ХЕРСОНСЬКИЙ НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ
ФАКУЛЬЕТ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ ТА ДИЗАЙНУ
КАФЕДРА ІНФОРМАТИКИ І КОМП'ЮТЕРНИХ НАУК

Пояснювальна записка
до кваліфікаційної роботи
магістра

на тему:

Моделювання систем захисту інформації з використанням технології Blockchain

Виконав: студент групи 6КІ спеціальності
122 – "Комп'ютерні науки"

Олійник Д.О.
Керівник: Доровський В.О.
Рецензент: к.т.н О.Є. Огнєва

Хмельницький – 2025 р.

Факультет Інформаційних технологій та дизайну

Кафедра Інформатики і комп'ютерних наук

Рівень вищої освіти магістр

Галузь підготовки 12 «Інформаційні технології»

(шифр і назва)

Освітньо-професійна програма Консолідована інформація

(назва)

Спеціальність 122 «Комп’ютерні науки»

(шифр і назва)

ЗАТВЕРДЖУЮ

В.о. завідувача кафедри ІКН,

к.т.н., доцент

_____ Моісеєнко С.В

«____» _____ 2025 року

З А В Д А Н Н Я

НА ДИПЛОМНУ РОБОТУ СТУДЕНТА

Олійник Даниїл Олександрович

(прізвище, ім’я, по батькові)

Тема роботи: Моделювання систем захисту інформації з використанням технології Blockchain.

1. Керівник роботи Доровський Володимир Олексійович, доктор технічних наук, професор кафедри програмних засобів і технологій
   (прізвище, ім’я, по батькові, науковий ступінь, вчене звання)
   затверджені наказом ХНТУ від «16» вересня 2025 р. № № 437-с_
2. Строк подання студентом роботи

_____

3. Вихідні дані до роботи: Аналіз основ захисту інформації з використання технології Blockchain. Вивчення ключових аспектів для реалізації моделі системи. Розробка систему захисту та перевірки інформації, а також порівняння з іншими системами інформаційного захисту.
4. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити): Вступ. 1 Теоретичні основи захисту інформації та технології Blockchain, 2 Аналіз та постановка задачі, 3 Розробка моделі системи захисту інформації, 4 Оцінка ефективності та перспективи використання.
5. Перелік графічного матеріалу (з точним зазначенням обов'язкових креслень) Рисунків – 35, Таблиць - 2, Формул – 2

6. Дата видачі завдання 13.10.2025

КАЛЕНДАРНИЙ ПЛАН

/п	Назва етапів дипломної роботи	Строк етапів роботи	Прим.
	Огляд літературних джерел	01.10.25-05.10.25	+
	Написання плану для дипломної роботи	06.10.25-12.10.25	+
	Написання першого розділу роботи з теоретичними основами захисту інформації та технології Blockchain	13.10.25-25.10.25	+
	Постанова задачі та написання другої частини з аналізом предметної області	26.10.25-11.11.25	+
	Розробка моделі системи захисту інформації	12.11.25-23.11.25	+
	Тестування та оцінка роботи моделі	24.11.25-26.11.25	+
	Оцінка ефективності та перспективи використання моделі	27.11.25-30.11.25	+
	Оформлення роботи, посилань, практичного прототипу	01.12.25-03.12.25	+

Студент _____ Олійник Д.О.

(підпис) (прізвище та ініціали)

Керівник роботи _____ Доровський В.О.

(підпис) (прізвище та ініціали)

ЗМІСТ

ПЕРЕЛІК УМОВНИХ СКОРОЧЕНЬ

ПЗ	Програмне забезпечення
RBAC	Role-Based Access Control
ІС	Інформаційна система
ІБ	Інформаційна безпека
ECDSA	Elliptic Curve Digital Signature Algorithm
MITM	Man-in-the-Middle
VPN	Virtual Private Network
MFA	Multi-Factor Authentication
PoW	Proof of Work
EVM	Ethereum Virtual Machine
DeFi	Decentralized Finance
BTC	Bitcoin
ETH	Ethereum
USDT	Tether
XRP	Ripple
DOGE	Dogecoin
АСУ	Автоматизована система управління
TPS	Transactions Per Second
PoS	Proof of Stake
PoA	Proof of Authority
EVM	Ethereum Virtual Machine
SPV	Simplified Payment Verification
CIA	Confidentiality, Integrity, Availability

АВТОРЕФЕРАТ

Робота присвячена аналізу основ захисту інформації з використання технології Blockchain з вивченням ключових аспектів для реалізації моделі системи. А також розробкою системи захисту та перевірки інформації, та її порівнянням з іншими системами інформаційного захисту.

