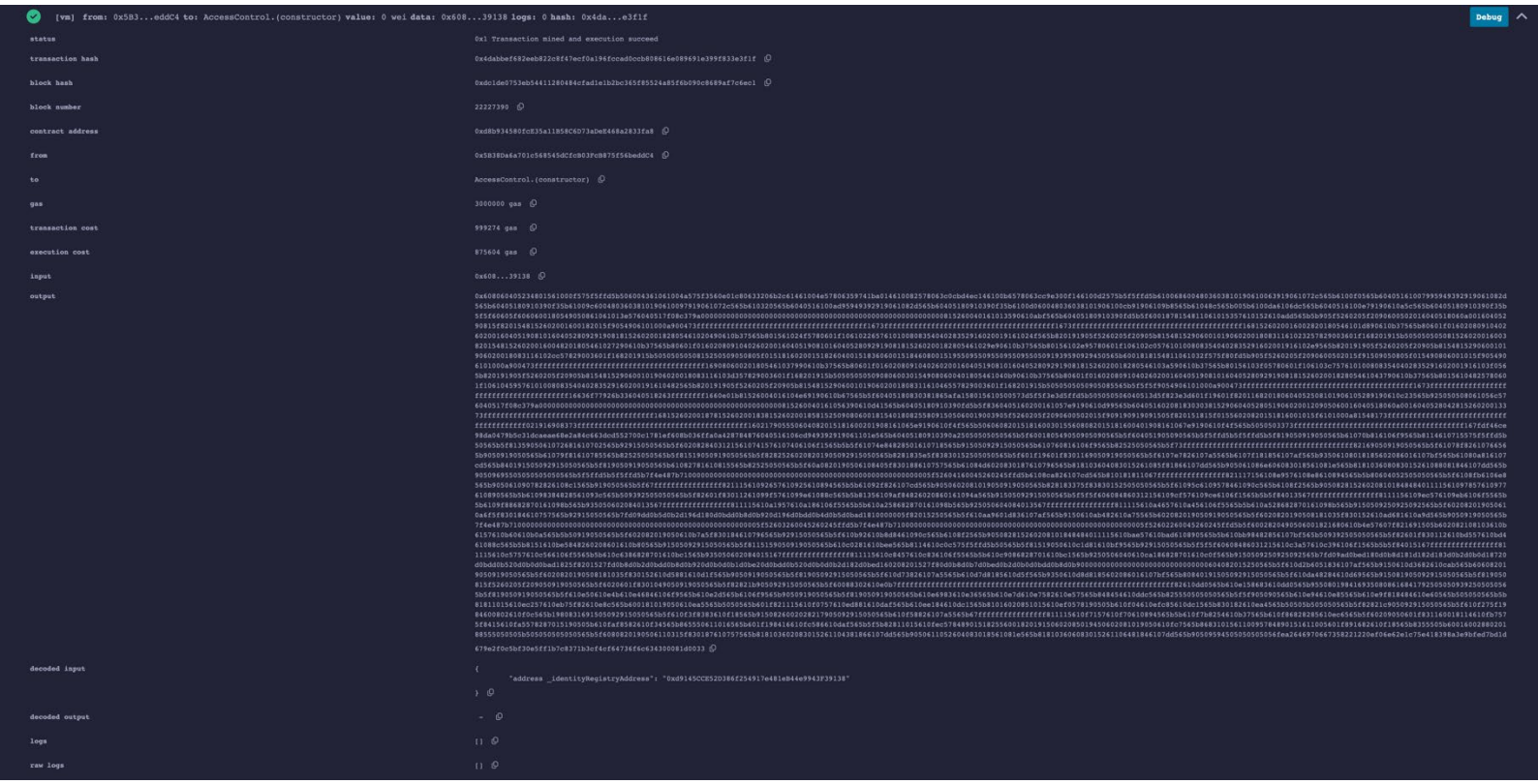


Рис. 5 – Результат успішного розгортання смартконтракту AccessControl з передачею адреси IdentityRegistry


