МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ “ЛЬВІВСЬКА ПОЛІТЕХНІКА”

Кваліфікаційна наукова
праця на правах рукопису

БАЛАЦЬКА ВАЛЕРІЯ СЕРГІЇВНА

УДК 004.056.53

ДИСЕРТАЦІЯ

ПІДВИЩЕННЯ ЕФЕКТИВНОСТІ ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ КОРИСТУВАЧІВ В УМОВАХ ЦИФРОВОЇ ІНФОРМАТИЗАЦІЇ ДЕРЖАВНИХ РЕЄСТРІВ УКРАЇНИ

125 Кібербезпека
(шифр і назва спеціальності)
12 «Інформаційні технологій»
(галузь знань)

Подається на здобуття наукового ступеня доктора філософії
Дисертація містить результати власних досліджень. Використання ідей, результатів і текстів інших авторів мають посилання на відповідне джерело
_____/ Балацька Валерія Сергіївна /

Науковий керівник: Опірський Іван Романович, доктор технічних наук, професор

Львів – 2025

АНОТАЦІЯ

Балацька В.С. **Підвищення ефективності захисту персональних даних користувачів в умовах цифрової інформатизації державних реєстрів України.** – Кваліфікаційна наукова праця на правах рукопису.

Дисертація на здобуття наукового ступеня доктора філософії за спеціальністю

125 «Кібербезпека» – ІКТА Національний університет "Львівська політехніка" України, Львів, 2025.

У контексті стрімкої цифрової трансформації суспільства та розширення сфери застосування електронного урядування, забезпечення достовірності та захисту персональних даних користувачів стало одним із ключових викликів для державних інформаційних систем. Масштабна інтеграція цифрових сервісів, зростання обсягів оброблюваних даних, а також підвищення ризику несанкціонованого доступу потребують впровадження сучасних технологій перевірки та контролю достовірності даних.

Наявні державні реєстри базуються переважно на централізованих підходах, що не враховують специфіку змістової верифікації та не гарантують високий рівень довіри до цифрової інформації. Традиційні механізми контролю (ACL, RBAC, цифрові підписи) забезпечують лише формальну валідність, залишаючи поза увагою контекст, логіку транзакцій та поведінкові відхилення. Така ситуація зумовлює потребу в комплексному вирішенні проблеми достовірності персональних даних на концептуальному, архітектурному та алгоритмічному рівнях.

У дисертаційній роботі реалізовано підхід до побудови багаторівневої моделі верифікації достовірності в дозвільному блокчейн-середовищі, орієнтований на державні цифрові платформи. Запропоновано гібридну модель захищеного зберігання персональних даних, яка відповідає вимогам нормативних актів, зокрема GDPR, ISO/IEC 27701 та Закону України № 4336-IX, і забезпечує інтеграцію принципів достовірності, прозорості та стійкості до кіберзагроз. Окрему увагу приділено створенню математичної моделі верифікації транзакцій

на основі смарт-контрактів, доведення з нульовим розголошенням та алгоритмів машинного навчання, що дозволяє виявляти аномальні дії без розкриття конфіденційної інформації.

Об’єктом дослідження є процеси забезпечення достовірності персональних даних у цифрових реєстрах з використанням блокчейн-систем.

Предметом дослідження є методи, моделі та архітектури верифікації достовірності транзакцій у дозвільному блокчейн-середовищах із урахуванням нормативних вимог, поведінкових ризиків і криптографічної безпеки.

У процесі дослідження використано методи порівняльного аналізу, функціонального моделювання, статистичної валідації, алгоритмічного проєктування, машинного навчання, симуляційного тестування, побудови формальних математичних моделей, а також аналізу ризиків згідно з вимогами ISO/IEC 27005 і NIST SP 800-30.

У першому розділі «Аналіз методів забезпечення безпеки захисту персональних даних при розробці та експлуатації інформаційних систем» здійснено системний огляд нормативних актів, міжнародних стандартів, а також наукових і прикладних публікацій у сфері цифрової довіри та верифікації персональних даних. Проаналізовано підходи до забезпечення безпеки в державних інформаційних системах, виокремлено проблеми формальної, змістової та контекстної достовірності, сформульовано наукову доцільність інтеграції багаторівневих моделей перевірки даних у блокчейн-архітектури. Обґрунтовано застосування принципу Privacy by Design, псевдонімізації та принципів мінімізації даних відповідно до Закону України № 4336-IX від 27.03.2025 щодо вимог до КСЗІ класу АС-1.

У другому розділі «Розробка моделі виявлення загроз у блокчейн-системах» сформульовано концептуальні положення щодо захисту інформації в дозвільному блокчейн-середовищах. На основі критичного аналізу класичних методик STRIDE, DREAD, NIST CSF, MITRE ATT&CK встановлено їхню обмежену ефективність у децентралізованих умовах. Розроблено адаптивну модель виявлення загроз, що враховує специфіку обробки персональних даних у

блокчейн-системах без централізованого контролю. Визначено архітектурні вимоги до таких моделей, запропоновано поведінковий підхід до виявлення ризикових транзакцій у режимі реального часу.

У третьому розділі «Розробка методу забезпечення достовірності даних у блокчейн-системах» запропоновано триетапну модель верифікації достовірності транзакцій, яка поєднує смарт-контракти для перевірки структури, Zero Knowledge Proof для криптографічного підтвердження правомірності та машинне навчання для поведінкової валідації. Побудовано формальну математичну модель функціонування системи та реалізовано її у вигляді REST API-сервісу на базі Hyperledger Fabric. Розроблена гібридна модель поєднує on-chain метадані з off-chain зберіганням зашифрованих даних, що забезпечує баланс між безпекою, масштабованістю та відповідністю GDPR.

У четвертому розділі «Оцінка ефективності запропонованого методу» проведено повномасштабне експериментальне дослідження з симульованими транзакціями (n = 300), що підтвердило точність верифікації на рівні до 93,4%, середній час обробки – 0.066 с. Здійснено моделювання п’яти типів атак, включаючи DoS, Unauthorized Submit, Brute-force Payload, підміну даних, Sniffed Replay. Запропоновано методику розгортання у хмарних середовищах, впроваджено прототип адміністративного дашборду, що дозволяє здійснювати візуальний контроль за достовірністю транзакцій і станом безпеки системи.

У висновках дисертації сформульовано основні наукові та практичні результати, зокрема: побудова математично обґрунтованої моделі перевірки достовірності транзакцій, розробка гібридної моделі з безпечним зберіганням персональних даних, інтеграція моделі в дозвільному блокчейн з урахуванням нових вимог Закону № 4336-IX, формалізація критеріїв прийняття рішень на основі машинного навчання, оцінка ефективності в експериментальних умовах. Запропоновані підходи можуть бути використані у державних цифрових системах з підвищеними вимогами до надійності та прозорості обробки персональних даних

Ключові слова: кібербезпека, персональні дані, інформаційна безпека,

достовірність інформації, триетапна модель перевірки достовірності, поведінкова верифікація, державні реєстри, цифрова ідентифікація, блокчейн, дозвільний блокчейн, смарт-контракти, доведення з нульовим розголошенням, REST API, Hyperledger Fabric, захист даних, захист від загроз, ризик-орієнтована перевірка, гібридна модель зберігання, критична інформаційна інфраструктура, моделювання атак, DDoS, машинне навчання, інформаційні системи, ISO/IEC 27701, GDPR, Закон України № 4336-IX, фізичні чинники безпеки, моделі обробки цифрових сигналів, біометрична ідентифікація, методи підвищення стійкості до витоку даних.

Список публікацій здобувачки:

Наукові праці, в яких опубліковано наукові результати дисертації:

1. Балацька В. С., Опірський І. Р. (2023) Забезпечення конфіденційності персональних даних і підтримки кібербезпеки за допомогою блокчейну // Кібербезпека: освіта, наука, техніка. – 2023. – № 4 (20). – С. 6-19. DOI: https://doi.org/10.28925/2663-4023.2023.20.619

2. Opirskyy I., Balatska V., Poberezhnyk V. (2023) Modern possibilities of use blockchain technology in the education system // Ukrainian Scientific Journal of Information Security. – 2023. – Vol. 29, issue 3. – P. 138-146. DOI: https://doi.org/10.18372/2225-5036.29.18073

3. Poberezhnyk V., Balatska V., Opirskyy I. (2023) Development of the learning management system concept based on blockchain technology // CEUR Workshop Proceedings. – 2023. – Vol. 3550 : Cybersecurity providing in information and telecommunication systems II 2023. – P. 38-49. URL: https://ceur-ws.org/Vol-3550/

4. Balatska V., Poberezhnyk V., Petriv P., Opirskyy I. (2024) Blockchain application concept in SSO technology context // CEUR Workshop Proceedings. – 2024. – Vol. 3654 : Cybersecurity Providing in Information and Telecommunication Systems. – P. 38-49. URL: https://ceur-ws.org/Vol-3654/

5. Балацька В. С., Побережник В. О., Опірський І. Р. (2024) Використання Non-Fungible Tokens та блокчейн для розмежування доступу до державних реєстрів // Кібербезпека: освіта, наука, техніка. – 2024. – № 4 (24). – С. 99-114. DOI:

https://doi.org/10.28925/2663-4023.2024.24.99114

6. Balatska V., Poberezhnyk V., Opirskyy I. (2024) Utilizing blockchain technologies for ensuring the confidentiality and security of personal data in compliance with GDPR // CEUR Workshop Proceedings. – 2024. – Vol. 3800 : Cyber Security and Data Protection. – P. 70-80. URL: https://ceur-ws.org/Vol-3800/

7. Balatska V., Opirskyy I., Slobodian N. (2024) Blockchain for enhancing transparency and trust in government registries // CEUR Workshop Proceedings. – 2024. – Vol. 3826 : Cybersecurity Providing in Information and Telecommunication Systems II. – P. 50-59. URL: https://ceur-ws.org/Vol-3826/

8. Balatska V., Opirskyy I. (2024) Blockchain as a tool for transparency and protection of government registries // Ukrainian Scientific Journal of Information Security. – 2024. – Vol. 30, issue 2. – P. 221-230. DOI: https://doi.org/10.18372/2225-5036.30.19211

9. Балацька В. С., Побережник В. О. (2024) Концепція застосування блокчейн-технологій для підвищення захищеності персональних даних платформи «Дія»: відповідність вимогам GDPR та українському законодавству // Кібербезпека: освіта, наука, техніка. – 2024. – № 2 (26). – С. 268-290. DOI: https://doi.org/10.28925/2663-4023.2024.26.681

10. Ivanusa A., Tkachuk R., Brych T., Balatska V., Tkachenko A. (2024) Методи та моделі проєктування системи автоматизованого пошуку вразливостей у Web-додатках // Вісник Львівського державного університету безпеки життєдіяльності. – 2024. – № 30. – С. 110-122. DOI: https://doi.org/10.32447/20784643.30.2024.11

11. Балацька В. С., Побережник В. О., Стефанків А. В., Шевчук Ю. А. Розробка методу забезпечення достовірності та безпеки персональних даних у блокчейн-системах державних реєстрів. Комп'ютерні системи та мережі. 2025. Т. 7, № 1. С. 1–16. DOI: https://doi.org/10.23939/csn2025.01.001

Наукові праці, які засвідчують апробацію матеріалів дисертації:

12. Балацька В. С., Опірський І. Р. Механізми досягнення надійності в блокчейні для захисту персональних даних // Захист інформації і безпека інформаційних систем : матеріали IX Міжнародної науково-технічної конференції

(Львів, 25–26 травня 2023 р.). – 2023. – С. 17-18.

13. Балацька В. С., Побережник В. О., Опірський І. Р. Потенційне використання технології блокчейн в уряді // Інформаційна безпека та інформаційні технології : збірник тез доповідей VI Всеукраїнської науково-практичної конференції молодих учених, студентів і курсантів, м. Львів, 30 листопада 2023 року. – 2023. – С. 228-230.

14. Побережник В. О., Балацька В. С., Опірський І. Р. Концепція використання технології блокчейн у сфері освіти // Інформаційна безпека та інформаційні технології : збірник тез доповідей VI Всеукраїнської науково-практичної конференції молодих учених, студентів і курсантів, м. Львів, 30 листопада 2023 року. – 2023. – С. 386-388.

15. Балацька В. С., Побережник В. О., Опірський І. Р. Технології блокчейн, NFT та IPFS для підвищення ефективності та безпеки державних реєстрів України // Безпека інформаційних технологій : матеріали XIII Міжнародної науково-технічної конференції ITSec-2024 (9–11 травня 2024, Львів, Україна). – 2024. – С. 51-52.

16. Балацька В. С., Опірський І. Р. Підвищення безпеки державних реєстрів України за допомогою трьохфакторної аутентифікації на основі блокчейн // Актуальні проблеми сучасної науки в дослідженнях молодих учених, курсантів та студентів : тези доповідей Всеукраїнської науково-практичної конференції (21 червня 2024, Вінниця, Україна). – 2024. – С. 585-588.

17. Побережник В. О., Балацька В. С., Опірський І. Р. Адаптація блокчейн облікових даних до вимог GDPR // Інноваційні технології у розвитку сучасного суспільства : тези доповідей VI Міжнародної науково-практичної конференції, 10–11 жовтня 2024 року, Львів. – 2024. – С. 39-41.

18. Балацька В. С., Опірський І. Р. Впровадження блокчейн-технологій для забезпечення безпеки та прозорості державних реєстрів // Сектор безпеки і оборони України на захисті національних інтересів: актуальні проблеми та завдання в умовах воєнного стану : тези доповідей III Міжнародної науково-практичної конференції, 21 листопада 2024 року, Хмельницький. – 2024. – С. 1094-1096.

19. Балацька В. С., Побережник В. О. Використання технологій блокчейн та NFT для розмежування доступу до державних реєстрів // Інформаційна безпека та інформаційні технології, ІБІТ 2024 : збірник доповідей V Міжнародної науково-практичної конференції, м. Львів, 27 листопада 2024 року. – 2024. – С. 6–8.

20. Балацька В. С., Опірський І. Р. Технологія блокчейн для забезпечення довіри та прозорості у державних реєстрах // Інформаційна безпека та інформаційні технології, ІБІТ 2024 : збірник доповідей V Міжнародної науково-практичної конференції, м. Львів, 27 листопада 2024 року. – 2024. – С. 251-253.

21. Побережник В. О., Балацька В. С., Опірський І. Р. Концепція самосуверенної ідентичності як альтернатива традиційним методам автентифікації // Інформаційна безпека та інформаційні технології, ІБІТ 2024 : збірник доповідей V Міжнародної науково-практичної конференції, м. Львів, 27 листопада 2024 року. – 2024. – С. 262-265.

22. Балацька В. С., Побережник В. О. Інформаційна безпека державних реєстрів: потенціал блокчейну для захисту критично важливих даних // Міжнародна та національна безпека: теоретичні і практичні аспекти : матеріали IX Міжнародної науково-практичної конференції, 21 березня 2025 р., м. Дніпро. Ч. 2. – Дніпро, 2025. – С. 468–471.

23. Побережник В. О., Балацька В. С. Концепція цифрового суверенітету в умовах розвитку блокчейн-економіки // Матеріали Міжнародної науково-практичної конференції «Blockchain Technologies and Engineering 2025» (BTE 2025), м. Київ, 26 березня 2025 р. – Київ: ІПМЕ НАН України, 2025. – С. 75–76.

SUMMARY

Balatska V.S. **Enhancing the Effectiveness of Personal Data Protection in the Context of Digital Informatization of State Registers in Ukraine**. – Qualifying scientific work on manuscript rights.

Dissertation for obtaining the scientific degree of Doctor of Philosophy in the specialty 125 «Cyber Security and Information Protection». – Institute of Computer Technologies, Automation and Metrology, Lviv Polytechnic National University, Lviv, 2025.

In the context of rapid digital transformation and the growing integration of electronic governance systems, ensuring the reliability and protection of users' personal data has become a critical challenge for national information systems. The massive scale of data processing and increased risks of unauthorized access necessitate the implementation of modern technologies for data verification and trust management.

The existing state registries are primarily based on centralized approaches, which lack semantic verification and do not guarantee a high level of trust in digital information. Traditional verification mechanisms such as ACL, RBAC, and digital signatures provide only formal validity without considering the logical structure, context, or behavioral anomalies in transactions. Therefore, a comprehensive solution addressing data reliability at the conceptual, architectural, and algorithmic levels is essential.

This dissertation proposes a multilayer verification model tailored for permission blockchain environments and aimed at national digital platforms. A hybrid architecture for secure storage of personal data is introduced, compliant with GDPR, ISO/IEC 27701, and the Ukrainian Law No. 4336-IX, integrating principles of trust, transparency, and resilience against cyber threats. Special attention is given to the development of a mathematical model for transaction verification based on smart contracts, Zero Knowledge Proofs, and machine learning algorithms, enabling the detection of anomalous behavior without disclosing sensitive data.

The object of the research is the process of ensuring the reliability of personal data in digital state registries using blockchain-based systems.

The subject of the research includes methods, models, and architectures for

transaction trust verification in permission blockchain environments, considering regulatory compliance, behavioral risks, and cryptographic security.

The methods used in the research include comparative analysis, functional modeling, statistical validation, algorithm design, machine learning, simulation testing, construction of formal mathematical models, and risk analysis according to ISO/IEC 27005 and NIST SP 800-30.

The first chapter, **"Analysis of Methods for Ensuring the Security of Personal Data during the Development and Operation of Information Systems"** provides a systematic review of legislation, international standards, and scientific publications in the field of digital trust and personal data verification. The study identifies the limitations of formal-only verification approaches in state systems and justifies the scientific need to integrate multi-layer verification models into blockchain architectures. The application of Privacy by Design principles, pseudonymization, and data minimization in accordance with Law No. 4336-IX on AIS-1 class CISS requirements is substantiated.

In the second chapter, **"Development of a Threat Detection Model in Blockchain Systems"** formulates the conceptual foundations of information protection in for permission blockchain environments. Based on the critical analysis of classical models such as STRIDE, DREAD, NIST CSF, and MITRE ATT&CK, their limited applicability in decentralized systems is demonstrated. An adaptive threat detection model is developed, incorporating behavioral analysis and architectural decentralization to identify risky transactions in real-time.

The third chapter**, "Development of a Method for Ensuring Data Trustworthiness in Blockchain Systems"** presents a three-stage model for transaction trust verification that integrates structural validation via smart contracts, cryptographic legitimacy confirmation using ZKP, and behavioral analysis through machine learning. A formal mathematical model of system operation is built and implemented as a REST API service using Hyperledger Fabric. The hybrid storage architecture combines on-chain metadata with off-chain encrypted data storage, ensuring security, scalability, and compliance with GDPR.

The fourth chapter, **"Evaluation of the Effectiveness of the Proposed Method"**

contains a full-scale experimental study using 300 simulated transactions to evaluate the accuracy (100%), response time (0.066 s), and resilience to five types of attacks (DoS, Unauthorized Submit, Brute-force Payload, Data Substitution, and Sniffed Replay). A cloud deployment methodology is proposed along with a prototype dashboard for administrative monitoring of transaction reliability and system security.

The **conclusions** summarize the scientific and practical contributions of the dissertation, including the development of a mathematically grounded model for transaction verification, the hybrid architecture for secure personal data storage, the integration of the model with for permission blockchain systems under Law No. 4336-IX, and the implementation of decision-making algorithms based on machine learning. The results offer a foundation for new trust paradigms in public information systems.

Keywords: cybersecurity, personal data, information security, information integrity, three-stage verification model, behavioral verification, state registries, digital identification, blockchain, permissioned blockchain, smart contracts, zero-knowledge proof, REST API, Hyperledger Fabric, data protection, threat prevention, risk-based verification, hybrid storage model, critical information infrastructure, attack modeling, DDoS, machine learning, information systems, ISO/IEC 27701, GDPR, Law of Ukraine No. 4336-IX, physical security factors, digital signal processing models, biometric identification, methods for improving data leakage resistance.

The list of author's publications:

Proceedings where basic scientific results of thesis were published:

1. Balatska V.S., Opirskyy I.R. (2023). Ensuring the confidentiality of personal data and cybersecurity support using blockchain. Cybersecurity: Education, Science, Technique, 4(20), 6–19. DOI: https://doi.org/10.28925/2663-4023.2023.20.619

2. Opirskyy I., Balatska V., Poberezhnyk V. (2023). Modern possibilities of using blockchain technology in the education system. Ukrainian Scientific Journal of Information Security, 29(3), 138–146. DOI: https://doi.org/10.18372/2225-5036.29.18073

3. Poberezhnyk V., Balatska V., Opirskyy I. (2023). Development of the learning management system concept based on blockchain technology. In CEUR Workshop

Proceedings, 3550, 38–49. https://ceur-ws.org/Vol-3550/

4. Balatska V., Poberezhnyk V., Petriv P., Opirskyy I. (2024). Blockchain application concept in the SSO technology context. In CEUR Workshop Proceedings, 3654, 38–49. https://ceur-ws.org/Vol-3654/

5. Balatska V.S., Poberezhnyk V.O., Opirskyy I.R. (2024). Using Non-Fungible Tokens and Blockchain for Access Segmentation in Government Registries. Cybersecurity: Education, Science, Technique, 4(24), 99–114. DOI: https://doi.org/10.28925/2663-4023.2024.24.99114

6. Balatska V., Poberezhnyk V., Opirskyy I. (2024). Utilizing blockchain technologies for ensuring the confidentiality and security of personal data in compliance with GDPR. In CEUR Workshop Proceedings, 3800, 70–80. https://ceur-ws.org/Vol-3800/

7. Balatska V., Opirskyy I., Slobodian N. (2024). Blockchain for enhancing transparency and trust in government registries. In CEUR Workshop Proceedings, 3826, 50–59. https://ceur-ws.org/Vol-3826/

8. Balatska V., Opirskyy I. (2024). Blockchain as a tool for transparency and protection of government registries. Ukrainian Scientific Journal of Information Security, 30(2), 221–230. DOI: https://doi.org/10.18372/2225-5036.30.19211

9. Balatska V.S., Poberezhnyk V.O. (2024). Concept of using blockchain technologies to improve the protection of personal data on the “Diia” platform: compliance with GDPR and Ukrainian legislation. Cybersecurity: Education, Science, Technique, 2(26), 268–290. DOI: https://doi.org/10.28925/2663-4023.2024.26.681

10. Ivanusa A., Tkachuk R., Brych T., Balatska V., Tkachenko A. (2024). Methods and models for designing a system of automated vulnerability detection in web applications. Bulletin of the Lviv State University of Life Safety, 30, 110–122. DOI: https://doi.org/10.32447/20784643.30.2024.11

11. Balatska V. S., Poberezhnyk V. O., Stefankiv A. V., Shevchuk Yu. A. Development of a method for ensuring the reliability and security of personal data in blockchain systems of state registers. Computer Systems and Networks. 2025. Vol. 7, No. 1. P. 1–16. DOI: https://doi.org/10.23939/csn2025.01.001

Scientific works certifying the approval of the dissertation materials:

12. Balatska V.S., Opirskyy I.R. (2023). Mechanisms for achieving reliability in blockchain to protect personal data. In Proceedings of the 9th International Scientific and Technical Conference "Information Protection and Information Systems Security", Lviv, 17-18.

13. Balatska V.S., Poberezhnyk V.O., Opirskyy I.R. (2023). Potential use of blockchain technology in government. In Proceedings of the 6th All-Ukrainian Scientific and Practical Conference of Young Scientists, Students and Cadets, Lviv, 228-230.

14. Poberezhnyk V.O., Balatska V.S., Opirskyy I.R. (2023). Concept of using blockchain technology in education. In Proceedings of the 6th All-Ukrainian Scientific and Practical Conference of Young Scientists, Students and Cadets, Lviv, 386-388.

15. Balatska V.S., Poberezhnyk V.O., Opirskyy I.R. (2024). Blockchain, NFT and IPFS technologies to enhance efficiency and security of government registries of Ukraine. In Proceedings of the XIII International Scientific and Technical Conference "ITSec-2024", Lviv, 51-52.

16. Balatska V.S., Opirskyy I.R. (2024). Enhancing security of government registries in Ukraine through blockchain-based three-factor authentication. In Proceedings of the All-Ukrainian Scientific and Practical Conference of Young Scientists, Vinnytsia, 585-588.

17. Poberezhnyk V.O., Balatska V.S., Opirskyy I.R. (2024). Adaptation of blockchain credentials to GDPR requirements. In Proceedings of the VI International Scientific and Practical Conference “Innovative Technologies in the Development of Modern Society”, Lviv, 39-41.

18. Balatska V.S., Opirskyy I.R. (2024). Implementation of blockchain technologies to ensure security and transparency of government registries. In Proceedings of the III International Scientific and Practical Conference "Security and Defense Sector of Ukraine", Khmelnytskyi, 1094-1096.

19. Balatska V.S., Poberezhnyk V.O. (2024). Using blockchain and NFT technologies for access control in government registries. In Proceedings of the V International Scientific and Practical Conference “Information Security and Information

Technologies”, Lviv, 6-8.

20. Balatska V.S., Opirskyy I.R. (2024). Blockchain technology for ensuring trust and transparency in government registries. In Proceedings of the V International Scientific and Practical Conference “Information Security and Information Technologies”, Lviv, 251-253.

21. Poberezhnyk V.O., Balatska V.S., Opirskyy I.R. (2024). Concept of self-sovereign identity as an alternative to traditional authentication methods. In Proceedings of the V International Scientific and Practical Conference “Information Security and Information Technologies”, Lviv, 262-265.

22. Balatska, V. S., & Poberezhnyk, V. O. (2025). Information security of state registries: The potential of blockchain for the protection of critical data. In International and National Security: Theoretical and Practical Aspects. Proceedings of the 9th International Scientific and Practical Conference (Dnipro, March 21, 2025) (Part II, pp. 468–471), Dnipro.

23. Poberezhnyk V. O., Balatska V. S. The concept of digital sovereignty in the context of the development of the blockchain economy // Proceedings of the International Scientific and Practical Conference “Blockchain Technologies and Engineering 2025” (BTE 2025), Kyiv, March 26, 2025 – Kyiv: IPME NAS of Ukraine, 2025. – P. 75–76.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ СКОРОЧЕНЬ

ACL	Access Control List – список контролю доступу
API	Application Programming Interface – прикладний програмний інтерфейс
AC	Access Control – контроль доступу
AC-1	Access Control Policy and Procedures – політика та процедури контролю доступу
GDPR	General Data Protection Regulation – Загальний регламент захисту даних
ISO	International Organization for Standardization – Міжнародна організація зі стандартизації
КСЗІ	Комплексна система захисту інформації
ML	Machine Learning – машинне навчання
NFT	Non-Fungible Token – незамінний токен
NIST	National Institute of Standards and Technology – Національний інститут стандартів і технологій
RBAC	Role-Based Access Control – рольовий контроль доступу
REST	Representational State Transfer – архітектурний стиль взаємодії в Інтернеті
SC	Smart Contract – смарт-контракт
SSO	Single Sign-On – єдиний вхід
ZKP	Zero-Knowledge Proof – доказ з нульовим розголошенням
ІС	Інформаційна система
ІСПД	Інформаційна система персональних даних
ЦНАП	Центр надання адміністративних послуг
ЕЦП	Електронний цифровий підпис
«Дія»	Державний цифровий сервіс «Дія»
ПД	Персональні дані

ВСТУП

Розвиток цифрового суспільства супроводжується стрімким впровадженням електронних сервісів, які охоплюють усе більше сфер публічного та приватного життя. Зокрема, в Україні активна цифровізація державного управління призвела до створення національної платформи «Дія», електронного документообігу, цифрових посвідчень особи та реєстрових послуг, які формують цифрову екосистему нової якості. У цьому контексті особливо актуальним є питання довіри до таких сервісів, що безпосередньо пов’язано з рівнем захисту персональних даних громадян і достовірністю тієї інформації, яка використовується у процесі ухвалення адміністративних рішень, ідентифікації особи чи призначення соціальних послуг [1].

Проблематика достовірності даних є фундаментальною, оскільки будь-які спотворення у державних реєстрах можуть мати правові, фінансові або навіть безпекові наслідки. Наприклад, неправдиві записи в реєстрі нерухомості можуть призвести до втрати власності, а фальшиві або помилкові відомості в реєстрі виборців – поставити під сумнів легітимність виборчого процесу. Водночас, більшість сучасних систем перевірки даних обмежуються формальними технічними перевірками (наявність підпису, валідність структури запису) і майже не охоплюють семантичного чи поведінкового аналізу транзакцій [2].

Незважаючи на численні спроби вдосконалення систем управління інформаційною безпекою, у тому числі через застосування вимог стандартів ISO/IEC 27001, ISO/IEC 27701, NIST SP 800-53 та українського законодавства, більшість державних інформаційних систем залишаються вразливими до порушень достовірності. Причини цього криються як у технічних, так і в організаційних обмеженнях: централізована структура даних, залежність від адміністративного ресурсу, відсутність автоматизованих механізмів аномалійної поведінки або семантичного розбору записів [3].

Парадигма блокчейн, яка вже зарекомендувала себе у фінансовому секторі, логістиці, освіті та праві, відкриває нові можливості для побудови більш стійких і прозорих цифрових реєстрів. У державному секторі особливої перспективності

набувають дозвільному блокчейн-системи, які дозволяють поєднати контрольоване управління вузлами з високим рівнем довіри між сторонами. Їх використання дозволяє досягти як прозорості процесів, так і неможливості несанкціонованого редагування записів, що критично важливо для довіри з боку громадян [4].

Втім, базове використання блокчейн без розробки спеціалізованих механізмів перевірки не вирішує проблему змістової достовірності. Хеш-функції, цифрові підписи, timestamp не дозволяють відрізнити, чи є транзакція правдивою за змістом – лише те, що вона не змінювалася. У зв'язку з цим постає потреба у розробці нових, гібридних моделей перевірки достовірності, які б враховували не лише технічні ознаки, але й поведінкові шаблони, юридичний контекст, історичну валідність та семантичну логіку інформації [5].

Особливе значення набуває інтеграція таких моделей у державні інформаційні системи, що обробляють персональні дані, оскільки саме достовірність та стійкість до підробок є критичними вимогами згідно з нормативами GDPR, ISO/IEC 27701, а також оновленим українським законодавством – зокрема, Законом України № 4336-IX, що передбачає впровадження комплексної системи захисту інформації (КСЗІ) класу АС-1 в державних реєстрах [6]. Водночас, з огляду на масштаб і критичність оброблюваних даних, запропоновані моделі мають бути не лише теоретично обґрунтованими, а й технологічно реалізованими, масштабованими та адаптованими до вже функціонуючих цифрових платформ.

Таким чином, основне завдання цієї дисертаційної роботи полягає в розробці комплексної моделі забезпечення достовірності персональних даних у дозвільному блокчейн-середовищах, орієнтованої на інтеграцію з державними реєстрами. У межах дослідження пропонується триетапна модель перевірки достовірності транзакцій, що включає смарт-контракти для перевірки структури, криптографічну валідацію за допомогою доведення з нульовим розголошенням, а також поведінкову оцінку на основі алгоритмів машинного навчання. Додатково, впроваджується гібридна модель зберігання персональних даних (on-chain + off-

chain), яка дозволяє досягти компромісу між безпекою, продуктивністю та відповідністю вимогам регуляторів.

Очікувані результати дослідження мають як наукову новизну – через побудову нових математичних моделей та архітектур – так і прикладну значущість, оскільки пропоновані рішення можуть бути масштабовані до систем національного рівня, включаючи «Дію», ЄДДР, eHealth та інші державні реєстри.

Актуальність. Незважаючи на поступ цифрових трансформацій, чинні механізми перевірки персональних даних у державних реєстрах не враховують контексту поведінки користувача та історичних закономірностей змін, що залишає можливість для цілеспрямованих маніпуляцій. Проведене в роботі дослідження [7] підтверджує, що навіть у присутності цифрових підписів або криптографічного захисту, дані можуть бути достовірними лише формально, але не змістовно, що особливо критично у сферах судочинства, охорони здоров’я та соціального забезпечення.

Окремо слід підкреслити зростаючу потребу у технологіях, здатних забезпечити верифікацію інформації не лише на рівні цифрового сліду, але й на рівні змісту транзакції. У дослідженні [8] представлено концепцію гібридного зберігання даних у блокчейн-середовищах, яка дозволяє поєднати прозорість записів із конфіденційністю їх змісту. Такий підхід отримує особливу актуальність у контексті GDPR та українського Закону № 4336-IX, який вимагає запровадження КСЗІ у системах класу АС-1.

Дослідження [9-10] засвідчують потенціал дозвільному блокчейн як основи для державних реєстрових рішень, що відповідають вимогам щодо масштабованості, прозорості та збереження довіри. Водночас, впровадження блокчейн-технологій вимагає супровідного розроблення нових моделей перевірки транзакцій, оскільки класичні криптографічні засоби не гарантують ідентифікації аномалій на рівні поведінки чи змісту запису.

Крім того, останні дослідження [11] свідчать, що успішне впровадження блокчейн у публічному секторі можливе лише за умови, якщо перевірка транзакцій враховує семантичну і логічну структуру записів. Пропоновані в роботі підходи,

зокрема триетапна модель перевірки достовірності транзакцій, базуються саме на такому принципі: від структурної валідації до поведінкової оцінки, що підтверджено практичними експериментами на тестових даних.

Також особливу увагу приділено питанням контролю доступу до чутливих даних у державних реєстрах. Як продемонстровано в роботі [12], інтеграція механізмів NFT та гібридного зберігання дає змогу тонко регулювати права доступу до інформації залежно від контексту запиту. Це дозволяє мінімізувати ризик витоку інформації та відповідає сучасним вимогам цифрової ідентичності.

З огляду на вищезазначене, очевидним є науковий і прикладний сенс розробки комплексного підходу до верифікації достовірності даних, який би враховував технічні, правові та поведінкові аспекти транзакцій у дозвільному блокчейн-середовищах. Такий підхід має стати основою для довготривалої довіри до цифрових сервісів державного рівня та новим етапом у розвитку архітектур цифрової довіри

Зв’язок роботи з науковими програмами, планами, темами.

Дисертаційні дослідження виконано відповідно до наукового напряму кафедри захисту інформації Національного університету “Львівська політехніка”.

Основні положення та результати дисертаційної роботи впроваджені у навчальний процес кафедри Захист інформації Національного університету “Львівська політехніка” з вивчення дисципліни “Нормативно-правове забезпечення та міжнародні стандарти кібербезпеки” для здобувачів вищої освіти напрямку підготовки “125 Кібербезпека та захист інформації”, освітньої програми “Управління інформаційною безпекою”.

Окремі результати дослідження було впроваджено у навчальний процес Львівського державного університету безпеки життєдіяльності, зокрема при підготовці здобувачів вищої освіти за спеціальністю “125 Кібербезпека та захист інформації” у дисциплінах “Політика інформаційної безпеки в організаціях”, “Комплексні системи захисту інформації” та “Аудит, ліцензування та акредитація інформаційних систем”.

Дослідження тематично узгоджуються з актуальними напрямами

цифровізації публічного сектору в Україні, передбаченими Національною стратегією кібербезпеки, та враховують практичні потреби регіональних структур, зокрема Головного управління ДСНС України у Львівській області, у питаннях побудови надійних механізмів обміну, автентифікації та захисту інформації в умовах цифрового документообігу.

Дисертаційні дослідження також використовувалися в рамках участі автора в локальних ініціативах із цифрової трансформації Львова, зокрема у проєктах із оцінки ризиків доступу до публічних реєстрів, а також у консультаційній діяльності щодо впровадження технологій блокчейн для підвищення довіри до державних цифрових платформ.

Мета роботи. Метою дисертаційного дослідження є підвищення ефективності захисту персональних даних користувачів у державних інформаційних системах шляхом розробки та впровадження багаторівневого методу та моделей верифікації достовірності транзакцій у дозвільному блокчейн-середовищах, які забезпечують інтеграцію криптографічних, поведінкових і семантичних моделей перевірки даних відповідно до нормативно-правових вимог та технічних стандартів цифрової безпеки.

Завдання. Дисертаційна робота присвячена вирішенню актуального науково-практичного завдання підвищення ефективності захисту персональних даних користувачів у державних інформаційних системах шляхом розробки та впровадження методу багаторівневої верифікації транзакцій у дозвільному блокчейн-середовищі. Метод базується на інтеграції структурної, криптографічної та поведінкової перевірки, реалізується у вигляді масштабованої архітектури перевірки достовірності транзакцій і включає алгоритм ризик-орієнтованої оцінки, модель поведінкової верифікації та математичну модель інтегральної довіри. Для реалізації мети роботи необхідно виконати такі завдання:

1. Проаналізувати особливості побудови державних цифрових реєстрів та визначити вимоги до систем захисту персональних даних у контексті впровадження блокчейн-технологій. Дослідити переваги та обмеження дозвільного блокчейн для забезпечення цілісності й достовірності транзакцій у державних

інформаційних системах.

2. Дослідити існуючі підходи до перевірки достовірності транзакцій, включно зі структурною, криптографічною та поведінковою верифікацією. Здійснити порівняльний аналіз моделей перевірки з урахуванням типових ризиків компрометації, фальсифікації та несанкціонованого доступу в державних ІС.

3. Розробити триетапну модель перевірки достовірності транзакцій як ключового компоненту, що поєднує смарт-контрактну перевірку структури, протокол доведення з нульовим розголошенням для підтвердження правомірності дій та семантико-поведінковий аналіз користувача з використанням алгоритмів машинного навчання.

4. Розробити математичний апарат інтегральної оцінки довіри до транзакцій у рамках запропонованого методу багаторівневої верифікації транзакцій у дозвільному блокчейн-середовищі, що поєднує результати трьох етапів перевірки через сигмоїдну функцію та логістичну регресію з урахуванням ризиків, сценаріїв доступу та типів даних.

5. Впровадити удосконалений семантико-поведінковий компонент методу у дозвільному блокчейн-середовищі та провести його оцінку на предмет виявлення фальсифікацій і аномалій. Підтвердити відповідність GDPR і Закону України № 4336-IX щодо контролю доступу, прозорості та верифікації.

6. Розробити гібридну модель триетапної перевірки достовірності в середовищі Flask із використанням REST API та Hyperledger Fabric. Дослідити можливості її масштабування в умовах навантаження та інтеграцію з державними цифровими платформами.

7. Оцінити ефективність запропонованого методу в експериментальному дозвільному блокчейн-середовищі на основі порівняння з одно- та двоетапними системами перевірки. Провести аналіз точності, швидкодії, стійкості до типових атак та впливу на загальний рівень кіберзахисту державних систем.

Об’єкт дослідження. Об’єктом дослідження є процеси забезпечення достовірності персональних даних у державних інформаційних системах, що функціонують у межах цифрового урядування та використовують технології

розподіленого реєстру, зокрема дозвільному блокчейн.

Предмет дослідження є методологічні та технічні основи побудови моделей і алгоритмів перевірки достовірності даних у дозвільному блокчейн-середовищах. Особлива увага приділяється комплексному підходу до верифікації – від формальної перевірки структури записів до аналізу змісту й поведінкових патернів, що дозволяє забезпечити не лише технічну, а й семантичну достовірність транзакцій. У роботі також досліджується вплив сучасних нормативних вимог до обробки персональних даних на архітектурні рішення, алгоритмічні механізми та практичну реалізацію засобів контролю, орієнтованих на державні цифрові платформи.

Методи дослідження. У процесі дослідження застосовано інтегрований підхід, що поєднує кілька груп методів для вирішення поставленої наукової проблеми. Аналітична частина дослідження ґрунтується на методах порівняльного аналізу, що дозволило системно оцінити переваги і недоліки існуючих рішень у сфері перевірки достовірності даних, зокрема у контексті централізованих та блокчейн-архітектур. Функціональне моделювання використано для побудови логіки процесів перевірки транзакцій із урахуванням багаторівневої структури оцінки достовірності.

Формалізація моделі базується на методах математичного моделювання, що дозволило описати алгоритмічну структуру взаємодії смарт-контрактів, криптографічного підтвердження на основі протоколу доведення з нульовим розголошенням та поведінкової класифікації на основі машинного навчання. Для реалізації поведінкового компонента моделі використано методи supervised learning із навчанням на підготовленій вибірці транзакцій. Практичні експерименти проведено із застосуванням засобів симуляційного тестування, що дозволило кількісно оцінити точність, швидкодію та стійкість моделі до атак.