Актуальність теми: "Моделювання систем захисту інформації з використанням технології Blockchain" є надзвичайн о актуальною через новітні способи зберігання інформації. У сучасному світі, де обсяг цифрових даних зростає з кожним роком, питання захисту інформації стає надзвичайно важливим.

Традиційні централізовані моделі зберігання та обробки даних мають суттєві недоліки: вони вразливі до кібератак, збоїв системи та несанкціонованого доступу**.**

Використання технології Blockchain дозволяє створювати децентралізовані, стійкі до змін і підробок системи, що забезпечують високу надійність і прозорість обміну інформацією. Завдяки криптографічним методам і механізмам консенсусу блокчейн гарантує цілісність і достовірність даних, що робить його перспективним інструментом у сфері інформаційної безпеки.

Розробка моделі системи захисту інформації з використанням блокчейну є актуальною через зростання потреби у надійних засобах захисту персональних, фінансових та корпоративних даних, особливо в умовах розвитку кіберзагроз і зростання кількості цифрових транзакцій.

Мета дослідження: полягає у розробці моделі системи захисту інформації з використанням технології Blockchain, яка забезпечує контроль доступу, збереження та перевірку цілісності даних у цифрових системах. Теоретично це передбачає аналіз існуючих методів захисту інформації, вивчення принципів децентралізованих систем, а також обґрунтування можливостей застосування Blockchain як основи для підвищення безпеки даних і прозорості процесів управління інформацією.

Наукова новизна: актуальність дослідження полягає у широких можливостях впровадження технології Blockchain у різні галузі — від державного управління до

фінансового сектору, медицини, логістики й освіти. Зі зростанням обсягів цифрової інформації та кіберзагроз роль блокчейну у побудові безпечних інформаційних систем лише посилюватиметься.

Практичне значення: Практичне значення виконаної дипломної роботи полягає у створенні працюючої моделі системи захисту даних на основі технології Blockchain, яка демонструє механізми забезпечення цілісності та неможливості підміни інформації. Розроблена архітектура може бути використана як основа для впровадження у реальні інформаційні системи — від електронного документообігу до систем аудиту, контролю доступу та логістичного відстеження. Модель є ефективним інструментом для навчальних та дослідницьких цілей, оскільки наочно показує принципи роботи блокчейну, структуру блоків, механізми верифікації та виявлення фальсифікацій. Запропоновані алгоритми можуть бути масштабовані та адаптовані для практичних рішень у сфері кібербезпеки.

Ключові слова**:** блокчейн, безпека, ланцюг, блок, криптографія, інформаційна безпека, цифровий підпис, верифікація, цілісність даних, автентифікація, модель загроз.

ABSTRACT

The work is devoted to the analysis of the fundamentals of information protection using Blockchain technology, focusing on the study of key aspects for the implementation of the system model. It also includes the development of a system for information protection and verification, as well as its comparison with other information security systems.

Relevance of the topic: "Modeling of information protection systems using Blockchain technology" is extremely timely due to the emergence of novel methods of information storage. In the modern world, where the volume of digital data increases every year, the issue of information protection is becoming crucially important.

Traditional centralized models of data storage and processing possess significant drawbacks: they are vulnerable to cyberattacks, system failures, and unauthorized access.

The use of Blockchain technology allows for the creation of decentralized systems that are resistant to changes and tampering, ensuring high reliability and transparency of information exchange. Thanks to cryptographic methods and consensus mechanisms, the blockchain guarantees data integrity and authenticity, making it a promising tool in the field of information security.

The development of a model for an information protection system using blockchain is relevant due to the growing need for reliable means of protecting personal, financial, and corporate data, especially in the context of evolving cyber threats and the increasing number of digital transactions.

The objective of the research: To develop a model of an information protection system using Blockchain technology that ensures access control, preservation, and verification of data integrity in digital systems. Theoretically, this involves the analysis of existing information protection methods, the study of the principles of decentralized systems, and the justification of the possibilities of applying Blockchain as a basis for improving data security and the transparency of information management processes.

Scientific novelty: the relevance of the study lies in the broad possibilities for implementing Blockchain technology across various sectors—from public administration

to the financial sector, medicine, logistics, and education. With the growth of digital information volumes and cyber threats, the role of blockchain in building secure information systems will only strengthen.

Practical significance: The practical value of the completed thesis lies in the creation of a working model of a data protection system based on Blockchain technology, which demonstrates mechanisms for ensuring integrity and preventing information tampering. The developed architecture can be used as a basis for implementation in real information systems - from electronic document management to audit systems, access control, and logistical tracking. The model serves as an effective tool for educational and research purposes, as it clearly illustrates the principles of blockchain operation, block structure, verification mechanisms, and fraud detection. The proposed algorithms can be scaled and adapted for practical solutions in the field of cybersecurity.