Рис. 6 - Розгортання смартконтракту MultiSigControl з параметрами доступу

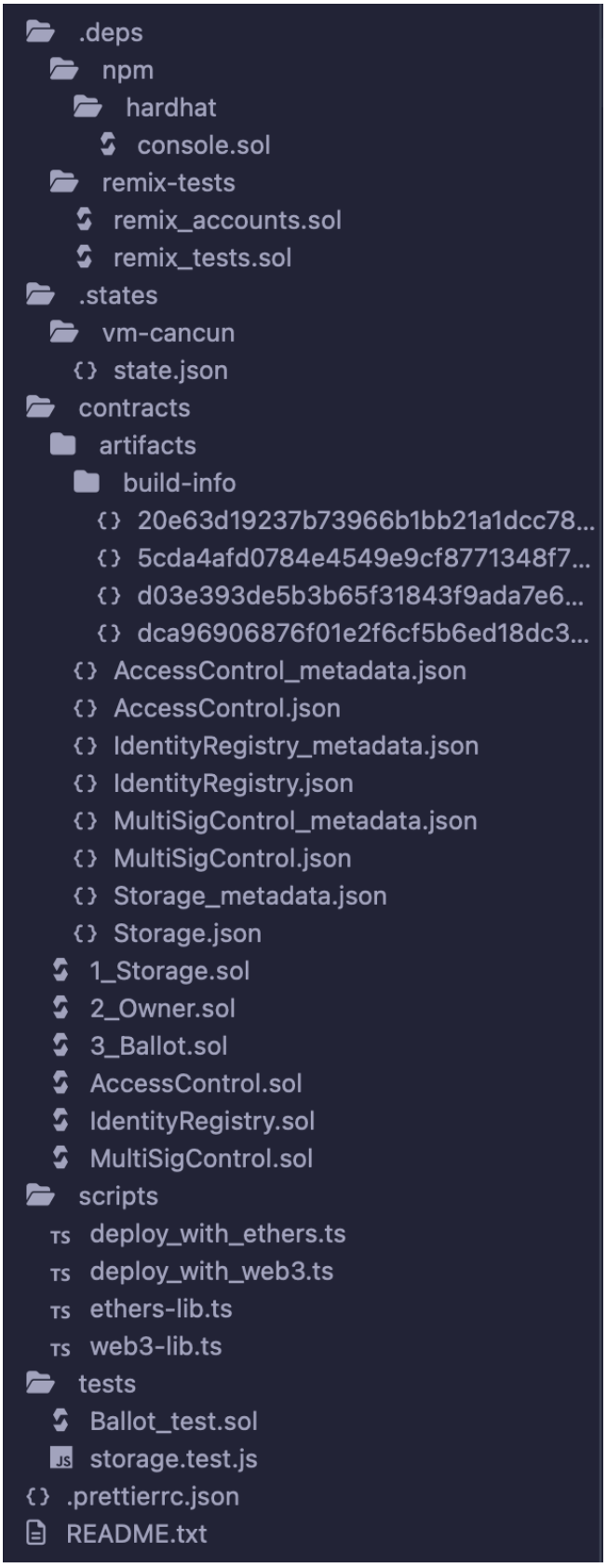


Рис. 7 – Структура проєкту

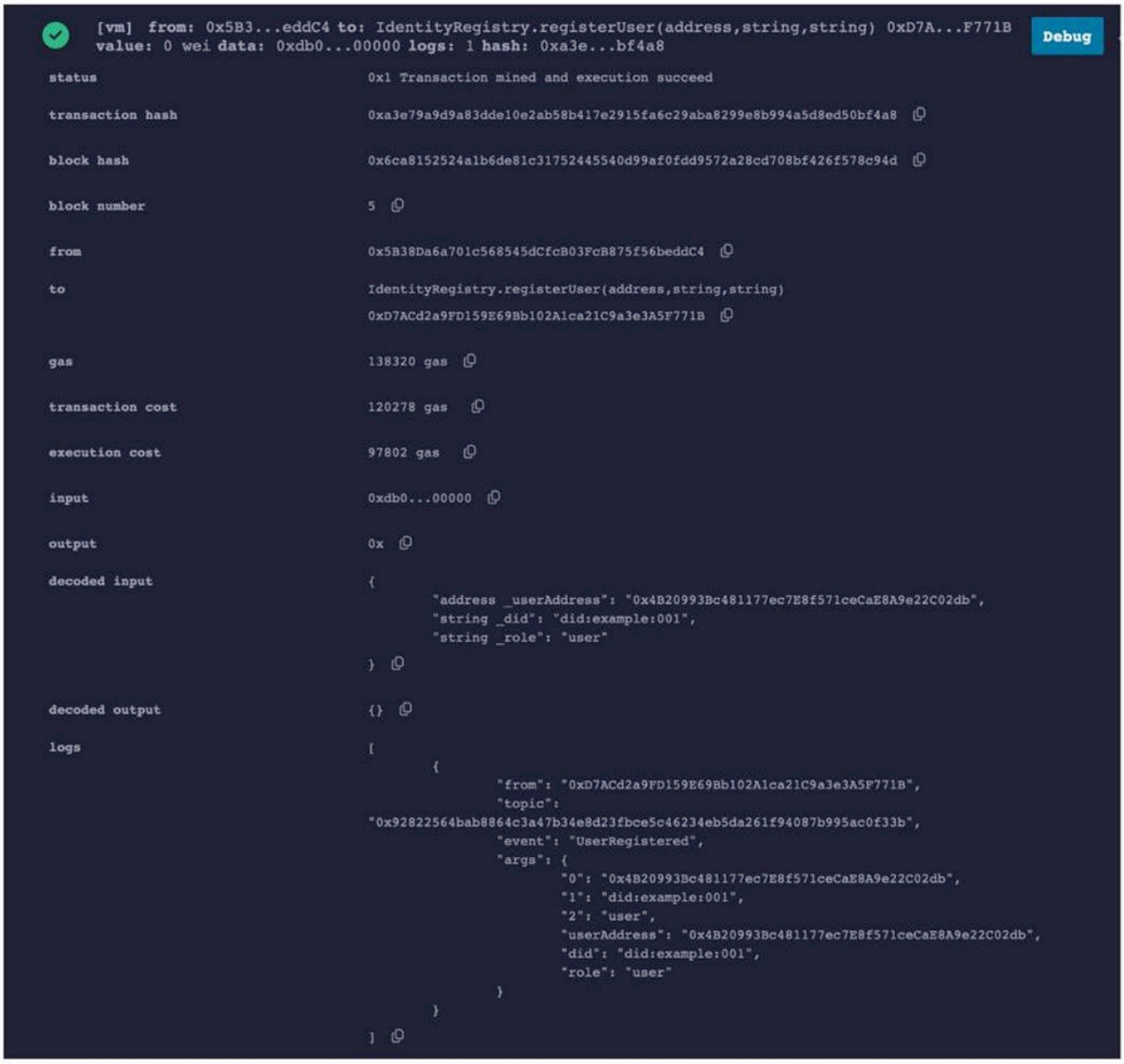