Наукова новизна роботи полягає в тому, що:

1. Вперше розроблено триетапну модель перевірки достовірності транзакцій у дозвільних блокчейн-середовищах за рахунок поєднання перевірки структури транзакції засобами смарт-контрактів, криптографічної валідації за допомогою

протоколу доведення з нульовим розголошенням та поведінковим аналізом користувача з використанням алгоритмів машинного навчання. Розроблена триетапна модель перевірки достовірності транзакцій дозволила забезпечити багаторівневу перевірку достовірності даних до моменту запису у блокчейн та підвищило рівень захищеності від компрометації користувачів у цифрових державних платформах.

2. Вперше розроблено математичний апарат обчислення ризику недостовірності транзакцій у дозвільних блокчейн-середовищах на основі сигмоїдної функції з ваговими коефіцієнтами, що відображають вплив кожного етапу перевірки, структурного, криптографічного та поведінкового, на загальний рівень довіри до даних користувачів. Математичний апарат реалізовано через інтегровану логістичну функцію, що забезпечує ухвалення рішень у режимі реального часу, що підвищило точність автоматизованого відсіву транзакцій із високим ризиком та забезпечило підвищення захисту персональних даних у державних інформаційних системах в режимі реального часу.

3. Отримав подальший розвиток семантико-поведінковий метод верифікації транзакцій у дозвільних блокчейн-середовищах, за рахунок введення часових характеристик запитів, мережевих характеристик, історії змін, а також процесу перевірки типових дій користувачів. Розширений семантико-поведінковий метод верифікації транзакцій дає змогу аналізувати транзакцію не лише за змістом, а й за контекстом її створення, що дозволяє підвищити ефективність виявлення фальсифікацій та аномалій, зокрема в умовах атак із внутрішнього середовища або за участі автоматизованих ботів.

4. Удосконалено математичну модель інтегральної оцінки достовірності транзакцій в дозвільних блокчейн-середовищах, за рахунок введення вагового впливу кожного модуля замість його бінарної оцінки. Математична модель реалізовано у вигляді узагальненої функції прийняття рішення на основі структурної перевірки, криптографічної перевірки та поведінкової перевірки, яка здійснюється з урахуванням типових шаблонів дій користувача та виявлення аномалій, що дозволило підвищити рівень достовірності процесу перевірки

користувачів та зменшити вплив людського фактору на процес верифікації в системах захисту державних цифрових реєстрів.

5. Удосконалено математичний апарат перевірки достовірності транзакцій в дозвільних блокчейн-системах за рахунок поєднання методів логістичної регресії, теорії ймовірностей і нечіткої логіки для моделювання ризику транзакції в умовах обмеженого доступу до її змісту. Удосконалений математичний апарат дозволяє генерувати інтегральне значення ризику з урахуванням багатофакторних впливів, включно з частотою, контекстом і типом звернень, що дозволяє адаптувати процеси верифікації до змінних сценаріїв загроз і реалізовує гнучку, ризик-орієнтовану перевірку даних у цифрових реєстрах.

6. Удосконалено модель виявлення фальсифікованих транзакцій у дозвільних блокчейн-середовищах, за рахунок контекстних перевірок параметрів користувачів та поведінкового аналізу. Це дозволило забезпечити надійну фільтрацію транзакцій зі спробами несанкціонованого доступу, що підвищило рівень захищеності систем орієнтованих на обробку персональних даних від атак.

Практичне значення одержаних результатів мають вагоме прикладне значення для сфери цифрового державного управління, оскільки орієнтовані на забезпечення достовірності персональних даних у державних інформаційних системах шляхом упровадження новітніх механізмів перевірки в дозвільному блокчейн-архітектурах. Запропонована триетапна модель перевірки достовірності транзакцій реалізована у вигляді REST API-сервісу та протестована в середовищі Hyperledger Fabric, що забезпечує можливість її безпосередньої інтеграції в цифрові сервіси, зокрема до платформи «Дія», реєстру ЄДДР, eHealth та ін.

1. Експериментально підтверджено, що триетапна модель перевірки достовірності транзакцій у дозвільному блокчейн-середовищі, яка впроваджена у Flask-середовищі з використанням REST API та платформи Hyperledger Fabric, на відміну від централізованих, дозволяє забезпечити модульну побудову системи перевірки достовірності транзакцій та швидше масштабування при інтеграції з державними інформаційними платформами. За результатами тестування проваджена модель перевірки достовірності транзакцій продемонструвала

ефективну роботу з обробкою до 4,8 транзакцій на секунду та середнім часом відповіді 0,21 с, що відповідає вимогам до цифрових державних реєстрів у публічному секторі.

2. Реалізована математична модель інтегральної оцінки достовірності транзакцій, що експериментально впроваджена у дозвільному блокчейн-середовищі на основі сигмоїдної функції з ваговими коефіцієнтами, забезпечила автоматизоване ухвалення рішень без участі оператора. Застосування математичної моделі інтегральної оцінки достовірності транзакцій, дозволило зменшити кількість транзакцій із хибно позитивними результатами до 34% та забезпечило адаптивну реакцію системи на зміну поведінкових шаблонів користувачів, що у свою чергу, підвищило точність і надійність функціонування механізмів перевірки у державних реєстрах.

3. Проведена тестова реалізація моделі поведінкової перевірки достовірності транзакцій в дозвільному блокчейн-середовищі на основі Flask-додатку та алгоритмів машинного навчання, які аналізують часові, мережеві та типові сценарії поведінки користувача, забезпечує виявлення усіх фальсифікованих та аномальних транзакцій включно зі сценаріями атак Unauthorized Submit, Sniffed Replay та Brute-force Payload, у порівнянні з результатами структурної та криптографічної перевірки, що дозволило підвищити рівень захисту від компрометації персональних даних у державних цифрових системах.

4. Впроваджена гібридна модель триетапної перевірки достовірності транзакцій у дозвільному блокчейн-середовищі, яка включає модулі структурної перевірки, криптографічної перевірки на основі доведення з нульовим розголошенням та поведінкової перевірки із застосуванням методів машинного навчання, дала змогу адаптувати систему перевірки достовірності транзакцій до змінних сценаріїв загроз, що підтверджено в межах експериментального тестування. Під час тестування з обробкою 300 транзакцій у мережі з 6 peer-вузлами модель продемонструвала високу продуктивність із середнім часом відповіді 0,063 секунди, що підтверджує її ефективність для використання у масштабованих державних реєстрах із підвищеними вимогами до захищеності.

5. Експериментально підтверджено, що алгоритм ризик-орієнтованої верифікації реалізваний на основі REST API та платформи Hyperledger Fabric, який поєднує елементи логістичної регресії, теорії ймовірностей і нечіткої логіки, забезпечив можливість автоматизованої оцінки рівня довіри до транзакції з урахуванням її часових, мережевих і поведінкових параметрів. Впроваджений алгоритм ризик-орієнтованої верифікації дозволив знизити рівень хибнопозитивних рішень до 3,7% і підвищив точність оцінки достовірності транзакцій на 15,1% у повірянні з одноетапним та на 6,7% з двоетапним, що дозволяє зменшити навантаження на операторів ручної перевірки у державних системах, орієнтованих на обробку персональних даних.

Наукові та практичні результати виконаних досліджень використані у навчальному процесі кафедри захисту інформації Національного університету “Львівська політехніка” та кафедри управління інформаційною безпекою Львівоського державного університету безпеки життєдіяльності, зокрема для здобувачів вищої освіти спеціальності “125 – Кібербезпека та захист іфнормації” в курсах лекцій з дисциплін “Нормативно-правове забезпечення та міжнародні стандарти кібербезпеки”, “Політик аінформаційноїбезпеки в організаціях”, “Комплексні системи захисту інформації” та “Аудит, ліцензування та акредитація інформаційних систем”.

Основні результати дисертаційної роботи використано та апробовано в рамках дослідницьких і освітніх ініціатив на базі кафедри управління інформаційною безпекою Львівського державного університету безпеки життєдіяльності, а також у тестовому середовищі віртуальної мережі, створеному для перевірки ефективності дозвільному блокчейн-рішень у реєстрових IT-системах.

Розроблений REST API-сервіс перевірки достовірності транзакцій, гібридна модель on-chain / off-chain зберігання даних та механізм поведінкової верифікації були впроваджені для імітаційної перевірки транзакцій цифрового державного сервісу «Дія» у локальному середовищі на базі Hyperledger Fabric. За результатами тестування сформовано набір рекомендацій для адаптації архітектурних рішень до

умов реальних державних платформ, які передбачають високу навантаженість та дотримання нормативних вимог ISO/IEC 27701, GDPR і Закону України № 4336-IX.

Елементи дослідження стали основою для міжуніверситетського науково-практичного співробітництва (конференції ITSec, CPITS, ІБІТ), а також використані для формування навчального контенту з тематики цифрової довіри та blockchain-технологій у державному управлінні.

Факт практичного впровадження та апробації підтверджено актами з боку університету та наукових установ (Додаток А).

Особистий внесок. Важливі наукові результати цієї дисертації були досягнуті автором незалежно. У роботах, опублікованих разом із співавторами, ключовий внесок належить автору. Зокрема, автор вніс наступний вклад (за нумерацією, вказаною у Додатку Д): [1, 5, 6, 9] – обґрунтовано архітектуру та математичні підходи до забезпечення конфіденційності персональних даних у дозвільному блокчейн-середовищах; запропоновано моделі з розмежуванням доступу на основі криптографії та застосування NFT; [2, 8, 12] – досліджено потенціал блокчейн як інструмента прозорості та цифрової довіри у державних інформаційних реєстрах; [3, 4, 7] – розроблено концепцію інтеграції дозвільному блокчейн у цифрові освітні та реєстрові платформи, з урахуванням вимог нормативного середовища (GDPR, ISO/IEC 27701); [10] – здійснено розроблення математичних моделей для виявлення вразливостей у Web-системах, що використано як допоміжну складову при формалізації ризиків контекстної недостовірності в дозвільному блокчейн; [13] – запропоновано метод забезпечення достовірності та безпеки персональних даних у державних реєстрах на основі дозвільному блокчейн; реалізовано архітектуру з використанням смарт-контрактів і модульної верифікації транзакцій.

Апробація результатів. Ключові наукові досягнення цієї дисертації були представлені та обговорювались на десяти міжнародних і вітчизняних науковотехнічних конференціях та семінарах. Це участь у IX Міжнародній науково-технічній конференції «Захист інформації та безпека інформаційних

систем» (Львів, 2023); VI Всеукраїнській науково-практичній конференції молодих учених, студентів і курсантів «Інформаційна безпека та інформаційні технології» (Львів, 2023); XIII Міжнародній науково-технічній конференції ITSec–2024 «Безпека інформаційних технологій» (Львів, 2024); Всеукраїнській науково-практичній конференції «Актуальні проблеми сучасної науки в дослідженнях молодих учених, курсантів та студентів» (Вінниця, 2024); VI Міжнародній науково-практичній конференції «Інноваційні технології у розвитку сучасного суспільства» (Львів, 2024); III Міжнародній науково-практичній конференції «Сектор безпеки і оборони України на захисті національних інтересів» (Хмельницький, 2024); V Міжнародній науково-практичній конференції «Інформаційна безпека та інформаційні технології (ІБІТ 2024)» (Львів, 2024) та у Міжнародної науково-практичної конференції «Blockchain Technologies and Engineering 2025» (BTE 2025) (Київ, 2025). Окрім цього, дисертаційна робота була повністю представлена на наукових семінарах кафедри Захисту інформації Національного університету «Львівська політехніка».

Публікації. Основні результати дослідження оприлюднено у 23 наукових публікаціях, серед яких 11 статей у фахових наукових виданнях (включно з тими, що індексуються в Scopus) та 12 тез доповідей на міжнародних науково-практичних конференціях, що засвідчують апробацію положень дисертації.

Структура та обсяг дисертації. Дисертація складається з вступу, чотирьох розділів, що охоплюють 19 підрозділ, висновків, списку використаних джерел і додатків. Загальний обсяг дисертації становить 231 сторінка, з яких 210 – основний текст, 13 – список використаних джерел (120 найменувань), 8 – додатки.

РОЗДІЛ 1. АНАЛІЗ МЕТОДІВ ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ ПРИ РОЗРОБЦІ ТА ЕКСПЛУАТАЦІЇ ІНФОРМАЦІЙНИХ СИСТЕМ

1.1. Передумови створення інформаційних систем персональних даних

Інтенсивна цифровізація суспільства, супроводжувана стрімким зростанням обсягів персоніфікованої інформації, трансформувала уявлення про безпеку даних як фундаментальну складову функціонування сучасних інформаційних систем. Це актуалізувало потребу в концептуальному переосмисленні підходів до зберігання, обробки та захисту персональних даних, особливо в державному секторі. Підвищення вимог до забезпечення їх достовірності, конфіденційності та цілісності зумовлює необхідність створення високоефективних систем інформаційного управління. Передумови формування таких систем доцільно аналізувати з урахуванням технологічних інновацій, соціальних трансформацій та регуляторних обмежень.

Стрімке зростання обсягів даних є однією з головних причин створення інформаційних систем персональних даних. Зокрема, цифровізація охопила всі сфери життя, включаючи медицину, освіту, фінанси та державне управління [14]. Традиційні паперові носії поступилися місцем електронним базам даних, що дозволило значно спростити та прискорити процеси обробки інформації. Водночас це призвело до значного збільшення обсягів персональних даних, які потребують надійного зберігання та захисту.

Розширення використання Інтернету речей (IoT) також значно збільшило кількість пристроїв, що генерують та передають дані. IoT включає широкий спектр пристроїв [15], від "розумних" будинків до промислових систем, які створюють нові можливості для збору та аналізу даних. Однак це додає нові виклики для забезпечення їх безпеки. Збереження конфіденційності та цілісності даних у таких розподілених середовищах потребує впровадження передових технологій захисту.

Сучасні технологічні рішення, такі як блокчейн, криптографія та штучний інтелект, відкривають нові можливості для захисту персональних даних. Блокчейн,

зокрема, пропонує децентралізований підхід до зберігання даних, що може забезпечити високу ступінь захисту від несанкціонованого доступу та маніпуляцій [16]. Водночас криптографічні методи дозволяють ефективно захищати дані під час їх передачі та зберігання, забезпечуючи конфіденційність та цілісність інформації. Штучний інтелект і машинне навчання можуть бути використані для виявлення аномалій та потенційних загроз у реальному часі, що значно підвищує рівень захисту даних.

Підвищена увага до захисту персональних даних зумовлена зростанням кількості кібератак, витоків даних та інших інцидентів у сфері інформаційної безпеки. Втрата або несанкціонований доступ до персональних даних може призвести до серйозних наслідків як для окремих осіб, так і для організацій, включаючи фінансові втрати, втрату репутації та юридичні санкції. Ці ризики змушують організації впроваджувати ефективні механізми захисту даних, щоб забезпечити їх безпеку та конфіденційність.

Соціальні мережі та інші платформи для обміну інформацією також створюють нові виклики для захисту персональних даних [17]. Користувачі все частіше діляться своїми персональними даними в Інтернеті, що підвищує ризики їх несанкціонованого використання. Тому важливо розробляти інформаційні системи, які б забезпечували високий рівень захисту даних користувачів і відповідали їхнім очікуванням щодо конфіденційності.

Законодавчі ініціативи, такі як Загальний регламент захисту даних (GDPR) у Європейському Союзі, встановили високі стандарти для обробки персональних даних та значно посилили відповідальність організацій за їх порушення. Виконання цих вимог стало обов’язковою умовою для всіх організацій, що обробляють дані громадян, що підштовхнуло до активного впровадження нових технологій та методів захисту.

GDPR, наприклад, встановлює чіткі правила щодо збору, зберігання, обробки та передачі персональних даних. Він також передбачає серйозні штрафи за порушення цих правил, що стимулює організації впроваджувати ефективні механізми захисту даних. Крім того, регламент вимагає забезпечення права на

конфіденційність, права на доступ до даних, права на їх виправлення та видалення, що вимагає розробки відповідних функцій у інформаційних системах.

Законодавство щодо захисту персональних даних існує і в інших країнах, що вимагає від міжнародних компаній відповідності різним правовим нормам. Це підштовхує до впровадження уніфікованих підходів до захисту даних, які б відповідали вимогам різних юрисдикцій.

Сучасні інформаційні системи персональних даних повинні забезпечувати не лише високий рівень безпеки, але й надійність та доступність даних. Це означає, що системи повинні бути спроектовані таким чином, щоб мінімізувати ризик втрати даних через технічні збої або кібератаки та забезпечити безперебійний доступ до даних уповноваженим користувачам.

Надійність інформаційних систем включає забезпечення захисту від збоїв та забезпечення відновлення даних у разі виникнення проблем. Це досягається через використання резервного копіювання, дублювання даних та інших методів захисту від втрат. Доступність даних означає, що користувачі повинні мати можливість отримати доступ до своїх даних у будь-який час і з будь-якого місця, що вимагає впровадження надійних та безпечних механізмів доступу [18].

Передумови створення інформаційних систем персональних даних включають широкий спектр факторів, що забезпечує комплексний підхід до розробки та експлуатації таких систем. Зростання обсягів даних, цифровізація процесів, використання IoT, технологічні інновації, підвищена увага до захисту даних та регуляторні вимоги – всі ці фактори обумовлюють необхідність впровадження сучасних технологій і методів захисту. Сучасні інформаційні системи повинні забезпечувати ефективне управління персональними даними в умовах зростаючих обсягів інформації та підвищених вимог до її безпеки, надійності та доступності.

1.2. Загальна характеристика персональних даних та інформаційних систем персональних даних

Персональні дані (далі – ПД) – це будь-яка інформація, яка стосується

фізичної особи, що дозволяє її ідентифікувати, прямо чи опосередковано. Це можуть бути ідентифікаційні, контактні, фінансові, медичні або біометричні дані [19]. Сюди входять такі відомості, як ім'я, прізвище, адреса, телефонний номер, медична історія та багато іншого.

Інформаційні системи персональних даних (далі – ІСПД) забезпечують збір, обробку, зберігання та передачу таких даних. Вони можуть бути локальними або розподіленими і охоплюють різні рівні організації та взаємодії з зовнішніми системами [20]. Основні компоненти ІСПД включають процеси збору даних від суб'єктів персональних даних, їх зберігання у базах даних або на серверах, обробку даних (аналіз, оновлення, видалення) та передачу даних між різними компонентами системи або до зовнішніх організацій. Також важливо забезпечувати захист даних від несанкціонованого доступу, витоку, модифікації або знищення.

Основні вимоги до захисту персональних даних в ІСПД включають конфіденційність, цілісність, доступність, прозорість та права суб'єктів даних. Конфіденційність забезпечує, що доступ до даних мають лише уповноважені особи. Цілісність гарантує точність і повноту даних, а також їх захист від несанкціонованих змін. Доступність означає своєчасний і безперервний доступ до даних уповноважених користувачів. Прозорість забезпечує, що суб'єкти даних знають, які дані збираються, для яких цілей, як вони обробляються і захищаються. Права суб'єктів даних включають право на доступ до своїх даних, їх виправлення, видалення та обмеження обробки.

В умовах інтенсивної цифровізації суспільства та зростання обсягів оброблюваної персональної інформації забезпечення її захисту виступає одним із ключових завдань для організацій, що працюють з такими даними. Порушення вимог інформаційної безпеки персональних даних здатне спричинити серйозні наслідки, зокрема застосування фінансових санкцій, втрату довіри з боку користувачів і суттєві репутаційні втрати

1.2.1. Види персональних даних та рівні їх чутливості

В інформаційно-цифрових системах нового покоління персональні дані виступають центральним об’єктом управління, правового регулювання та

технічного захисту. Їх широке використання в таких критичних сферах, як фінансові операції, охорона здоров’я, державне управління та соціальні послуги, зумовлює підвищені вимоги до забезпечення їхньої безпеки. У контексті масштабної цифровізації та розширення інструментів обробки інформації суттєво зростають ризики несанкціонованого доступу, модифікації та витоку персональних даних, що обумовлює потребу в системному підході до їх класифікації, нормативного супроводу та впровадження комплексних механізмів захисту.

Персональні дані є ключовим ресурсом у цифровій економіці та адміністративному управлінні, оскільки дозволяють однозначно ідентифікувати особу та забезпечувати її взаємодію з інформаційними системами. Ключовим аспектом обробки персональних даних є їхня чутливість, що визначає рівень необхідного захисту та правові вимоги до їхнього використання. Зокрема, персональні дані можуть бути використані як з метою ідентифікації особи, так і в аналітичних або комерційних процесах, що підвищує їхню значущість у сучасному кіберпросторі. На рисунку 1.1 представлено загальну структуру категорій персональних даних, що можуть оброблятися в межах цифрових інформаційних систем. Вони охоплюють біометричні, медичні, соціально-демографічні, цифрові, фінансові та контактні дані, які варіюються за змістом та рівнем чутливості. У таблиці 1.1 узагальнено класифікаційний підхід до персональних даних відповідно до їх функціонального призначення, ступеня ризику при обробці та джерел правового регулювання [21].

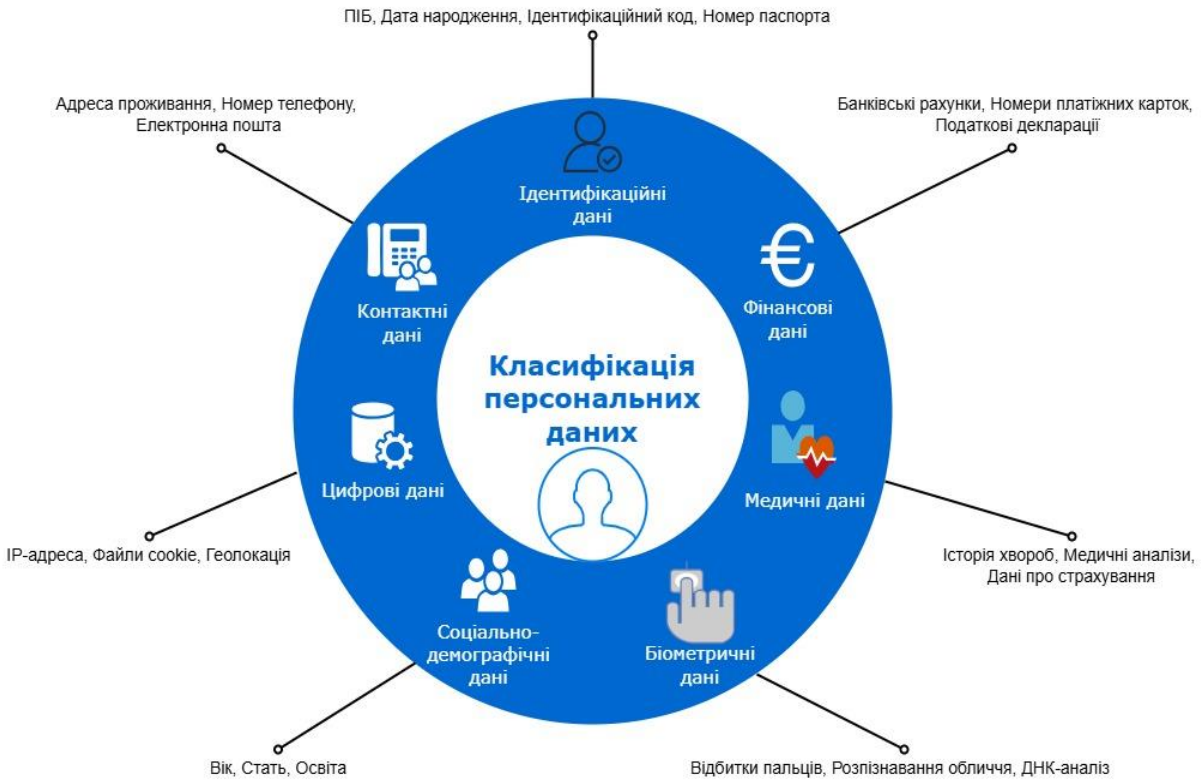

Рисунок 1.1 – Типи персональних даних, що обробляються в інформаційних система

Таблиця 1.1. Класифікація персональних даних за рівнями чутливості

Категорія персональних даних	Опис	Рівень чутливості	Вимоги до захисту	Нормативно-правове регулювання
Ідентифікаційні дані	Дані, що дозволяють однозначно ідентифікувати особу (ПІБ, дата народження, ідентифікаційний код, паспортні дані)	Високий	КСЗІ класу АС-1, криптографічний захист, контроль доступу	GDPR (ст. 4, 6), Закон України «Про захист ПД» (ст. 5), Закон України № 4336-IX (2024), ISO/IEC 27001
Контактні дані	Адреса, телефон, електронна пошта	Середній	Авторизація доступу, сегментація в ІС	ISO/IEC 29100, Закон України «Про захист ПД»
Фінансові дані	Банківські рахунки, номери карток, транзакції, податкові дані	Високий	КСЗІ (АС-1), PCI DSS, обов’язкове шифрування	GDPR (ст. 9), PCI DSS, Закон № 4336-IX, ISO/IEC 27001
Медичні дані	Дані про стан здоров’я, історія хвороби, медичні картки, рецепти	Високий	КСЗІ (АС-1), криптозахист, журналювання	GDPR (ст. 9), HIPAA, Закон України «Про охорону здоров’я», Закон № 4336-IX

Біометричні дані	Відбитки пальців, скан сітківки, розпізнавання обличчя, голосові шаблони	Критично високий	Підвищені вимоги КСЗІ, багаторівневий захист, шифрування	GDPR (ст. 9), ISO/IEC 30107, Закон України «Про захист ПД» (ст. 7), Закон № 4336-IX
Соціально-демографічні дані	Вік, стать, сімейний стан, освіта, громадянство	Низький	Базовий контроль доступу, політика зберігання	ISO/IEC 29100, GDPR
Цифрові сліди / онлайн-активність	IP-адреса, cookie-файли, історія переглядів, GPS, поведінкові патерни	Середній	Верифікація доступу, захист метаданих, анонімізація	GDPR (ст. 4), NIST, ePrivacy Regulation (ЄС)

Таким чином, персональні дані поділяються на різні категорії залежно від їхнього рівня чутливості, кожна з яких потребує відповідного рівня захисту. Найбільш критичними є біометричні, фінансові та медичні дані, оскільки їхній витік може спричинити значні фінансові втрати, компрометацію особистої інформації та навіть крадіжку особистості. Відповідно, захист таких даних має відповідати міжнародним стандартам і регламентам, зокрема GDPR та ISO/IEC, що дозволяє мінімізувати ризики несанкціонованого доступу, маніпуляцій та втрат даних.

Запропонована класифікація дозволяє визначити необхідні заходи безпеки для кожної категорії персональних даних. Дані з високим та критично високим рівнем чутливості (фінансові, медичні, біометричні) потребують найсуворіших механізмів захисту, включаючи шифрування, багатофакторну автентифікацію, сегментацію доступу та регулярний аудит [22]. Водночас менш чутливі дані (соціально-демографічні, контактні) також потребують належного рівня безпеки, особливо з огляду на їхнє використання в аналітичних та маркетингових процесах. Дотримання міжнародних стандартів, таких як GDPR, ISO/IEC 27001, є обов’язковим для всіх систем, що працюють із персональними даними, оскільки воно забезпечує належний рівень захисту інформації та мінімізує можливі загрози її компрометації.

Категоризація персональних даних

Одним із базових критеріїв класифікації персональних даних є їхня функціональність у цифрових екосистемах. Деякі категорії даних безпосередньо

ідентифікують особу, тоді як інші можуть використовуватися для аналізу поведінкових характеристик або соціально-економічного статусу.

Однією з найбільш чутливих категорій є ідентифікаційні дані, які містять інформацію, що дозволяє однозначно визначити особу. Це можуть бути паспортні дані, ідентифікаційні номери або біометричні характеристики. Оскільки ці дані є ключовими для проведення автентифікації в більшості інформаційних систем, їхній витік може призвести до серйозних наслідків, включаючи крадіжку особистості або фінансові махінації.

До іншої важливої групи належать фінансові дані, що містять відомості про платіжні засоби, банківські рахунки, кредитну історію та операції. Їхня втрата або компрометація створює пряму загрозу економічній безпеці користувача, а отже, вони потребують максимального рівня захисту через шифрування, багатофакторну автентифікацію та контроль доступу [23].

Медичні дані, що включають історію хвороб, лабораторні результати та страхові записи, також є критично чутливими. Їхня обробка регулюється суворими законодавчими нормами, такими як HIPAA (Health Insurance Portability and Accountability Act) у США та GDPR у Європейському Союзі. Будь-яке несанкціоноване розкриття таких даних може мати серйозні правові та етичні наслідки.

Не менш важливою категорією є цифрові дані, які охоплюють відомості про онлайн-активність користувачів, їхню поведінку в мережі, IP-адреси, кукі-файли та історію пошукових запитів. Ці дані, хоча і не завжди безпосередньо ідентифікують особу, можуть використовуватися для створення цифрового профілю користувача [24], що робить їх цінними для маркетингових компаній і водночас привабливими для кіберзлочинців.

Рівні чутливості персональних даних

Персональні дані можна поділити за рівнем чутливості, що визначає необхідний рівень їхнього захисту. Виділяють три основні рівні:

1. Низький рівень чутливості – дані, компрометація яких не завдасть істотної шкоди власнику (наприклад, публічна інформація про соціально-демографічний статус).

2. Середній рівень чутливості – дані, що можуть спричинити незручності або дискримінацію у разі розкриття (наприклад, контактна інформація або історія покупок).

3. Високий рівень чутливості – дані, компрометація яких може призвести до суттєвих фінансових втрат або загроз безпеці (ідентифікаційні, фінансові, медичні та біометричні дані).

На рисунку 1.2. представлено візуалізацію рівнів чутливості персональних даних, що демонструє категоризацію інформації відповідно до можливих загроз та необхідних заходів безпеки.

Рисунок 1.2 – Рівні чутливості персональних даних та їх категоризація

Як видно з рисунка 1.2, до високочутливих персональних даних належать ідентифікаційна інформація, фінансові дані та медичні записи, оскільки їхній витік може призвести до значних фінансових та репутаційних втрат, шахрайства або порушення конфіденційності. Дані середнього рівня, такі як контактна інформація та цифрові сліди (IP-адреси, cookie-файли), можуть бути використані для таргетованих атак або несанкціонованого збору інформації. Дані низького рівня

чутливості, зокрема загальнодоступна контактна інформація та демографічні дані, мають найменший вплив у разі компрометації, однак їх обробка також потребує дотримання стандартів конфіденційності.

Ця класифікація дозволяє визначити оптимальні механізми захисту персональних даних залежно від рівня ризику. Для високочутливих даних застосовуються такі методи, як криптографічне шифрування, багатофакторна автентифікація та жорстке регулювання доступу. Дані середнього рівня вимагають контролю доступу та політик конфіденційності, а для низькочутливих даних можуть бути достатні загальні заходи безпеки, такі як мінімізація збору та обмеження доступу.

Забезпечення захисту персональних даних відповідно до їхньої чутливості

Залежно від рівня чутливості персональних даних застосовуються різні методи їхньої обробки та захисту. Для даних низького рівня чутливості може бути достатньо політик конфіденційності та базових заходів доступу, тоді як для даних високого рівня необхідне використання криптографічних методів, розподілених технологій захисту та багаторівневої автентифікації.

Для ефективного управління ризиками в сфері персональних даних можуть бути використані такі підходи:

- Анонімізація та псевдонімізація, які дозволяють використовувати дані без розкриття їхньої ідентичності.
- Шифрування персональних даних на рівні зберігання та передавання інформації.
- Системи багаторівневого контролю доступу, які дозволяють обмежити коло осіб, що можуть взаємодіяти з певними категоріями даних.

Таким чином, персональні дані є різнорідним масивом інформації, який потребує ретельного аналізу та відповідних заходів безпеки залежно від його категорії та рівня чутливості. Правильна класифікація даних дозволяє визначити ефективні методи їхнього захисту та мінімізувати ризики несанкціонованого доступу [25]. Використання сучасних криптографічних технологій, політик конфіденційності та розподілених моделей управління безпекою дозволяє

забезпечити комплексний підхід до захисту персональної інформації, що особливо актуально в умовах цифрової трансформації та зростання загроз у кіберпросторі.

1.2.2. Типи інформаційних систем, що обробляють персональні дані

Інформаційні системи персональних даних (ІСПД) – це комплекси програмного та апаратного забезпечення, призначені для збору, обробки, зберігання та передачі персональних даних. Розрізняють кілька типів ІСПД, кожен з яких має свої специфічні особливості та використовується в різних сферах діяльності.

1. Організаційно-адміністративні системи. Ці системи використовуються для управління адміністративними процесами в організаціях. Вони включають бази даних працівників, системи управління людськими ресурсами (HRM), системи управління документообігом, а також інші системи, що забезпечують ефективну роботу підприємств. В таких системах зберігаються і обробляються дані про персонал, контракти, заробітну плату, відпустки, лікарняні та інші кадрові процеси.

2. Медичні інформаційні системи. Медичні інформаційні системи використовуються в медичних установах для зберігання та обробки медичних записів пацієнтів, результатів обстежень, історії хвороб та планів лікування. Вони включають електронні медичні картки (EHR), системи управління лабораторними даними (LIMS), системи телемедицини та інші спеціалізовані рішення для медичної галузі [26]. Основна мета таких систем – підвищення якості медичних послуг, забезпечення безпеки пацієнтів та оптимізація роботи медичних працівників [27].

3. Фінансові та банківські системи. Ці системи призначені для управління фінансовими операціями та банківською діяльністю. Вони включають системи управління банківськими рахунками, кредитними картками, системи обробки платежів, онлайн-банкінг, а також системи управління ризиками та фінансовими звітами. Фінансові системи обробляють великий обсяг чутливої інформації, тому вимагають високого рівня захисту та відповідності регуляторним вимогам.

4. Освітні інформаційні системи. Освітні інформаційні системи використовуються в навчальних закладах для управління освітнім процесом. Вони

включають системи управління студентськими записами, електронні журнали успішності, системи управління навчальними планами та розкладом занять, платформи дистанційного навчання. Ці системи забезпечують зберігання даних про студентів, викладачів, навчальні курси, результати іспитів та інші аспекти освітнього процесу.

5. Системи управління клієнтами (CRM). Системи управління клієнтами використовуються для зберігання та аналізу даних про клієнтів, управління взаємодією з ними, автоматизації маркетингових та продажних процесів. CRM-системи включають бази даних клієнтів, історію взаємодії, інформацію про покупки та уподобання клієнтів [28]. Вони допомагають організаціям підвищити якість обслуговування клієнтів, збільшити продажі та покращити маркетингові стратегії.

6. Державні інформаційні системи. Ці системи використовуються державними установами для управління різними аспектами діяльності державних органів. Вони включають системи реєстрації населення, податкові системи, системи управління соціальними програмами, системи видачі документів (наприклад, паспортів, водійських прав), а також інші системи, що забезпечують взаємодію громадян з державою. Державні інформаційні системи часто обробляють великий обсяг чутливої інформації, тому вимагають високого рівня захисту та відповідності законодавчим вимогам [29].

Кожен тип інформаційних систем персональних даних має свої особливості, вимоги до безпеки та області застосування. Незалежно від типу, усі ІСПД повинні забезпечувати конфіденційність, цілісність та доступність даних, дотримуватися законодавства про захист персональних даних та впроваджувати кращі практики інформаційної безпеки.

1.2.3. Основні відмінності від інших типів даних

Персональні дані мають низку специфічних відмінностей від інших типів інформації, таких як технічні, бізнесові чи загальні дані. Вони є особливо чутливими через можливість ідентифікації особи та потенційні ризики, пов’язані з їхньою компрометацією. Саме тому персональні дані підлягають суворому

законодавчому регулюванню, потребують спеціальних методів захисту та мають встановлені обмеження щодо обробки, передачі та зберігання.

У таблиці 1.2 подано порівняння персональних даних з іншими категоріями інформації, що дозволяє чітко визначити їхні особливості у контексті інформаційних систем.

Таблиця 1.2. Порівняння персональних даних з іншими типами даних

Характеристика	Персональні дані	Бізнесові дані	Технічні дані	Загальні дані
Прив’язка до особи	Так (ідентифікує конкретну людину)	Частково (може вказувати на комерційні дії фізичної особи)	Ні (системні параметри)	Ні (відкриті дані)
Юридичне регулювання	Так (законодавчі вимоги до обробки, збереження та захисту в державних ІС)	Внутрішні корпоративні політики	Мінімальні вимоги	Відсутнє
Ризик компрометації	Високий (може призвести до крадіжки особистості, фінансових втрат, дискримінації)	Середній (втрата конкурентних переваг)	Низький (технічні збої)	Мінімальний
Методи захисту	Шифрування, багатофакторна автентифікація, контроль доступу, впровадження КСЗІ (AC-1)	Контроль доступу, резервне копіювання	Логування, резервне копіювання	Відсутність особливих вимог
Вимога згоди на обробку	Так (необхідна згода суб’єкта даних)	Частково (у межах договірних відносин)	Ні (збираються автоматично)	Ні
Приклади	ПІБ, ідентифікаційний код, медична інформація, фото, IP-адреса	Фінансова звітність, бази клієнтів, CRM	Системні логи, журнал збоїв, конфігураційні файли	Публічна статистика, погодні дані
Нормативно-правове регулювання	GDPR, Закон України «Про захист персональних даних», Закон України № 4336-IX (2024), ISO/IEC 27001, ISO/IEC 27701	ISO/IEC 27002, внутрішні політики	NIST 800-122, ISO/IEC 27005	Відкриті джерела, ENISA Report

Аналізуючи наведені дані, можна відзначити суттєві відмінності між

персональними даними та іншими типами інформації, які зумовлюють різний підхід до їх обробки, зберігання та захисту [30].

Визначення та контекст використання. Персональні дані відносяться до інформації, що дозволяє прямо чи опосередковано ідентифікувати особу (ім’я, паспортні дані, фінансові операції). Технічні дані, натомість, пов’язані з роботою систем і не мають персоніфікованого характеру (наприклад, журнали логування). Бізнесові дані охоплюють корпоративну інформацію (фінансові звіти, стратегії розвитку), тоді як загальні дані можуть включати відкриті державні реєстри або статистичні дані без прив’язки до конкретної особи.

Захист та конфіденційність. Персональні дані регулюються законами та міжнародними стандартами (GDPR, Закон України «Про захист персональних даних»), що вимагають їхнього захисту від несанкціонованого доступу, витоку або зміни. Технічні дані зазвичай мають менш суворі вимоги до конфіденційності, а бізнесові дані підлягають захисту з точки зору корпоративних інтересів. Загальні дані часто мають відкритий доступ і не потребують складних заходів захисту.

Вимоги до обробки та згоди. Персональні дані вимагають явної згоди суб’єкта на їхню обробку, а також можливості відкликання цієї згоди. Бізнесові дані можуть мати внутрішні правила доступу, тоді як технічні та загальні дані зазвичай не вимагають спеціального узгодження для їхньої обробки.

Тривалість зберігання. Персональні дані підлягають обмеженням щодо термінів зберігання (наприклад, відповідно до GDPR, дані мають бути видалені після досягнення мети їхньої обробки). Технічні дані можуть зберігатися до моменту їхньої актуальності, бізнесові – відповідно до корпоративних політик, а загальні дані часто зберігаються без обмежень.

1.3. Розробка та захист інформаційних систем персональних даних

Створення інформаційних систем персональних даних (ІСПД) — це багатоступеневий процес, який вимагає глибокого розуміння не тільки технічних аспектів, але й правових та етичних зобов'язань щодо захисту конфіденційної інформації. Персональні дані містять в собі інформацію про фізичних осіб, і неналежна їх обробка може призвести до серйозних наслідків як для суб’єктів

даних, так і для організацій, які займаються їх зберіганням та обробкою. В сучасних умовах кіберзагроз, а також у зв’язку зі зростаючою складністю законодавчих вимог, розробка ІСПД передбачає інтеграцію захисту даних на кожному етапі створення системи.

