АНОТАЦІЯ

Ситник Р.С. **Моделі і методи організації та забезпечення цілісності даних у реєстрах інформаційних систем**. – Кваліфікаційна наукова праця на правах рукопису. Дисертація на здобуття наукового ступеня доктора філософії за спеціальністю 122 «Комп'ютерні науки». – Український державний університет науки і технологій. – Дніпро, 2025.

Дисертаційну роботу виконано на кафедрі інформаційних технологій і систем науково навчального інституту «Дніпровський металургійний інститут» Українського державного університету науки і технологій

Актуальність дослідження. В умовах стрімкого розвитку Industry 4.0 та цифровізації логістичних процесів виникає гостра необхідність вирішення критичних проблем безпеки даних у сучасних інформаційних системах.

Традиційні централізовані архітектури логістичних інформаційних систем демонструють суттєві обмеження при роботі з глобальними ланцюжками постачання, включаючи відсутність ефективних механізмів верифікації даних, недостатню прозорість, вразливість до кібератак та складність забезпечення цілісності інформації.

Дисертація складається зі вступу, чотирьох розділів, висновків, списку використаних джерел та додатку. Повний обсяг дисертації – 139 сторінок; список використаних джерел зі 68 найменувань, 2 додатків. Робота проілюстрована 12 рисунками та містить 5 таблиць.

Метою роботи є підвищення рівня безпеки та ефективності управління даними у логістичних інформаційних системах шляхом розробки методу забезпечення достовірності та цілісності на основі технології блокчейн.

Наукова новизна одержаних результатів

- Вперше розроблено нову модель оцінки загроз безпеці в логістичних інформаційних системах, яка враховує специфіку блокчейн-архітектури та базується на комплексному аналізі вразливостей, що

дозволило розширити можливості виявлення потенційних атак та підвищити точність оцінки ризиків в умовах розподіленої обробки даних.

- Вперше запропоновано оригінальний метод забезпечення достовірності даних, що ґрунтується на удосконалених деревах Меркла та інтелектуальних смарт-контрактах, який дозволив суттєво підвищити рівень захищеності системи, автоматизувати процеси верифікації та забезпечити незмінність даних у ланцюжку постачання.
- Отримав подальший розвиток процес верифікації транзакцій у розподілених логістичних системах на основі багаторівневої системи криптографічних механізмів, що дозволило значно підвищити надійність передачі даних між учасниками, мінімізувати ризики несанкціонованої модифікації інформації та забезпечити прозорість операцій.
- Удосконалено механізми контролю доступу до даних шляхом впровадження ієрархічної системи смарт-контрактів та криптографічних токенів, що розширило можливості гнучкого управління правами користувачів, підвищило адаптивність системи та забезпечило надійну ізоляцію конфіденційних даних.
- Розвинуто методи захисту інформаційних потоків у логістичних системах за рахунок впровадження механізмів проактивного моніторингу блокчейн-транзакцій, що дозволило своєчасно виявляти спроби несанкціонованого доступу та підвищити загальний рівень безпеки системи.

Основний зміст дисертаційної роботи

Дисертаційна робота присвячена задачам забезпечення достовірності та цілісності даних у логістичних інформаційних системах на основі технології блокчейн.

За результатами дослідження розроблено:

- Модель виявлення актуальних загроз безпеці в логістичних інформаційних системах, що враховує специфіку блокчейн-архітектури та базується на комплексному аналізі вразливостей;

- Метод забезпечення достовірності даних на основі удосконалених дерев Меркла та інтелектуальних смарт-контрактів.

У **першому розділі** проведено комплексний аналіз сучасного стану логістичних інформаційних систем та виявлено критичні проблеми забезпечення безпеки даних в умовах Industry 4.0. На основі дослідження традиційних централізованих архітектур охарактеризовано їх основні недоліки: відсутність ефективних механізмів верифікації даних між незалежними учасниками ланцюжка постачання, недостатню прозорість процесів, вразливість до кібератак та складність забезпечення цілісності інформації при розподіленій обробці. З'ясовано, що глобальні ланцюжки постачання характеризуються високою складністю взаємодії множини постачальників, виробників, транспортних компаній та дистриб'юторів з різних країн, кожен з яких має власні інформаційні системи та стандарти обробки даних. Окреслено перспективні напрями використання блокчейн-технології для вирішення виявлених проблем, включаючи забезпечення довіри між учасниками без централізованого посередника, автоматизацію бізнес-процесів через смарт-контракти та створення незмінного аудиторського сліду логістичних операцій.