Рис. 8 – Візуалізація транзакції реєстрації користувача в системі ідентифікації

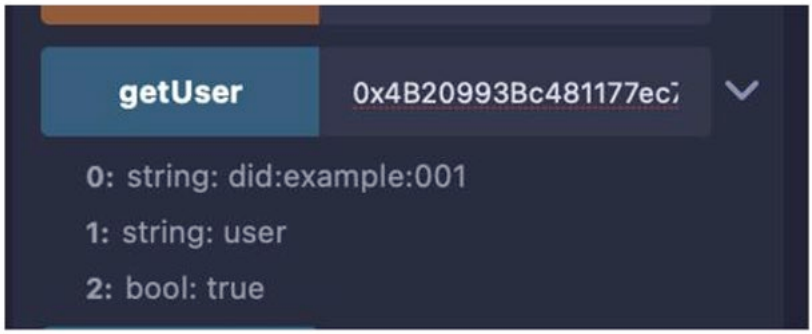


Рис. 9 – Результат перевірки даних зареєстрованого користувача методом getUser

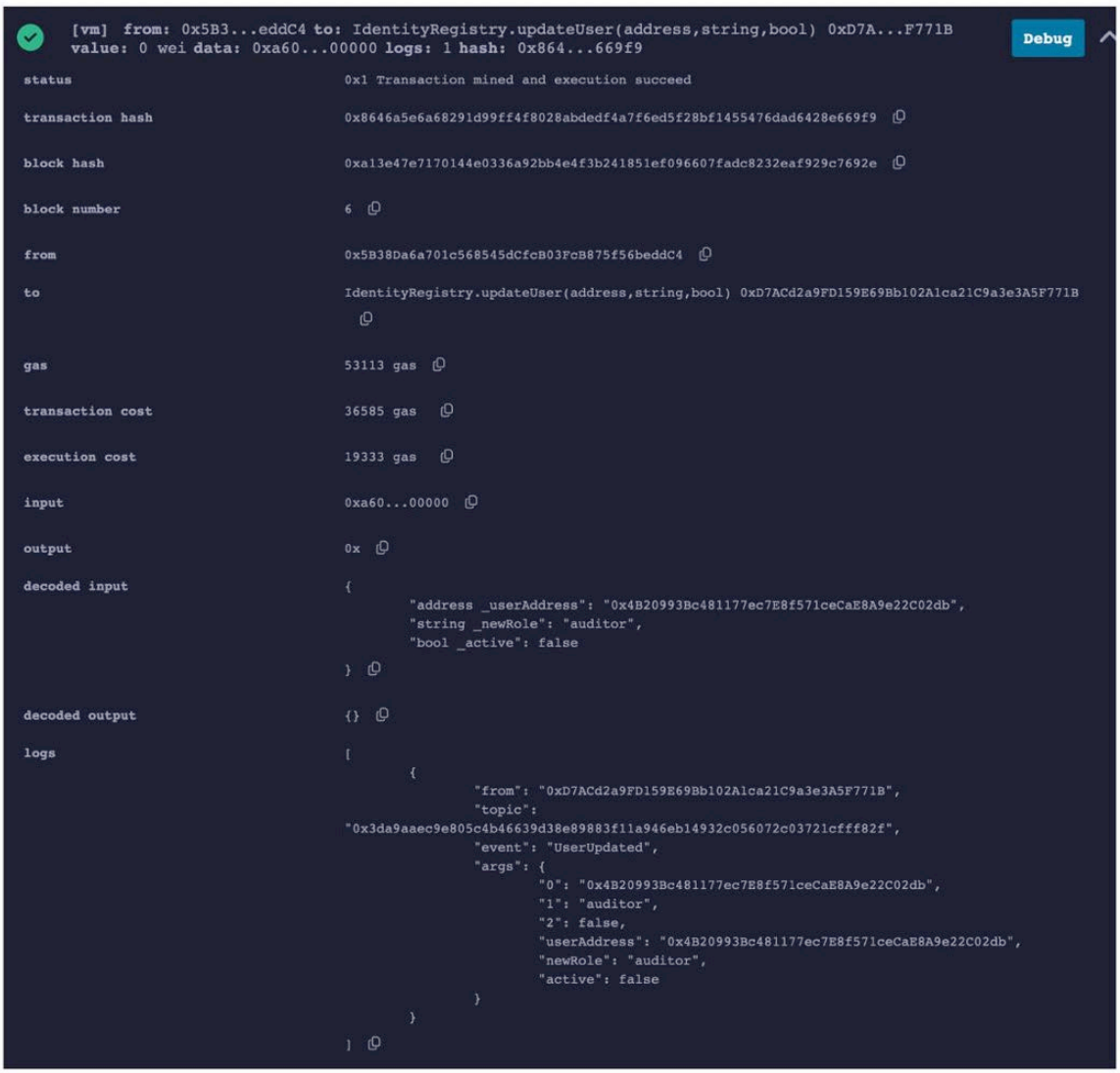


Рис. 10 – Результат виконання транзакції оновлення ролі користувача в системі ідентифікації