Keywords: blockchain, security, chain, block, cryptography, information security, digital signature, verification, data integrity, authentication, threat model.

ВСТУП

У сучасних умовах стрімкого розвитку цифрових технологій питання забезпечення надійного захисту інформації набуває особливої актуальності. Зі збільшенням обсягів даних та зростанням кількості кіберзагроз традиційні методи безпеки вже не завжди здатні ефективно протистояти підмінам, несанкціонованим змінам або втраті даних.

Одним із перспективних напрямів підвищення рівня захищеності інформаційних систем є впровадження технології Blockchain, яка завдяки своїй децентралізованій природі та криптографічним механізмам забезпечує високу цілісність, прозорість і достовірність інформації.[1]

Технологія блокчейн дозволяє побудувати невразливе до фальсифікацій середовище, де кожна зміна даних фіксується у вигляді окремого блоку, пов’язаного з попередніми за допомогою криптографічного хешування.

Такий підхід унеможливлює приховану модифікацію інформації та забезпечує повну простежуваність її історії. Використання Blockchain у системах захисту даних відкриває нові можливості для створення безпечних журналів подій, систем документообігу, реєстрів доступу та багатьох інших сфер, де важливо гарантувати незмінність та достовірність інформації.

Під час процесу моделювання систем захисту інформації важливим етапом є вибір мови програмування та середовища розробки, які забезпечують зручність створення, тестування та відлагодження програмних рішень.[1]

У даній роботі для реалізації моделі було обрано мову програмування Python, що є однією з найпоширеніших та найуніверсальніших мов сучасності. Python вирізняється простим і зрозумілим синтаксисом, високою читабельністю коду та широкою екосистемою бібліотек, що дозволяють ефективно реалізовувати криптографічні алгоритми, працювати з даними та моделювати складні системи.

Для організації програмної частини роботи використано інтегроване середовище розробки Thonny, створене спеціально для навчальних і дослідницьких цілей. Thonny забезпечує зручний інтерфейс, покроковий відлагоджувач і вбудовану

інтерактивну консоль, що дозволяє детально відстежувати виконання програми та виявляти логічні помилки на ранніх етапах.

Завдяки мінімалістичному дизайну та простоті використання це середовище ідеально підходить для розробки моделей, що потребують максимальної прозорості та керованості виконання.

Поєднання можливостей Python та функціоналу Thonny забезпечує ефективні умови для реалізації програмної частини дипломної роботи та дозволяє створити наочну модель системи захисту інформації на основі технології Blockchain. Це робить обрані інструменти оптимальними для виконання поставлених дослідницьких і практичних завдань. [2]

У ході виконання роботи було:

1. Проаналізовано теоретичні основи та методи захисту інформації**.** Встановлено, що технологія Blockchain завдяки архітектурі розподіленого реєстру та криптографічному зв’язуванню блоків дозволяє нівелювати ризики несанкціонованої модифікації даних. Визначено, що поєднання алгоритмів хешування (SHA-256) та асиметричного шифрування (ECDSA) створює надійний базис для побудови довірених систем без центрального адміністратора.
2. Сформульовано вимоги та спроектовано архітектуру системи**.** Розроблено структурну схему моделі, яка включає підсистеми ідентифікації користувачів (Wallet), обробки транзакцій, досягнення консенсусу PoW та імітації мережевої взаємодії (P2PNode). Обґрунтовано вибір мови програмування Python та середовища Thonny як оптимальних інструментів для реалізації криптографічних алгоритмів та навчального моделювання.
3. Здійснено програмну реалізацію моделі захищеного реєстру**.** Створено повнофункціональний програмний комплекс, який реалізує замкнений цикл обробки даних:
    - цілісність**:** - рабезпечено використанням хеш-функції SHA-256, що унеможливлює непомітну зміну історії транзакцій завдяки лавинному ефекту.

- автентичність**:** - реалізовано механізм цифрового підпису ECDSA, що гарантує невідмовність авторства та захист від підробки транзакцій.
- доступність та стійкість - впроваджено алгоритм консенсусу Proof-of-Work, який захищає мережу від спам-атак та узгоджує стан реєстру між вузлами.