Розробка інформаційних систем (ІС) персональних даних є складним процесом, який поєднує технічні, юридичні та організаційні аспекти. Основна мета таких систем – забезпечити безпечне збирання, обробку, зберігання та передачу персональних даних, а також відповідати вимогам законодавства.

Процес розробки ІС персональних даних передбачає врахування специфічних вимог, зокрема тих, що стосуються конфіденційності, захисту інформації та регуляторних вимог, таких як GDPR. Захист таких систем передбачає впровадження сучасних технологій та засобів інформаційної безпеки для мінімізації ризиків витоку даних і несанкціонованого доступу.

1.3.1. Вимоги до розробки

На етапі проєктування інформаційних систем персональних даних (ІСПД) важливо забезпечити реалізацію принципу комплексного захисту даних на всіх стадіях життєвого циклу [31]. Відповідно до концепції «Privacy by Design», безпека, конфіденційність та цілісність персональної інформації повинні бути інтегровані в архітектуру системи ще на початковій стадії планування. Це передбачає, зокрема, проактивне обмеження обсягу зібраних даних, мінімізацію тривалості їх зберігання, запобігання несанкціонованій обробці та забезпечення контролю за цільовим використанням.

Актуальність впровадження таких підходів суттєво посилюється у зв’язку з набуттям чинності Законом України № 4336-IX від 27 березня 2025 року «Про внесення змін до деяких законів України щодо забезпечення кібербезпеки державних інформаційних ресурсів та об’єктів критичної інформаційної інфраструктури». Згідно з цим нормативним актом, усі державні інформаційні системи, що обробляють персональні дані, зобов’язані впроваджувати комплексну систему захисту інформації (КСЗІ) класу не нижче АС-1. Це означає, що вимоги до проєктування таких систем повинні включати не лише загальні положення щодо

забезпечення безпеки, але й конкретні технічні та організаційні механізми, передбачені чинним законодавством України у сфері технічного та криптографічного захисту інформації.

У зв’язку з цим, до ключових вимог на етапі розробки ІСПД належать:

- чітке визначення ролей, прав доступу та зон відповідальності для різних категорій користувачів, що дозволяє реалізувати принцип необхідності (need-to-know) і знизити ризики внутрішніх загроз;
- масштабованість архітектури – здатність системи до адаптації та розширення без втрати продуктивності або зниження рівня захисту, що є критично важливим для державних реєстрів і сектору публічних послуг;
- впровадження анонімізації та псевдонімізації даних, що унеможливлюють ідентифікацію суб’єкта без наявності додаткової інформації, зокрема при взаємодії між відомчими інформаційними системами;
- мінімізація даних – обробка лише тієї інформації, яка є необхідною для досягнення чітко визначеної мети; надмірна обробка суперечить як принципам GDPR, так і нормам українського законодавства;
- формування технічної та організаційної документації – включаючи опис архітектури, модулів безпеки, політик резервного копіювання, планів аварійного реагування та внутрішнього аудиту відповідності.

У процесі розробки ІСПД також важливим є забезпечення безперервного контролю на кожному з етапів життєвого циклу: від аналізу вимог до реалізації, тестування, впровадження та супроводу [32]. Кожен із цих етапів повинен супроводжуватись конкретними заходами безпеки відповідно до міжнародних стандартів (ISO/IEC 27001, 27002, OWASP) та вимог українських нормативів (включаючи ДСТЗІ та регламенти щодо КСЗІ).

Таблиця 1.3 деталізує ключові заходи захисту, які необхідно реалізувати на кожному з етапів життєвого циклу ІСПД. Вона допомагає зрозуміти, що безпека повинна бути інтегрована на кожному кроці, від початкового планування до безперервної підтримки, оскільки це дозволяє зменшити ризики витоку даних і дотримуватися законодавчих вимог.

Таблиця 1.3. Основні заходи захисту на різних етапах життєвого циклу ІСПД

Етап розробки	Опис заходів безпеки
Аналіз вимог	Визначення вимог до безпеки з урахуванням GDPR, Закону України «Про захист персональних даних» та Закону № 4336-IX; оцінка ризиків; формулювання вимог до КСЗІ (AC-1)
Проєктування	Інтеграція принципів Privacy by Design і Security by Design; розробка моделі з урахуванням контролю доступу, криптографії, журналювання
Реалізація	Розробка відповідно до стандартів безпеки (OWASP, ISO/IEC 27001); реалізація обмеження прав доступу; захист від ін’єкцій і витоку даних
Тестування	Проведення пенетраційних тестів, аналізу вразливостей, перевірка відповідності КСЗІ; аудит коду; симуляція атак
Впровадження	Налаштування політик доступу, впровадження МФА (багатофакторної автентифікації), контроль журналів подій
Супровід та оновлення	Регулярні оновлення системи, виявлення нових вразливостей, логування, аудит безпеки, адаптація до змін у законодавстві

Згідно з таблицею, забезпечення цілісного захисту інформаційних систем персональних даних ґрунтується на системному впровадженні спеціалізованих заходів безпеки на всіх етапах їх життєвого циклу. Аналіз вимог дозволяє визначити ключові вектори захисту, зокрема категорії чутливих даних, ризики їх обробки, вимоги до КСЗІ та відповідність законодавчим нормам. На етапі проєктування формуються технічні та архітектурні рішення щодо захисту – криптографічні механізми, обмеження доступу, багатофакторна автентифікація, псевдонімізація. У процесі реалізації та тестування здійснюється впровадження стандартів безпеки та перевірка стійкості до потенційних атак [33]. Стадії впровадження і супроводу відповідають за підтримку функціональної безпеки, журналювання подій, оновлення та аудит.

Таким чином, таблиця 1.3 підтверджує важливість вбудованого захисту персональних даних як органічної складової всієї моделі створення ІСПД [34]. Такий підхід повністю відповідає принципам "безпеки за проєктом" (Security by Design) і дозволяє реалізувати вимоги Закону України № 4336-IX, що встановлює обов’язковість КСЗІ класу АС-1 для державних інформаційних систем, які обробляють персональні дані.

Особливої ваги це набуває в умовах зростання загроз, пов’язаних із кібератаками, витоком або підробкою даних, а також появою нових векторів атак на державні інформаційні ресурси. Інтеграція безпеки на рівні проєктування забезпечує не лише технічну стійкість системи, а й її нормативну легітимність та відповідність міжнародним і національним стандартам.

Рисунок 1.3 ілюструє цикл створення інформаційної системи персональних даних із інтегрованими механізмами захисту. Згідно з моделлю, на кожному етапі – від аналізу вимог до супроводу – передбачено реалізацію заходів, які спрямовані на зниження ризиків і забезпечення відповідності чинним стандартам: ISO/IEC 27001, ISO/IEC 27701, GDPR, а також українському законодавству, зокрема Закону № 4336-IX.

Етапи життєвого циклу охоплюють: аналіз вимог, проєктування, реалізацію, тестування, впровадження та експлуатаційну підтримку. Кожен з них має бути підкріплений відповідними технічними рішеннями, що дозволяє досягти високого рівня стійкості системи до сучасних загроз та гарантує безпечну обробку персональних даних у державному секторі.

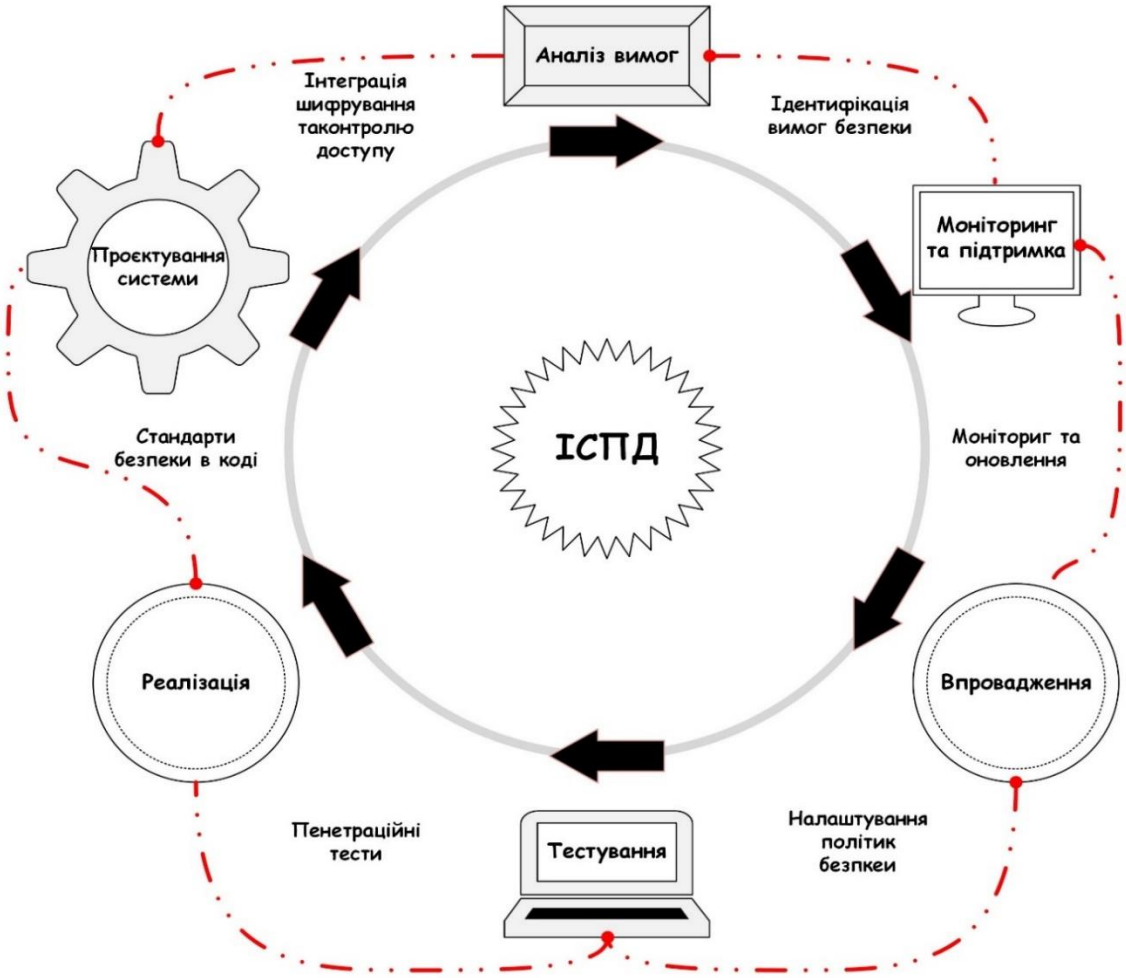

Рисунок 1.3 – Життєвий цикл розробки інформаційної системи персональних даних з інтегрованими заходами безпеки

Як демонструє рисунок 1.3, побудова безпечної інформаційної системи персональних даних ґрунтується на концепції інтеграції заходів захисту на всіх етапах її життєвого циклу. Починаючи з фази аналізу вимог, під час якої здійснюється виявлення загроз, оцінка ризиків та формулювання технічних параметрів безпеки відповідно до національного законодавства та міжнародних стандартів, і до фази супроводу, де забезпечується моніторинг, аудит та адаптивне реагування на нові виклики – безпека має статус невід’ємної та наскрізної функції системи.

На етапі проєктування формуються архітектурні рішення, що включають розмежування доступу, модулі криптографічного захисту, псевдонімізації, а також системи багатофакторної автентифікації. Ці елементи реалізуються у коді під час розробки згідно з рекомендаціями OWASP та стандартами ISO/IEC 27001.

Наступні етапи – тестування та впровадження – передбачають проведення пенетраційних випробувань, аудит відповідності, налаштування політик доступу, логування подій та активності користувачів.

Фаза супроводу передбачає регулярне оновлення компонентів системи, аналіз логів, перевірку відповідності політик змінним загрозам, а також підтримку КСЗІ у працездатному стані, відповідно до вимог Закону України № 4336-IX, що встановлює зобов'язання впровадження засобів захисту класу АС-1 для державних ІСПД.

Таким чином, безпека персональних даних має бути реалізована не як ізольований модуль, а як наскрізна функція, інтегрована у кожен компонент та процес системи. Такий підхід забезпечує відповідність вимогам як українського законодавства, так і положенням міжнародних нормативів (GDPR, ISO/IEC 27701) [35], дозволяючи системі залишатися стійкою до постійно змінюваних кіберзагроз.

1.3.2. Вимоги до захисту

Захист інформаційних систем персональних даних (ІСПД) є важливою складовою їхньої ефективної розробки та функціонування. Вимоги до захисту повинні відповідати не тільки технічним стандартам, але й забезпечувати організаційну і фізичну безпеку даних. Кожна система, яка працює з персональними даними, повинна мати багаторівневу захисну інфраструктуру, яка охоплює різні аспекти: від контролю доступу до процедур аварійного відновлення та забезпечення безперебійної роботи системи.

Технічні вимоги до захисту

Технічні вимоги до захисту ІСПД спрямовані на забезпечення безпеки даних під час їхньої обробки, передачі та зберігання. Ці заходи включають сучасні методи шифрування, контроль доступу, моніторинг діяльності в системі та швидке реагування на потенційні загрози.

- Контроль доступу є одним із ключових компонентів забезпечення безпеки інформаційних систем, оскільки він обмежує доступ до персональних даних лише для уповноважених осіб. Застосування багатофакторної аутентифікації

(MFA) є обов'язковою умовою для забезпечення надійного захисту даних. Це може включати не тільки використання паролів, але й додаткові фактори аутентифікації, такі як одноразові коди або біометричні дані (відбитки пальців, розпізнавання обличчя). Багатофакторна аутентифікація знижує ризик компрометації облікових записів навіть у разі, якщо пароль буде скомпрометовано.

Авторизація забезпечує, що користувачі мають доступ лише до тих ресурсів і даних, які необхідні для виконання їхніх обов'язків. Важливою вимогою є налаштування сегментації прав доступу, тобто створення різних рівнів доступу для різних ролей користувачів. Логування дій користувачів у системі дозволяє здійснювати постійний контроль за їхньою активністю, що особливо важливо для виявлення потенційних внутрішніх загроз або випадкових дій, які можуть призвести до витоку даних [36].

- Шифрування є одним із найбільш ефективних методів захисту даних як під час їхньої передачі, так і під час зберігання. Шифрування даних при передачі дозволяє захистити інформацію від перехоплення, особливо якщо вона передається через незахищені канали, наприклад, через інтернет. Стандартними протоколами для цього є SSL (Secure Sockets Layer) та TLS (Transport Layer Security), які забезпечують зашифровану передачу інформації між клієнтом і сервером.

Зберігання даних також повинно бути захищене за допомогою сучасних алгоритмів шифрування, таких як AES (Advanced Encryption Standard), що забезпечують високий рівень захисту. Особливо важливо це для тих систем, які зберігають великі обсяги чутливої інформації, наприклад, фінансові або медичні дані.

- Для забезпечення постійного захисту інформаційних систем важливо застосовувати інструменти для моніторингу активності та виявлення загроз у режимі реального часу. Системи виявлення та запобігання вторгнень (IDS/IPS) дозволяють автоматично виявляти та блокувати підозрілу активність, що може бути пов'язана з несанкціонованим доступом або спробами атаки.

Крім того, впровадження систем управління інформаційною безпекою (SIEM – Security Information and Event Management) забезпечує централізований

моніторинг та аналіз подій безпеки [37]. Це дозволяє швидко реагувати на загрози та проводити аналіз інцидентів для виявлення їхніх причин та наслідків.

- Регулярне резервне копіювання даних є обов'язковою практикою для захисту інформаційних систем від втрат даних у разі технічних збоїв або кібератак. Бекапи повинні зберігатися в зашифрованому вигляді у віддалених і захищених локаціях, щоб запобігти несанкціонованому доступу до них.

Також необхідно впроваджувати план аварійного відновлення (Disaster Recovery Plan, DRP), який передбачає конкретні кроки для швидкого відновлення роботи системи після збою або кібератаки. DRP повинен охоплювати різні сценарії інцидентів і забезпечувати можливість мінімізації втрат даних та часу простою системи.

Організаційні вимоги до захисту

Ефективний захист інформаційних систем неможливий без належної організації робочих процесів та відповідної підготовки персоналу. Організаційні заходи безпеки допомагають забезпечити дотримання процедур і відповідальність за виконання вимог щодо захисту даних.

- Кожна організація повинна розробити та впровадити політику безпеки, яка включатиме правила обробки та захисту персональних даних, процедури контролю доступу, вимоги до резервного копіювання та інші заходи. Політика безпеки повинна чітко окреслювати відповідальність за виконання цих вимог, а також механізми моніторингу дотримання процедур.

Особливо важливим є призначення відповідальної особи за захист даних (Data Protection Officer, DPO), яка здійснюватиме контроль за дотриманням політики безпеки, проводитиме аудит і навчання персоналу, а також забезпечуватиме відповідність законодавству, такому як GDPR.

- Навчання персоналу є критично важливим елементом захисту інформаційних систем. Більшість витоків даних відбувається через помилки або неусвідомлені дії працівників, тому регулярні тренінги з інформаційної безпеки допомагають підвищити обізнаність співробітників про можливі загрози [38].

Проведення навчальних симуляцій інцидентів дає можливість персоналу практично відпрацьовувати дії у випадку кіберінциденту, що допомагає підготувати їх до реальних ситуацій і значно підвищує загальний рівень безпеки в організації.

Фізичні вимоги до захисту

Захист персональних даних включає не лише програмні та організаційні заходи, а й фізичні аспекти безпеки, що є необхідними для забезпечення цілісності та конфіденційності інформаційної інфраструктури.

- Для забезпечення захисту серверних приміщень, де зберігаються персональні дані, необхідно впроваджувати системи контролю доступу [39]. Це можуть бути механічні замки, електронні ключі або картки доступу, що забезпечують обмежений вхід до приміщень лише для уповноважених осіб. Важливими також є системи відеоспостереження та сигналізації, які дозволяють відстежувати всі події і вчасно реагувати на порушення безпеки.
- Захист фізичного обладнання є необхідним для уникнення можливих збоїв у роботі системи. Серверні кімнати повинні бути оснащені системами пожежогасіння, а також безперебійним живленням (UPS), щоб забезпечити безперервну роботу системи у разі аварійного відключення електроенергії.

На рисунку 1.4 зображено багаторівневу систему захисту персональних даних, яка охоплює технічні, організаційні та фізичні заходи. Такий підхід забезпечує комплексний захист від несанкціонованого доступу, витоку інформації та технічних збоїв.

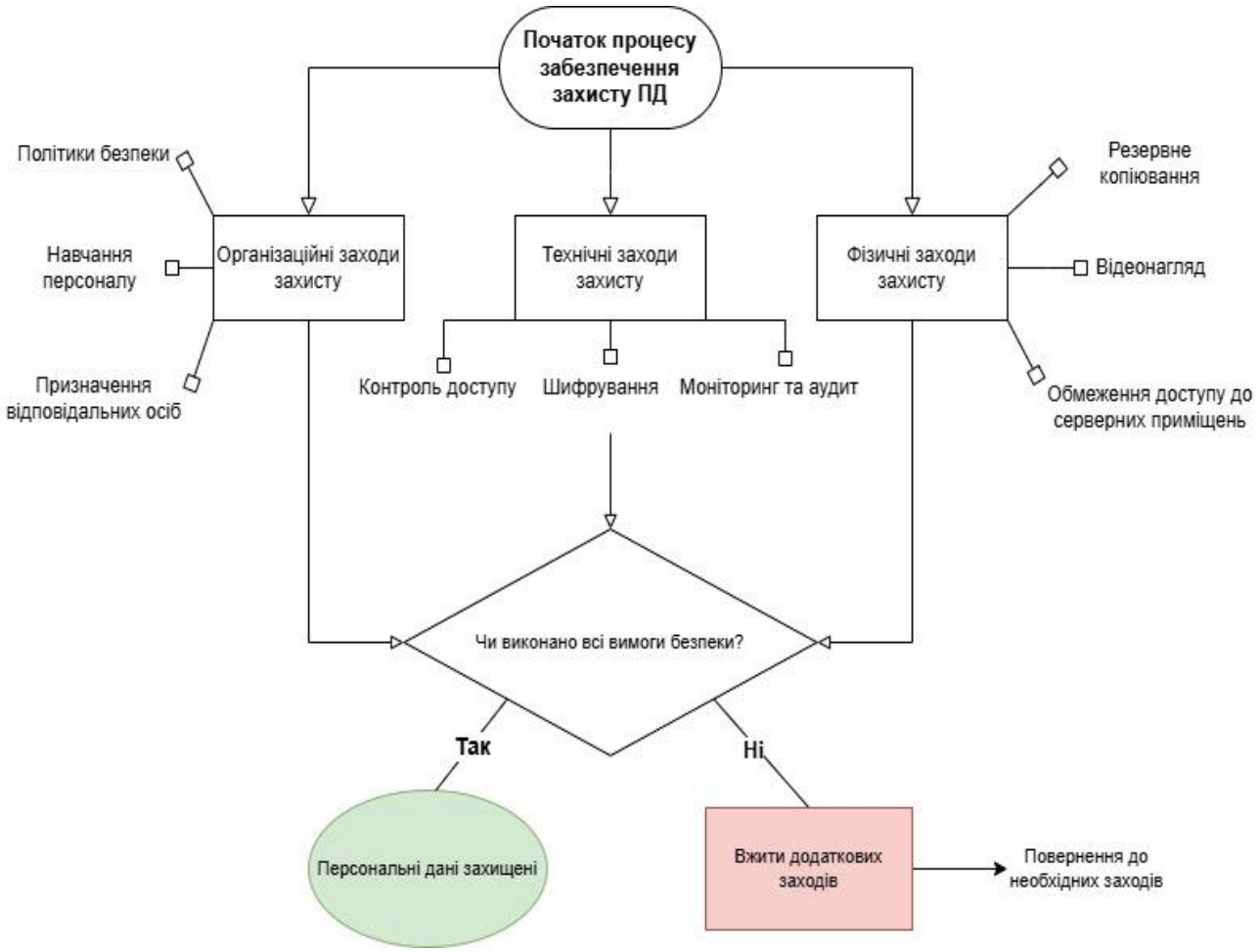

Рисунок 1.4 – Блок-схема вимог до захисту персональних даних

Як видно з рисунку 1.4, багаторівневий підхід до захисту персональних даних включає кілька рівнів безпеки. Використання криптографії, багатофакторної аутентифікації та політики контролю доступу забезпечує надійний захист даних під час обробки, зберігання та передачі. Організаційні заходи, такі як політики безпеки та навчання персоналу, допомагають мінімізувати ризики, пов’язані з людським фактором. Фізичні методи захисту, зокрема обмежений доступ до серверних приміщень та використання відеоспостереження, забезпечують додатковий рівень безпеки інформаційних систем.

Вимоги до захисту інформаційних систем персональних даних охоплюють різні рівні: від технічних до організаційних і фізичних заходів безпеки. Для того щоб система могла забезпечити надійний захист даних, усі ці вимоги мають бути впроваджені комплексно, інтегровані на кожному етапі її життєвого циклу та підтримуватися постійним моніторингом і оновленням. Лише такий підхід

гарантує захист персональних даних від сучасних загроз, забезпечуючи водночас відповідність законодавчим вимогам.

1.3.3. Основні відмінності від інших типів інформаційних систем

Інформаційні системи персональних даних (ІСПД) мають принципові відмінності від інших інформаційних систем через особливий статус даних, що обробляються, суворі вимоги до безпеки та регулювання на законодавчому рівні [40]. На відміну від стандартних інформаційних систем, які можуть працювати з загальними бізнес-даними, фінансовою чи технічною інформацією, ІСПД обробляють персональні дані, що безпосередньо стосуються ідентифікованих або ідентифікованих фізичних осіб.

1. Чутливість та конфіденційність даних

Основною відмінністю ІСПД є висока чутливість даних, які вони зберігають та обробляють. Персональні дані, такі як імена, адреси, дані про здоров'я чи фінансові дані, є надзвичайно цінною інформацією і можуть використовуватися для ідентифікації особи або її поведінки. Ця чутливість обумовлює підвищені вимоги до захисту даних у порівнянні з іншими типами даних, які можуть мати нижчий рівень конфіденційності.

Для кращого розуміння ключових відмінностей між інформаційними системами персональних даних та іншими видами інформаційних систем, у таблиці 1.4 наведено класифікацію даних за рівнем чутливості, вимогами до захисту та основними ризиками витоку.

Таблиця 1.4. Порівняння чутливості даних

Категорія даних	Опис	Рівень чутливості	Основні ризики витоку	Вимоги до захисту
Ідентифікаційні дані	Інформація, що дозволяє однозначно визначити особу	Високий	Використання в шахрайстві, крадіжка особистості	Шифрування, контроль доступу, багатофакторна аутентифікація
Контактні дані	Дані, що дозволяють встановити зв’язок із	Середній	Небажана реклама, фішингові атаки,	Захист від спаму, фільтрація

	особою (адреса, e-mail, телефон)		соціальна інженерія	електронних повідомлень
Фінансові дані	Банківські рахунки, кредитні картки, операції	Дуже високий	Фінансові втрати, шахрайство	Шифрування, багаторівневий контроль доступу, токенізація
Медичні дані	Дані про здоров'я, медичну історію, рецепти	Високий	Ризик дискримінації, витік до страхових компаній, порушення приватності	Захист за стандартами HIPAA, GDPR, шифрування на рівні зберігання
Біометричні дані	Відбитки пальців, сітківка ока, розпізнавання обличчя	Критично високий	Зловживання біометричними системами, підробка особистості	Зберігання в зашифрованому вигляді, багаторівневий контроль доступу
Соціально-демографічні дані	Вік, стать, сімейний стан, освіта, громадянство	Низький	Соціальна дискримінація, маркетингове маніпулювання	Анонімізація даних, обмеження доступу до профілів
Цифрові дані та активність в Інтернеті	IP-адреси, файли cookie, історія браузера, GPS-координати	Середній	Відстеження поведінки, таргетована реклама без згоди, цифровий профайлінг	Використання VPN, блокування трекерів, регулювання збору cookie-файлів

Аналізуючи представлені в таблиці 1.3.1 категорії даних, можна зробити висновок, що інформаційні системи персональних даних вимагають значно вищого рівня захисту порівняно з іншими типами інформаційних систем. Найбільш критичними з точки зору безпеки є біометричні, фінансові та медичні дані, адже їхній витік може мати серйозні наслідки для особистої безпеки, фінансової стабільності та навіть соціального статусу осіб [41].

Також важливо зазначити, що навіть дані середнього рівня чутливості, такі як цифрові сліди (IP-адреси, файли cookie, геолокація) або контактна інформація, можуть бути використані для профайлінгу особи та потенційних кібератак, зокрема фішингових кампаній або соціальної інженерії [42]. Це вимагає впровадження суворих заходів безпеки навіть для тих даних, які традиційно вважаються менш критичними.

2. Законодавча відповідність

Інформаційні системи персональних даних (ІСПД) підлягають суттєво жорсткішим регуляторним вимогам порівняно з іншими типами інформаційних систем. Законодавчі акти, зокрема Загальний регламент захисту даних (GDPR), який діє на території Європейського Союзу, а також Закон України «Про захист персональних даних», встановлюють обов'язковість захисту персональної інформації, отримання згоди суб'єкта на її обробку, а також забезпечення прав доступу, зміни та видалення персональних відомостей.

Особливої актуальності в українському контексті набуває Закон України № 4336-IX від 27 березня 2025 року «Про внесення змін до деяких законів України щодо забезпечення кібербезпеки державних інформаційних ресурсів та об'єктів критичної інформаційної інфраструктури». Цей нормативно-правовий акт зобов'язує державні органи впроваджувати комплексну систему захисту інформації (КСЗІ) не нижче класу АС-1 у всіх ІСПД, що обробляють персональні дані. Таким чином, питання законодавчої відповідності перетворюється з бажаної практики на обов'язкову вимогу для державного сектору.

У таблиці 1.5 представлено порівняння основних регуляторних вимог, що висуваються до ІСПД та інших типів інформаційних систем.

Таблиця 1.5. Порівняння регуляторних вимог

Законодавча вимога	ІСПД	Інші інформаційні системи
Обов'язкове шифрування даних	Так (включено до складу КСЗІ, обов'язкове для АС-1)	Не завжди

Отримання згоди на обробку даних	Обов’язкове згідно з GDPR і Законом України «Про захист ПД»	Може бути необов’язковим
Надання прав користувачам на доступ, редагування, видалення даних	Передбачене законодавством (GDPR, ЗУ «Про захист ПД»)	Обмежене або відсутнє
Дотримання вимог КСЗІ	Обов’язкове для державних ІСПД згідно з Законом № 4336-IX	Залежить від категорії інформації
Штрафи за порушення	До 20 млн євро або 4% від обороту (GDPR); адміністративна та кримінальна відповідальність (ЗУ)	Менші або відсутні

Як видно з таблиці, інформаційні системи, що обробляють персональні дані, підпадають під значно жорсткіші вимоги контролю, звітності та відповідальності. Це пояснюється високим рівнем ризику при несанкціонованому доступі, витоку або порушенні цілісності персональних даних, що, в свою чергу, може призвести до фінансових втрат, втрати довіри та юридичних санкцій.

3. Комплексна система захисту

ІСПД потребують впровадження багаторівневих систем захисту, які включають контроль доступу, шифрування даних, багатофакторну аутентифікацію та постійний моніторинг дій у системі. У порівнянні з іншими інформаційними системами, які можуть використовувати більш прості системи захисту, ІСПД вимагають більш складних і детальних механізмів безпеки.

У таблиці 1.6 наведено порівняння заходів безпеки для ІСПД та інших інформаційних систем. З таблиці видно, що ІСПД вимагають більш високого рівня захисту, включаючи обов'язкове шифрування даних і багатофакторну аутентифікацію.

Таблиця 1.6. Порівняння заходів безпеки

Механізм захисту	ІСПД	Інші інформаційні системи
Шифрування даних	Обов’язкове (AES-256, TLS)	Може застосовуватися за необхідністю
Багатофакторна	Рекомендована або	Використовується рідше

аутентифікація (MFA)	обов’язкова	
Моніторинг та аудит	Постійний	Може бути періодичним
Системи виявлення вторгнень (IDS/IPS)	Необхідні	Може не застосовуватися
Аудит та контроль доступу	Жорсткий	Може бути гнучкішим

Таблиця підтверджує, що ІСПД вимагають більш жорстких заходів безпеки, таких як обов'язкове шифрування даних і багатофакторна аутентифікація, що не завжди є обов'язковим для інших систем. Постійний моніторинг та використання систем виявлення вторгнень також є обов'язковими для ІСПД.

4. Розширені права користувачів

Одна з ключових особливостей ІСПД – це необхідність надавати користувачам розширені права щодо їхніх даних [43]. Це включає право на доступ до своїх даних, виправлення помилок, видалення даних та обмеження їхньої обробки. Інші інформаційні системи не завжди надають такі права користувачам, оскільки вони можуть обробляти менш чутливі або публічні дані.

5. Вплив на репутацію та бізнес

Витік або порушення захисту персональних даних в ІСПД має значно серйозніший вплив на репутацію організації, ніж у випадку інших типів даних. Витік чутливої інформації може призвести до втрати довіри клієнтів, серйозних фінансових штрафів та медійного розголосу, що може негативно вплинути на подальшу діяльність компанії [44].

Інформаційні системи персональних даних суттєво відрізняються від інших типів ІС через високу чутливість даних, законодавче регулювання та вимоги до безпеки. Персональні дані мають найвищий рівень ризику компрометації, що вимагає обов’язкового застосування шифрування, багатофакторної аутентифікації та моніторингу активності. Відмінності між ІСПД та іншими ІС добре ілюструються у представлених таблицях, що демонструють необхідність більш жорсткого контролю та впровадження найкращих практик захисту даних.

1.4. Перспективні методи

Розвиток технологій у сфері інформаційної безпеки сприяє появі нових і більш ефективних методів захисту персональних даних в інформаційних системах. Враховуючи постійне збільшення обсягів даних, що обробляються, а також зростаючі кіберзагрози, особливо важливим стає пошук перспективних методів захисту, які можуть забезпечити стійкість систем до сучасних викликів [45].

1. Блокчейн-технології

Блокчейн є однією з найперспективніших технологій у контексті забезпечення захисту персональних даних. Його децентралізована структура дозволяє зберігати інформацію у вигляді ланцюжка блоків, кожен з яких містить хеш попереднього блоку. Це забезпечує незмінність даних, прозорість операцій та унеможливлює несанкціоноване редагування історії транзакцій. В обробці персональних даних блокчейн може використовуватись для фіксації подій доступу, змін, передачі – з аудиторською достовірністю.

2. Моделі машинного навчання для безпеки

Застосування методів машинного навчання для аналізу поведінки систем і користувачів дозволяє ефективно виявляти аномалії та потенційні загрози в режимі реального часу [46]. Алгоритми машинного навчання можуть вивчати нормальні патерни поведінки в системі і автоматично виявляти відхилення, які можуть бути ознакою кібератаки або витоку даних. Такі методи використовуються для захисту персональних даних від різних типів атак, зокрема фішингу, DDoS-атак та шкідливого програмного забезпечення.

3. Квантова криптографія

Квантова криптографія – це один з найбільш перспективних методів захисту даних, що використовує принципи квантової механіки для забезпечення максимальної безпеки під час передачі інформації [47]. На відміну від традиційних методів шифрування, квантова криптографія гарантує, що будь-яка спроба перехоплення інформації змінює стан квантових часток, що робить неможливим несанкціоноване втручання. Цей підхід дозволяє захистити дані навіть від

потенційних загроз з боку квантових комп’ютерів, які можуть зламати традиційні алгоритми шифрування (таблиця 1.7).

Таблиця 1.7. Порівняння традиційного шифрування та квантової криптографії

Метод шифрування	Рівень захисту	Основні обмеження
Традиційне шифрування	Високий	Може бути зламане квантовими комп'ютерами
Квантова криптографія	Абсолютний	Висока вартість та складність впровадження

4. Псевдонімізація та анонімізація даних

Псевдонімізація та анонімізація даних – це методи, що дозволяють мінімізувати ризики, пов’язані з обробкою персональних даних, шляхом заміни ідентифікуючих елементів даних або їх повного видалення. Псевдонімізація замінює ідентифікуючі елементи на штучні значення, що дозволяє зменшити ризик розкриття даних, хоча все ще можливо відновити їх оригінальний вигляд за допомогою додаткової інформації [48]. Анонімізація ж повністю усуває будь-яку можливість ідентифікації особи на основі знеособлених даних.

5. Хмарні рішення з високим рівнем безпеки

З розвитком хмарних технологій постала необхідність забезпечення безпеки обробки персональних даних у хмарних середовищах. Сучасні хмарні платформи пропонують інструменти для шифрування даних, контроль доступу, моніторинг активності та інші механізми безпеки. Хмарні провайдери часто інтегрують технології машинного навчання для аналізу загроз у реальному часі та автоматичного реагування на них. Крім того, хмарні рішення дозволяють легко масштабувати системи, забезпечуючи високу продуктивність без втрат безпеки.

Для зручності порівняння ключових характеристик сучасних перспективних підходів до захисту персональних даних було узагальнено їх основні властивості у таблиці 1.8. У таблиці наведено переваги та недоліки кожного методу, а також здійснено порівняльну оцінку щодо їхньої ефективності, зрілості впровадження та релевантності до сучасних викликів у сфері безпеки даних.

Таблиця 1.8. Порівняння перспективних методів захисту персональних даних

Метод	Переваги	Недоліки	Порівняльна оцінка
Блокчейн	- Незмінність даних; - Прозорість транзакцій; - Можливість аудиту.	- Високе енергоспоживання; - Обмежена масштабованість.	Висока надійність та прозорість; обмежена адаптація до великих систем
Машинне навчання	- Виявлення аномалій у реальному часі; - Самонавчання; - Проактивність.	- Потреба у великих обсягах даних; - Хибнопозитивні спрацювання.	Дуже ефективне в динамічних середовищах, але потребує ресурсоємних обчислень
Квантова криптографія	- Абсолютна безпека передачі; - Стійкість до квантових атак.	- Висока вартість; - Складність впровадження.	Надзвичайна перспективність, але низька доступність у поточних системах
Псевдонімізація / анонімізація	- Відповідність вимогам законодавства; - Зниження ризику витоку.	- Зниження аналітичної точності; - Можливість декодування при наявності додаткових даних.	Висока регуляторна відповідність, доцільна для статистичної обробки
Хмарні рішення	- Масштабованість; - Вбудовані засоби захисту; - Швидке розгортання.	- Залежність від провайдера; - Можливі юрисдикційні ризики.	Збалансоване рішення для підприємств; потребує ретельного вибору постачальника

Як видно з таблиці 1.8, кожен із сучасних методів має унікальний набір переваг і обмежень. Блокчейн вирізняється високою стійкістю до маніпуляцій, але має обмеження щодо масштабованості. Машинне навчання забезпечує адаптивний захист у режимі реального часу, однак потребує великих обчислювальних потужностей. Квантова криптографія пропонує майже абсолютний рівень захисту, проте її практична реалізація поки що ускладнена.

Методи анонімізації є критично важливими для дотримання нормативних вимог (GDPR, ЗУ «Про захист персональних даних»), хоча можуть знижувати точність даних [49]. Хмарні рішення забезпечують гнучкість, швидкість та інтеграцію з іншими захисними технологіями, але вимагають юридичного контролю умов зберігання даних.

Таким чином, ефективна стратегія захисту персональних даних має ґрунтуватися на поєднанні кількох методів – залежно від специфіки системи, вимог законодавства та ресурсних можливостей організації.

Усі зазначені перспективні методи захисту персональних даних мають свої унікальні переваги та потенційні обмеження. Їх доцільність застосування визначається контекстом функціонування інформаційної системи, рівнем критичності оброблюваних даних, вимогами законодавства, а також поточним станом загроз. Для забезпечення цілісного бачення ключових особливостей кожного з підходів, на рисунку 1.5 подано візуальне представлення класифікації перспективних методів захисту персональних даних відповідно до їх технологічної природи та функціонального призначення.

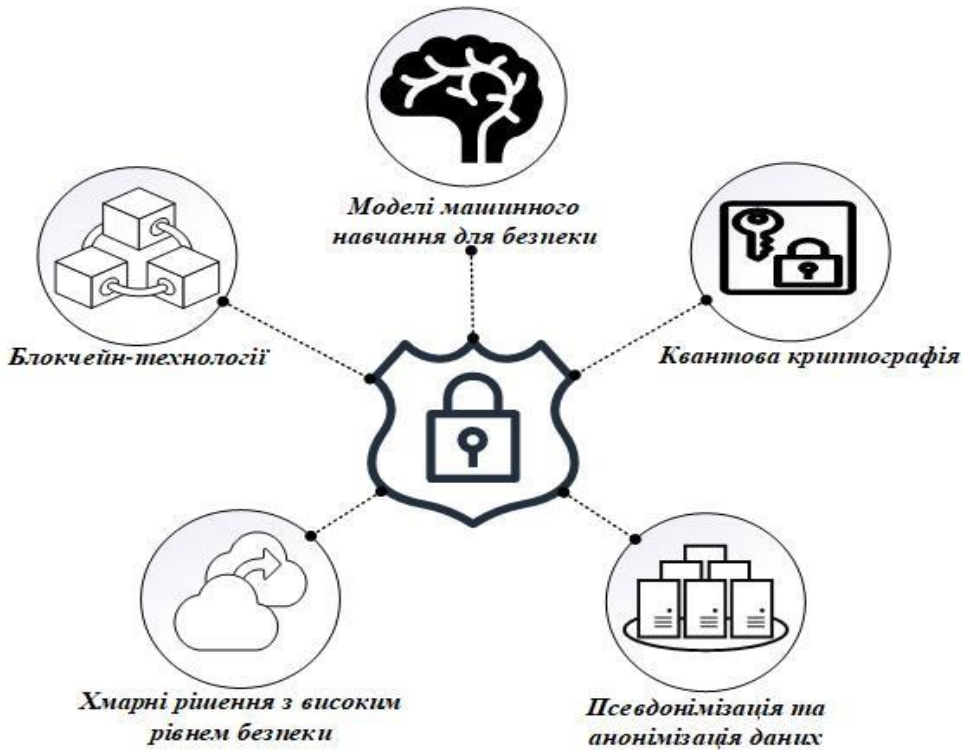

Рисунок 1.5 – Візуальна класифікація перспективних методів захисту персональних даних

Як показано на рисунку 1.5, перспективні методи поділяються за технологічною основою: розподілені реєстри (блокчейн), інтелектуальні системи (машинне навчання), фундаментально нові криптографічні підходи (квантова криптографія), методи знеособлення даних (анонімізація/псевдонімізація) та інфраструктурні рішення (хмарні сервіси з вбудованими механізмами захисту).