У **другому розділі** розроблено модель виявлення актуальних загроз порушення інформаційної безпеки даних в блокчейн-системах логістичного призначення. Проаналізовано специфічні загрози, властиві розподіленим системам: атаки на механізми консенсусу, вразливості смарт-контрактів на рівні мови програмування Solidity, загрози подвійної трати, атаки Сибілли та DDoS-атаки на мережеву інфраструктуру. Формалізовано математичний апарат для оцінки ризиків на основі теорії нечітких множин, де кожен деструктивний вплив описується коефіцієнтами порушення конфіденційності, цілісності, доступності та достовірності. Запропоновано багаторівневу класифікацію загроз: рівень блокчейн-протоколу, рівень смарт-контрактів, рівень бізнес-логіки та рівень зовнішньої взаємодії. Розроблено методику

визначення небезпечності загроз через комплексний аналіз характеристик об'єкта захисту, типу загрози та потенційного деструктивного впливу.

У **третьому розділі** розроблено комплексний метод забезпечення достовірності та цілісності персональних даних на основі модифікованих дерев Меркла та інтелектуальних смарт-контрактів. Запропоновано архітектуру децентралізованої логістичної системи, яка використовує технологію Ethereum Virtual Machine для виконання бізнес-логіки без централізованого сервера. Детально описано структуру смарт-контрактів для управління правами власності на ресурси, відстеження їх переміщень та автоматизації процесів верифікації. Формалізовано протоколи взаємодії між чотирма основними ролями учасників системи: постачальниками, виробниками, транспортерами та дистриб'юторами. Описано механізми криптографічного захисту через цифрові підписи на основі еліптичних кривих та процедури валідації транзакцій через протоколи консенсусу.

У **четвертому розділі** проведено експериментальну валідацію ефективності запропонованого методу через порівняльне тестування з традиційними MySQL-системами на наборах даних різного обсягу. Результати показали суттєві переваги блокчейн-підходу: час верифікації цілісності даних зменшився завдяки логарифмічній складності дерев Меркла проти квадратичної складності SQL JOIN-операцій. Продемонстровано практичну реалізацію системи на базі Ethereum з використанням 10 незалежних вузлів, що емулюють реальну мережу учасників логістичного ланцюжка. Підтверджено можливість забезпечення незмінності та повної простежуваності логістичних операцій при збереженні високої продуктивності та масштабованості системи.

Результати дослідження можуть бути використані при проектуванні та модернізації інформаційних систем у сфері логістики, управління ланцюжками постачання та інших галузях з розподіленою обробкою даних, що сприятиме підвищенню загальної ефективності та

безпеки логістичних операцій в умовах цифрової трансформації промисловості.

Ключові слова: блокчейн, логістичні інформаційні системи, смарт-контракти, модель, безпека даних, метод, ланцюжки постачання, дерева Меркла, цифрова трансформація, криптографічні методи, розподілені системи.

ABSTRACT

Sytnyk R.S. Models and Methods for Organization and Ensuring Data Integrity in Information System Registries. – Qualifying scientific work on the rights of a manuscript. Dissertation for obtaining the scientific degree of Doctor of Philosophy in specialty 122 "Computer Sciences". – Ukrainian State University of Science and Technology. – Dnipro, 2025.

Research Relevance

In the context of rapid Industry 4.0 development and digitalization of logistics processes, there is an urgent need to address critical data security problems in modern information systems. Traditional centralized architectures of logistics information systems demonstrate significant limitations when working with global supply chains, including the absence of effective data verification mechanisms, insufficient transparency, vulnerability to cyberattacks, and complexity in ensuring information integrity.

The dissertation consists of an introduction, four chapters, a conclusion, a list of sources used and appendices. The full volume of the dissertation is 139 pages; list of used sources of 68 titles, 2 appendices. The work is illustrated with 12 drawings and contains 5 tables.

Research Objective

The objective of this work is to enhance the level of security and efficiency of data management in logistics information systems by developing a method for ensuring authenticity and integrity based on blockchain technology.