4. Проведено комплексне тестування та верифікацію моделі**.** Експериментальні дослідження підтвердили працездатність та надійність розробленої системи:
   - функціональне тестування довело коректність роботи всіх модулів: генерація ключів, майнінг, валідація ланцюга.
   - навантажувальне тестування Benchmarking дозволило визначити пропускну здатність системи та підтвердило експоненціальну залежність часу генерації блоку від складності задачі, що свідчить про ефективність захисту PoW.
   - симуляція атаки - довела стійкість системи до несанкціонованої модифікації даних. Спроба прямого втручання в пам’ять вузла була миттєво виявлена алгоритмом валідації через невідповідність хеш-сум, що призвело до автоматичного відхилення скомпрометованого ланцюга.
5. Визначено перспективи практичного застосування**.** Показано, що розроблена архітектура може бути ефективно використана не лише для фінансових розрахунків, але й у системах електронного документообігу, цифрового нотаріату, голосування та захисту журналів аудиту критичних систем. Запропоновано шляхи подальшого вдосконалення, зокрема перехід на енергоефективні алгоритми консенсусу PoS та впровадження смарт-контрактів для автоматизації бізнес-процесів.

Актуальність теми: "Моделювання систем захисту інформації з використанням технології Blockchain" є надзвичайн о актуальною через новітні способи зберігання інформації. У сучасному світі, де обсяг цифрових даних зростає з кожним роком, питання захисту інформації стає надзвичайно важливим.

Традиційні централізовані моделі зберігання та обробки даних мають суттєві недоліки: вони вразливі до кібератак, збоїв системи та несанкціонованого доступу**.**

Використання технології Blockchain дозволяє створювати децентралізовані, стійкі до змін і підробок системи, що забезпечують високу надійність і прозорість обміну інформацією. Завдяки криптографічним методам і механізмам консенсусу блокчейн гарантує цілісність і достовірність даних, що робить його перспективним інструментом у сфері інформаційної безпеки. [3]

Розробка моделі системи захисту інформації з використанням блокчейну є актуальною через зростання потреби у надійних засобах захисту персональних, фінансових та корпоративних даних, особливо в умовах розвитку кіберзагроз і зростання кількості цифрових транзакцій.

Мета дослідження: полягає у розробці моделі системи захисту інформації з використанням технології Blockchain, яка забезпечує контроль доступу, збереження та перевірку цілісності даних у цифрових системах. Теоретично це передбачає аналіз існуючих методів захисту інформації, вивчення принципів децентралізованих систем, а також обґрунтування можливостей застосування Blockchain як основи для підвищення безпеки даних і прозорості процесів управління інформацією.

Об'єкт дослідження: це процес захисту інформації **у** комп’ютерних системах з використанням технології Blockchain, що включає в себе методи зберігання, та перевірки надійності даних у розподіленому середовищі.

Предмет дослідження: це модель системи захисту інформації, побудована на базі технології Blockchain, її архітектура, принципи функціонування, алгоритми безпеки та методи забезпечення цілісності й конфіденційності даних.

Завдання дослідження:

- Ознайомитися з теоретичними основи захисту інформації та технології Blockchain;
- Провести аналіз сучасних загроз інформаційній безпеці та існуючих методів захисту даних у розподілених системах;
- Продемонструвати архітектуру blockchain;

– Обгрунтувати вибір технологічного стеку та криптографічних примітивів для реалізації моделі;

– Розробити модель системи захисту інформації.

Методи дослідження:

– Системний аналіз для оцінки перспектив використання технології blockchain;

– Моделювання та проектування моделі захисту інформації мовою python;

– Методи системного аналізу для визначення вимог до системи захисту інформації та класифікації загроз;

– Порівняльний аналіз для зіставлення ефективності розробленої моделі з традиційними централізованими базами даних;

– Методи прикладної криптографії — для реалізації функцій хешування та електронного цифрового підпису з метою забезпечення цілісності та автентичності даних.

Наукова новизна: актуальність дослідження полягає у широких можливостях впровадження технології Blockchain у різні галузі — від державного управління до фінансового сектору, медицини, логістики й освіти. Зі зростанням обсягів цифрової інформації та кіберзагроз роль блокчейну у побудові безпечних інформаційних систем лише посилюватиметься.

Практичне значення: Практичне значення виконаної дипломної роботи полягає у створенні працюючої моделі системи захисту даних на основі технології Blockchain, яка демонструє механізми забезпечення цілісності та неможливості підміни інформації. Розроблена архітектура може бути використана як основа для впровадження у реальні інформаційні системи — від електронного документообігу до систем аудиту, контролю доступу та логістичного відстеження. Модель є ефективним інструментом для навчальних та дослідницьких цілей, оскільки наочно показує принципи роботи блокчейну, структуру блоків, механізми верифікації та виявлення фальсифікацій. Запропоновані алгоритми можуть бути масштабовані та адаптовані для практичних рішень у сфері кібербезпеки. [4]