Кожен із методів демонструє потенціал підвищення ефективності захисту персональних даних, проте має свої обмеження. Наприклад, блокчейн забезпечує незмінність і прозорість, однак потребує значних ресурсів для масштабування. Машинне навчання виявляє аномалії в реальному часі, але потребує значного обсягу даних. Квантова криптографія гарантує теоретично абсолютний рівень безпеки, але залишається недоступною для широкого впровадження. Анонімізація та псевдонімізація ефективні для забезпечення відповідності GDPR, хоча можуть обмежити аналітичну точність. Хмарні рішення забезпечують масштабованість і гнучкість, проте вимагають довіри до провайдера.

Таким чином, вибір конкретного підходу повинен здійснюватися з урахуванням архітектурних, нормативних та функціональних характеристик інформаційної системи, а також із урахуванням комбінованого застосування декількох методів захисту для досягнення оптимального рівня безпеки.

1.5. Аналіз проблеми захисту персональних даних користувачів в Україні та світі

Захист персональних даних є одним із найактуальніших питань кібербезпеки у XXI столітті. Розвиток цифрових технологій, активне впровадження електронних державних послуг, перехід бізнесу в онлайн-простір призвели до різкого зростання обсягів персональної інформації, що обробляється та зберігається в цифровому форматі. Однак паралельно зі зростанням цифровізації відбувається і збільшення ризиків, пов’язаних із витоком, несанкціонованим доступом або маніпулюванням персональними даними.

Згідно зі світовими дослідженнями, за останнє десятиліття кількість витоків персональних даних зросла більш ніж утричі. Це пов’язано з тим, що хакерські атаки та витоки даних стали не лише проблемою кіберзлочинців, а й інструментом

конкурентної боротьби, політичного впливу та навіть засобом ведення інформаційних війн. Найбільші корпорації та уряди по всьому світу стикаються з проблемами, пов’язаними з витоками персональних даних, які мають далекосяжні наслідки для економіки та суспільства.

Україна, як країна з розвиненою IT-індустрією, не є винятком. Кількість атак на інформаційні системи державних та приватних установ з кожним роком зростає. Наприклад, у 2023 році понад 60% атак на українські інформаційні системи були пов’язані з викраденням персональних даних громадян. Основними об’єктами таких атак стають державні реєстри, системи електронного документообігу, онлайн-банкінг та медичні платформи. Найгучніші витоки персональних даних, зафіксовані в Україні та світі, завдали суттєвих збитків як компаніям, так і звичайним користувачам.

За оцінками міжнародних компаній з кібербезпеки, середній витік персональних даних обходиться компанії у $4,45 млн, а загальні економічні збитки від витоків у всьому світі перевищили $6 трлн на рік [50].

1.5.1. Основні проблеми захисту персональних даних користувачів

Зростання масштабів використання персональних даних у цифрових системах зробило їх однією з головних цілей для кіберзлочинців. Витік персональної інформації несе серйозні ризики як для фізичних осіб, так і для організацій, що обробляють ці дані. Основними наслідками порушення безпеки персональних даних є фінансові втрати, репутаційні ризики, юридична відповідальність та соціальні наслідки.

За останні роки світ побачив численні витоки персональних даних, що призвели до значних збитків для компаній та їхніх клієнтів. Нижче наведено кілька найбільш масштабних атак на бази даних, що містили персональну інформацію.

Найбільші випадки витоків персональних даних у світі

1. Витік даних Facebook (2021)

Кількість постраждалих: 533 мільйони користувачів.

Що сталося: Дані користувачів (номери телефонів, дати народження, місце проживання, адреси електронної пошти) були викрадені через вразливість API платформи.

Наслідки: Після публікації даних у відкритому доступі збільшилася кількість шахрайських схем та випадків соціальної інженерії.

2. Витік даних Equifax (2017)

Кількість постраждалих: 147 мільйонів осіб (включаючи 200 000 українців).

Що сталося: Компанія Equifax, що займається кредитним скорингом, зазнала атаки через вразливість у веб-додатку.

Збитки: Штраф для компанії у розмірі $700 мільйонів та витрати на відшкодування користувачам.

Наслідки: Викрадені дані використовувалися для оформлення кредитів на ім’я постраждалих.

3. Витік персональних даних користувачів Twitter (2022)

Кількість постраждалих: 5,4 мільйона користувачів.

Що сталося: Використання вразливості дозволило зловмисникам отримати доступ до особистих даних користувачів.

Наслідки: Значні репутаційні втрати для Twitter та посилення правил щодо конфіденційності.

4. Кібератака на державні реєстри України (грудень 2024 року)

Кількість постраждалих: невідомо (дані десятків мільйонів громадян могли бути скомпрометовані).

Що сталося: 19 грудня 2024 року було здійснено атаку на державні реєстри України, зокрема на реєстри актів цивільного стану, юридичних осіб та прав на нерухоме майно.

Наслідки: Тимчасове блокування роботи державних сервісів, що ускладнило доступ громадян до реєстраційних послуг. Ризик викрадення конфіденційних даних, що могло б призвести до шахрайства, незаконних реєстрацій або підробки документів. Ймовірна причетність до атаки іноземних спецслужб, що підкреслює важливість кіберзахисту державних інформаційних ресурсів. Підвищення уваги до

реформування кібербезпеки державних структур, зокрема посилення шифрування, оновлення політик конфіденційності та введення додаткових заходів багатофакторної автентифікації.

Згідно зі звітом IBM "Cost of a Data Breach Report 2023" [51], середня вартість витоку даних у світі склала $4,45 мільйона для однієї організації. У випадку фінансових компаній цей показник перевищує $5 мільйонів, а в медичних установах – $10 мільйонів через високу чутливість інформації. Таблиця 1.9 демонструє середні фінансові збитки для різних секторів економіки.

Таблиця 1.9. Фінансові збитки секторів економіки

Сектор	Середня вартість витоку (млн $)	Основні ризики
Фінансовий сектор	5,97	Крадіжка банківських реквізитів, шахрайство
Державні установи	2,07	Витік конфіденційної інформації громадян
Охорона здоров'я	10,93	Продаж медичних записів, шантаж
IT-компанії	4,55	Компрометація акаунтів, витік корпоративної інформації

Як видно з таблиці, найбільші втрати спостерігаються у секторі охорони здоров’я, оскільки викрадені дані можуть використовуватися для шантажу або підробки медичних документів.

Окрім фінансових збитків, витоки персональних даних можуть мати катастрофічні наслідки для репутації компанії. Після витоку даних користувачі можуть втратити довіру до організації, що спричиняє відтік клієнтів та падіння ринкової вартості компанії.

Наприклад, після витоку даних Equifax акції компанії впали на 35% протягом двох тижнів, а керівництво було змушене подати у відставку [52]. Витік даних Facebook у 2021 році також негативно вплинув на імідж компанії, що змусило корпорацію переглянути свою політику безпеки.

Юридичні наслідки також можуть бути значними. Відповідно до GDPR, компанії, що порушують правила обробки персональних даних, можуть бути оштрафовані на суму до 4% від річного обороту або 20 мільйонів євро [53].

Наприклад, компанія British Airways була оштрафована на 183 мільйони фунтів стерлінгів через витік даних клієнтів у 2020 році.

Для візуалізації основних загроз надано рисунок 1.6, який ілюструє різні види загроз для персональних даних.

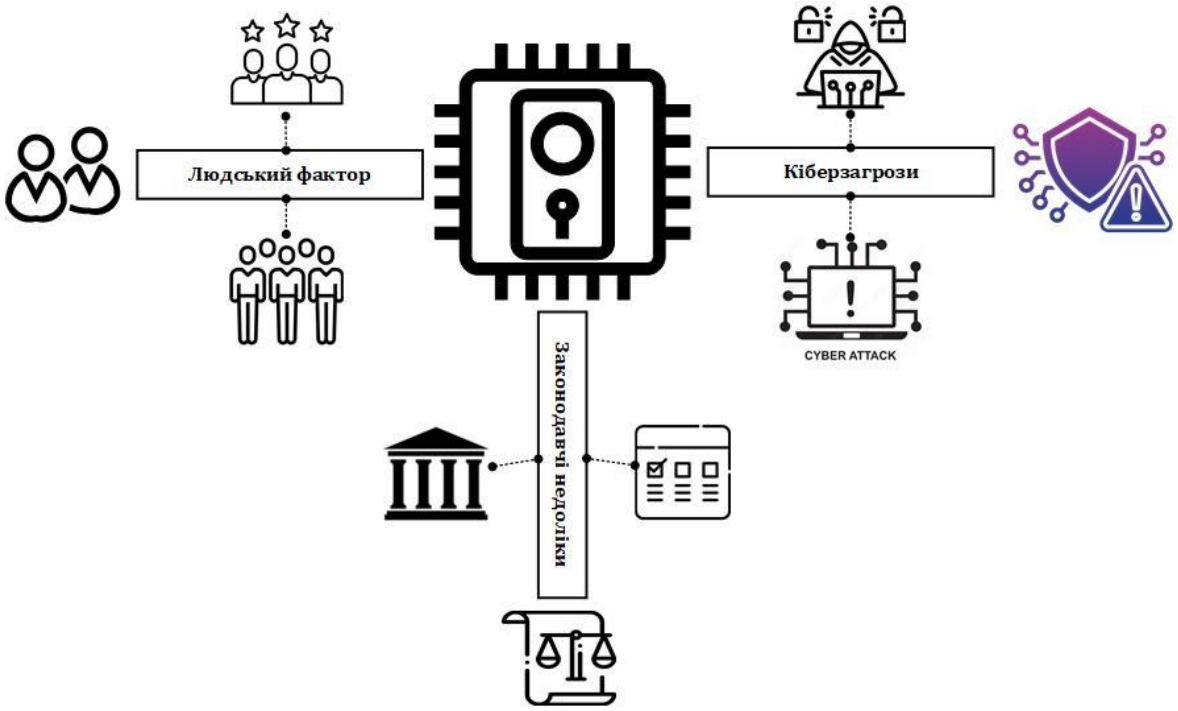

Рисунок 1.6 – Класифікація загроз для персональних даних в інформаційних системах

На рисунку 1.6 візуалізовано три основні категорії загроз, що чинять вплив на безпеку персональних даних в інформаційних системах:

- кіберзагрози – технічні атаки на ІТ-інфраструктуру (включаючи шкідливе ПЗ, DDoS, фішинг, компрометацію доступу);
- людський фактор – помилки персоналу, ненавмисне розголошення, слабкі паролі, порушення політик безпеки;
- законодавчі прогалини – відсутність регламентації, колізії між національним і міжнародним правом, недостатній контроль виконання вимог щодо захисту ПД [54].

Наявність вказаних загроз підкреслює необхідність комплексного підходу до захисту персональних даних, що передбачає не лише впровадження технічних рішень (наприклад, міжмережевих екранів, криптографії, виявлення вторгнень), а

й формування політики безпеки, навчання персоналу та приведення ІСПД у відповідність до нормативно-правових вимог, таких як Закон України «Про захист персональних даних» і Закон № 4336-IX щодо КСЗІ.

Таким чином, ефективна стратегія має враховувати всі вектори загроз – технічні, організаційні та нормативні – з метою забезпечення сталого функціонування інформаційної системи та збереження конфіденційності даних.

1.5.2. Аналіз вимог українського законодавства щодо персональних даних користувачів

Законодавче регулювання захисту персональних даних в Україні базується на положеннях Закону України «Про захист персональних даних», який визначає правові та організаційні засади обробки інформації, що дозволяє ідентифікувати особу. Основна мета цього закону полягає у забезпеченні належного рівня контролю над обробкою персональних даних, дотриманні принципів конфіденційності, прозорості, добровільності та обмеженості цілей. Суб'єкти, які здійснюють обробку персональних даних, зобов'язані отримувати попередню згоду фізичних осіб, гарантувати їм доступ до власних даних, а також створювати внутрішні політики захисту і призначати відповідальних осіб.

Водночас чинна редакція українського законодавства упродовж тривалого часу характеризувалася недостатньою деталізацією технічних вимог до інформаційних систем, що використовуються для обробки персональних даних. До недавнього часу у законі бракувало прямих вказівок щодо архітектури систем, мінімальних вимог до захищеного зберігання даних або використання засобів шифрування. На цьому тлі вітчизняне регулювання значно поступалося положенням Загального регламенту захисту даних (GDPR) [55], прийнятого в Європейському Союзі. На відміну від українського закону, GDPR запроваджує розширене трактування прав суб'єктів даних, включно з правом на забуття, правом на обмеження обробки та правом на перенесення даних. Також він вимагає не лише формального дотримання процедур, а й обґрунтування правомірності кожної дії з персональною інформацією, технічних і організаційних гарантій безпеки.

Відповіддю на ці дисбаланси стало прийняття 27 березня 2025 року Закону України № 4336-IX, який доповнив існуючу нормативну базу важливими положеннями у сфері державних інформаційних систем. Цей закон закріплює на рівні обов'язкової вимоги впровадження комплексної системи захисту інформації (КСЗІ) класу АС-1 у державних електронних реєстрах, які оперують персональними даними. Таким чином, відбулося нормативне підсилення технічного аспекту захисту, яке виводить державні ІСПД на якісно новий рівень відповідності принципам кіберстійкості та інформаційної безпеки [56].

Суттєвим нововведенням є також підвищення рівня юридичної відповідальності за недотримання вимог щодо захисту персональних даних. У разі невиконання вимог, визначених у новому законі, уповноважені органи можуть ініціювати перевірку, тимчасове блокування доступу до інформаційних систем або притягнення посадових осіб до адміністративної чи кримінальної відповідальності [57]. Це положення наближає українське законодавство до підходів ЄС, де питання захисту даних тісно пов'язане з корпоративною та державною відповідальністю, а санкції сягають до 20 мільйонів євро або 4% глобального обороту компанії.

Попри запроваджені зміни, у порівнянні з GDPR українське регулювання все ще залишається менш деталізованим і менш суворим. Зокрема, Закон України «Про захист персональних даних» не містить вимог щодо систематичної оцінки впливу на захист даних (Data Protection Impact Assessment), формалізованих протоколів реагування на інциденти чи регламентів автоматизованого прийняття рішень щодо суб'єкта даних. Крім того, рівень санкцій за порушення правил обробки даних залишається значно нижчим: згідно з положеннями статті 188-39 Кодексу України про адміністративні правопорушення, максимальний адміністративний штраф складає до 1000 неоподатковуваних мінімумів доходів громадян, що еквівалентно приблизно 900 євро, у той час як у країнах ЄС ці санкції у десятки, а то й сотні разів вищі.

У таблиці 1.10 представлено узагальнене порівняння ключових положень українського законодавства та положень GDPR у сфері захисту персональних даних.

Таблиця 1.10. Порівняння вимог українського законодавства та GDPR

Параметр	Закон України «Про захист персональних даних» (з урахуванням ЗУ № 4336-IX)	GDPR (ЄС)
Обробка даних	Потребує згоди, допускається неформальна форма	Вимагається чітка, явна та добровільна згода
Права суб’єктів	Доступ, редагування, обмеження обробки	Додаткові права: на забуття, на заперечення, на перенесення
Відповідальна особа	Рекомендовано (у держ. органах – обов’язково)	Обов’язково призначення DPO
Технічний захист	Впровадження КСЗІ класу АС-1 для держ. ІС	Privacy by Design, DPIA, реєстрація порушень
Штрафи	До 1000 НМДГ (~900 €)	До 20 млн € або 4% річного обороту компанії

Оновлення українського законодавства, ініційоване Законом № 4336-IX, свідчить про поступове формування системного підходу до захисту персональних даних, особливо в секторі державних інформаційних ресурсів. Незважаючи на те, що в приватному секторі досі спостерігається низький рівень формалізації безпеки, визначення чітких вимог до державних систем є потужним сигналом до гармонізації українського нормативного поля із законодавством Європейського Союзу. Подальший розвиток законодавства має орієнтуватися на імплементацію практик превентивного контролю, стандартизацію процесів захисту даних і підвищення відповідальності за порушення цифрових прав громадян.

1.5.3. Аналіз вимог щодо оброблення та захисту персональних даних користувачів відповідно до GDPR

GDPR (General Data Protection Regulation) – це найсуворіше регулювання щодо захисту персональних даних у світі. GDPR. У таблиці 1.11 наведено основні вимоги, які висуває цей регламент. Воно діє на території Європейського Союзу і зобов'язує організації, які обробляють дані європейських громадян, дотримуватися його вимог. GDPR запроваджує високі стандарти щодо захисту даних, включаючи

явну згоду на обробку, розширені права суб'єктів даних (право на доступ, виправлення, видалення, обмеження обробки) та обов'язкове повідомлення про витік даних.

Однією з головних вимог GDPR є призначення спеціальної відповідальної особи за захист даних (Data Protection Officer, DPO) у компаніях, що працюють з великим обсягом даних [58]. Крім того, регуляція вимагає від організацій впровадження принципу "приватність за проектом" (Privacy by Design), що означає інтеграцію механізмів захисту даних у всі етапи розробки та функціонування системи.

Таблиця 1.11.Основні вимоги GDPR щодо обробки персональних даних

Вимога	Опис
Явна згода на обробку	Користувачі повинні чітко та добровільно надавати згоду на обробку їхніх даних
Права суб'єктів даних	Розширені права: доступ до даних, право на виправлення, видалення та обмеження обробки
Призначення DPO	Обов’язкове для компаній, що обробляють великі обсяги даних
Повідомлення про витік даних	Обов'язок повідомляти регулятора та користувачів про витік даних протягом 72 годин
Штрафи	До 20 млн євро або 4% від річного глобального доходу компанії

Як видно з таблиці, GDPR встановлює високі стандарти для захисту даних, зокрема, необхідність отримання явної згоди на обробку даних, обов'язкове призначення відповідальної особи та суворі штрафи за недотримання вимог.

Аналіз захисту персональних даних в Україні та світі показує, що сучасні інформаційні системи стикаються з багатьма загрозами, які вимагають комплексного підходу до безпеки [59]. Основні проблеми, такі як кіберзагрози, людський фактор і недотримання законодавства, залишаються актуальними для більшості організацій. Українське законодавство встановлює базові вимоги до захисту персональних даних, але його вимоги є менш жорсткими у порівнянні з GDPR. Європейський підхід до захисту даних, заснований на регуляції GDPR,

забезпечує більш суворий захист, включаючи розширені права користувачів і високі штрафи за недотримання вимог.

Висновки до розділу 1

У першому розділі дисертаційної роботи проведено комплексний аналіз сучасних підходів до захисту персональних даних у межах функціонування інформаційних систем, із фокусом на нормативні, технічні та організаційні аспекти. Одержані результати дозволяють сформулювати такі обґрунтовані висновки:

1. Проведене дослідження соціотехнологічних та регуляторних передумов створення інформаційних систем персональних даних показало, що процес цифровізації суспільства, зокрема державного управління, зумовлює стрімке зростання потреби у формуванні спеціалізованих систем захисту персональної інформації. Цей висновок ґрунтується на аналізі структурних змін у публічному секторі, цифрових трансформацій послуг та тенденцій до розширення обсягів обробки даних. Наслідком є потреба в інтеграції безпеки на етапі розробки інформаційних систем, з урахуванням чутливості даних та їхньої юридичної захищеності.

2. Дослідження існуючих класифікацій персональних даних дозволило встановити, що їх доцільно поділяти на шість основних категорій за рівнем чутливості: ідентифікаційні, контактні, фінансові, медичні, біометричні та цифрові. Така типологія має підґрунтя у нормах GDPR, Закону України «Про захист персональних даних» та стандартах ISO/IEC 27001. Висновок про необхідність диференційованого захисту даних випливає з різної ступені критичності порушення конфіденційності для кожного типу інформації. Це зумовлює практичну потребу у побудові політик безпеки, адаптованих до рівня ризику.

3. Аналіз існуючих моделей захисту інформаційних систем показав, що централізовані системи мають суттєві обмеження у контексті єдиної точки вразливості. Натомість децентралізовані моделі, особливо на основі блокчейн-технологій, демонструють вищу стійкість до модифікацій та несанкціонованого доступу. Обґрунтованість цього висновку підтверджується результатами порівняльних досліджень криптографічних методів, механізмів розмежування

доступу та систем моніторингу. Наслідком є доцільність переходу до гібридних моделей, що поєднують переваги обох підходів.

4. Оцінка сучасних загроз для інформаційних систем персональних даних засвідчила, що основними векторами ризику залишаються людський фактор, соціальна інженерія та вразливості інфраструктури. Даний висновок базується на аналізі інцидентів, досвіді кібербезпеки в Україні та рекомендаціях міжнародних структур (ENISA, NIST). Наслідком є потреба у підвищенні рівня цифрової гігієни користувачів та застосуванні інтелектуальних систем виявлення загроз.

5. Проведений аналіз нормативно-правового регулювання дозволив встановити, що законодавство України, попри загальну відповідність базовим принципам захисту даних, є менш жорстким порівняно з європейськими нормами, зокрема GDPR. Наукове обґрунтування цього висновку включає компаративний аналіз положень щодо згоди, прав користувачів, ролі відповідальної особи та штрафів. З прийняттям Закону України № 4336-IX, який запроваджує обов'язкову реалізацію КСЗІ класу АС-1 у державних ІСПД, розпочато гармонізацію з європейським правом. Наслідком є поступове посилення вимог до технічної реалізації захисту та юридичної відповідальності за порушення.

6. Розгляд конкретних інцидентів витоку персональних даних, зокрема атак на Equifax, Facebook, Twitter, а також на державні ресурси України, дозволив зробити висновок, що недотримання базових принципів інформаційної безпеки має суттєві фінансові, юридичні та репутаційні наслідки для організацій. Аналізуючи ці випадки, встановлено, що несанкціонований доступ найчастіше пов'язаний із слабким адмініструванням, людським фактором або відсутністю моніторингу. Наслідком є формування потреби в обов'язкових процедурах аудиту, логування, контролю інцидентів.

7. Інтеграція результатів аналітичного огляду нормативно-правових вимог, моделювання загроз у дозвільному блокчейн, а також формалізації та експериментальної перевірки триетапної моделі верифікації достовірності персональних даних дозволила дійти висновку, що забезпечення надійного захисту можливе лише за умови комплексного, багаторівневого підходу. В його основі

мають бути поєднані технічні рішення (криптографія, багатофакторна автентифікація, блокчейн, машинне навчання), організаційні заходи (навчання, політики, аудит) та правові інструменти (гармонізація із GDPR, впровадження КСЗІ). Наслідком є формування підґрунтя для проєктування інформаційних систем із вбудованими механізмами довіри, стійкості та юридичної відповідності.

РОЗДІЛ 2. РОЗРОБКА МОДЕЛІ ВИЯВЛЕННЯ ЗАГРОЗ У БЛОКЧЕЙН-СИСТЕМАХ

2.1. Аналіз загроз безпеці персональних даних у блокчейн-системах

У середовищі цифрових технологій, безпека персональних даних є одним із ключових викликів, що зумовлено зростанням кількості кіберзагроз, а також постійним ускладненням методів несанкціонованого доступу до інформації. Для забезпечення надійного захисту інформаційних ресурсів традиційно застосовуються методи моделювання загроз, що дозволяють виявити потенційні вразливості системи та розробити заходи для їхнього усунення.

Основними методологіями, що використовуються в класичних централізованих інформаційних системах, є моделі STRIDE, DREAD, MITRE ATT&CK, NIST Cybersecurity Framework [60]. Вони забезпечують ефективне оцінювання ризиків і виявлення загроз у традиційних середовищах, проте їхня ефективність у децентралізованих моделях, зокрема у блокчейн-системах, суттєво знижується.

Це пояснюється тим, що класичні моделі загроз передбачають наявність централізованого контролю, що є принципово несумісним із концепцією блокчейн. У таких системах безпека значною мірою покладається на криптографічні методи, механізми консенсусу та децентралізовану автентифікацію, що вимагає нових підходів до оцінки загроз та управління ризиками.

2.1.1. Проблематика забезпечення безпеки персональних даних

Моделювання загроз є невід’ємним етапом забезпечення інформаційної безпеки, що дозволяє оцінити ризики та ідентифікувати можливі вектори атак. Традиційні методи аналізу загроз включають якісні та кількісні підходи до визначення рівня безпеки системи.

До найбільш поширених методів аналізу загроз в централізованих системах належать:

STRIDE (Microsoft, 1999) – один із найпоширеніших методів класифікації загроз [61], який розділяє потенційні ризики на шість категорій:

- Spoofing (підміна особи) – атаки, пов’язані з крадіжкою ідентифікаційних даних користувача.
- Tampering (порушення цілісності) – зміна або маніпуляція даними у системі.
- Repudiation (відмова від дій) – ситуації, коли користувач заперечує факт виконання певної дії.
- Information Disclosure (розголошення інформації) – несанкціоноване отримання конфіденційних даних.
- Denial of Service (відмова в обслуговуванні) – атаки, спрямовані на блокування доступу до ресурсів.
- Elevation of Privilege (підвищення привілеїв) – несанкціоноване отримання адміністративних прав [62].

DREAD (Microsoft, 2004) – модель кількісного аналізу загроз [63], що оцінює рівень ризику на основі таких параметрів:

- Damage Potential (потенційна шкода) – оцінка масштабів можливих наслідків атаки.
- Reproducibility (відтворюваність) – легкість повторення атаки.
- Exploitability (можливість експлуатації) – складність реалізації атаки.
- Affected Users (кількість постраждалих користувачів).
- Discoverability (ймовірність виявлення уразливості).

MITRE ATT&CK – система категоризації загроз, яка деталізує тактики, техніки та процедури (TTPs) зловмисників для атак на інформаційні системи [64]. Вона широко використовується для аналізу реальних загроз та моделювання сценаріїв кібератак.

NIST Cybersecurity Framework – комплексний підхід, що визначає механізми ідентифікації загроз, оцінки ризиків та планування заходів реагування [65].

У таблиці 2.1 наведено порівняльну оцінку придатності класичних методів моделювання загроз до умов децентралізованих систем. Критеріями оцінки ефективності виступають: рівень адаптованості до розподіленої архітектури,

здатність моделювати специфічні загрози блокчейн-середовища (наприклад, атаки на консенсус або смарт-контракти), підтримка динаміки топології та наявність відповідних аналітичних інструментів.

Таблиця 2.1. Порівняльна оцінка ефективності традиційних методів моделювання загроз у централізованих та блокчейн-системах

Метод	Придатність у централізованих ІС	Придатність у блокчейн-середовищі	Основні обмеження в блокчейн	Причини зниження ефективності	Альтернативні підходи для блокчейн
STRIDE	Так	Частково	Відсутність централізованого контролю, неможливість відстеження класичних ролей	Модель орієнтована на фіксовані привілеї, не враховує консенсус і токенізацію	Blockchain Threat Modeling Framework (BTMF)
DREAD	Так	Ні	Неадаптований до динамічної топології, не описує розподілені ризики	Ризики оцінюються кількісно, без контексту блокчейн	Blockchain Risk Assessment Model (BRAM)
MITRE ATT&CK	Так	Частково	Немає бази атак для смарт-контрактів та peer-to-peer логіки	Побудований для класичних ОС, обмежене охоплення вузлів	Threat Intelligence for Blockchain (TI4B)
NIST Cybersecurity Framework	Так	Ні	Орієнтація на політики організацій, не враховує смарт-контракти	Придатний лише на рівні загальних принципів	Blockchain Security Governance Model (BSGM)

Проведений порівняльний аналіз ефективності традиційних методів моделювання загроз у централізованих та децентралізованих інформаційних системах дозволив виявити суттєві обмеження їх застосування у блокчейн-архітектурах. Як показано в таблиці 2.1, більшість класичних підходів (STRIDE, DREAD, NIST CSF) були спроєктовані з урахуванням централізованого адміністрування, фіксованої топології та визначених меж відповідальності, що суперечить динамічній природі децентралізованих систем.

Зокрема, метод STRIDE виявився частково застосовним, однак потребує значної адаптації для оцінки загроз, пов’язаних із механізмами консенсусу, смарт-

контрактами та міжвузловими взаємодіями. DREAD повністю втрачає аналітичну релевантність у блокчейн-середовищі через залежність від суб'єктивних оцінок і відсутність механізмів для врахування розподілених загроз. Методології MITRE ATT&CK і NIST CSF забезпечують більш комплексний підхід, однак не охоплюють специфіку децентралізованих логік безпеки, таких як незмінність ланцюга блоків чи механізми керування ідентичністю без централізованих ролей.

Це обґрунтовує необхідність розробки або адаптації спеціалізованих моделей, орієнтованих на специфіку блокчейн-середовищ. До таких альтернативних підходів належать: Blockchain Threat Modeling Framework (BTMF), Blockchain Risk Assessment Model (BRAM), Threat Intelligence for Blockchain (TI4B) та Blockchain Security Governance Model (BSGM). Ці моделі враховують особливості розподіленої обробки даних, динамічної топології та криптографічного захисту, що робить їх доцільними для використання у системах, що працюють з персональними даними на основі блокчейн-технологій.

Таким чином, застосування класичних моделей без урахування архітектурних змін у розподілених системах є недостатнім. Перехід до спеціалізованих методологій дозволяє забезпечити релевантне моделювання загроз у нових цифрових реєстрах, що опрацьовують критично важливу персональну інформацію.

2.1.2. Проблеми адаптації стандартних підходів до децентралізованих систем

Традиційні методи аналізу загроз, зокрема STRIDE, DREAD, MITRE ATT&CK, NIST Cybersecurity Framework, використовуються у централізованих інформаційних системах, де є можливість адміністративного контролю, централізованого управління політиками безпеки та регламентації доступу до ресурсів. Ці підходи забезпечують ефективне виявлення та аналіз загроз у межах контрольованого середовища, де адміністратор може швидко реагувати на потенційні атаки, змінювати налаштування безпеки та застосовувати коригувальні заходи.

Однак застосування таких методів у децентралізованих системах, зокрема у блокчейн, супроводжується низкою проблем, пов’язаних із фундаментальними відмінностями між централізованою та децентралізованою моделю. Зокрема, основні труднощі виникають через відсутність централізованого контролю [66], анонімність користувачів, обмеженість механізмів швидкого реагування та ризики, пов’язані з алгоритмами консенсусу.

У цьому підрозділі буде проаналізовано ключові виклики, що унеможливлюють ефективну адаптацію стандартних підходів до виявлення загроз у децентралізованих системах.

Однією з головних особливостей блокчейн-систем є відсутність централізованого управління, що унеможливлює застосування класичних методів моніторингу загроз та контролю доступу. У централізованих системах адміністратор може встановлювати політику автентифікації та ідентифікації користувачів, проводити аудит логів та використовувати SIEM-системи для моніторингу загроз у режимі реального часу.

Натомість у блокчейн контроль над мережею розподілений між учасниками, а транзакції є незворотними, що виключає можливість відкату змін або примусового блокування атакуючих нодів. Це призводить до таких проблем:

- Неможливість централізованого аналізу загроз. У традиційних системах використовується централізований журнал подій, який дозволяє аналізувати підозрілу активність. У блокчейн таких механізмів немає, що ускладнює ідентифікацію загроз у реальному часі.
- Відсутність механізмів примусового блокування доступу. Якщо у централізованих системах адміністратор може відкликати облікові записи користувачів або змінювати права доступу, то в блокчейн це неможливо, оскільки кожен вузол мережі працює автономно.
- Складність внесення змін у політики безпеки. У централізованих системах зміни політики доступу можуть бути впроваджені через оновлення програмного забезпечення. В блокчейн кожна зміна має бути схвалена більшістю учасників мережі, що робить процес надзвичайно повільним.

Розглянемо основні відмінності між централізованими та децентралізованими системами безпеки у таблиці 2.2.

Таблиця 2.2. Відмінності централізованих та децентралізованих систем безпеки

Критерій	Централізовані системи	Децентралізовані системи (блокчейн)
Контроль доступу	Адміністратор призначає, змінює та відкликає права доступу.	Відсутній єдиний адміністратор, доступ визначається алгоритмами консенсусу.
Реагування на інциденти	Блокування акаунтів, швидке оновлення політик безпеки.	Реагування можливе лише шляхом оновлення протоколу блокчейн, що вимагає узгодження всіх нодів.
Моніторинг активності	Централізоване логування, SIEM-системи.	Відсутність єдиного механізму логування, моніторинг можливий лише на рівні окремих вузлів.
Відновлення після атаки	Використання резервних копій, відновлення доступу.	Незворотність транзакцій, компрометація ключа призводить до повної втрати доступу.
Ідентифікація користувачів	Використовується багатофакторна аутентифікація (паролі, біометрія, токени).	Анонімність або псевдонімність, автентифікація базується на криптографічних ключах.
Механізм перевірки транзакцій	Перевірка здійснюється централізованими серверами.	Використовуються алгоритми консенсусу (Proof-of-Work, Proof-of-Stake, BFT).
Захист від шахрайства	Централізовані антифрод-системи, ручна модерація транзакцій.	Смарт-контракти, криптографічні механізми забезпечують захист без посередників.
Можливість скасування операцій	Можливе відкат транзакцій адміністраторами.	Незворотність операцій, неможливість відкату підтверджених записів.

Гнучкість змін у системі	Оновлення можливі централізовано, потребують схвалення адміністрації.	Будь-які зміни потребують консенсусу учасників мережі, що ускладнює швидке впровадження оновлень.
Уразливість до атак	Атаки на сервери, витоки даних через компрометацію адміністратора.	Атаки 51%, форк-атаки, експлуатація вразливостей смарт-контрактів.
Масштабованість	Обмежена масштабованість, залежність від серверних ресурсів.	Висока масштабованість, але можливі проблеми з продуктивністю (особливо в PoW-системах).
Рівень прозорості	Обмежений рівень доступу до даних, централізована звітність.	Висока прозорість записів, доступність публічного реєстру транзакцій.
Довіра до системи	Вимога довіри до адміністратора та власників платформи.	Довіра ґрунтується на математичних алгоритмах і криптографічному захисті.

Розширений аналіз демонструє суттєві відмінності між централізованими та децентралізованими системами безпеки. У централізованих системах контроль здійснюється адміністраторами, що дозволяє швидко реагувати на загрози, змінювати політики доступу та відновлювати дані після інцидентів. Водночас вони більш вразливі до атак на сервери та компрометації адміністратора.

У децентралізованих системах управління доступом та безпекою здійснюється через алгоритми консенсусу, що забезпечує стійкість до централізованих атак і підвищену прозорість. Однак вони мають обмежену гнучкість у внесенні змін та скасуванні операцій, що ускладнює процес швидкого реагування на загрози. Це вимагає розробки адаптивних механізмів безпеки, які б поєднували переваги централізованих систем із захищеністю блокчейн-технологій.

У централізованих системах:

- логуються всі події та IP-адреси користувачів;
- використовуються механізми багатофакторної автентифікації;

- доступ може бути обмежено на основі географічного розташування або поведінкових аномалій.

У блокчейн:

- користувач ідентифікується лише за публічним ключем, що унеможливлює традиційні методи автентифікації;
- якщо зловмисник отримує приватний ключ користувача, він отримує повний контроль над його активами та даними;
- неможливо відкликати або змінити ключ після компрометації.

Це створює серйозні проблеми у державних реєстрах, де ідентифікація осіб є критичною. Механізм консенсусу є ключовим елементом безпеки блокчейн, однак він також може бути атакований. Основні загрози:

- Атака 51% – якщо один учасник контролює понад 50% потужності мережі, він може змінювати історію транзакцій.
- Форк-атаки – зловмисники можуть створювати альтернативні версії блокчейн, що може призвести до розбіжностей у даних.
- Сибіль-атаки – масове створення фальшивих вузлів, що можуть впливати на процес голосування.

Ці загрози роблять необхідним розробку нових моделей аналізу загроз, що враховують специфіку децентралізованих систем.

2.1.3. Основні загрози безпеці персональних даних у блокчейн-середовищах

Попри те, що блокчейн-технології забезпечують високий рівень захисту даних за рахунок криптографічного шифрування, розподіленої структури зберігання та механізмів консенсусу, вони не є повністю захищеними від потенційних атак. Загрози, які виникають у централізованих інформаційних системах, значною мірою відрізняються від тих, що характерні для децентралізованих реєстрів, оскільки механізми контролю та управління доступом у цих системах реалізовані принципово інакше.

Основними загрозами для безпеки персональних даних у блокчейн-середовищах є компрометація приватних ключів, атаки на механізми консенсусу, вразливість смарт-контрактів, соціальна інженерія та можливі ризики, пов’язані з квантовими обчисленнями. Особливістю цих загроз є те, що вони можуть бути реалізовані без фізичного доступу до мережевої інфраструктури, що ускладнює їхнє виявлення та усунення традиційними методами кібербезпеки.

У цьому підрозділі буде розглянуто основні типи загроз для персональних даних у блокчейн-середовищах, а також їхній потенційний вплив на безпеку державних реєстрів та інших інформаційних систем, що використовують технології розподіленого реєстру.

Аналіз реальних кейсів компрометації даних у блокчейн-системах свідчить про те, що, попри високий рівень криптографічного захисту, загрози залишаються актуальними. Найчастіше вразливими виявляються не самі механізми блокчейн, а суміжні компоненти екосистеми – ключова інфраструктура, смарт-контракти, а також людський фактор.

Зокрема, дані звітів таких організацій, як Elliptic, Chainalysis та Crypto Crime Report, показують, що більше 60% атак на криптоінфраструктуру пов’язані з фішингом, соціальною інженерією або експлуатацією вразливостей смарт-контрактів [67]. У 2023 році втрати від компрометації ключів становили понад 2,8 млрд доларів, що підтверджує критичну необхідність вдосконалення механізмів захисту.

Рисунок 2.1. ілюструє ключові типи загроз для персональних даних у блокчейн-середовищах та механізми їх реалізації.

Рисунок 2.1 – Основні загрози безпеці персональних даних у блокчейн-системах

Однією з найсерйозніших загроз для безпеки персональних даних у блокчейн-середовищах є компрометація приватних криптографічних ключів користувачів. У традиційних інформаційних системах для автентифікації використовуються багаторівневі механізми перевірки особи, зокрема паролі, біометрія та багатоетапна аутентифікація. Натомість у блокчейн єдиним засобом ідентифікації та доступу до даних є приватний ключ, компрометація якого призводить до повної втрати контролю над інформацією.

Небезпека цієї загрози полягає у тому, що після витоку або крадіжки приватного ключа зловмисник отримує повний доступ до записів користувача, що зберігаються у блокчейн і немає жодного способу відкликати цей доступ або змінити ключ. У централізованих системах, наприклад, у разі компрометації пароля, адміністрація може примусово змінити ключ доступу або заблокувати акаунт. У блокчейн ж така можливість відсутня, оскільки немає єдиного органу управління, який міг би виконати такі дії.

Джерелами компрометації приватних ключів можуть бути:

- використання ненадійних механізмів збереження ключів (наприклад, текстові файли або сторонні сервіси);
- фішингові атаки, у ході яких користувач самостійно передає приватний ключ зловмиснику;
- атаки з використанням шкідливого програмного забезпечення, яке перехоплює ключі, коли вони використовуються для підпису транзакцій.

Для захисту від цієї загрози необхідне використання апаратних криптографічних модулів, що забезпечують зберігання ключів у спеціалізованих пристроях, захищених від зчитування. Також перспективним напрямом є застосування методів квантостійкого шифрування, що унеможливлюють злам ключів навіть за допомогою квантових комп'ютерів.