Scientific Novelty of Obtained Results

- First development of a new security threat assessment model for logistics information systems that considers the specifics of blockchain architecture and is based on comprehensive vulnerability analysis, which expanded the capabilities for detecting potential attacks and improved risk assessment accuracy in distributed data processing conditions.

- First proposal of an original data authenticity assurance method based on enhanced Merkle trees and intelligent smart contracts, which significantly improved system security level, automated verification processes, and ensured data immutability in the supply chain.

- Further development of transaction verification processes in distributed logistics systems based on a multi-level system of cryptographic mechanisms, which significantly improved data transmission reliability between participants, minimized risks of unauthorized information modification, and ensured operation transparency.

- Enhancement of data access control mechanisms through implementation of a hierarchical system of smart contracts and cryptographic tokens, which expanded flexible user rights management capabilities, increased system adaptability, and ensured reliable isolation of confidential data.

- Development of information flow protection methods in logistics systems through implementation of proactive blockchain transaction monitoring mechanisms, which enabled timely detection of unauthorized access attempts and improved overall system security level.

Main Content of Dissertation Work

The dissertation work is devoted to problems of ensuring data authenticity and integrity in logistics information systems based on blockchain technology.

Based on research results, the following were developed:

- A model for identifying current security threats in logistics information systems that considers blockchain architecture specifics and is based on comprehensive vulnerability analysis;

- A method for ensuring data authenticity based on enhanced Merkle trees and intelligent smart contracts.

Chapter 1 conducts a comprehensive analysis of the current state of logistics information systems and identifies critical problems in ensuring data security under Industry 4.0 conditions. Based on the study of traditional centralized architectures, their main disadvantages are characterized: absence of effective data verification mechanisms between independent supply chain participants, insufficient process transparency, vulnerability to cyberattacks, and complexity in ensuring information integrity during distributed processing. It was determined that global supply chains are characterized by high complexity of interaction among multiple suppliers, manufacturers, transport companies, and distributors from different countries, each having their own information systems and data processing standards. Promising directions for using blockchain technology to solve identified problems are outlined, including ensuring trust between participants without a centralized intermediary, automating business processes through smart contracts, and creating an immutable audit trail of logistics operations.

Chapter 2 develops a model for identifying current threats to information security data breaches in blockchain systems for logistics purposes. Specific threats inherent to distributed systems are analyzed: attacks on consensus mechanisms, smart contract vulnerabilities at the Solidity programming language level, double-spending threats, Sybil attacks, and DDoS attacks on network infrastructure. Mathematical apparatus for risk assessment based on fuzzy set theory is formalized, where each destructive impact is described by coefficients of confidentiality, integrity, availability, and authenticity violations. A multi-level threat classification is proposed: blockchain protocol level, smart contract level, business logic level, and external interaction level. A methodology for determining threat danger through comprehensive analysis of protection object characteristics, threat type, and potential destructive impact is developed.

Chapter 3 develops a comprehensive method for ensuring personal data authenticity and integrity based on modified Merkle trees and intelligent smart

contracts. A decentralized logistics system architecture using Ethereum Virtual Machine technology for executing business logic without a centralized server is proposed. The structure of smart contracts for managing resource ownership rights, tracking their movements, and automating verification processes is described in detail. Interaction protocols between four main participant roles are formalized: suppliers, manufacturers, transporters, and distributors. Cryptographic protection mechanisms through digital signatures based on elliptic curves and transaction validation procedures through consensus protocols are described.

Chapter 4 conducts experimental validation of the proposed method's effectiveness through comparative testing with traditional MySQL systems on datasets of various volumes. Results showed significant advantages of the blockchain approach: data integrity verification time decreased by due to logarithmic complexity of Merkle trees versus quadratic complexity of SQL JOIN operations. Practical system implementation based on Ethereum using 10 independent nodes emulating a real network of logistics chain participants is demonstrated. The possibility of ensuring immutability and complete traceability of logistics operations while maintaining high system performance and scalability is confirmed.

Practical Application

Research results can be used in designing and modernizing information systems in logistics, supply chain management, and other industries with distributed data processing, which will contribute to improving overall efficiency and security of logistics operations under industrial digital transformation conditions.

Keywords: blockchain, logistics information systems, smart contracts, Merkle trees, model, data security, method, supply chains, digital transformation, cryptographic methods, distributed systems.