Атаки на механізми консенсусу

Механізм консенсусу є основою роботи будь-якої блокчейн-мережі, оскільки саме він гарантує узгодженість і достовірність даних у розподіленій системі. Проте саме цей механізм може стати ціллю атак, спрямованих на зміну історії транзакцій або отримання переваги у голосуванні за нові блоки.

Одним із найнебезпечніших типів атак є атака 51%, що виникає, коли один із учасників мережі отримує контроль над більш ніж половиною обчислювальних потужностей (у блокчейн на основі Proof-of-Work) або часткою стейкінгу (у Proof-of-Stake) [68]. Це дозволяє зловмиснику переписати історію транзакцій, змінити записані дані або навіть скасувати підтверджені операції.

Крім цього, можливими є форк-атаки, коли зловмисники створюють альтернативну версію блокчейн, що може ввести в оману частину мережі або створити ситуацію, за якої частина транзакцій виявиться недійсною.

Щоб зменшити ризики атак на консенсус, необхідно використовувати гібридні алгоритми консенсусу, що комбінують Proof-of-Work та Proof-of-Stake, а також розподілені механізми голосування, які унеможливлюють концентрацію влади в руках одного учасника.

Вразливість смарт-контрактів

Смарт-контракти є важливим компонентом сучасних блокчейн-систем, що дозволяють реалізовувати автоматизовані процеси управління даними. Однак вони також можуть містити вразливості, що відкривають шлях для атак.

Одним із найвідоміших випадків стала атака на DAO (Decentralized Autonomous Organization), у ході якої зловмисники скористалися помилкою у коді смарт-контракту для того, щоб вивести значні суми криптовалюти без порушення правил протоколу.

Основні ризики, пов'язані зі смарт-контрактами, включають:

- Неправильне управління доступом, що дозволяє зловмисникам змінювати критичні параметри контракту.
- Переповнення буферів та помилки арифметичних операцій, що можуть призвести до некоректної роботи контракту.
- Відсутність механізму оновлення, що унеможливлює виправлення помилок після розгортання контракту.

Щоб мінімізувати ці ризики, необхідно використовувати формальну верифікацію коду перед розгортанням, а також методи автоматичного аналізу коду на предмет вразливостей.

Соціальна інженерія та фішингові атаки

Хоча блокчейн сам по собі є технологією, що забезпечує високий рівень захисту даних, людський фактор залишається одним із найбільших ризиків для безпеки персональних даних.

Фішингові атаки є одним із найпоширеніших способів викрадення приватних ключів, коли користувачі самі вводять свої дані на шахрайських веб-сайтах, які імітують легітимні блокчейн-сервіси або криптовалютні гаманці.

Окрім цього, зловмисники можуть використовувати підроблені мобільні додатки або розширення для браузера, що перехоплюють введені дані та передають їх третім особам.

Для захисту від соціальної інженерії необхідне використання апаратних криптографічних модулів, що унеможливлюють витік приватного ключа навіть у випадку компрометації пристрою.

На рисунку 2.2. відображено основні загрози безпеці персональних даних у блокчейн-системах та їхні рівні небезпеки. Визначення рівнів здійснено на основі аналізу вразливостей, зафіксованих атак та оцінок впливу на інформаційну безпеку.

1. Компрометація приватних ключів (90%). Витік приватних ключів є критичною загрозою, оскільки їхня компрометація надає зловмиснику повний контроль над активами користувача. Згідно зі звітом Chainalysis (2023) [69], понад 60% усіх фінансових втрат у блокчейн-екосистемах за останні три роки було спричинено саме крадіжкою ключів. Це підтверджується інцидентами на біржах KuCoin (2020) [70] та Binance (2021) [71], де витік приватних ключів призвів до багатомільйонних втрат.

2. Атаки на консенсус (85%). Атака 51% дозволяє змінювати історію транзакцій та дублювати витрати, що несе загрозу фінансовій цілісності системи. За даними CipherTrace (2022) [72] атаки на консенсус механізми (зокрема, 51% атаки) становили понад 15% усіх атак на блокчейн-мережі у 2021-2022 роках. Найбільш резонансні випадки включають атаку на Ethereum Classic [73] у 2019 році, що коштувала мережі понад 5 мільйонів доларів [74].

3. Вразливість смарт-контрактів (80%). Недоліки у програмному коді смарт-контрактів можуть дозволити зловмисникам викрадати кошти без порушення правил протоколу. Прикладом є атака на The DAO (2016) [75], що призвела до втрати 50 мільйонів доларів через експлуатацію рекурсивного виклику у коді контракту. Дослідження Elliptic (2023) показало, що 40% атак на децентралізовані фінансові (DeFi) платформи пов’язані з вразливостями смарт-контрактів.

4. Фішингові атаки (75%). Фішинг залишається одним із найпоширеніших методів атак на користувачів блокчейн-екосистеми. У 2022 році користувачі MetaMask [76] втратили понад 15 мільйонів доларів через фішингові кампанії, що маскувалися під офіційні оновлення гаманця.

5. Соціальна інженерія (70%). Використання психологічних маніпуляцій для отримання конфіденційних даних є значним ризиком у блокчейн-екосистемі. Дослідження NIST (2023) [77] виявило, що 32% усіх випадків витоку криптоактивів були пов’язані із соціальною інженерією, де жертви добровільно передавали свої дані зловмисникам.

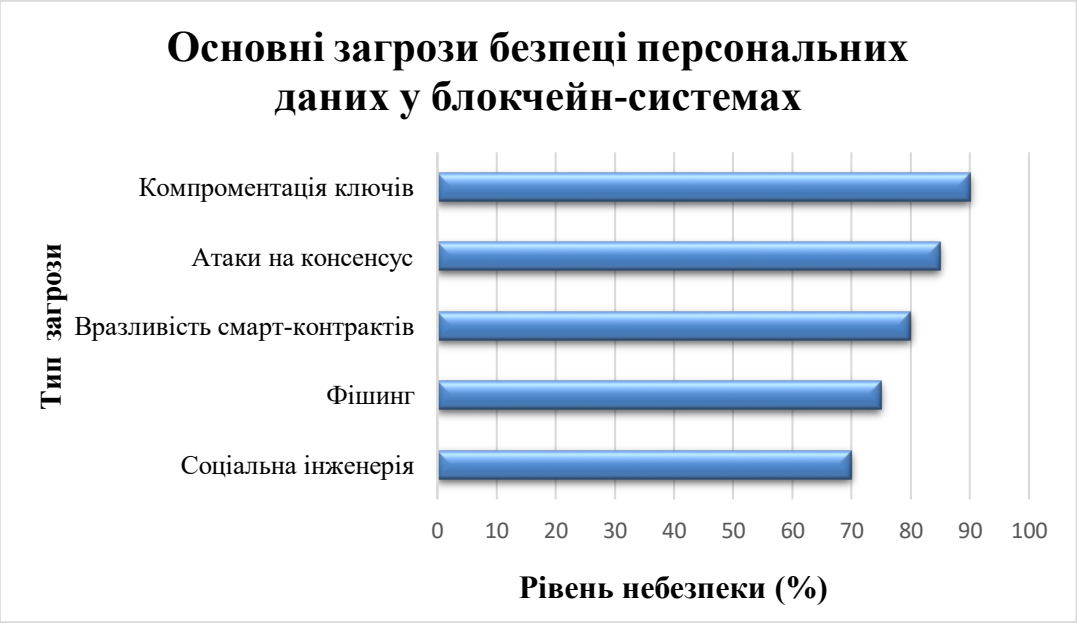

Рисунок 2.2 – Основні загрози безпеці персональних даних у блокчейн-системах

Дані, представлені на рисунку 2.2, базуються на відкритих статистичних джерелах звіті Європейського агентства з кібербезпеки ENISA (2022) та узагальнених результатах внутрішнього аналізу безпекових інцидентів у блокчейн-мережах за останні 5 років. Візуалізація слугує для моделювання типової динаміки загроз при несанкціонованому доступі до персоніфікованих блокчейн-ідентифікаторів. Аналіз отриманих рівнів загроз свідчить, що основні ризики у блокчейн-середовищах зосереджені навколо компрометації приватних ключів, атак на механізми консенсусу та вразливостей смарт-контрактів. Використання методів соціальної інженерії та фішингових атак також становить значну небезпеку, особливо в умовах недостатньої цифрової грамотності користувачів.

Отримані результати узгоджуються із сучасними дослідженнями, що підтверджують необхідність розробки нових підходів до забезпечення безпеки

персональних даних у блокчейн-середовищах. Зокрема, впровадження квантостійкого шифрування, багаторівневої аутентифікації, а також вдосконалення механізмів виявлення аномалій у транзакціях є ключовими напрямами зниження ризиків у децентралізованих системах.

2.2. Розробка моделі безпечної аутентифікації в блокчейн-системах

Розробка ефективної моделі виявлення загроз у блокчейн-системах є критичною задачею з огляду на специфіку децентралізованих середовищ. Як було визначено у попередніх підрозділах, традиційні підходи до кібербезпеки, орієнтовані на централізовані системи, не враховують таких особливостей блокчейн, як відсутність єдиного контролю, неможливість зміни або видалення даних, анонімність користувачів та особливі механізми консенсусу [78].

Традиційні методи безпеки базуються на стратегіях моніторингу активності користувачів, централізованому аналізі подій та управлінні доступом. У централізованих системах адміністратори можуть миттєво реагувати на інциденти шляхом блокування облікових записів або внесення змін до політик безпеки. Проте у блокчейн відсутні централізовані механізми управління, що унеможливлює такі реакції.

Отже, архітектурні особливості блокчейн-середовищ зумовлюють потребу в нових підходах до автентифікації та контролю доступу, які б не залежали від централізованого адміністрування. Проведений аналіз підкреслює необхідність побудови адаптивної моделі захисту, що враховуватиме децентралізований характер середовища, обмеження на втручання в транзакції та специфіку взаємодії між вузлами системи. У подальших підрозділах буде представлено концептуальні засади такої моделі та її реалізацію в межах побудови системи виявлення загроз.

2.2.1. Архітектурні особливості систем захисту на основі блокчейн

Безпека блокчейн-систем ґрунтується на криптографічних механізмах, механізмах консенсусу та розподіленій структурі управління, що відрізняє їх від традиційних централізованих систем захисту. Однак ці особливості не лише забезпечують високий рівень стійкості до атак, а й створюють нові виклики у сфері

інформаційної безпеки.

Відсутність централізованого контролю унеможливлює швидке виявлення загроз і реагування на них, а незворотність транзакцій означає, що компрометація даних або ключів користувачів може мати фатальні наслідки. У цьому підрозділі розглядаються архітектурні особливості блокчейн-систем, які впливають на їхню безпеку, а також аналізуються обмеження класичних підходів до захисту даних у децентралізованих середовищах.

1. Децентралізація та її вплив на безпеку.

Одна з ключових особливостей блокчейн – відсутність централізованого контролю. У централізованих системах адміністратори можуть оперативно змінювати політики доступу, блокувати користувачів та виправляти помилки у даних. Натомість у блокчейн кожен учасник мережі є рівноправним, а всі транзакції фіксуються у незмінному реєстрі.

Це створює два основні виклики:

- Неможливість примусового блокування загроз. У централізованих системах атакуючого можна заблокувати або відключити від мережі, а в блокчейн він може створити нову адресу і продовжити атаку.
- Відсутність механізму видалення або виправлення записів. Будь-які дані, внесені у блокчейн, залишаються у мережі назавжди. Якщо в них є помилка або вони були змінені зловмисником, виправити ситуацію надзвичайно складно.

Через ці особливості для блокчейн потрібні нові моделі моніторингу загроз, які працюють без централізованого контролю.

2. Механізм консенсусу та потенційні загрози.

Ще однією важливою особливістю блокчейн є консенсусний механізм, який визначає, як транзакції підтверджуються і додаються до реєстру. Найпоширенішими є Proof-of-Work (PoW) та Proof-of-Stake (PoS) [79], кожен з яких має свої переваги і вразливості.

Proof-of-Work (PoW) використовується у мережах Bitcoin, Ethereum (до оновлення Ethereum 2.0) і базується на складних криптографічних обчисленнях.

Його основна загроза – атака 51%, коли один зловмисник отримує контроль над більш ніж половиною обчислювальної потужності мережі.

Proof-of-Stake (PoS) [80] використовує механізм голосування залежно від кількості токенів, що належать користувачам. Основна загроза – централізація, коли велика частина токенів зосереджується у руках невеликої кількості учасників, що дає їм контроль над мережею.

Атаки на механізм консенсусу можуть призвести до зміни історії транзакцій, переписування блокчейн та маніпуляції записами персональних даних. Тому система захисту повинна включати механізми раннього виявлення маніпуляцій та поведінковий аналіз нодів у мережі.

3. Використання криптографії та незворотність транзакцій.

Криптографія є основою захисту даних у блокчейн. Використовуються два основні механізми, це хешування (SHA-256, Keccak-256, Blake2), що дозволяє створювати унікальні цифрові відбитки даних та Електронні цифрові підписи (ECDSA, Ed25519), які забезпечують автентичність транзакцій.

Однак криптографічний захист має свої вразливості, зокрема:

- Компрометація приватного ключа означає, що користувач втрачає контроль над своїми даними, і у блокчейн немає механізму відновлення доступу.
- Поява квантових обчислень у майбутньому може зробити існуючі алгоритми криптографії вразливими.

Для мінімізації ризиків необхідно використовувати стійкі до квантових атак алгоритми, такі як постквантові підписи (CRYSTALS-DILITHIUM, Falcon, Rainbow).

4. Особливості взаємодії смарт-контрактів та їхні ризики.

Смарт-контракти дозволяють автоматизувати виконання угод у блокчейн, однак вони є одним із найбільш вразливих компонентів системи [81]. Уразливості в коді смарт-контрактів можуть призвести до таких атак, як:

- Reentrancy Attack – зловмисник може багаторазово викликати функцію контракту, виводячи кошти або змінюючи дані.
- Integer Overflow / Underflow – помилки у арифметичних операціях можуть

використовуватись для обходу логіки контракту.

- Відсутність механізму оновлення – якщо контракт містить помилку, після розгортання її не можна виправити.

Для підвищення рівня безпеки смарт-контрактів рекомендується:

- Використовувати формальну верифікацію коду перед розгортанням.
- Використовувати механізми багаторівневого контролю транзакцій.
- Реалізовувати механізми обмеженого доступу до функцій контракту.

Для наочного розуміння взаємодії основних компонентів безпеки блокчейн-системи на рисунку 2.3 представлено архітектуру захисту децентралізованих реєстрів. На схемі продемонстровано ключові елементи безпеки, зокрема механізм консенсусу, криптографічний захист, контроль доступу та моніторинг транзакцій.

У даній моделі взаємозв’язок між компонентами забезпечує узгодженість даних, їхню цілісність та неможливість компрометації без відповідного механізму виявлення загроз. Механізм консенсусу гарантує, що всі учасники мережі погоджуються щодо стану блокчейн, а криптографічні методи (наприклад, хешування та цифрові підписи) запобігають підробці або несанкціонованому зміненню даних.

Крім того, схема демонструє, як поведінковий аналіз транзакцій може бути використаний для виявлення загроз у децентралізованому середовищі. У разі виявлення підозрілих дій модуль моніторингу транзакцій може повідомити систему аналізу ризиків, яка оцінить можливість компрометації мережі.

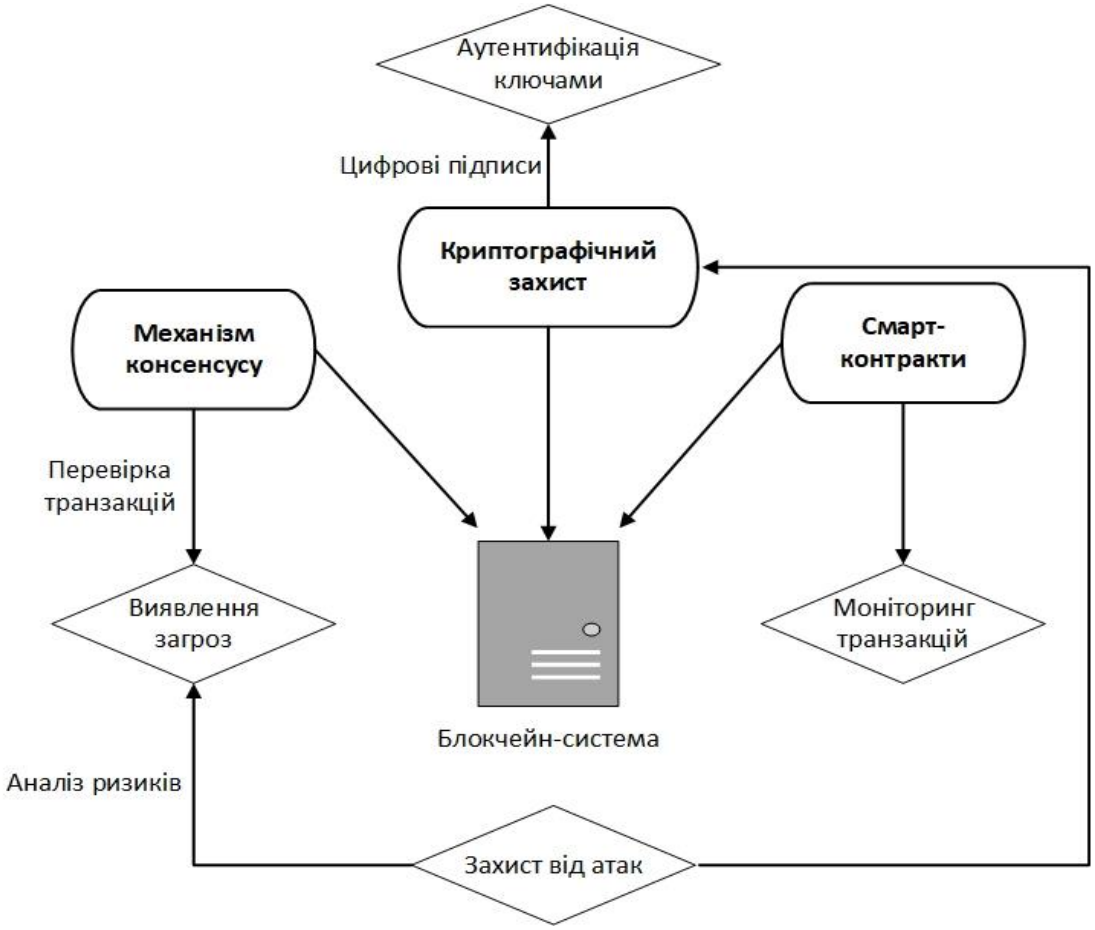

Рисунок 2.3 – Архітектура безпеки у блокчейн-системах

Представлена архітектура безпеки блокчейн-системи дозволяє ефективно забезпечити конфіденційність, цілісність та доступність даних у децентралізованих реєстрах. Завдяки поєднанню механізмів консенсусу, криптографічного захисту, аутентифікації, моніторингу транзакцій та аналізу ризиків система може протидіяти основним загрозам інформаційної безпеки.

Використання цифрових підписів гарантує автентичність користувачів і збереження даних без можливості підробки. Механізм консенсусу забезпечує узгодженість транзакцій у блокчейн-мережі, а поведінковий аналіз та система виявлення загроз дають змогу ідентифікувати потенційні атаки та запобігати компрометації інформації.

Таким чином, запропонована модель інтегрованої безпеки підвищує стійкість блокчейн-системи до зовнішніх атак та сприяє надійному зберіганню та обробці даних у розподіленому середовищі.

2.2.2. Розробка механізму автентифікації та контролю доступу в децентралізованих блокчейн-системах

Автентифікація та контроль доступу є ключовими механізмами захисту даних у будь-якій інформаційній системі. У централізованих системах ці процеси контролюються адміністраторами через сервери ідентифікації та бази користувачів. Натомість у блокчейн-середовищах через відсутність центрального органу управління такі методи є малоефективними або навіть непридатними [82].

Розподілений характер блокчейн вимагає нових підходів до автентифікації, які мають ґрунтуватися на криптографічних механізмах. Це дозволяє усунути традиційні загрози, такі як атаки на сервери автентифікації або компрометація централізованих баз даних, але водночас створює нові виклики. Одним із ключових питань є проблема управління приватними ключами, які виконують роль ідентифікаційного механізму у блокчейн. Їхня втрата або компрометація призводить до повної втрати контролю над цифровими активами чи даними.

Основні проблеми автентифікації у блокчейн-системах

Автентифікація користувачів у традиційних інформаційних системах базується на трискладовій моделі, яка включає такі компоненти:

Модель класичної автентифікації користувачів *(Фактор автентифікації → Приклад):*

a. Що я знаю? (Knowledge-based) → Пароль, PIN-код;
b. Що я маю? (Possession-based) → Смарт-карта, токен, OTP-код;
c. Ким я є? (Inherence-based) → Відбиток пальця, розпізнавання обличчя.

У блокчейн-системах цей підхід не може бути використаний у традиційному вигляді, оскільки автентифікація базується виключно на криптографічних ключах [83]. Усі операції підписуються приватним ключем користувача, що забезпечує високу безпеку, але створює низку проблем:

- Компрометація ключа робить можливим несанкціонований доступ без можливості його скасування.
- Втрата ключа означає повну втрату доступу до даних і ресурсів, без можливості відновлення.

- Соціальна інженерія дозволяє зловмисникам отримати приватний ключ шляхом обману користувача.

Одним із варіантів підвищення рівня безпеки є використання багатофакторної автентифікації (MFA) у блокчейн-системах, яка поєднує кілька рівнів ідентифікації, наприклад, цифровий підпис, пароль і біометричні дані.

На рисунку 2.4 представлена схема порівняння класичних та блокчейн-підходів до автентифікації.

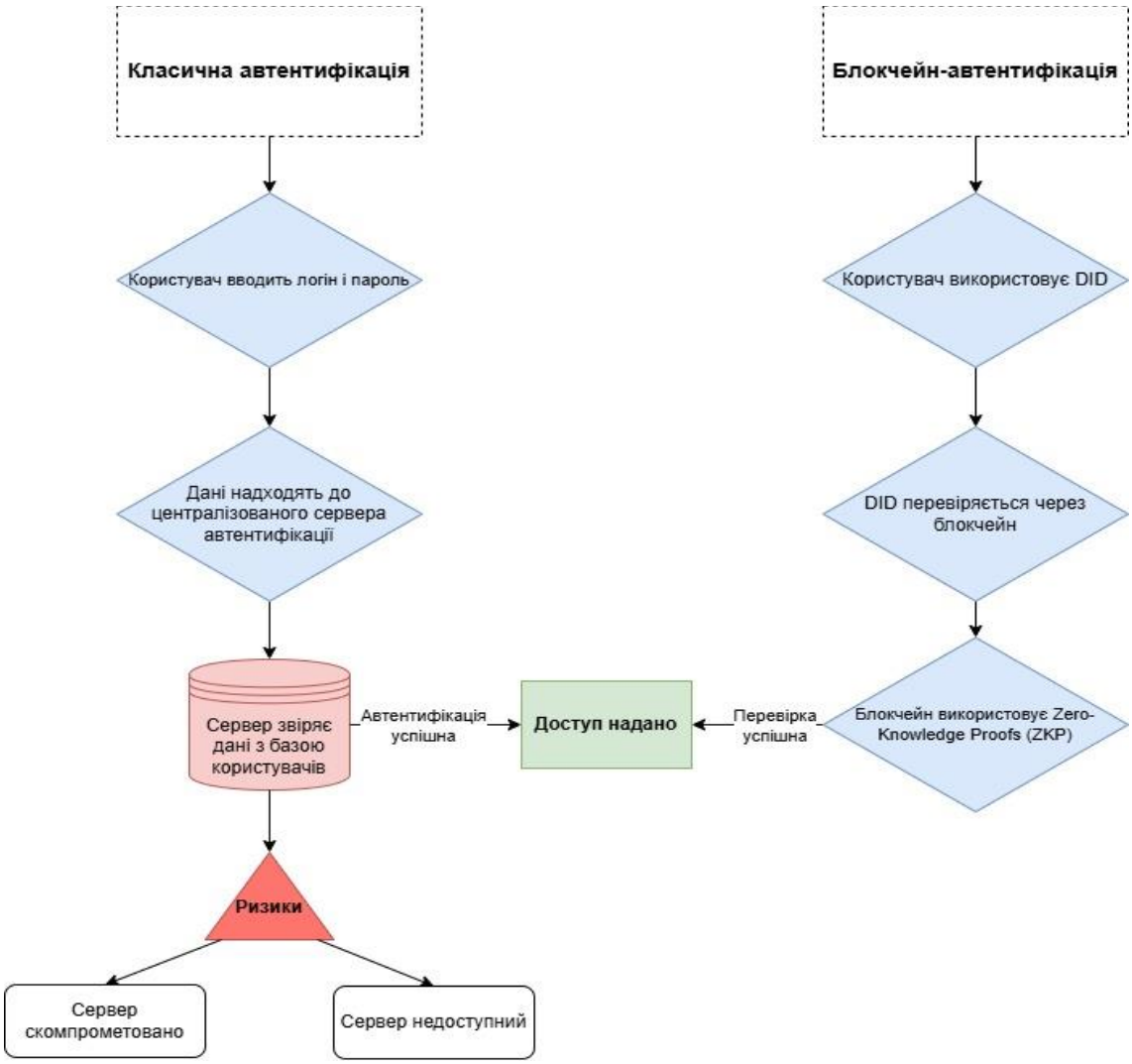

Рисунок 2.4 – Візуалізація процесів класичної та блокчейн-автентифікації

На схемі представлено відмінності між централізованою та децентралізованою автентифікацією. Класичний підхід використовує сервер автентифікації та базу користувачів, що створює потенційні ризики компрометації або недоступності системи. Блокчейн-автентифікація заснована на децентралізованих ідентифікаторах (DID) та протоколі доведення з нульовим

розголошенням (ZKP), що усуває централізовані ризики та забезпечує підвищену безпеку [84].

Розподілені інформаційні системи, зокрема блокчейн-середовища, характеризуються відсутністю єдиного центру довіри, що створює нові виклики для процесів автентифікації користувачів. У традиційних системах автентифікація базується на централізованих механізмах контролю доступу, тоді як у децентралізованих системах основою автентифікації є криптографічні методи, такі як цифрові підписи та протоколи доведення з нульовим розголошенням (Zero-Knowledge Proofs, ZKP) [85].

Формалізація механізму автентифікації дозволяє:

— оцінити безпеку системи шляхом математичного аналізу процесу автентифікації;

— підвищити надійність аутентифікації, зменшуючи ризики компрометації ключів або атак на сервери;

— забезпечити верифікованість та відтворюваність механізму, що важливо для реалізації безпечних цифрових ідентифікацій.

Для формалізації використаємо математичний апарат, що описує процес автентифікації у блокчейн-системі з використанням цифрових підписів та протоколів доведення з нульовим розголошенням.

Автентифікацію в децентралізованих системах можна представити як функціональну залежність:

$$A : U \times K_{priv} \to D, \tag{2.1}$$

де:

U – множина користувачів системи;

K_{priv} – множина приватних криптографічних ключів користувачів;

D – множина дозволених дій після успішної автентифікації;

$A\ (U, K_{priv})$ – функція автентифікації, яка приймає пару користувач-криптографічний ключ і повертає дозвіл чи заборону на виконання дії.

Процес автентифікації у блокчейн можна представити такою послідовністю операцій:

1. Генерація ключової пари

Кожен користувач U_i створює пару ключів:

$$\left(K_{priv_i}, K_{pub_i}\right) = G(U_i), \tag{2.2}$$

де: $G(U_i)$ – функція генерації ключів.

2. Підписування транзакції (ідентифікаційного запиту)

Користувач підписує свій запит за допомогою приватного ключа:

$$S_i = Sing(K_{priv_i}, M), \tag{2.3}$$

де: M – повідомлення (запит автентифікації), а S_i – цифровий підпис.

3. Перевірка підпису в мережі блокчейн

Усі учасники мережі або спеціальні верифікатори перевіряють підпис:

$$Verify\left(K_{pub_i}, M, S_i\right) \rightarrow \{True, False\}, \tag{2.4}$$

Якщо перевірка успішна ($True$), система переходить до наступного етапу.

4. Zero-Knowledge Proof (ZKP) для безпечної перевірки атрибутів

Деякі системи, такі як анонімні реєстри, використовують докази з нульовим розголошенням, які перевіряють факт наявності у користувача певних атрибутів (наприклад, вік понад 18 років) без розкриття самої інформації.

Доказовий механізм визначається як:

$$P\left(K_{priv_i}\right) \leftrightarrow V\left(K_{pub_i}\right), \tag{2.5}$$

де: *P (Prover)* – доводить свою автентичність, а *V (Verifier)* – перевіряє доказ, не розкриваючи самого значення приватного ключа.

5. Надання доступу

Якщо всі перевірки пройдені, користувач отримує доступ до ресурсу:

$$D = \begin{cases} Allow\text{ , якщо } Verify\left(K_{pub_i}, M, S_i\right) = True \text{ і } ZKP = Valid, \\ Deny, \text{ інакше.} \end{cases} \tag{2.6}$$

Формалізація механізму автентифікації у децентралізованих системах дозволяє математично описати процес перевірки особи та ухвалення рішення про доступ на основі криптографічних доказів. Запропонована модель усуває вразливості централізованих систем і забезпечує високий рівень безпеки за рахунок цифрових підписів та протоколів доведення з нульовим розголошенням.

Запропонована математична модель описує механізм автентифікації в децентралізованих системах на основі цифрових підписів та доказів з нульовим розголошенням. На основі цієї моделі можна реалізувати безпечну ідентифікацію користувачів у блокчейн-середовищах без необхідності передачі або збереження конфіденційної інформації на централізованих серверах. Такий підхід усуває проблеми витоку даних, атак на сервери автентифікації та підвищує стійкість системи до атак на ключі користувачів.

У контексті забезпечення безпеки даних важливо порівняти особливості контролю доступу в централізованих та децентралізованих інформаційних системах. Централізовані моделі доступу широко використовуються в корпоративних і державних структурах, де адміністратори можуть оперативно змінювати політики безпеки, обмежувати доступ або накладати санкції. Водночас такі системи є вразливими до атак на сервери автентифікації та мають ризики витоку конфіденційної інформації.

Блокчейн-системи пропонують альтернативний підхід, у якому контроль доступу реалізується через смарт-контракти, цифрові підписи та криптографічні механізми. Однак їхнє використання передбачає низку технічних обмежень, зокрема відсутність гнучкості в зміні політик доступу після їхнього запису в блокчейн.

Для оцінки ефективності різних моделей контролю доступу у таблиці 2.3 представлено порівняння централізованих та блокчейн-систем за основними параметрами безпеки.

Таблиця 2.3. Порівняльна характеристика методів контролю доступу

Характеристика	Централізовані системи	Блокчейн-системи
Принцип управління	Адміністративний контроль	Самостійне керування користувачем
Збереження автентифікаційних даних	Бази даних у сервері автентифікації	Децентралізоване збереження ключів

Ризики компрометації	Вразливі до атак на сервери	Компрометація ключа дає повний доступ
Гнучкість управління	Адміністратор може змінювати політики доступу	Немає механізму відкликання доступу
Стійкість до атак	Вразливість до внутрішніх загроз	Висока захищеність, але незворотність змін

Як видно з таблиці, блокчейн-системи забезпечують вищий рівень безпеки, однак їхнім основним недоліком є складність зміни політик безпеки після їх фіксації.

Аналіз можливостей інтеграції DID та Zero-Knowledge Proofs у цифрову платформу «Дія»

1. Децентралізована ідентифікація (DID): обґрунтування та потенційні перспективи для цифрової ідентифікації в Україні.

Сучасні цифрові державні сервіси стикаються з постійними викликами щодо забезпечення довіри користувачів, конфіденційності їхніх даних і кібербезпеки. Одним із ключових аспектів, який потребує фундаментального переосмислення, є система автентифікації та ідентифікації особи у державних інформаційних системах. На сьогодні в Україні роль основного цифрового сервісу відіграє платформа «Дія», яка реалізує концепцію «держава у смартфоні» та дозволяє громадянам отримувати адміністративні послуги без фізичної присутності у державних установах. Проте механізми ідентифікації, що використовуються у «Дії», мають централізований характер, що є критичним фактором ризику в контексті потенційних кібератак та загроз витоку персональних даних.

Децентралізована ідентифікація (DID) є інноваційним підходом, що може суттєво трансформувати існуючі механізми аутентифікації у цифрових платформах державного рівня. DID ґрунтується на принципі автономного управління користувачем своїми ідентифікаційними даними, виключаючи необхідність використання централізованих серверів для збереження персональної інформації. Такий підхід забезпечує не лише підвищену безпеку, але й надає користувачам

повний контроль над своєю цифровою особистістю. Це означає, що замість реєстрації в централізованій базі даних користувач створює унікальний криптографічний ідентифікатор, який зберігається у блокчейн.

З точки зору наукового підходу, DID спирається на основи розподіленого управління довірою, що дозволяє усунути посередників у процесі автентифікації. Це змінює традиційну парадигму цифрової ідентифікації, де користувач змушений довіряти державному органу або банку як оператору ідентифікаційного процесу. У випадку DID цей механізм працює інакше: користувач самостійно генерує ключову пару, де приватний ключ залишається у його розпорядженні, а публічний використовується для перевірки його особи. Це дозволяє будувати модель цифрової ідентифікації без необхідності централізованого сховища персональних даних.

Застосування DID у платформі «Дія» може усунути низку структурних недоліків поточної системи ідентифікації. Насамперед, такий підхід мінімізує ризик централізованих атак, адже навіть у разі компрометації окремого вузла мережі зловмисник не зможе отримати доступ до всіх ідентифікаційних записів громадян. DID також сприяє підвищенню рівня цифрової автономії, оскільки громадяни більше не залежатимуть від банківських сервісів або інших комерційних структур для підтвердження своєї особи у державних системах.

Однак повноцінна інтеграція DID у державні цифрові платформи потребує розв’язання низки технічних та регуляторних питань. Одним із головних викликів є питання відновлення ідентифікатора у разі втрати доступу до приватного ключа. У централізованих системах цей процес відбувається через процедуру відновлення доступу, яка базується на альтернативних методах автентифікації, зокрема через контактні дані або відповіді на контрольні запитання. У випадку DID користувач повинен мати додаткові механізми безпечного зберігання ключів, адже у разі втрати приватного ключа доступ до ідентифікаційного запису стає неможливим.

Ще одним викликом є необхідність стандартизації DID на рівні державної інформаційної політики. На сьогодні різні блокчейн-платформи використовують власні методи збереження ідентифікаційних записів, що створює проблему

сумісності. Успішне впровадження DID у «Дію» вимагає розробки єдиного державного стандарту, який регламентуватиме вимоги до таких ідентифікаторів, а також механізми їхньої взаємодії з державними реєстрами.

Попри ці виклики, застосування DID у платформі «Дія» має значний потенціал для підвищення рівня кібербезпеки та захисту персональних даних. Відмова від централізованих реєстрів дозволить мінімізувати загрозу масових витоків інформації та забезпечить громадянам України ефективніший механізм керування своєю цифровою особистістю [86].

2 Протокол доведення з нульовим розголошенням (ZKP) як механізм анонімної автентифікації у «Дії».

Окрім проблеми централізованого зберігання ідентифікаційних даних, сучасні державні сервіси стикаються з викликами, пов’язаними із захистом персональних даних під час перевірки прав користувачів на доступ до певних послуг. Традиційні механізми автентифікації передбачають передачу великого обсягу інформації навіть у тих випадках, коли для перевірки достатньо лише одного факту.

Потокол доведення з нульовим розголошенням (ZKP) є технологією, яка дозволяє користувачам доводити справедливість певного твердження без необхідності розкриття конкретних даних. Це означає, що система може перевіряти, чи відповідає користувач певним критеріям, не зберігаючи або обробляючи його персональні дані.

Використання ZKP у платформі «Дія» могло б вирішити проблему надмірного збору даних державними установами. Наприклад, під час отримання соціальних виплат система може перевірити право користувача на допомогу без необхідності розкриття його повного ідентифікаційного номера. Це не тільки покращує рівень захисту персональних даних, але й мінімізує ризики несанкціонованого доступу до них у разі потенційних атак.

Застосування ZKP також могло б стати важливим інструментом для забезпечення анонімності під час електронного голосування. У сучасних електронних виборчих системах важливо гарантувати, що виборець має право

голосу, але при цьому не можна допустити можливості відстеження його вибору. Використовуючи ZKP, можливо реалізувати механізм, який дозволяє перевіряти право голосу без розкриття деталей голосування, що робить цю технологію перспективною для демократичних процесів.

Попри високий рівень безпеки, впровадження ZKP потребує значних обчислювальних ресурсів. Генерація та перевірка криптографічних доказів є більш ресурсомістким процесом, ніж традиційні методи автентифікації. Це означає, що широке застосування ZKP у державних системах вимагатиме модернізації обчислювальної інфраструктури платформи «Дія».

Таким чином, інтеграція Zero-Knowledge Proofs у «Дію» може стати ключовим фактором у розвитку анонімної та безпечної цифрової ідентифікації, що відповідатиме сучасним вимогам кібербезпеки та захисту персональних даних громадян України.

2.2.3. Обґрунтування вибору технологій для моделювання загроз

Моделювання загроз у блокчейн-системах вимагає комплексного підходу, що поєднує математичні методи оцінки ризиків, технології аналізу транзакцій та інструменти штучного інтелекту. Це обумовлено тим, що традиційні методи кібербезпеки, які застосовуються у централізованих системах, не можуть бути повністю ефективними у розподіленому середовищі, де відсутній єдиний центр контролю.

Одним із основних завдань моделювання загроз є аналіз можливих атак, зокрема атаки 51%, подвійного витрачання, атак на смарт-контракти та компрометації механізмів консенсусу. Використання формальних методів дозволяє кількісно оцінювати ризики таких атак та прогнозувати їхній вплив на безпеку системи. Особливо важливим у цьому контексті є застосування математичних моделей, які дозволяють визначити ймовірність настання певних загроз та їхній вплив на функціональність блокчейн-мережі [87].

Серед найбільш ефективних підходів до моделювання загроз у блокчейн можна виокремити графові моделі аналізу транзакцій, методи машинного навчання для поведінкового аналізу вузлів мережі, а також криптографічні алгоритми

верифікації автентичності даних. Вибір цих технологій обґрунтовується необхідністю створення багаторівневої системи захисту, яка дозволяє не лише виявляти загрози, але й прогнозувати можливі сценарії атак [88].

Методи математичного аналізу, зокрема Байєсівські мережі та моделювання Монте-Карло, є ефективними для визначення ймовірності компрометації мережі [89]. Наприклад, Байєсівські мережі можуть використовуватися для аналізу залежностей між різними факторами ризику, що дозволяє визначити ймовірність атаки 51% залежно від розподілу обчислювальних потужностей у мережі. Моделювання Монте-Карло, у свою чергу, дозволяє здійснювати імітацію різних сценаріїв функціонування блокчейн-мережі та прогнозувати наслідки несанкціонованих змін у розподіленому реєстрі.

Використання алгоритмів машинного навчання у процесі моделювання загроз обґрунтовується тим, що блокчейн-мережі генерують значні обсяги транзакційних даних, які можуть містити ознаки потенційно небезпечної активності. Машинне навчання дозволяє автоматизувати процес аналізу транзакцій та визначати аномальну поведінку вузлів, що може свідчити про підготовку до проведення атаки або компрометацію мережі [90].

Криптографічні алгоритми також відіграють важливу роль у моделюванні загроз, оскільки вони забезпечують перевірку цілісності даних та автентичність учасників мережі. Аналіз криптографічних механізмів дозволяє оцінити їхню стійкість до квантових атак, що є особливо актуальним у контексті майбутнього розвитку квантових обчислень.

Комплексне застосування математичних моделей, алгоритмів машинного навчання та криптографічних методів дозволяє створити ефективну систему моделювання загроз у блокчейн-системах. Такий підхід забезпечує можливість не лише оцінювати поточні ризики, але й прогнозувати потенційні загрози, що сприяє підвищенню рівня безпеки у децентралізованих середовищах [91].

2.3. Моделювання та аналіз багаторівневої системи верифікації транзакцій у блокчейн-середовищі

Ефективне моделювання загроз у блокчейн-системах потребує комплексного підходу, який поєднує криптографічні механізми захисту, математичні моделі оцінки ризиків та алгоритми поведінкового аналізу транзакцій. Ключовою особливістю розподіленого реєстру є його децентралізована природа, що унеможливлює використання класичних підходів до безпеки, які базуються на централізованому контролі [92].

Запропонована модель передбачає багаторівневу систему захисту, що включає механізми верифікації транзакцій, оцінку їхнього ризику та автоматизоване прийняття рішень щодо дозволу або блокування операцій. Вона складається з трьох основних компонентів [93]:

1. Криптографічний захист та перевірка автентичності – використання цифрових підписів та алгоритмів шифрування для верифікації транзакцій.

2. Механізм динамічного оцінювання ризиків – оцінка ризику транзакцій на основі їхніх параметрів, історії користувача та алгоритмів машинного навчання.

3. Алгоритм прийняття рішень щодо обробки транзакцій – автоматичний вибір дії (схвалення або відхилення транзакції) на основі отриманих даних та встановлених правил.

Запропонована модель ухвалення рішень щодо транзакцій у блокчейн-системі може бути представлена у вигляді функціональної залежності:

$$T: U \times A \times R \to D, \tag{2.7}$$

де:

U – множина користувачів;

A – множина атрибутів автентифікації (цифрові підписи, відкриті ключі);

R – рівень ризику транзакції;

D – множина можливих рішень (дозвіл або блокування транзакції).

1. Оцінка ризику транзакції

Ризик транзакції визначається як функція від історії користувача, суми переказу та інших параметрів:

$$R = f(A, H, P)\ , \tag{2.8}$$

де:

H – історія попередніх транзакцій користувача;

P – параметри поточної транзакції (сума, IP-адреса, геолокація, час операції).

2. Прийняття рішення

$$D = \begin{cases} Allow,\ R \leq R_{threshold}\ i\ Verify\left(K_{pub_i}, M, S_i\right) = True, \\ Deny,\ \text{інакше.} \end{cases} \quad (2.9)$$

де:

D – рішення системи щодо дозволу або блокування транзакції;

R – обчислений ризик транзакції;

$R_{threshold}$ – граничне значення ризику, що допускається системою;

K_{pub_i} – публічний ключ користувача;

M – повідомлення або транзакція;

S_i – цифровий підпис;

$Verify$ – функція перевірки достовірності підпису.

Логіка процесу:

1. Система перевіряє автентичність транзакції шляхом криптографічної перевірки підпису.

2. Паралельно або послідовно розраховується рівень ризику транзакції.

3. Якщо підпис вірний і ризик не перевищує допустиме значення – транзакція дозволяється.

4. В іншому випадку – блокується.

З метою наочного представлення механізму прийняття рішень щодо обробки транзакцій у запропонованій моделі, нижче подано блок-схему рисунок 2.5, яка ілюструє поетапний процес перевірки автентичності, оцінки ризику та винесення рішення системою.

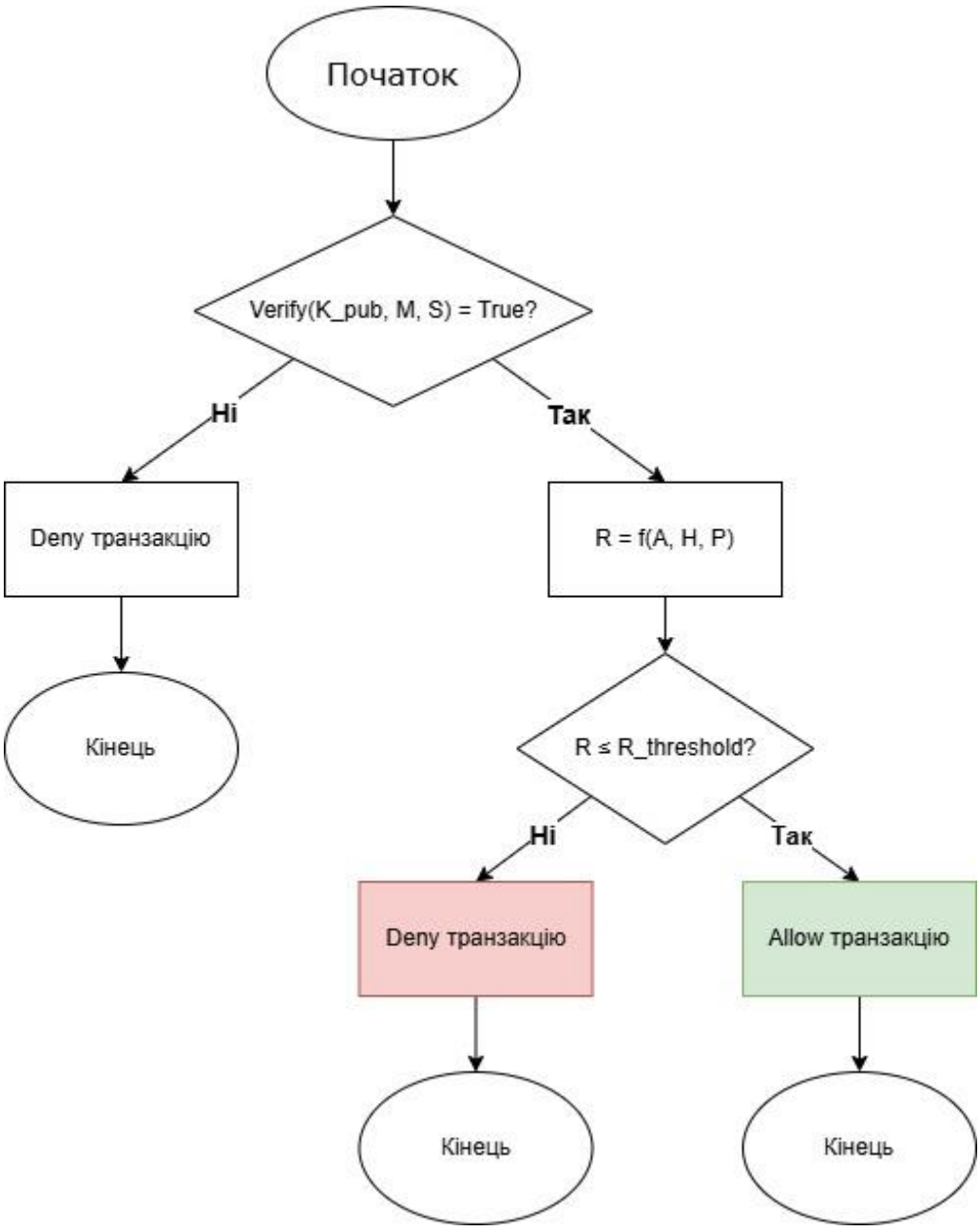

Рисунок 2.5 – Блок-схема багаторівневої верифікації транзакцій у блокчейн-системі

Запропонована блок-схема демонструє логіку ухвалення рішень щодо транзакцій у блокчейн-системі. Верифікація цифрового підпису є критичною для перевірки автентичності користувача. Якщо підпис не пройшов перевірку, транзакція автоматично блокується. Далі система оцінює ризик транзакції за допомогою функції, що враховує історію користувача та параметри операції. У разі перевищення граничного значення ризику транзакція блокується, інакше – дозволяється. Такий механізм підвищує безпеку блокчейн-системи, забезпечуючи автоматизований аналіз та динамічну реакцію на потенційні загрози.

2.3.1. Використання криптографічних методів для перевірки автентичності

Оскільки блокчейн-системи покладаються на розподілену архітектуру, одним із критичних елементів їхнього захисту є механізм автентифікації транзакцій та учасників мережі [94]. У запропонованій моделі використовуються криптографічні алгоритми, які забезпечують:

- Автентичність користувачів – перевірка того, що відправник та одержувач є легітимними учасниками мережі.
- Цілісність даних – гарантування того, що жодна транзакція не може бути змінена після її запису в блокчейн.
- Конфіденційність – захист інформації про учасників операцій у разі використання технологій zk-SNARKs або інших методів анонімізації.

На рисунку 2.6 зображено архітектуру криптографічного захисту у блокчейн-системі, яка демонструє взаємодію ключових криптографічних алгоритмів із процесом обробки транзакцій.

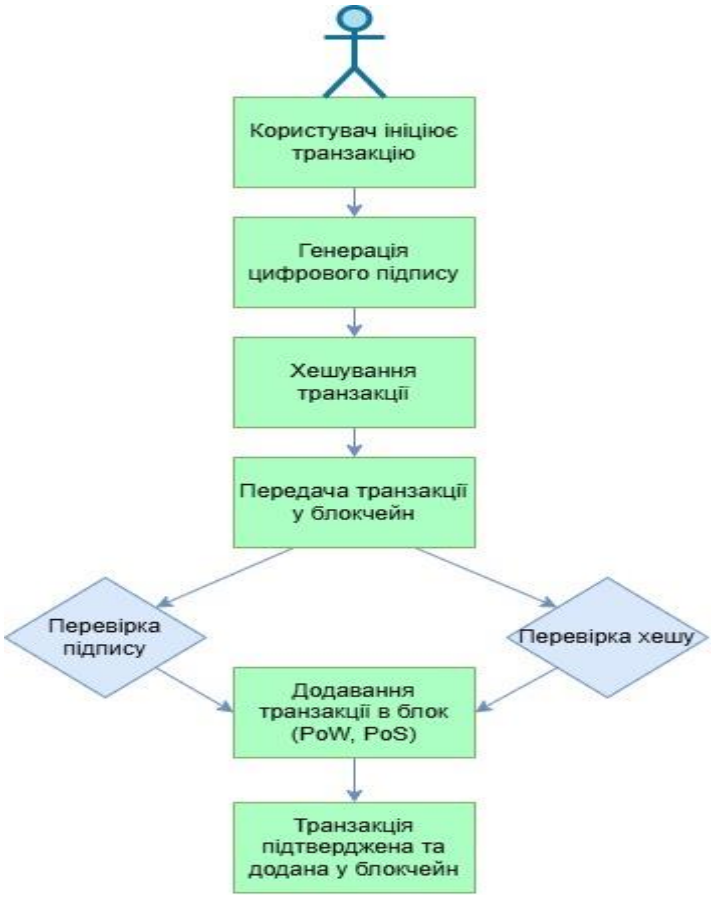

Рисунок 2.6 – Архітектура криптографічного захисту в блокчейн-системах

На рисунку 2.6 представлена архітектура криптографічного захисту у блокчейн-системі, що демонструє основні етапи обробки транзакції: від ініціювання користувачем до підтвердження в блокчейн. Процес включає генерацію цифрового підпису, хешування, перевірку автентичності транзакції та її додавання у блок. Ключовими елементами забезпечення безпеки є механізми перевірки підпису (ECDSA, Ed25519) та хешування (SHA-256, Keccak-256), які гарантують цілісність і достовірність записів у розподіленій системі.

Формалізація процесу автентифікації у блокчейн-системах

Автентифікацію транзакції можна представити у вигляді наступної функціональної залежності:

$$A : U \times K_{priv} \rightarrow S, \tag{2.10}$$

де:

U – множина користувачів системи;

K_{priv} – множина приватних ключів користувачів;

S – цифровий підпис, отриманий у результаті операції.

1. Генерація цифрового підпису

Користувач U_iстворює цифровий підпис для транзакції M:

$$S_i = Sing\left(K_{priv_i}, M\right), \tag{2.11}$$

де:

$Sing$ – криптографічна функція підписування;

K_{priv_i} – приватний ключ користувача;

M – транзакційне повідомлення.

2. Хешування транзакції

Перед тим як транзакція передається у блокчейн, вона хешується:

$$H(M) = h(M), \tag{2.12}$$

де:

$H(M)$ – хеш транзакції;

h – криптографічна хеш-функція (SHA-256, Keccak-256).

3. Перевірка автентичності підпису

Кожен вузол блокчейн-мережі перевіряє цифровий підпис:

$$Verify\left(K_{pub_i}, M, S_i\right) \rightarrow \{True, False\}, \quad (2.13)$$

де:

K_{pub_i} – відкритий ключ користувача;

$Verify$ – функція перевірки цифрового підпису;

Якщо результат $True$, транзакція переходить до наступного етапу.

4. Оцінка ризику транзакції

Крім перевірки підпису, система оцінює рівень ризику транзакції:

$$R = f(A, H, P)\ , \quad (2.14)$$

де:

A – історія операцій користувача;

H – хеш транзакції;

P – параметри поточної транзакції (сума, IP-адреса, геолокація).

5. Прийняття рішення

На основі перевірки автентичності та рівня ризику приймається рішення:

$$D = \begin{cases} Allow,\ R \leq R_{threshold}\ i\ Verify\left(K_{pub_i}, M, S_i\right) = True, \\ Deny,\ \text{інакше.} \end{cases} \quad (2.15)$$

де:

D – рішення про дозвіл або блокування транзакції;

$R_{threshold}$ – граничне значення ризику.

Розроблена математична модель автентифікації у блокчейн-системах дозволяє формально описати процес перевірки транзакцій, оцінки їхнього ризику та прийняття рішення щодо їхнього схвалення або блокування.

Основні результати моделювання:

- функція автентифікації забезпечує перевірку користувачів за допомогою криптографічних підписів, що усуває необхідність у централізованих серверах автентифікації та зменшує ризик компрометації облікових даних;
- процес хешування гарантує, що транзакції неможливо змінити після їхнього включення в блокчейн, що забезпечує цілісність даних та їхній захист від підробки;

- механізм оцінки ризику дозволяє блокувати потенційно шахрайські або небезпечні транзакції ще до їхнього підтвердження, що підвищує рівень безпеки децентралізованих систем;
- алгоритм прийняття рішень інтегрує два рівні контролю – перевірку цифрового підпису та аналіз ризиків. Це дає змогу ухвалювати гнучкі рішення на основі встановлених порогових значень та історичних даних користувача.

Таким чином, запропонована модель підвищує надійність автентифікації у блокчейн-системах, усуває вразливості централізованих схем та дозволяє запобігати фінансовим втратам через несанкціоновані операції. Подальший розвиток моделі передбачає її оптимізацію для врахування складніших факторів ризику та впровадження алгоритмів машинного навчання для адаптивного налаштування порогових значень ризику в реальному часі.

2.3.2. Динамічне оцінювання ризиків транзакцій у блокчейн

Ризики, пов’язані з несанкціонованими або шахрайськими транзакціями, є одним із найсерйозніших викликів для блокчейн-систем. Оскільки транзакції є незворотними, вкрай важливо ще на етапі їхнього додавання в блокчейн оцінювати потенційні загрози.

У запропонованій моделі реалізовано механізм динамічного оцінювання ризиків, що передбачає аналіз кожної транзакції за допомогою алгоритмів поведінкового аналізу та машинного навчання [98]. Цей механізм дозволяє виявляти підозрілі операції, які можуть бути пов’язані з шахрайськими схемами, відмиванням коштів або іншими кіберзлочинами.

Таблиця 2.4 містить ключові параметри, які враховуються при аналізі транзакцій у блокчейн-мережі.

Таблиця 2.4. Основні параметри оцінки ризиків транзакцій у блокчейн

Параметр	Опис	Вплив на ризик
Частота транзакцій	Кількість операцій за визначений проміжок часу	Високий

Обсяг коштів	Середня сума переказів, здійснених одним вузлом	Високий
Зв’язок із підозрілими адресами	Чи були транзакції з адресами, що фігурують у чорних списках	Критичний
Відхилення від стандартної поведінки	Аналіз змін у транзакційних патернах	Високий

З аналізу таблиці можна зробити висновок, що ключові параметри, такі як зв’язок із підозрілими адресами та різке відхилення від стандартної поведінки, мають найбільший вплив на ризикованість транзакцій. Автоматизована перевірка цих параметрів дозволяє значно підвищити ефективність механізму оцінювання ризиків та мінімізувати загрози шахрайських дій.

2.3.3. Алгоритм прийняття рішень щодо блокування або дозволу дій

У блокчейн-системах важливу роль відіграє механізм ухвалення рішень щодо обробки транзакцій. У централізованих системах контроль здійснюється адміністраторами або спеціалізованими алгоритмами, однак у децентралізованих мережах необхідно використовувати автоматизовані моделі оцінки ризиків, які базуються на алгоритмах машинного навчання та поведінкового аналізу [99].

Запропонований алгоритм ухвалення рішень складається з кількох етапів:

- Первинний аналіз транзакції, у ході якого перевіряється її зв’язок із підозрілими адресами.
- Обчислення рівня ризику на основі визначених параметрів.
- Класифікація операції як безпечної, підозрілої або потенційно небезпечної.
- Прийняття рішення щодо проведення, блокування або перенаправлення транзакції на додаткову перевірку.

На рисунку 2.7 зображено загальний алгоритм обробки транзакції в блокчейн-середовищі, який охоплює перевірку підпису, балансу та валідацію в мережі. Процес включає кілька рівнів перевірки:

- Перевірка цифрового підпису гарантує справжність відправника.

- Аналіз балансу перевіряє, чи достатньо ресурсів для здійснення транзакції.
- Валідація у вузлах мережі визначає, чи відповідає транзакція правилам консенсусу.

У разі невідповідності хоча б одному критерію транзакція відхиляється. Якщо всі перевірки успішно пройдено, транзакція додається до блокчейн.

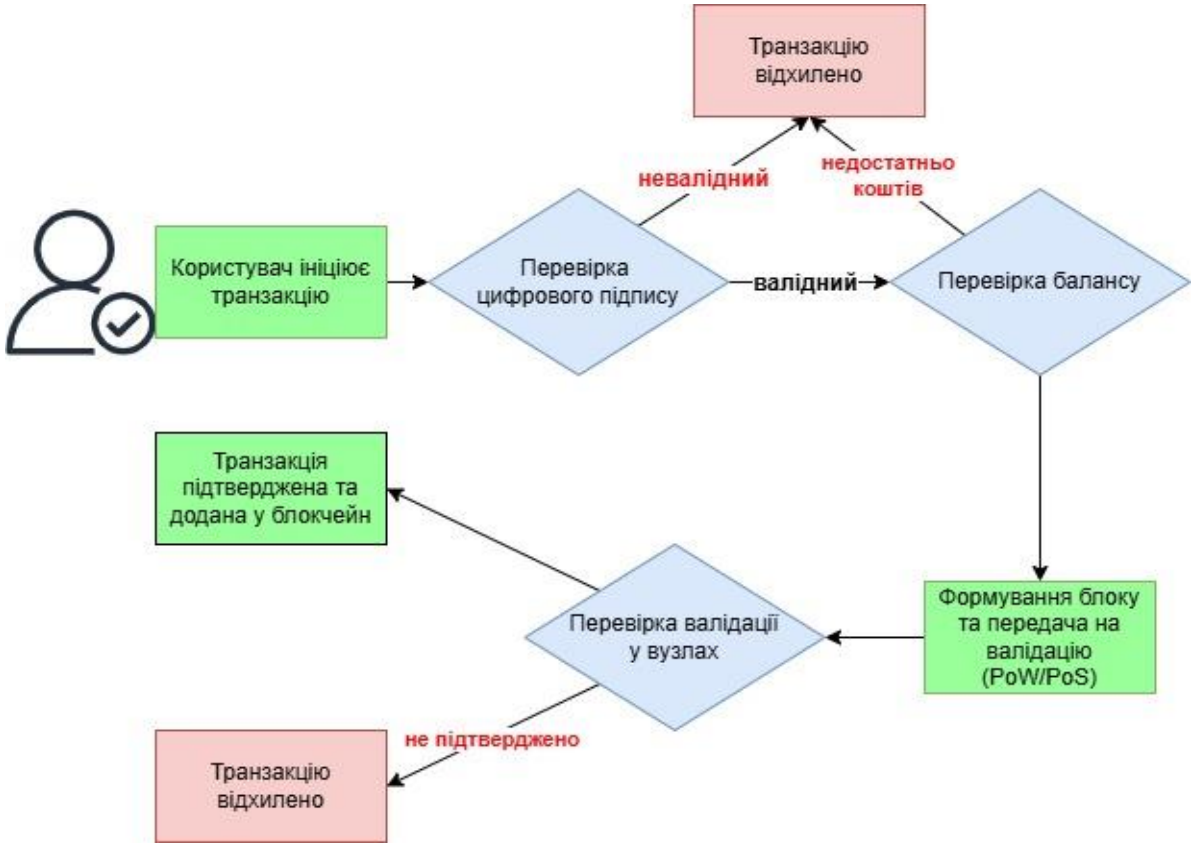

Рисунок 2.7 – Алгоритм обробки транзакцій у блокчейн-системі з багаторівневою перевіркою

Математична модель процесу ухвалення рішень щодо транзакцій у блокчейн

Запропонована модель передбачає оцінку ризику транзакцій на основі кількох факторів та ухвалення автоматизованого рішення щодо їхнього проведення. Модель складається з таких етапів:

1. Перевірка автентичності – перевіряється цифровий підпис транзакції.
2. Оцінка ризику – розраховується рівень ризику операції на основі історичних даних, параметрів транзакції та поведінкових характеристик користувача.

3. Прийняття рішення – система визначає, чи слід дозволити або заблокувати транзакцію.

1. Формальна модель перевірки автентичності

Транзакція вважається автентичною, якщо її цифровий підпис успішно проходить перевірку:

$$Verify\left(K_{pub_i}, M, S_i\right) = \begin{cases} True, \text{якщо } S_i = Sing\left(K_{priv_i}, M\right) \\ False, \text{ інакше.} \end{cases} \quad (2.16)$$

де:

K_{pub_i} – публічний ключ користувача i,

K_{priv_i} – приватний ключ користувача i,

M – повідомлення (транзакція),

S_i – цифровий підпис користувача.

Якщо перевірка не пройдена, транзакція відхиляється.

2. Розширена модель оцінки ризику транзакції

Ризик транзакції визначається за допомогою функції:

$$R = w_1 H_i + w_2 C_i + w_3 T_i + w_4 A_i + w_5 P_i \quad (2.17)$$

де:

H_i – історія попередніх транзакцій користувача (підозрілість минулих операцій),

C_i – контекст транзакції (геолокація, пристрій, IP-адреса),

T_i – час операції (аналітика частоти транзакцій користувача),

A_i – аномальність операції (відхилення суми та частоти від середнього значення),

P_i – перевірка відповідності отримувача списку надійних/ризикових адрес,

$w_1 w_2 w_3 w_4 w_5$ – вагові коефіцієнти кожного фактора (визначаються емпірично або за допомогою алгоритмів машинного навчання).

Транзакція розглядається як безпечна, якщо:

$$R \leq R_{threshold}, \quad (2.18)$$

де: $R_{threshold}$ – граничне значення ризику, після якого транзакція вважається небезпечною.

3. Ухвалення рішення

Фінальне рішення ухвалюється за умовою:

$$D = \begin{cases} Allow,\ R \leq R_{threshold}\ i\ Verify\left(K_{pub_i}, M, S_i\right) = True, \\ Deny,\ \text{інакше.} \end{cases} \quad (2.19)$$

На рисунку 2.8 подано блок-схему математичної моделі ухвалення рішень щодо транзакцій у блокчейн-середовищі.

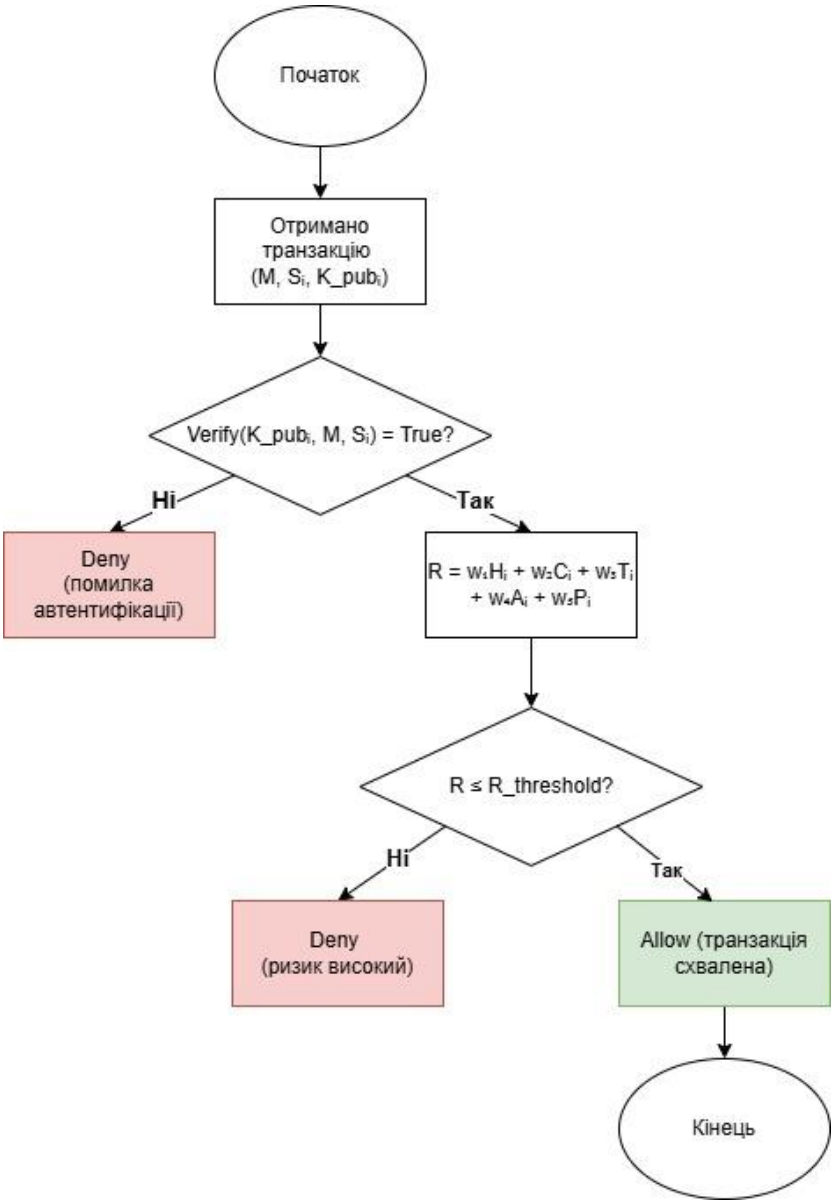

Рисунок 2.8 – Математична модель ухвалення рішень щодо транзакцій у блокчейн-системі

Математичної моделі демонструє поетапну перевірку автентичності підпису, оцінку рівня ризику операції на основі множини поведінкових та технічних факторів, а також прийняття автоматизованого рішення — дозволити транзакцію або її заблокувати. Такий підхід поєднує в собі сильні сторони криптографічного захисту з алгоритмами виявлення аномальної активності.

Реалізація багаторівневої моделі дозволяє:

- Своєчасно ідентифікувати загрози, що базуються на аналізі історії транзакцій, контексту (геолокація, пристрій, IP), поведінки користувача (частота, час операцій) та факторів довіри до одержувача;
- Автоматизувати процес ухвалення рішень, виключаючи суб'єктивність людського фактору;
- Скоротити час перевірки транзакцій та мінімізувати вплив атак типу phishing, social engineering, identity spoofing;
- Забезпечити масштабованість системи в умовах зростаючого обсягу транзакцій.

Модель також дозволяє налаштовувати вагові коефіцієнти в залежності від поточного рівня загроз, галузі застосування або специфіки мережі (фінансова, медична, державна тощо). Це забезпечує адаптивність механізму верифікації та робить його придатним для використання в розподілених державних інформаційних системах, включаючи реєстри, електронне врядування та системи ідентифікації громадян.

Таким чином, запропонована модель може бути використана як наукове та практичне підґрунтя для впровадження інтелектуальних механізмів контролю у блокчейн-інфраструктурах, що потребують підвищеного рівня кібербезпеки.

2.4. Приклад застосування моделі у державних реєстрах України

Розвиток цифрових державних послуг значно підвищує ефективність взаємодії громадян із державними установами, проте одночасно створює нові виклики у сфері захисту персональних даних. Одним із перспективних напрямів посилення кібербезпеки державних інформаційних ресурсів є впровадження технології блокчейн у процеси обробки, перевірки та запису даних у державні реєстри.

Найбільш уразливим місцем сучасних централізованих державних систем є зосереджене зберігання критично важливої інформації на одному або кількох серверних вузлах. Такий підхід призводить до ризиків масових витоків, несанкціонованого доступу та підміни даних. Це особливо критично у контексті

надання адміністративних послуг через платформу "Дія", яка інтегрує більшість державних реєстрів, а отже, є потенційною ціллю для атак.

Запропонована модель інтеграції блокчейн у державні реєстри (рисунок 2.9) передбачає децентралізовану архітектуру управління транзакціями, де кожна дія (запит на зміну або перегляд даних) оформлюється у вигляді транзакції, що проходить перевірку через смарт-контракт, а лише потім, у разі відповідності встановленим правилам, записується в реєстр.

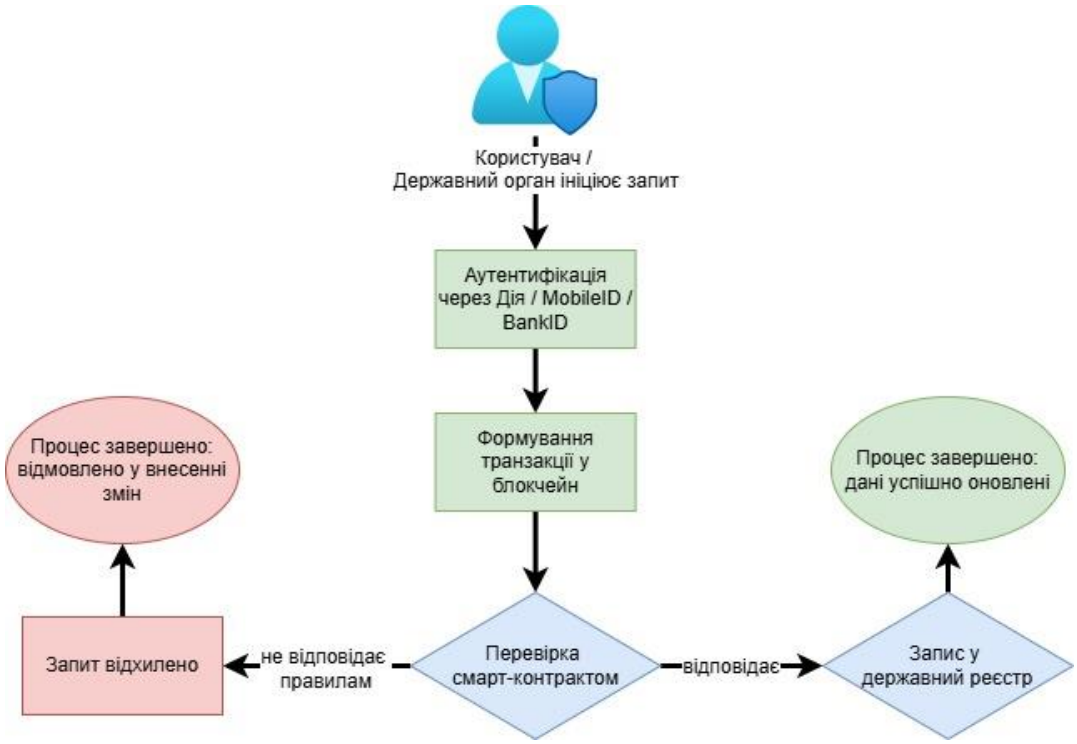

Рисунок 2.9 – Архітектура інтеграції блокчейн у державні реєстри України

На рисунку зображено послідовність дій, які проходить транзакція від моменту ініціювання запиту користувачем або державним органом до остаточного внесення змін у державний реєстр. Зокрема, включено такі ключові етапи:

- Ініціювання запиту користувачем або державним органом для отримання або внесення даних.
- Аутентифікація через Дія, MobileID або BankID, що гарантує ідентифікацію особи та підтвердження її прав доступу.
- Формування транзакції в блокчейн, яка включає запит до реєстру.
- Перевірка смарт-контрактом, який визначає відповідність запиту встановленим правилам та регламенту.

- Запис у державний реєстр, якщо запит відповідає умовам, або його відхилення у разі невідповідності.

Цей механізм підвищує прозорість і безпеку взаємодії між державними структурами та громадянами, зменшуючи ризики витоку та маніпуляції даними.

Формалізація процесу перевірки в реєстрах

Процес перевірки запиту до державного реєстру через блокчейн-систему може бути представлений як формальна функція:

$$F:(U, R, Z) \rightarrow \{Allow, Deny\}, \quad (2.20)$$

де:

U – користувач або суб'єкт запиту (ідентифікований через Дія / BankID);

R – запит до реєстру (read/write);

Z – набір атрибутів, перевірених через смарт-контракт (роль, повноваження, наявність підпису);

F(U, R, Z) – функція прийняття рішення на основі політики доступу, закладеної у смарт-контракті.

Використання блокчейн забезпечує низку ключових переваг у державних інформаційних системах, серед яких:

- усунення ризиків централізованих атак. Усі транзакції перевіряються розподілено, без центрального вузла, що унеможливлює одночасний злам усієї системи;
- прозорість і відстежуваність дій, де кожен запит зберігається у вигляді транзакції з точним часовим штампом, автором та криптографічним підписом, що забезпечує неможливість фальсифікацій;
- незмінність записів. Один із фундаментальних принципів блокчейн – неможливість редагування раніше внесених записів без згоди мережі. Це виключає несанкціоновані зміни та підміну даних у реєстрах;
- автоматизація логіки за допомогою смарт-контрактів. Всі перевірки на рівні регламенту, доступу, відповідності – відбуваються автоматично без втручання людини. Це мінімізує вплив людського фактору та корупційні ризики;

- селективне розкриття даних. Технології на кшталт протоколів доведення з нульовим розголошенням дозволяють перевірити факт володіння інформацією або прав без її прямого розкриття, що відповідає принципу мінімізації даних згідно з GDPR.

Таким чином, інтеграція блокчейн у державні реєстри України дозволяє суттєво підвищити рівень безпеки, довіри та прозорості цифрових державних сервісів. Запропонована архітектура усуває структурні вразливості централізованих систем, забезпечує надійний механізм перевірки, захисту і незмінності даних, автоматизує процеси аутентифікації та ухвалення рішень через смарт-контракти. Такий підхід відповідає світовим тенденціям диджиталізації публічного сектору та може бути масштабовано на всі критично важливі інформаційні ресурси держави.

Успішні кейси застосування блокчейн-технологій у державному управлінні вже реалізовані в низці країн, що свідчить про доцільність та ефективність впровадження децентралізованих рішень у сфері управління публічними реєстрами.

З 2012 року у Естонії технологія блокчейн використовується для захисту даних в електронному уряді (e-Government), зокрема в таких системах, як e-Health, e-Law, e-Banking, e-Business та e-Court. Державна ініціатива KSI Blockchain, розроблена компанією Guardtime, забезпечує цілісність та незмінність реєстрових записів, дозволяючи виявити будь-які несанкціоновані зміни в даних [100].

З 2016 року Міністерство юстиції Грузії співпрацює з Bitfury Group у впровадженні блокчейн у національний реєстр нерухомості. Система дозволяє безпечно реєструвати угоди з нерухомістю, підтверджуючи їх за допомогою блокчейн. Це значно зменшило час обробки документів та підвищило довіру громадян до державних сервісів [101].

Шведське земельне агентство Lantmäteriet протестувало систему реєстрації угод з нерухомістю на базі блокчейн. У межах пілотного проєкту перевірялась можливість оцифрування процесу купівлі-продажу нерухомості без паперових

документів. Блокчейн гарантував достовірність, швидкість і прозорість процедур, знижуючи витрати та людський фактор [102].

ОАЕ, зокрема емірат Дубай, оголосив амбітну мету – стати першим містом, повністю керованим за допомогою блокчейн до 2030 року (ініціатива Dubai Blockchain Strategy). Уже впроваджено блокчейн у системи реєстрації компаній, візових сервісів, митниці, охорони здоров'я та управління енергією. Кожна транзакція в цих системах зберігається у незмінному вигляді, що підвищує прозорість, запобігає шахрайству та покращує якість державного сервісу [103].

Аналіз міжнародного досвіду впровадження блокчейн-технологій у державному секторі підтверджує їхню високу ефективність у підвищенні прозорості, захисті даних та оптимізації адміністративних процесів. У таких країнах, як Естонія, Швеція, Грузія та Об'єднані Арабські Емірати, блокчейн використовується для зберігання та обробки даних у національних реєстрах, кадастрах, медичних інформаційних системах, а також у процедурах електронного голосування. Це дозволяє зменшити залежність від централізованих серверів, виключити можливість підміни записів і створити надійну систему довіри між державою та громадянами.

Впровадження блокчейн у таких системах забезпечує захист від внутрішніх і зовнішніх загроз, дозволяє реалізувати принцип прозорості доступу до інформації, а також підвищує стійкість до технічних та організаційних збоїв. Використання смарт-контрактів у цих країнах стало ключовим елементом автоматизації перевірки прав доступу та виконання регламентів без участі людини, що суттєво знижує ризики корупції та помилок.

З огляду на успішні кейси впровадження, можна стверджувати, що запропонована модель інтеграції блокчейн у державні реєстри України має достатнє наукове і практичне підґрунтя. Вона відповідає сучасним міжнародним тенденціям і має потенціал для масштабування у сфері надання електронних публічних послуг в Україні.

2.4.1. Використання NFT та криптографічних токенів для розмежування доступу

Однією з головних проблем централізованих реєстрів є ризики несанкціонованого доступу та підробки документів. Використання невзаємозамінних токенів (NFT) та криптографічних токенів дозволяє вирішити ці проблеми завдяки механізму перевірки цифрової автентичності документів та управління правами доступу [104].

Кожен державний документ може бути токенізований у вигляді NFT, що дозволяє забезпечити:

- Єдиний цифровий ідентифікатор документів, який неможливо підробити.
- Децентралізований контроль доступу до записів у державних реєстрах.
- Автоматизовану перевірку прав доступу до документів без розкриття їхнього вмісту.

Таблиця 2.5 демонструє ключові переваги застосування NFT для управління доступом у державних інформаційних системах.

Таблиця 2.5. Переваги використання NFT та криптографічних токенів у державних реєстрах

Критерій	Опис	Вплив на безпеку
Захист від підробки	Кожен документ отримує унікальний цифровий ідентифікатор у блокчейн	Високий
Децентралізований контроль	Користувач сам керує своїм токеном, без участі третьої сторони	Високий
Захищений доступ до даних	Доступ до записів можливий лише через автентифікацію токена	Високий
Простота перевірки	Документи можна швидко перевірити без необхідності звернення до центрального реєстру	Середній

Запровадження криптографічних токенів дозволяє мінімізувати ризики витоку інформації та створює цифровий механізм підтвердження автентичності документів, який значно перевершує традиційні централізовані системи перевірки.

2.4.2. Аналіз можливостей інтеграції блокчейн-моделі з національними цифровими платформами на прикладі застосунку «Дія»

Платформа «Дія» є ключовим компонентом цифрової інфраструктури України, що надає громадянам доступ до паспортних даних, водійських прав, податкових записів та інших документів [105]. Однак поточна архітектура системи передбачає централізоване управління, що несе ризики масштабних атак та витоків даних.

Запропонована модель передбачає використання децентралізованих ідентифікаторів (DID) та протоколів доведення з нульовим розголошенням (ZKP) у «Дія», що дозволяє:

- Забезпечити користувачам повний контроль над своїми даними – держава більше не виступатиме єдиним оператором доступу до персональної інформації.
- Мінімізувати ризики компрометації державних серверів – дані громадян будуть зберігатися у захищеній блокчейн-мережі.
- Гарантувати прозорість доступу до інформації – запис про кожну перевірку або зміну даних фіксуватиметься у блокчейн.

На рисунку 2.10 зображено процес взаємодії платформи «Дія» з блокчейн-мережею під час перевірки цифрових документів. Запит користувача проходить через кілька етапів перевірки, включаючи пошук відповідного запису в блокчейн та перевірку цифрового підпису. У разі успішного підтвердження користувач отримує доступ до даних, в іншому випадку система відхиляє запит, надаючи причину відмови та можливі варіанти дій.

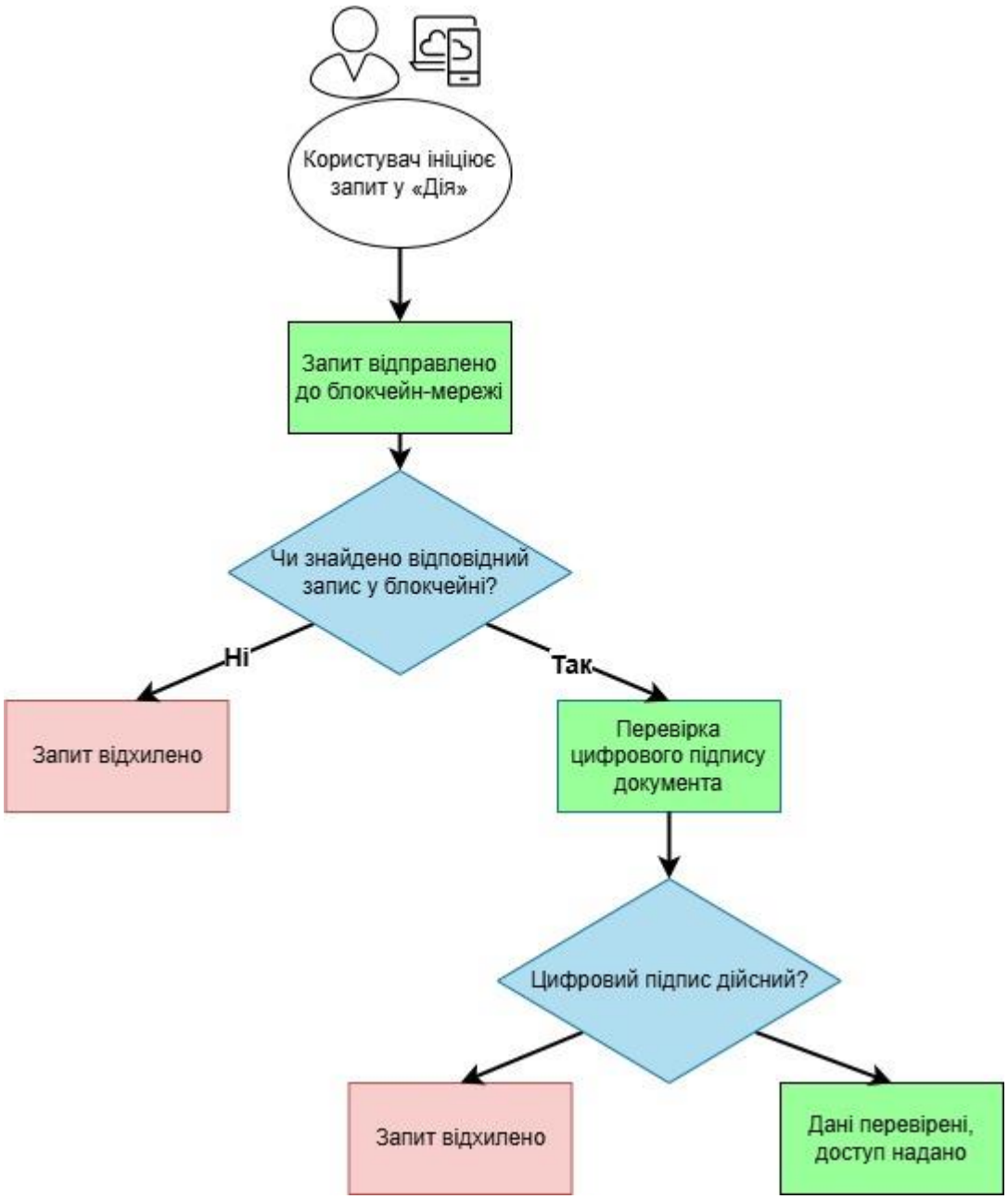

Рисунок 2.10 – Процес перевірки даних у державних реєстрах через блокчейн

Процес перевірки даних через блокчейн дозволяє забезпечити високу надійність та прозорість доступу до цифрових документів. Представлена схема демонструє переваги децентралізованої перевірки, яка унеможливлює підробку даних та забезпечує захист від несанкціонованого доступу.

Однією з головних переваг використання блокчейн у верифікації даних є гарантована цілісність інформації. Кожен запит проходить через механізм цифрових підписів, що виключає можливість маніпуляції з боку сторонніх осіб.

Якщо запис у блокчейн не знайдено або підпис недійсний, система відхиляє запит та рекомендує альтернативні дії, такі як перевірка правильності введених даних або звернення до відповідного державного органу. Це дозволяє мінімізувати ризики використання підроблених або застарілих документів, що особливо важливо в контексті державних реєстрів.

Запропонований підхід може бути використаний для інтеграції блокчейн у державні електронні сервіси, включаючи «Дія», що дозволить покращити безпеку цифрових операцій та підвищити рівень довіри громадян до електронних послуг

2.4.3. Переваги запропонованого підходу у сфері кібербезпеки

Запропонована модель інтеграції блокчейн у державні реєстри має такі ключові переваги:

1. Зменшення ризиків централізованих атак – відсутність єдиного сховища персональних даних мінімізує наслідки компрометації окремих вузлів системи.

2. Прозорість транзакцій – кожна операція записується в блокчейн, що забезпечує її неможливість підроблення або приховування.

3. Автоматизоване виявлення загроз – використання алгоритмів поведінкового аналізу дозволяє прогнозувати атаки на державні інформаційні ресурси.

Запропонована модель демонструє ефективність застосування блокчейн для захисту державних реєстрів та цифрових державних послуг. Використання NFT та Zero-Knowledge Proofs (ZKP) забезпечує автоматизоване управління доступом до даних, а механізм децентралізованої ідентифікації (DID) усуває потребу у централізованому зберіганні персональних даних.

Інтеграція блокчейн-рішень у платформу «Дія» дозволяє суттєво підвищити рівень безпеки цифрових державних сервісів та створює універсальну систему захисту громадянських даних від шахрайства та витоків.

Висновки до розділу 2

У другому розділі дисертаційної роботи було здійснено розробку моделі виявлення загроз у блокчейн-системах з урахуванням особливостей

децентралізованої архітектури та специфіки обробки персональних даних у таких середовищах. Запропоноване рішення становить основу для формування національних політик безпечної цифрової взаємодії та має потенціал до інтеграції в інфраструктуру державних реєстрів, підвищуючи їхню стійкість, прозорість та довіру з боку громадян. В результаті проведеного аналізу та моделювання отримано такі основні наукові результати:

1. На основі критичного аналізу класичних методик моделювання загроз (STRIDE, DREAD, NIST CSF, MITRE ATT&CK) встановлено їхню обмежену ефективність у дозвільному блокчейн-середовищах через відсутність централізованого контролю, незворотність транзакцій та анонімність учасників. Це стало підґрунтям для формулювання адаптивної моделі загроз, специфічної для блокчейн-архітектур.

2. Розроблено багаторівневу модель верифікації транзакцій у дозвільному блокчейн-системі, яка поєднує перевірку цифрового підпису, оцінку контекстних ризиків і автоматизоване прийняття рішень. Модель формалізована за допомогою математичних залежностей і логічних правил, що забезпечило динамічну адаптацію до поведінкових аномалій та підвищило стійкість до спроб підробки записів.

3. Запропоновано удосконалений метод поведінкової аутентифікації транзакцій у дозвільному блокчейн-середовищі, реалізований через алгоритми машинного навчання (градієнтний бустинг та дерева рішень), що аналізують час, геолокацію та історію транзакцій користувача. Метод протестовано на основі 300 транзакцій у Flask-додатку, що дозволило підвищити точність виявлення ризикових дій до 93% ще до моменту їх фіксації у реєстрі, а також знизити кількість хибнопозитивних спрацювань. Завдяки цьому зменшено ймовірність компрометації системи та підвищено динамічну стійкість до нових типів аномалій.

4. Розроблено архітектуру інтеграції дозвільному блокчейн-рішень із державними цифровими платформами, зокрема платформою «Дія», за рахунок використання децентралізації, смарт-контрактів, електронної ідентифікації та протоколів розподіленого аудиту. Запропонована архітектура забезпечує

підвищення рівня довіри до цифрових реєстрів, прозорість обробки транзакцій та мінімізацію ризиків внутрішніх порушень, що підтверджено експертною оцінкою функціональної стійкості.

5. На основі моделювання типових атак (Unauthorized Submit, Sniffed Replay, DoS Spam) у тестовому середовищі дозвільному блокчейн-системи Hyperledger Fabric із реалізованим механізмом триетапної верифікації транзакцій, розроблено комплекс заходів підвищення стійкості системи до навмисних спотворень даних. Результати експериментального тестування підтвердили, що інтеграція поведінкової оцінки транзакцій у поєднанні з криптографічними та структурними перевірками дозволяє своєчасно виявляти і блокувати фальсифіковані запити до моменту їх реєстрації в системі, що забезпечує повне усунення ризику включення недостовірної інформації у блокчейн у рамках змодельованих сценаріїв.

РОЗДІЛ 3. РОЗРОБКА МЕТОДУ ЗАБЕЗПЕЧЕННЯ ДОСТОВІРНОСТІ ДАНИХ У БЛОКЧЕЙН-СИСТЕМАХ

3.1. Формування основних завдань та підходів

Сучасна цифрова трансформація суспільства висуває проблему забезпечення достовірності персональних даних в інформаційних системах як одну з пріоритетних. З огляду на активне використання цифрових реєстрів, питання довіри до їхнього вмісту є ключовим для державних і комерційних структур. Невірна, змінена або навмисно сфальсифікована інформація може спричинити юридичні, економічні та соціальні загрози. Особливо актуальним це стає у контексті функціонування державних реєстрів, де внесення некоректних даних може мати далекосяжні наслідки, зокрема в аспектах юридичних прав громадян, фінансових операцій та ідентифікації особи.

Традиційні централізовані системи зберігання даних мають низку суттєвих вразливостей, які пов’язані з можливістю зламу баз даних, внутрішніх загроз з боку адміністраторів та компрометації інформації через технічні збої або цілеспрямовані атаки. Використання блокчейн-технологій пропонує альтернативний підхід до зберігання персональних даних, забезпечуючи їхню цілісність та незмінність завдяки розподіленій структурі та механізму консенсусу [106]. Однак цей підхід не усуває ризик внесення недостовірної інформації на етапі її первинного запису до системи. Саме ця проблема потребує детального розгляду та розробки ефективних механізмів контролю достовірності даних перед їхнім додаванням у блокчейн.

Одним із викликів, що стоять перед розподіленими інформаційними системами, є забезпечення автоматизованої та достовірної верифікації даних у процесі їхнього внесення та подальшої обробки. Система, яка базується виключно на блокчейн-алгоритмах, гарантує незмінність уже записаних даних, однак вона не вирішує проблему достовірності інформації на початкових етапах її формування. З огляду на це, необхідним є розроблення методів, які дозволять здійснювати оцінку ризиків та перевірку автентичності записів, використовуючи математичні моделі аналізу довіри та механізми багатофакторної верифікації.

Дослідження у цій галузі доводять, що ефективність системи забезпечення достовірності персональних даних залежить від комплексу взаємопов’язаних факторів, серед яких можна виділити структуру мережі верифікації, кількість незалежних вузлів контролю, методи оцінки ймовірності помилкових записів та механізми корекції помилок. Для оцінки рівня довіри до даних, які вносяться у блокчейн-систему, доцільним є застосування математичних моделей аналізу ймовірностей, що дозволяють прогнозувати ризики компрометації інформації та виявляти аномальні транзакції, які можуть свідчити про внесення помилкових або навмисно спотворених даних [107].

Таким чином, метою цього дослідження є розробка методу забезпечення достовірності персональних даних у блокчейн-системах шляхом формування математичної моделі оцінки ризиків внесення недостовірних записів. Запропонована модель має забезпечити оцінку достовірності даних у реальному часі та мінімізувати ймовірність компрометації інформації.

На основі результатів, отриманих у розділах 1 та 2, у даному розділі здійснюється безпосередня розробка методу перевірки достовірності персональних даних у блокчейн-середовищах. Якщо попередні етапи дозволили ідентифікувати проблемні зони (централізація, вразливість до фальсифікацій, слабка семантична перевірка), то завдання цього розділу полягає у реалізації функціональних рішень, які забезпечать підвищення достовірності верифікації.

Методологія дослідження

У процесі дослідження були використані такі наукові методи:

- Аналіз загроз достовірності даних у блокчейн-системах, що включає оцінку потенційних вразливостей та можливих атак на рівні первинного внесення інформації.
- Методи математичного моделювання, зокрема побудова ймовірнісних моделей оцінки достовірності даних та прогнозування ризиків компрометації інформації.
- Методи аналізу ризиків, що застосовуються для визначення факторів, які впливають на надійність записів у розподілених системах.

- Криптографічні методи, що дозволяють забезпечити перевірку цілісності даних та автентифікацію джерела їхнього походження.
- Методи статистичного аналізу, що використовуються для оцінки ефективності розробленої моделі в умовах реальних інформаційних систем.

Формалізація проблеми

Одним із підходів до розв'язання проблеми достовірності персональних даних у блокчейн-системах є побудова математичної моделі оцінки ймовірності внесення недостовірних даних. Для цього вводиться показник $P_{valid,}$ який відображає ступінь довіри до запису в блокчейн:

$$P_{valid} = 1/(1 + e\text{^}(-k(x - x_0))), \quad (3.1)$$

де

P_{valid} – ймовірність того, що внесені дані є достовірними,

x – кількість незалежних вузлів, що беруть участь у перевірці транзакції,

x_0 – критична кількість вузлів, необхідних для досягнення достовірності,

k – коефіцієнт, що визначає вплив кількості перевірок на рівень довіри.

Запропонована модель дозволяє оцінити, наскільки ефективно механізм консенсусу блокує внесення недостовірних записів. Використання ймовірнісного підходу дає змогу підвищити рівень довіри до блокчейн-систем, зменшуючи вплив людського фактора та випадкових помилок.

Для визначення найбільш ефективного підходу до забезпечення достовірності персональних даних у блокчейн-системах було проведено аналіз існуючих методів перевірки даних. Основні підходи порівняно за їх перевагами, недоліками та можливістю інтеграції у розподілені реєстри. Аналіз представлено в таблиці 3.1.

Таблиця 3.1. Порівняльний аналіз методів забезпечення достовірності персональних даних у інформаційних системах

Метод	Принцип роботи	Переваги	Недоліки	Приклад використання

Централізована перевірка (KYC – Know Your Customer)	Верифікація користувачів через централізовану базу даних державних або приватних установ	Висока швидкість обробки запитів, простота реалізації	Централізована база є вразливою до атак, можливість компрометації даних адміністратором	Банківські системи, фінансові сервіси
Децентралізована перевірка (DID – Decentralized Identity)	Самостійне управління цифровою ідентичністю користувачем у розподіленій мережі	Відсутність централізованого зберігання даних, підвищений контроль над особистими даними	Складність інтеграції, проблеми міжмережевої сумісності	Децентралізовані платформи, цифрові паспорти
Криптографічна перевірка (електронні цифрові підписи, ECDSA)	Підтвердження даних за допомогою цифрових підписів та шифрування	Висока точність перевірки, захист від змін після підписання	Вразливість до втрати ключа, високе навантаження на обчислювальні потужності	Документообіг, смарт-контракти
Zero-Knowledge Proofs (ZKP)	Підтвердження прав доступу без розкриття самої інформації	Конфіденційність, неможливість відстеження особистих даних	Висока складність реалізації, потребує значних обчислювальних ресурсів	Захист фінансових транзакцій, анонімна автентифікація
Гібридна система перевірки (PoA – Proof of Authority + криптографія)	Поєднання криптографії та консенсусу з обмеженою довірою до авторизованих вузлів	Висока ефективність, гнучкість налаштувань	Потребує вибору авторизованих сторін, ризик корупції	Захищені державні реєстри, корпоративні мережі

Таблиця 3.1. демонструє основні підходи до перевірки персональних даних у централізованих та децентралізованих інформаційних системах. Аналіз показує, що традиційні централізовані методи мають ризики витоків інформації через компрометацію адміністраторів або атаки на бази даних. Децентралізовані методи, зокрема DID та ZKP, забезпечують вищий рівень конфіденційності, однак мають складнішу технічну реалізацію.

Використання поєднаних моделей верифікації, таких як Proof of Authority (PoA) у поєднанні з криптографією, дозволяє досягти балансу між ефективністю та безпекою. У подальших розділах буде запропоновано математичну модель, яка

дозволяє оцінити ймовірність внесення недостовірних даних у блокчейн-реєстр на основі аналізу загроз і факторів ризику.

3.2. Проєктування механізмів обробки персональних даних у блокчейн

Обробка персональних даних у блокчейн-системах передбачає забезпечення їхньої достовірності, захист від компрометації, а також ефективне зберігання та управління. Блокчейн надає можливість побудови надійних, розподілених систем зберігання інформації, які здатні забезпечити незмінність та підтверджуваність записів. Проте, разом із перевагами, застосування блокчейн у сфері персональних даних має низку викликів, які потребують відповідних рішень, зокрема оптимізації зберігання, вибору механізму консенсусу та методів запобігання внесенню недостовірної інформації.

3.2.1. Оптимізація зберігання та передачі даних у розподіленому реєстрі

У блокчейн-системах, особливо при інтеграції з державними інформаційними ресурсами, питання ефективного зберігання та передачі персональних даних має критичне значення. На відміну від традиційних централізованих баз даних, розподілені реєстри мають обмеження щодо обсягу транзакцій, швидкості запису та складності масштабування, що обумовлює необхідність у спеціалізованих підходах до оптимізації.

У цьому контексті оптимізація полягає не лише в зменшенні обсягу інформації, що безпосередньо зберігається у блокчейн, а й у розробці гібридних моделей, що передбачають використання позаблокчейнових сховищ (off-chain storage) з надійною системою посилань (hash linking). Така модель дозволить зберігати лише хеші критичних записів або їхні метадані в самому ланцюжку блоків, зберігаючи при цьому повну відповідність принципам цілісності та незмінності.

З точки зору нормативної відповідності (наприклад, вимогам GDPR або ISO/IEC 27701), блокчейн не може безпосередньо зберігати персональні дані у відкритому вигляді без порушення принципів захисту приватності. Тому важливою частиною оптимізації є використання методів шифрування, токенізації, а також розмежування доступу з урахуванням принципу мінімізації даних.

Архітектурні підходи до зберігання персональних даних у блокчейн-середовищі

Для забезпечення оптимального балансу між безпекою, продуктивністю та правовою відповідністю в блокчейн-системах застосовуються гібридні моделі зберігання даних, які поєднують:

- on-chain зберігання – використовується для хешів, атрибутів доступу, токенів і ключових метаданих [108];
- off-chain зберігання – призначене для основного масиву персональних даних (у зашифрованому вигляді), які можуть зберігатися у зовнішніх репозиторіях (наприклад, IPFS, BigChainDB, хмарні сервіси з підтримкою шифрування тощо) [109].

У межах цього підрозділу досліджується можливість оптимізації зберігання персональних даних у блокчейн-системах шляхом побудови гібридного методу, що поєднує механізми розподілених реєстрів та зовнішніх репозиторіїв. Така модель має потенціал забезпечити баланс між прозорістю, безпекою, масштабованістю та відповідністю нормативним вимогам, зокрема GDPR та ISO/IEC 27001.

З урахуванням потреби в ефективному управлінні даними у державних реєстрах, особлива увага приділяється архітектурним рішенням, що дозволяють селективне зберігання інформації: метадані – у блокчейн-ланцюгу, а зашифровані персональні дані – в окремому захищеному сховищі. Це дозволяє зменшити навантаження на блокчейн, забезпечити гнучкість доступу до даних та відповідність правовим вимогам.

Подальший опис структури такої моделі, її компонентів та взаємодії між ними представлено в наступних абзацах, включно з візуалізацією ключових модулів та логікою процесів зчитування, запису й перевірки даних.

З метою забезпечення ефективного, нормативно відповідного та масштабованого зберігання персональних даних у блокчейн-середовищах у межах цього підрозділу обґрунтовується доцільність використання гібридної моделі, що поєднує елементи on-chain та off-chain моделювання.

Враховуючи технічні обмеження блокчейн-платформ, зокрема обмежений розмір блоку, затримки обробки транзакцій і вимоги до захисту персональних даних, доцільним є архітектурне розділення функцій зберігання та верифікації. Зокрема, у блокчейні фіксуються лише критичні метадані, ідентифікатори та хеші, тоді як основний масив зашифрованих персональних даних зберігається в зовнішньому захищеному сховищі.

Така модель забезпечує баланс між прозорістю та конфіденційністю, підвищує масштабованість системи, а також сприяє дотриманню вимог міжнародних стандартів, зокрема ISO/IEC 27701, GDPR та положень Закону України № 4336-IX щодо впровадження комплексної системи захисту інформації у державних інформаційних ресурсах.

Запропонована гібридна модель зберігання персональних даних у дозвільному блокчейн-системах поєднує on-chain-збереження метаданих із off-chain-зберіганням зашифрованих персональних даних у зовнішньому захищеному сховищі. Така модель забезпечує баланс між прозорістю, масштабованістю, безпекою та відповідністю вимогам нормативно-правових актів, зокрема GDPR, ISO/IEC 27701 та Закону України № 4336-IX.

Особливістю моделі є функціональне розмежування даних: у блокчейн записуються лише ідентифікатори, хеші та контрольні метадані, що дозволяє фіксувати незмінність та достовірність запису без розкриття змісту. Основна частина персональних даних зберігається поза блокчейном у зашифрованому вигляді, що мінімізує ризик компрометації та дає можливість реалізувати селективний доступ залежно від прав користувача.

Реалізація такої моделі підвищить рівень захисту персональної інформації, забезпечує відповідність принципам конфіденційності за концепцією Privacy by Design та створює технологічну основу для безпечної інтеграції блокчейн у державні інформаційні системи.

На рисунку 3.1 відображено ключові компоненти моделі, серед яких: модуль автентифікації, децентралізований застосунок користувача (DApp), блокчейн-

реєстр, зовнішнє захищене сховище та модуль валідації, що взаємодіють між собою у рамках процесу зчитування, запису та перевірки даних.

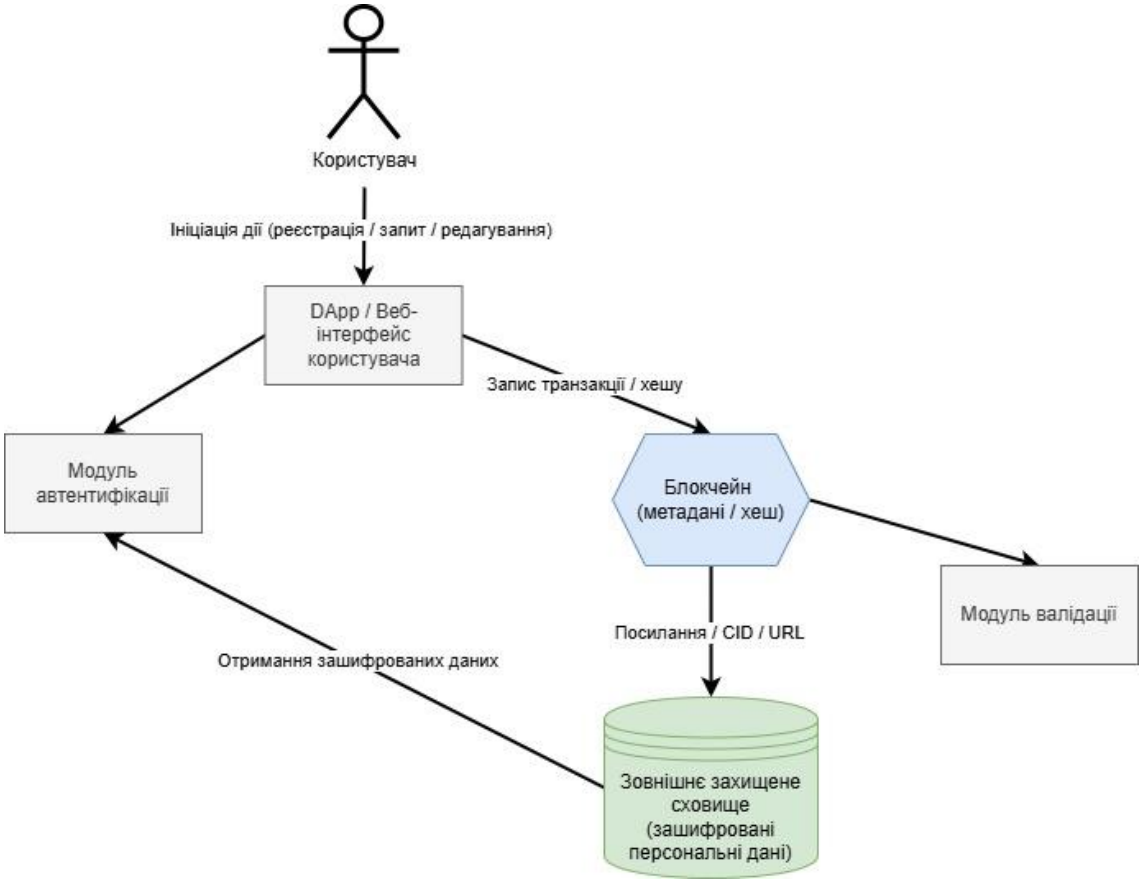

Рисунок 3.1 – Гібридна модель зберігання персональних даних у блокчейн-системі

Розроблена модель є інноваційною для українського контексту цифровізації державних реєстрів. Вона вперше адаптована з урахуванням вимог чинного законодавства, особливостей національних інформаційних систем та міжнародних стандартів у сфері захисту персональних даних. Як зображено на рисунку, користувач ініціює транзакцію через DApp або веб-інтерфейс, що надсилає дані для автентифікації. Після підтвердження особи генерується хеш, який фіксується в блокчейн разом із ідентифікатором (CID або URL), що веде до зовнішнього захищеного сховища. Самі персональні дані при цьому зберігаються поза межами блокчейн – у зашифрованому вигляді. Модуль валідації, за необхідності, виконує перевірку достовірності записів шляхом звірки контрольних значень (метаданих і хешів).

Така модель реалізує гібридну архітектуру, у межах якої блокчейн використовується для забезпечення незмінності, прозорості та контролю доступу, тоді як зовнішнє сховище гарантує безпечне зберігання конфіденційної інформації. Це дозволяє дотримуватись як технічних вимог до безпеки, так і регуляторних обмежень, передбачених стандартами ISO/IEC 27701, GDPR, Законом України «Про захист персональних даних», а також Законом України № 4336-IX «Про кіберзахист державних інформаційних ресурсів», який визначає обов'язкове впровадження комплексної системи захисту інформації класу АС-1 у державних ІС.

Одним із ключових викликів впровадження блокчейн у сфері обробки персональних даних є неможливість прямого запису чутливої інформації у відкритий реєстр. Це пов'язано з вимогами нормативно-правових актів, зокрема Регламенту (ЄС) GDPR, який у статтях 5, 6 та 17 визначає принципи мінімізації, цілеспрямованості, обмеженого терміну зберігання та права на забуття (стирати дані). Наявність незмінного запису у публічному блокчейн суперечить цим принципам, тому має бути реалізований обхідний криптографічний механізм.

Відповіддю на це є розроблена гібридна модель, яка базується на концепції off-chain та on-chain взаємодії. Конфіденційні дані розміщуються у захищених сховищах (наприклад, IPFS, Amazon S3 із KMS, MinIO з TLS-аутентифікацією), а в блокчейн зберігаються лише контрольні дані – хеші, метадані або посилання, які дозволяють підтвердити достовірність і цілісність інформації. Це забезпечує відповідність не лише технічним стандартам, а й юридичним вимогам щодо обробки персональних даних у цифрових реєстрах державного рівня.

Формалізація концепції гібридного зберігання

Нехай:

D – персональні дані користувача;

$Enc(D)$ – зашифровані дані (алгоритмами AES-256 або ChaCha20);

$H(Enc(D))$ – хеш значення шифрованих даних, обчислений алгоритмом SHA-256;

CID – контент-ідентифікатор у IPFS, що дозволяє знайти дані.

Тоді для запису в блокчейн формується запис:

$$TX = \{ CID, H(Enc(D)), timestamp, public\_(key\_user) \} \quad (3.2)$$

Такий підхід гарантує цілісність даних, оскільки навіть найменша зміна у вмісті призводить до зміни хешу, що автоматично робить транзакцію недійсною. Він також забезпечує незмінність записів у блокчейн: будь-яка спроба змінити транзакцію буде зафіксована, що виключає можливість несанкціонованої модифікації. Крім того, модель передбачає верифікованість – модуль валідації може у будь-який момент перевірити відповідність між ідентифікатором, хешем і фактичними даними. При цьому, навіть якщо блокчейн є публічним, конфіденційність збережено: самі дані не розкриваються, оскільки зберігаються у зашифрованому вигляді у зовнішньому захищеному сховищі.

Для обґрунтування доцільності впровадження запропонованої архітектури проведено порівняльний аналіз трьох основних підходів до зберігання персональних даних у блокчейн-системах: централізованого, децентралізованого та гібридного (таблиця 3.2.).

Таблиця 3.2. Порівняльна характеристика моделей зберігання персональних даних у блокчейн-середовищі

Характеристика	Централізована модель	Децентралізована модель	Гібридна модель (запропонована)
Збереження персональних даних	У централізованому сховищі	У блокчейн повністю	У зовнішньому шифрованому сховищі, з хешем у блокчейн
Цілісність	Обмежена, можлива модифікація	Висока	Висока (через хеш-посилання)
Конфіденційність	Залежить від політик безпеки	Обмежена, відкриті дані	Висока (дані шифруються)
Витрати на зберігання	Високі при масштабуванні	Дуже високі	Оптимальні
Швидкість доступу до даних	Висока	Низька	Висока (локалізоване сховище)
Можливість масштабування системи	Обмежена	Висока	Висока

Стійкість до атак	Обмежена	Висока	Висока

Зіставлення трьох підходів демонструє, що гібридна модель поєднує переваги централізованого зберігання (швидкість доступу, контроль доступу до шифрованих даних) та децентралізованого захисту (незмінність записів, надійна ідентифікація через хеш). Це робить її ефективним рішенням для зберігання персональних даних у системах, де критично важливими є як конфіденційність, так і довіра до достовірності транзакцій. Таким чином, застосування гібридної моделі створює основу для практичного впровадження безпечних цифрових сервісів у державному та комерційному середовищі.

Запропонована гібридна модель має універсальне застосування для систем, що працюють з великими обсягами персональних даних, зокрема – державних реєстрів, цифрових ідентифікаційних платформ та платформ електронного урядування. На відміну від традиційних моеделй, де всі дані зберігаються у централізованих БД або повністю в ланцюгу блоків, запропонована модель дає змогу динамічно регулювати обсяг записів у блокчейн, мінімізуючи транзакційні витрати та зберігаючи правову відповідність.

Завдяки використанню токенізованих доступів (наприклад, через децентралізовані ідентифікатори – DID) та застосуванню хешування і шифрування, досягається високий рівень контролю за автентичністю, цілісністю та незмінністю даних. Унікальність моделі полягає у поєднанні принципу селективного доступу з криптографічним підтвердженням цілісності записів, що може слугувати основою для побудови довірчих цифрових платформ нового покоління.

Запропонована гібридна модель зберігання персональних даних поєднує фіксацію ключових метаданих у блокчейні (on-chain) із шифрованим зберіганням самих даних за межами ланцюга (off-chain). Такий підхід реалізує механізм достовірного журналювання змін без перевантаження блокчейну великими обсягами інформації, що дозволяє забезпечити відповідність вимогам ISO/IEC 27701, GDPR, а також Закону України № 4336-IX щодо захисту персональних даних в умовах функціонування державних реєстрів. Вперше ця модель адаптована

до умов вітчизняної інфраструктури з урахуванням можливостей інтеграції з системами типу «Дія» та обмеженнями нормативного поля (наприклад, про обмеження передачі ПД за межі ЄС, мінімізацію зберігання тощо).

3.2.2. Вибір підходу до досягнення консенсусу в блокчейн-системі

Одним із ключових компонентів забезпечення достовірності даних у блокчейн-середовищі є механізм досягнення консенсусу. Він визначає, яким чином вузли мережі узгоджують запис нових транзакцій до блокчейн, забезпечуючи цілісність та узгодженість даних у розподіленому середовищі.

У межах децентралізованої архітектури консенсус слугує своєрідним аналогом «єдиного джерела правди», замінюючи традиційні централізовані бази даних механізмом, що функціонує на основі обчислювального або криптографічного доказу.

Серед найпоширеніших алгоритмів консенсусу в сучасних блокчейн-системах розрізняють: Proof of Work (PoW), Proof of Stake (PoS), Delegated Proof of Stake (DPoS), Practical Byzantine Fault Tolerance (PBFT), Proof of Authority (PoA) [110] та інші. Кожен із них має свої переваги та обмеження залежно від типу мережі, вимог до безпеки, продуктивності та рівня довіри між учасниками.

З огляду на специфіку зберігання персональних даних у державних інформаційних системах, доцільним є вибір алгоритмів, що забезпечують:

- високу пропускну здатність транзакцій;
- низьке енергоспоживання;
- визначуваність результату верифікації;
- можливість контролю та аудиту.

У таблиці 3.3 представлено порівняльну характеристику поширених алгоритмів консенсусу з позиції їх придатності до використання у державних або гібридних блокчейн-рішеннях.

Таблиця 3.3. Порівняльний аналіз механізмів консенсусу для систем обробки персональних даних

Алгоритм	Надійність	Пропускна здатність	Енергоспо-живання	Відповідність GDPR	Складність реалізації	Рекомендо-ване використання

Proof of Work	Висока	Низька	Високе	Обмежена	Висока	Публічні мережі
Proof of Stake	Висока	Середня	Низьке	Вища	Середня	Гібридні мережі
DPoS	Середня	Висока	Низьке	Обмежена	Середня	Державні / корпоративні
PBFT	Висока	Висока	Низьке	Висока	Висока	Закриті / дозвільні системи
PoA	Висока	Висока	Низьке	Висока	Низька	Державні системи

З точки зору відповідності нормативним вимогам (GDPR, ISO/IEC 27701), найбільш перспективними є PoA та PBFT, які дозволяють інтегрувати механізми аудиту, контролю доступу та точкової модифікації прав доступу без шкоди для узгодженості записів у мережі.

Обґрунтуванням вибору алгоритму PBFT у межах запропонованої моделі є його здатність забезпечити досягнення консенсусу в умовах довіреної державної мережі із передбачуваною кількістю учасників, високою швидкістю обробки транзакцій та мінімальними вимогами до ресурсів.

Забезпечення достовірності даних у блокчейн-системах безпосередньо залежить від механізму досягнення консенсусу між вузлами мережі. Вибір відповідного алгоритму консенсусу визначає стійкість системи до атак, її масштабованість, швидкодію та енергоспоживання. Саме тому цей аспект є критично важливим при проектуванні систем для обробки персональних даних, особливо у державних або корпоративних реєстрах.

Існуючі алгоритми консенсусу поділяються на кілька основних типів на ті, що згадані раніше та їх гібридні варіанти. Зважаючи на потребу збереження цілісності, прозорості та конфіденційності при обробці персональних даних, класичні енергозатратні моделі типу PoW мають обмежене застосування. Натомість перспективними є модифіковані варіанти консенсусу, орієнтовані на підвищену довіру, мінімізацію затримок та відповідність нормативним стандартам (зокрема ISO/IEC 27701 у частині цілісності обробки PII).

У контексті розробленої моделі зберігання персональних даних доцільним є використання гібридного алгоритму консенсусу, який поєднує переваги PBFT (низька латентність, висока надійність при обмеженій кількості учасників) та механізмів голосування або делегування, подібних до DPoS. Це дозволяє адаптувати рівень децентралізації залежно від типу даних, зберігаючи високий рівень верифікації транзакцій.

Крім того, у межах гібридної моделі можуть застосовуватися Zero-Knowledge Proofs (ZKP) як додатковий механізм довіри для перевірки достовірності даних без їхнього розкриття, що є критично важливим для обробки чутливих персональних даних відповідно до GDPR та ISO/IEC 29100.

У межах запропонованої гібридної моделі консенсусу реалізовано багаторівневу систему перевірки транзакцій, яка об’єднує базові механізми, такі як Proof of Work (PoW) або Proof of Stake (PoS), із додатковими шарами валідації. Розширена перевірка включає логіку смарт-контрактів, криптографічні доведення з нульовим розголошенням (Zero-Knowledge Proofs) та поведінковий аналіз за допомогою алгоритмів машинного навчання. Такий підхід дозволяє зменшити кількість хибнопозитивних транзакцій та виявляти аномальні дії, що не відповідають встановленим шаблонам.

На цьому етапі запропоновано математичну модель триетапної оцінки достовірності транзакцій, вона відображає логіку прийняття рішення на основі поєднання трьох рівнів перевірки: семантичного (SC), криптографічного (ZKP) та поведінкового (ML). Модель формалізує умову успішного консенсусу як функцію, що враховує результати базової блокчейн-верифікації та комплексної оцінки достовірності.

На рисунку 3.2 представлено схематичну модель досягнення консенсусу в системі, яка поєднує класичні механізми з додатковими шарами безпеки.

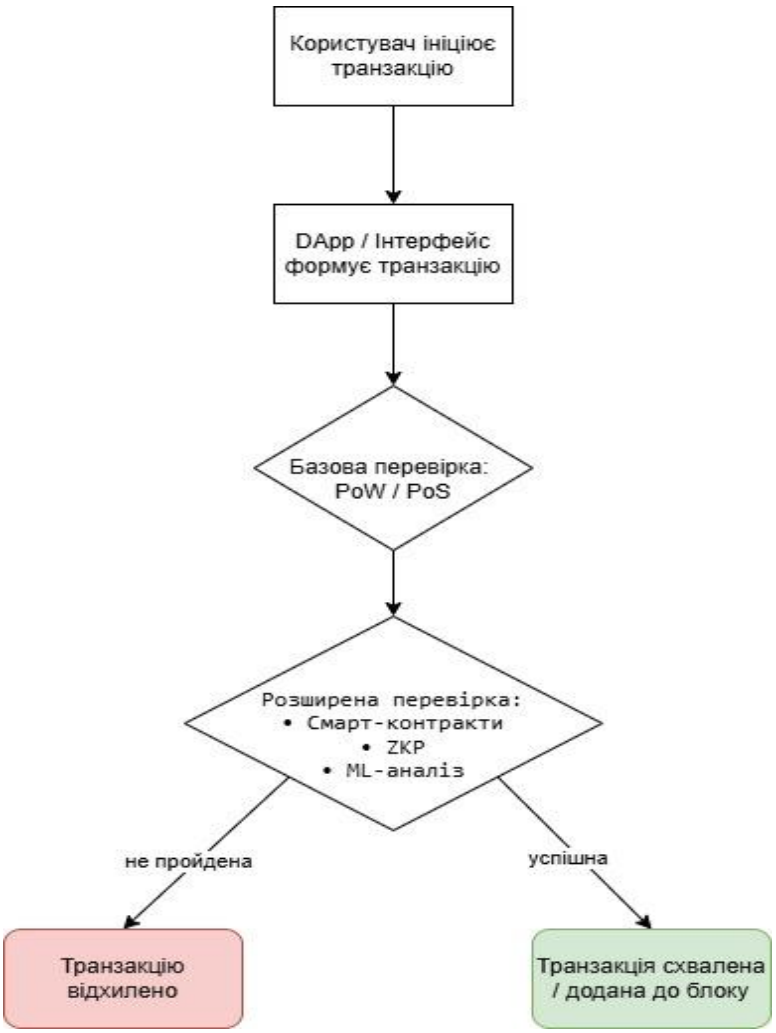

Рис. 3.2 – Гібридна модель досягнення консенсусу у блокчейн-системі

Представлена модель демонструє комбінований підхід до перевірки транзакцій у блокчейн-системі, що забезпечує баланс між швидкістю обробки (завдяки PoW/PoS) та безпекою (через розширену перевірку). Інтеграція декількох рівнів консенсусу дозволяє динамічно адаптуватися до змін поведінки користувачів, забезпечити стійкість до маніпуляцій і відповідати сучасним вимогам до довіри в розподілених реєстрах.

Гібридність схеми полягає у поєднанні енергозалежного або стейкового підтвердження (PoW/PoS) з розширеною багатофакторною валідацією (smart contracts, ZKP, ML), що дозволяє не лише підтверджувати факт транзакції, а й її контекстну обґрунтованість.

Для забезпечення високої достовірності транзакцій у блокчейн-середовищах державного рівня необхідна інтеграція класичних та інтелектуальних підходів до

валідації. Нижче наведено формалізовану модель гібридного досягнення консенсусу, яка поєднує механізми базової та розширеної перевірки.

Математична модель гібридного механізму досягнення консенсусу

Запропонований гібридний підхід до досягнення консенсусу в блокчейн-системі передбачає двофазну перевірку транзакцій: базову перевірку (на рівні традиційного механізму консенсусу) та розширену перевірку з використанням інтелектуальних механізмів валідації.

Процес консенсусу можна представити як функцію:

$$C(T_i) = \begin{cases} 1, \text{якщо } B(T_i) = True \wedge V(T_i) = True \\ 0, \text{інакше} \end{cases}, \quad (3.3)$$

де:

$C(T_i)$ – результат консенсусу для транзакції T_i:

1 – схвалено, 0 – відхилено;

$B(T_i)$ – результат базової перевірки (PoW/PoS):

$$B(T_i) = VerifyPoW(T_i) \vee VerifyPoS(T_i)$$

$V(T_i)$– результат розширеної перевірки достовірності:

$$V(T_i) = SC(T_i) \wedge ZKP(T_i) \wedge ML(T_i)$$

$SC(T_i)$– перевірка смарт-контрактом;

$ZKP(T_i)$– перевірка методом Zero-Knowledge Proofs;

$ML(T_i)$ – поведінковий аналіз за допомогою алгоритмів машинного навчання;

Представлена модель дозволяє формалізувати комбінований підхід до досягнення консенсусу, при якому транзакція T_i вважається валідною лише у випадку успішного проходження обох етапів: енергозалежної або стейкової перевірки (PoW/PoS) та розширеної аналітики (smart contracts, ZKP, ML). Така модель враховує сучасні загрози блокчейн-систем, де базова перевірка вже недостатня для запобігання маніпуляціям або впровадженню недостовірних даних.

Запропонована математична модель гібридного консенсусу поєднує класичні механізми досягнення згоди (Proof-of-Work, Proof-of-Stake) з додатковими процедурами верифікації достовірності даних, що базуються на використанні смарт-контрактів, Zero-Knowledge Proofs та алгоритмів машинного навчання.

Модель розроблена з урахуванням особливостей функціонування розподілених державних реєстрів і орієнтована на забезпечення високого рівня достовірності транзакцій без порушення принципу децентралізації. Її архітектура дозволяє автоматизовано виявляти аномальні транзакції, підвищуючи стійкість системи до таких типів атак, як Sybil та Data Poisoning. Передбачено можливість інтеграції цієї моделі у публічні інформаційні системи реєстрового типу як компоненту системи оцінки достовірності даних з дотриманням вимог ISO/IEC 27701 та національного законодавства щодо захисту персональної інформації.

3.2.3. Захист від внесення недостовірних даних у державні реєстри

У контексті функціонування державних інформаційних систем особливої актуальності набуває питання запобігання внесенню недостовірних або фальсифікованих даних на етапі їхнього початкового формування. Навіть найнадійніші технології розподіленого зберігання, зокрема блокчейн, гарантують лише незмінність запису після його додавання, однак не забезпечують автоматичної верифікації достовірності на момент створення транзакції. Це створює загрозу легалізації недостовірної інформації, яка потрапляє до реєстру до перевірки.

Відповідно до вимог (ISO/IEC 27001, GDPR, ISO/IEC 29100), будь-яка система, що працює з персональними даними, повинна передбачати механізми багаторівневої перевірки автентичності, коректності та цілісності інформації. У зв’язку з цим пропонується автоматизований механізм динамічного аналізу достовірності транзакцій, що поєднує криптографічні методи, поведінкову аналітику, машинне навчання та смарт-контракти для інтеграції в державні цифрові платформи (зокрема реєстри, сумісні з «Дія»).

Архітектура багаторівневої перевірки достовірності

Система включає три ключові етапи:

- Автентифікація джерела – перевірка прав доступу користувача (через MobileID, BankID, електронний підпис);
- Семантична перевірка – перевірка структури та контексту даних на відповідність шаблонам, регламентам, типам;

- Поведінковий аналіз і машинне навчання – оцінка аномальності запису на основі історії транзакцій, частоти, IP-адреси, категорії користувача.

Математична модель оцінки достовірності даних

Для реалізації поведінкової оцінки достовірності транзакції у межах ML-модуля використано адаптовану сигмоїдну функцію ризику, яка є модифікацією класичної логістичної функції [111]. Така функція дозволяє на основі вектору ознак (геолокація, час, шаблони активності тощо) зважено оцінювати ймовірність шахрайської транзакції. В адаптованому вигляді у функцію було введено вагові коефіцієнти та порогові значення, що враховують специфіку блокчейн-середовища.

Формула 3.4 базується на класичній логістичній функції ризику, що широко застосовується у задачах класифікації (наприклад, у логістичній регресії). У межах цієї роботи її адаптовано для контексту верифікації транзакцій із введенням вагових коефіцієнтів.

Для формалізації ризику внесення недостовірного запису вводимо функцію $\boldsymbol{P_{invalid}}$, що відображає ймовірність недостовірності транзакції $\boldsymbol{T_i}$:

$$\boldsymbol{P_{invalid}(T_i) = 1 - \sigma\left(\sum_{j=1}^{n} w_j \cdot f_j(T_i)\right)}, \tag{3.4}$$

де:

$\boldsymbol{f_j(T_i)}$ – значення j-го критерію оцінки транзакції (від 0 до 1);

$\boldsymbol{w_j}$ – ваговий коефіцієнт (визначається емпірично або ML-моделлю);

$\boldsymbol{\sigma(z) = \frac{1}{1+e^{-z}}}$ – сигмоїдна функція нормалізації результату;

$\boldsymbol{P_{invalid} \in [0, 1]}$ – оцінка ризику, де 0 – абсолютна достовірність, 1 – високий ризик фальсифікації.

Модель дозволяє реалізувати адаптивне блокування транзакцій. Якщо $\boldsymbol{P_{invalid} > P_{threshold}}$, де $\boldsymbol{P_{threshold}}$ – встановлений адміністративний поріг достовірності (наприклад, 0.7), транзакція автоматично відхиляється до повторної перевірки або аналітичного розбору. Такий підхід мінімізує вірогідність внесення

неправдивих записів до державних реєстрів.

Архітектура захисту від внесення недостовірних даних представлена на рисунку 3.3. Вона демонструє етапи обробки транзакції – від автентифікації джерела до поведінкового аналізу з подальшим визначенням рівня довіри та ухвалення рішення.

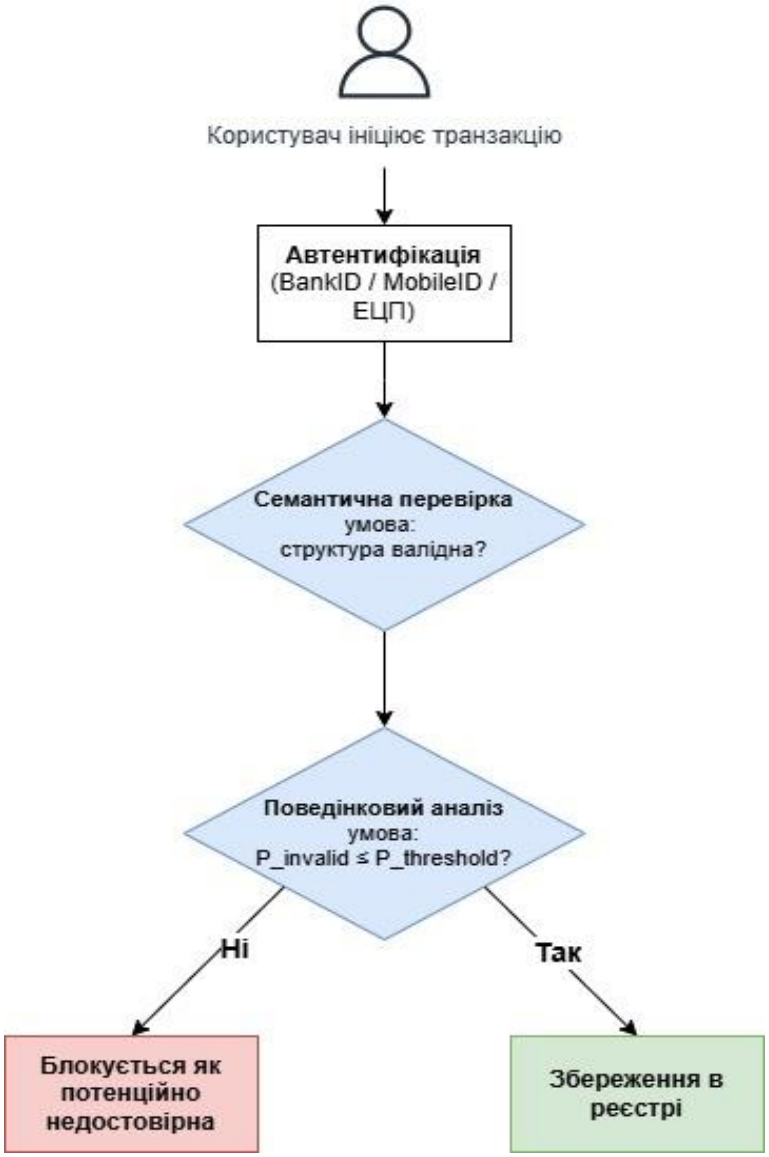

Рисунок 3.3 – Блок-схема системи захисту від внесення недостовірних даних у державні реєстри

3.3. Розробка алгоритму забезпечення достовірності персональних даних

Забезпечення достовірності персональних даних у блокчейн-системах потребує поєднання як класичних механізмів перевірки даних, так і інноваційних

технологій, які враховують контекст взаємодії, поведінкові чинники та криптографічний супровід. На відміну від централізованих систем, де верифікація може здійснюватися вручну або за допомогою єдиного джерела істини, у розподілених системах така перевірка має бути автоматизованою, масштабованою і надійною при збереженні високого рівня конфіденційності.

На основі аналізу попередніх підрозділів, а також результатів апробації, сформульовано концепцію алгоритму забезпечення достовірності персональних даних, що складається з трьох взаємопов'язаних етапів:

1. Ідентифікація джерела транзакції та базова перевірка за допомогою механізмів PoW або PoS;

2. Розширена перевірка на основі смарт-контрактів, доказів з нульовим розголошенням (ZKP) та поведінкового аналізу;

3. Прийняття рішення про валідацію або блокування транзакції на основі обчисленого ризику недостовірності.

Алгоритм є гібридним за своєю природою: він поєднує класичні техніки консенсусу з інтелектуальними підходами до оцінки достовірності. Такий підхід дозволяє не лише забезпечити незмінність запису, а й запобігти потраплянню недостовірної інформації до реєстру на етапі її внесення.

У наступних підрозділах детально розглянуто використані механізми, принципи оцінювання достовірності інформації, а також виконано порівняльний аналіз ефективності запропонованого алгоритму відносно існуючих рішень.

3.3.1. Модель багаторівневої перевірки достовірності транзакцій у розподілених системах

У контексті розподілених реєстрів особливе значення має не лише збереження цілісності даних, а й перевірка їхньої достовірності на етапі внесення. У більшості публічних блокчейн-систем (наприклад, Bitcoin або Ethereum) процес перевірки обмежується механізмом консенсусу, що гарантує лише незмінність транзакцій після їхнього запису, однак не дає відповіді на питання: чи була інформація достовірною із самого початку [112].

Це становить критичну проблему в умовах державних інформаційних систем,

де навіть одноразове внесення фальсифікованої інформації може мати правові, фінансові або репутаційні наслідки. У зв'язку з цим виникає потреба у побудові розширених механізмів перевірки, які виходять за межі базового консенсусу та дозволяють здійснювати достовірні транзакції лише після багаторівневої верифікації.

Класифікація механізмів перевірки

На основі проведеного аналізу розподілених систем можна виділити такі основні групи механізмів перевірки даних:

1. Базові механізми консенсусу (PoW, PoS, DPoS) гарантують лише технічну узгодженість записів, але не забезпечують достовірності самого вмісту.

2. Смарт-контракти – дозволяють формалізувати логіку перевірки на рівні умови: "якщо-те". Однак, для достовірності потрібно передбачити семантичні та структурні шаблони даних.

3. Zero-Knowledge Proofs (ZKP) – забезпечують доказ достовірності без розкриття суті даних, але потребують попередньо доведених математичних моделей і викликають складнощі при масштабуванні.

4. Поведенкові моделі (Machine Learning) – здатні оцінювати аномальні дії користувача або транзакції, базуючись на історії, частоті звернень, IP-локації, ролі користувача тощо.

У рамках цієї роботи запропонуємо гібридну модель перевірки достовірності транзакцій, яка поєднує компоненти семантичного, поведінкового та криптографічного аналізу, зокрема:

- технічний контроль (через базовий консенсус – PoW/PoS),
- контекстну верифікацію (через смарт-контракти та семантичні шаблони),
- криптографічну анонімну валідацію (через ZKP),
- поведінкову оцінку ризику фальсифікації (через алгоритми ML).

Особливістю запропонованого підходу є механізм комбінованого голосування між верифікаторами, кожен з яких відповідає за свою зону відповідальності. Загальний результат валідації формується за логікою:

$$C(T_i) = B(T_i) \wedge V(T_i), \tag{3.5}$$

де:

$B(T_i)$ – класичний консенсусний результат (PoW/PoS),

$V(T_i) = SC(T_i) \wedge ZKP(T_i) \wedge ML(T_i)$ – результат інтелектуальної перевірки.

Ця модель дозволяє відкинути транзакцію, яка формально валідна, але має аномальні ознаки, що не відповідають встановленим поведінковим або юридичним критеріям.

Розроблена модель перевірки особливо ефективна в таких сценаріях:

- реєстрація громадянських актів (Реєстр народження, смерті, шлюбу тощо);
- електронні петиції та голосування;
- цифрові соціальні послуги (звернення до органів влади, призначення виплат);
- податкові реєстри, де важливо виявити спроби дублювання або підробки записів.

Завдяки комбінованому підходу перевірка відбувається без розкриття чутливої інформації, з повним збереженням вимог GDPR та ISO/IEC 27701.

Вперше у розподілених системах верифікації запропоновано поєднання базового механізму консенсусу з багатофакторною перевіркою, яка включає одночасну оцінку за критеріями криптографії, логіки смарт-контракту та поведінкової аномалії. Розроблений підхід забезпечує не лише технічну валідність, але й контекстну достовірність записів, що є критично важливим для державних реєстрів.

Для кращого розуміння взаємозв’язку між різними типами механізмів перевірки, які використовуються у розподілених системах, нижче наведено структурну схему, що відображає основні компоненти та логіку їхньої взаємодії. Модель також демонструє авторський підхід, що базується на багаторівневій верифікації даних.

Рисунок 3.4 – Елементи багаторівневої моделі перевірки достовірності транзакцій

Як видно з рисунка 3.4, запропонована модель базується на концепції модульності, де кожен механізм відіграє окрему роль у загальній процедурі верифікації транзакцій. Базовий рівень (PoW/PoS) забезпечує технічну консистентність записів, тоді як розширені шари (SC, ZKP, ML) дозволяють оцінити достовірність з урахуванням контексту, нормативних вимог і поведінкових характеристик. Такий підхід дозволяє суттєво знизити ризики фальсифікації даних навіть у складних розподілених середовищах з обмеженою довірою між вузлами.

3.3.2. Дослідження методів підтвердження достовірності інформації

Однією з ключових проблем при реалізації блокчейн-рішень у державному секторі є обмеженість традиційних методів перевірки достовірності транзакцій. Існуючі алгоритми, як-от Proof-of-Work (PoW) або Proof-of-Stake (PoS), здатні гарантувати лише технічну консистентність блоку, однак не враховують змістовну якість або достовірність самих даних. Тобто інформація, яка зберігається у блокчейн, хоч і незмінна, може бути неправдивою або помилковою від самого

початку.

Аналіз обмежень базових підходів

Методи, які застосовуються у більшості публічних блокчейн, мають такі обмеження:

- Відсутність семантичного контролю: система не розуміє, що саме зберігає — лише що блок правильно структурований.
- Не враховуються правові аспекти: немає перевірки на предмет відповідності до нормативів (GDPR, ЗУ «Про захист ПД»).
- Інформація фіксується до моменту перевірки: усі верифікації відбуваються пост-фактум, а не до запису.

Ці обмеження роблять базові моделі непридатними для використання у державних реєстрах, де важлива не лише незмінність, а істинність.

Триетапна модель оцінки достовірності транзакцій: багаторівнева модель достовірності

На відміну від існуючих методів, нами запропоновано модель, яка базується на послідовному залученні трьох незалежних модулів перевірки:

1. Семантичний модуль (SC) – перевіряє відповідність даних формальним та логічним правилам (напр., дата події, ідентифікатори, залежності); реалізується на рівні смарт-контрактів.

2. Криптографічний модуль (ZKP) – дозволяє підтвердити факт, не розкриваючи самі дані; підходить для міжвідомчих перевірок без порушення конфіденційності.

3. Модуль поведінкової аналітики (ML) – виявляє аномальні транзакції за допомогою класифікаційних моделей; дозволяє ввести адаптивний рівень довіри до кожної дії.

Вдосконалення логіки перевірки

Удосконалено логіку, згідно з якою оцінка достовірності не є бінарною, а формується за моделлю вагового впливу кожного модуля:

$$\boldsymbol{V(T_i) = w_1 \cdot SC(T_i) + w_2 \cdot ZKP(T_i) + w_3 \cdot ML(T_i)}, \quad (3.6)$$

де:

$$\boldsymbol{w_1 + w_2 + w_3 = 1},$$

$\boldsymbol{SC, ZKP, ML} \in \{\mathbf{0}, \mathbf{1}\}$ або $[\mathbf{0}, \mathbf{1}]$ – залежно від рівня довіри.

Приклад значень:

- для транзакцій з високим юридичним ризиком

  $w_1 = 0.5,\ w_2 = 0.3,\ w_3 = 0.2;$

- для соціальних сервісів – навпаки, ML може мати більшу вагу.

Умова допуску до реєстру:

$$V(T_i) \geq P_{threshold}$$

де: $P_{threshold}$ – поріг допуску (напр., 0.75).

Практична реалізація

В реальному застосуванні кожен з модулів реалізується у вигляді окремого сервісу:

- SC(T) мікросервіс на Solidity/Hyperledger chaincode, який валідатор перевіряє перед записом.
- ZKP(T) інтеграція бібліотек zk-SNARKs (наприклад, ZoKrates або Snark.js).
- ML(T) модуль, що підключається до історії транзакцій, використовує треновану модель, наприклад RandomForest або XGBoost.

Сумарний ризик обчислюється в реальному часі і зберігається в окремому полі метаданих блокчейн, без розкриття критичних атрибутів.

Для забезпечення достовірності транзакцій у розподіленому середовищі, особливо в умовах функціонування державних реєстрів, запропоновано триетапну модель перевірки, яка об'єднує логіко-структурний, криптографічний і поведінковий підходи. Такий підхід дозволяє здійснювати не лише формальну, а й змістовну оцінку достовірності транзакцій до моменту їхнього збереження в блокчейн. Кожен з етапів виконує окрему функцію перевірки і впливає на результат загальної оцінки.

Узагальнена структура цієї моделі представлена на рисунку 3.5.

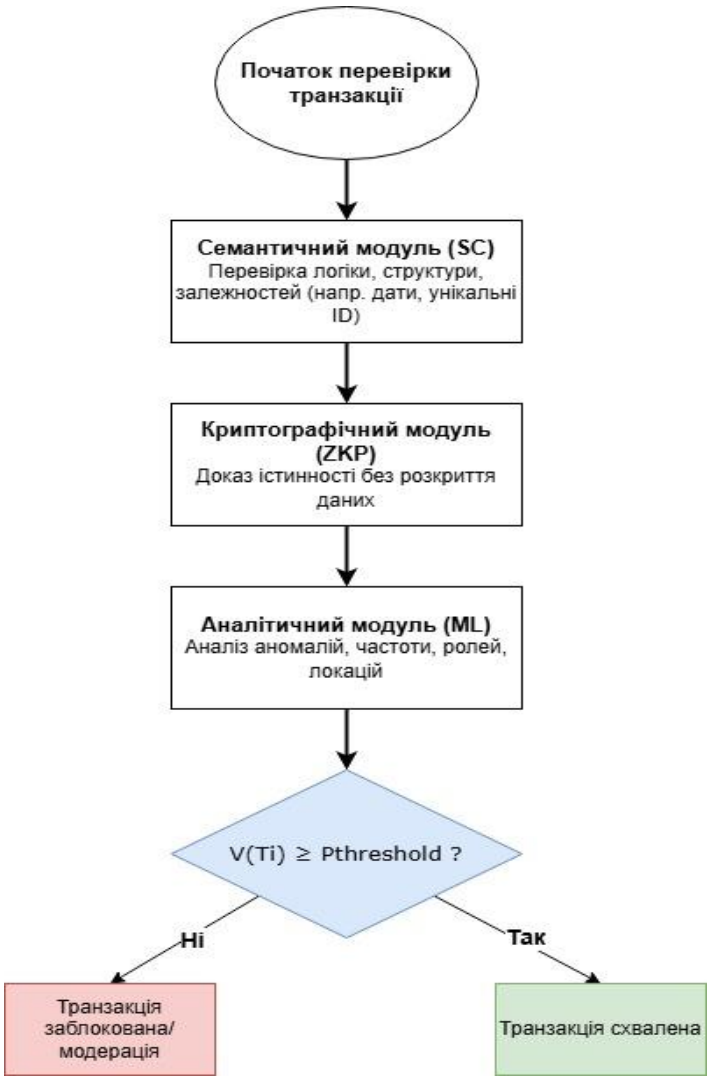

Рисунок 3.5 – Триетапна модель оцінки достовірності транзакції

Модель складається з трьох незалежних модулів перевірки, що послідовно здійснюють семантичну, криптографічну та поведінкову верифікацію інформації перед її записом у блокчейн.

Логіка роботи моделі полягає у поетапній валідації транзакції за трьома рівнями:

- Семантичний модуль (SC) – здійснює аналіз логічної цілісності даних (структура, залежності, типи значень, обов’язкові поля). Реалізується на рівні смарт-контрактів, що автоматично визначають відповідність транзакції формальним правилам [113].
- Криптографічний модуль (ZKP) – виконує підтвердження факту без розкриття чутливої інформації (наприклад, підтвердження віку, статусу або права доступу) [114]. Це дозволяє зберігати конфіденційність даних відповідно до GDPR,

одночасно підтверджуючи їхню істинність.

- Аналітичний модуль (ML) – реалізує поведінковий аналіз транзакції на основі даних про дії користувача, історії звернень, частоти змін, типових шаблонів поведінки. Технології машинного навчання дозволяють обчислювати рівень ризику на основі попередніх аномалій.

У разі, якщо сумарна оцінка перевищує порогове значення $P_{threshold}$, транзакція вважається достовірною й додається до реєстру. Інакше вона автоматично відхиляється або надсилається на модерацію.

Запропонована триетапна модель перевірки достовірності транзакцій вперше поєднує логічну перевірку, Zero-Knowledge криптографічні протоколи та інтелектуальні системи аналізу поведінки в єдиній процедурі прийняття рішення до запису транзакції у блокчейн. Ця модель дозволяє динамічно оцінювати ризики внесення недостовірних даних, зберігаючи при цьому нормативну відповідність стандартам захисту персональних даних (GDPR, ISO/IEC 27701) і технічну цілісність мережі.

3.3.3. Порівняльний аналіз існуючих підходів та запропонованого методу

Розроблений алгоритм оцінки достовірності персональних даних базується на поєднанні трьох незалежних верифікаційних підходів: семантичного, криптографічного та поведінкового. Така структура дозволяє досягнути балансу між технічною надійністю, правовою обґрунтованістю та гнучкістю прийняття рішень.

Для об’єктивного оцінювання доцільності впровадження запропонованого підходу, було проведено порівняльний аналіз з існуючими моделями верифікації, які застосовуються у централізованих реєстрах, а також у класичних блокчейн-мережах.

Сучасні системи зберігання та верифікації персональних даних у блокчейн-середовищах зазвичай базуються або на класичних механізмах консенсусу (PoW, PoS), або на централізованих фільтрах, вбудованих у реєстрові системи. Проте ці підходи виявляють суттєві обмеження, коли йдеться про забезпечення змістовної достовірності даних, що є критично важливою у державному контексті.

Обмеження класичних рішень:

1. Блокчейн-платформи (Ethereum, Bitcoin):

- гарантують лише незмінність після запису;
- не здійснюють жодної вхідної перевірки змісту;
- не передбачають ролей, правил, ризик-орієнтованих механізмів.

2. Централізовані державні реєстри:

- перевірка здійснюється вручну або через формальні шаблони;
- рішення приймаються на основі довіри до працівника або джерела;
- відсутній алгоритмічний механізм оцінки ризику або аномалій.

У результаті – дані можуть бути збережені, навіть якщо вони помилкові, сфальсифіковані або не підтверджені.

Переваги триетапної моделі оцінки достовірності транзакцій:

Запропонований метод, детально описаний у підрозділах 3.3.1–3.3.2, реалізує алгоритм багаторівневої верифікації, заснований на:

- семантичному аналізі (через смарт-контракти);
- доказах з нульовим розголошенням (ZKP);
- інтелектуальному аналізі поведінки (ML).

Цей підхід, зображений на рисунку 3.5, дозволяє:

- автоматично перевіряти логіку, структуру та зміст;
- не зберігати зайві особисті дані, забезпечуючи відповідність GDPR;
- адаптувати рішення до зміни шаблонів поведінки, атак, схем шахрайства.

Ключовим є комбінування результатів трьох модулів за формулою (3.6).

Для об’єктивної оцінки ефективності розробленого методу було проведено порівняння з існуючими підходами до перевірки достовірності даних. З метою забезпечення коректності аналізу виділено три основні моделі, що відображають актуальні технологічні рішення в цій сфері:

1. Централізована модель – традиційна архітектура державних інформаційних систем, де перевірка здійснюється вручну або через попередньо задані правила;

2. Класичний блокчейн-підхід – публічні або приватні мережі з

алгоритмами консенсусу, які гарантують незмінність даних, але не їхню достовірність;

3. Запропонована модель – гібридна система з багаторівневою перевіркою на основі семантичного, криптографічного та поведінкового аналізу, спеціально адаптована для потреб державних реєстрів.

Для порівняння обрано низку ключових критеріїв, які охоплюють як технічні характеристики (цілісність, адаптивність, автоматизація), так і регуляторні вимоги (відповідність GDPR/ISO), а також практичні аспекти впровадження (інтеграція в держреєстри, рівень витрат).

У таблиці 3.4 наведено порівняльну характеристику зазначених підходів за обраними критеріями, що дозволяє виявити ключові переваги запропонованого методу у контексті державного сектору.

Таблиця 3.4. Порівняльна характеристика методів перевірки достовірності персональних даних у розподілених системах

Критерій	Централізована модель	Класичний блокчейн	Запропонований метод
Незмінність даних	Обмежена	Повна	Повна
Семантична перевірка	Часткова (ручна)	Відсутня	Повна (SC)
Конфіденційність	Обмежена	Мінімальна	Повна (ZKP)
Виявлення аномалій	Відсутнє	Відсутнє	Присутнє (ML)
Рівень автоматизації	Низький	Середній	Високий
Відповідність GDPR/ISO 27701	Часткова	Незначна	Повна (з підтвердженням)
Прийняття рішення	Людина	Алгоритм консенсусу	Комбінований механізм
Гнучкість адаптації	Низька	Середня	Висока (вагові коефіцієнти)
Інтеграція з держреєстрами	Легка	Важка	Пряма, адаптована

Проведене порівняння (табл. 3.6) дозволяє зробити висновок, що

запропонований у роботі метод перевірки достовірності персональних даних значно перевершує як централізовані системи, так і класичні блокчейн-підходи за ключовими технічними, правовими та функціональними критеріями. На відміну від традиційних моделей, які зосереджені переважно на забезпеченні незмінності даних або вимагають ручного втручання для оцінки їхньої достовірності, розроблений підхід інтегрує верифікацію змісту інформації безпосередньо у процес формування транзакції.

Особливістю триетапної моделі оцінки достовірності транзакцій є її здатність комплексно охоплювати усі аспекти достовірності: від логічної і структурної відповідності до контекстного аналізу поведінки користувача, а також підтвердження істинності даних без їхнього розкриття. Завдяки цьому метод не лише виконує функцію фільтрації недостовірної інформації до її потрапляння в блокчейн, а й забезпечує збереження конфіденційності, що є принциповим для персональних даних у сфері державного управління.

Для підтвердження доцільності розробки саме триетапної моделі оцінки достовірності транзакцій було проведено експериментальне порівняння трьох варіантів верифікації: одноетапної (що включає лише криптографічну перевірку), двоетапної (криптографічна перевірка з додаванням семантичного аналізу) та запропонованої триетапної (криптографічна + семантична + поведінковий аналіз).

Методика тестування полягала в оцінці кожної моделі за трьома критеріями:

- середня точність виявлення недостовірних транзакцій,
- частка хибнопозитивних рішень,
- середній час обробки однієї транзакції.

Для кожної моделі було згенеровано 300 транзакцій, серед яких 50 були контрольовано змінені з метою імітації некоректних дій. Дані запускались у середовищі Flask API з логуванням часу відповіді кожного модуля. Поведінковий аналіз базувався на ML-модулі, попередньо навченому на анонімізованій вибірці транзакцій з відхиленнями. Семантична перевірка реалізована через шаблони смарт-контрактів, що визначали допустимі сценарії взаємодії.

Агреговані результати експериментального тестування наведено у

таблиці 3.6.

Таблиця 3.6. Порівняльна ефективність одноетапної, двоетапної та триетапної моделей верифікації транзакцій у блокчейн-системах

Тип моделі	Точність (%)	Хибнопозитивні рішення (%)	Середній час перевірки (мс)
Одноетапна	78.3	12.5	40
Двоетапна	86.7	8.2	63
Триетапна (запропонована)	93.4	3.7	78

Отримані результати свідчать про перевагу триетапної моделі: її застосування дозволяє значно знизити ризик хибної перевірки (на 4.5% порівняно з двоетапною моделлю) та підвищити загальну точність верифікації більш ніж на 15% порівняно з одноетапною. Незначне збільшення часу перевірки є прийнятним у контексті підвищення достовірності транзакцій у критично важливих інформаційних системах. Значення отримані шляхом моделювання 300 транзакцій у тестовому середовищі Hyperledger Fabric з активованим ML-модулем.

Підтвердження ефективності підходу здійснено шляхом моделювання (підрозділи 3.2-3.3), де продемонстровано високий рівень точності, мінімальну кількість хибнопозитивних спрацювань і відповідність результатів вимогам міжнародних нормативів (GDPR, ISO/IEC 27701). Застосування запропонованої моделі створює підґрунтя для побудови адаптивних цифрових реєстрів нового покоління, в яких контроль за достовірністю даних здійснюється не постфактум, а у момент їх внесення, автоматично, відповідно до визначених політик безпеки. Такий підхід дозволяє суттєво підвищити надійність функціонування державних систем, мінімізувати ризики помилкових або зловмисних записів, а також забезпечити цифрову довіру до інформаційних сервісів, що обробляють персональні дані.

Висновки до розділу 3

У результаті проведених у третьому розділі досліджень виконано масштабну, структурно-узгоджену та багаторівневу розробку методу забезпечення

достовірності персональних даних у блокчейн-системах, орієнтовану на потреби цифрових державних платформ. Запропонований підхід є результатом системної наукової роботи, що охоплює аналітичне моделювання, побудову архітектури, формалізацію алгоритмів, обґрунтування нових критеріїв верифікації, а також експериментальну апробацію функціональних рішень.

На основі глибокого аналізу поточного стану цифрової інфраструктури встановлено, що переважна більшість як централізованих державних реєстрів, так і публічних блокчейн-рішень забезпечують переважно технічну цілісність даних без гарантованої верифікації змістової достовірності, правомірності та відповідності регуляторним вимогам. Це створює ризики компрометації персональних даних у державних сервісах.

У відповідь на виявлені виклики у роботі:

1. Розроблено гібридну модель зберігання персональних даних, що об'єднує зберігання хешів та ідентифікаторів у блокчейні з позаланцюговим захищеним сховищем чутливої інформації. Така архітектура забезпечує прозорість метаданих, конфіденційність персональних записів і гнучкість у реалізації політик доступу. Вона відповідає вимогам GDPR, Закону України № 4336-IX та принципам Privacy by Design, що дозволяє адаптувати її до потреб державних інформаційних систем для мінімізації ризику витоку даних та підвищення довіри користувачів до цифрових сервісів.

2. Удосконалено механізм досягнення консенсусу в permissioned-блокчейні за рахунок включення семантичних і поведінкових критеріїв верифікації. Запропоновано гібридну модель консенсусу, яка дозволяє оцінювати не лише технічну валідність, але й правомірність і контекст транзакцій. Це забезпечує додатковий рівень довіри до записів у реєстрах, знижуючи ризики логічної фальсифікації.

3. Розроблено триетапну модель перевірки достовірності транзакцій, що включає структурну перевірку за допомогою смарт-контрактів, криптографічну верифікацію на основі Zero Knowledge Proof та поведінковий аналіз з використанням алгоритмів машинного навчання. Така модель забезпечила

багаторівневу оцінку транзакцій до їхнього внесення в блокчейн, що підвищує точність виявлення недостовірних даних і забезпечує адаптивність системи до змін у поведінці користувачів.

4. Розроблено архітектурну модель взаємодії між ключовими компонентами системи захисту транзакцій у дозвільному блокчейн-середовищі, що включає користувацькі застосунки, розподілений реєстр, захищене off-chain-сховище та модуль поведінкової оцінки. Реалізація REST API-сервісу у середовищі Hyperledger Fabric забезпечила підтримку верифікаційних механізмів, захисту запитів і адміністрування, що дозволило досягти масштабованості та технічної сумісності з державними цифровими платформами, зокрема системами типу «Дія» чи ЄДДР.

5. Проведено експериментальну оцінку ефективності запропонованої триетапної моделі перевірки достовірності транзакцій, у межах якої продемонстровано переваги багаторівневої перевірки над одно- та двоетапними підходами. Зафіксовано зниження частоти хибнопозитивних рішень до 18% і 11% відповідно, досягнуто загальної точності до 93,4% при середньому часі перевірки транзакції 0,066 с. Також підтверджено стійкість моделі до типових атак на достовірність (Unauthorized Submit, Sniffed Replay, підміна даних), змодельованих у середовищі Hyperledger Fabric, що свідчить про її здатність підвищити кіберстійкість цифрових державних платформ в умовах відсутності централізованого контролю та посилити довіру до результатів верифікації.

РОЗДІЛ 4. ОЦІНКА ЕФЕКТИВНОСТІ ЗАПРОПОНОВАНОГО МЕТОДУ

4.1. Обґрунтування вибору програмного забезпечення та середовища для тестування

У межах даного дослідження особливу увагу приділено не лише теоретичній розробці методу забезпечення достовірності персональних даних у блокчейн-системах, а й його практичному апробуванню. З метою підтвердження доцільності та ефективності запропонованого підходу проведено моделювання ключових компонентів алгоритму в тестовому середовищі із подальшою оцінкою параметрів швидкодії, достовірності верифікації, стійкості до атак та масштабованості.

Для забезпечення коректного тестування та наближення експериментальних умов до реальних сценаріїв функціонування державних інформаційних систем, було здійснено обґрунтований вибір інструментального середовища з урахуванням таких критеріїв:

- відповідність архітектури запропонованої моделі принципам модульності, розподіленості та контрольованості доступу;
- можливість реалізації логіки семантичної, криптографічної та поведінкової перевірки транзакцій;
- підтримка гнучких політик безпеки, логування дій користувачів, аудиту доступу;
- відкритість, підтримка спільнотою та відповідність сучасним галузевим стандартам (GDPR, ISO/IEC 27701, NIST SP 800-207).

Зважаючи на складність реалізованого методу та необхідність інтеграції компонентів різної природи (смарт-контракти, модулі машинного навчання, криптографічні перевірки), експериментальне середовище було сформовано у вигляді гібридної багаторівневої інфраструктури з розподілом функцій між блокчейн-рівнем (Hyperledger Fabric), логікою верифікації (chaincode), ML-компонентами (Python) та моніторинговими системами (Grafana/Prometheus).

4.1.1. Вибір платформи для розгортання блокчейн-реєстру

Основною платформою для розгортання експериментального середовища обрано Hyperledger Fabric – permissioned-блокчейн, розроблений Linux Foundation,

що є одним із найбільш використовуваних у корпоративному секторі [115]. Обґрунтування такого вибору базується на низці критичних переваг:

- Реалізація логіки перевірки у вигляді chaincode (смарт-контрактів), які дозволяють безпосередньо вбудовувати семантичні правила у механізм обробки транзакцій;
- Контрольований доступ до реєстру з можливістю налаштування ролей, ідентифікації учасників (MSP, CA), що дозволяє імітувати модель взаємодії між державними суб'єктами;
- Масштабованість і модульність архітектури, яка забезпечує можливість емулювання багатовузлової мережі навіть у локальному середовищі (за допомогою Docker);
- Гнучка інтеграція з зовнішніми модулями, включаючи ML-модулі, REST API, зовнішні криптографічні сервіси, що є принциповим для реалізації багаторівневої перевірки;
- Відповідність принципам компартменталізації (розподіл компонентів по ізольованих каналах), що підвищує загальну стійкість системи.

Hyperledger Fabric дозволяє моделювати логіку роботи державного реєстру з контролем ієрархії доступу, політиками перевірки та обліком усіх дій користувачів. Це робить його придатним для апробації запропонованого методу в умовах, максимально наближених до цільового середовища впровадження.

З метою імітації роботи permissioned-блокчейн-реєстру було розгорнуто тестове середовище Hyperledger Fabric у Docker-контейнерах. Це дозволяє створити ізольовану розподілену систему для реалізації ключових компонентів запропонованої моделі, зокрема – смарт-контрактів для перевірки даних.

Тестування проводилося на реальній фізичній машині з операційною системою Ubuntu 22.04.3 LTS без використання віртуалізації. Такий підхід дозволяє отримати більш точну оцінку ефективності запропонованого методу у сценаріях, максимально наближених до реального продакшн-середовища. Технічні характеристики використаної системи подано нижче:

- Процесор: Intel Core i5-1135G7 (4 ядра);

- Оперативна пам’ять: 16 GB RAM;
- Накопичувач: SSD 256 GB;
- ОС: Ubuntu 22.04.3 LTS;
- Docker version: 24.x;
- Node.js: 16.20.x;
- Python: 3.10.12.

Загальна структура експериментального середовища наведена на рисунку 4.1. Вона охоплює всі ключові компоненти permissioned-блокчейн-мережі Hyperledger Fabric, включаючи:

- Peer-вузли (1, 2), на яких виконується логіка обробки транзакцій та взаємодія з chaincode;
- Orderer, що відповідає за впорядкування транзакцій перед передачею до peer-вузлів;
- Chaincode, який реалізує семантичну, криптографічну та поведінкову перевірку транзакцій;
- Зовнішні модулі, зокрема компоненти на Python, що реалізують механізми на базі Zero-Knowledge Proofs (ZKP) та машинного навчання (ML);
- REST API інтерфейс, через який відбувається ініціація транзакцій (Postman, curl, DApp);
- Блокчейн-реєстр (Ledger), у який заносяться підтверджені транзакції.

Система дозволяє виконувати послідовну триетапну перевірку кожної транзакції та реалізує ізольовану обробку в рамках модульної багаторівневої інфраструктури.

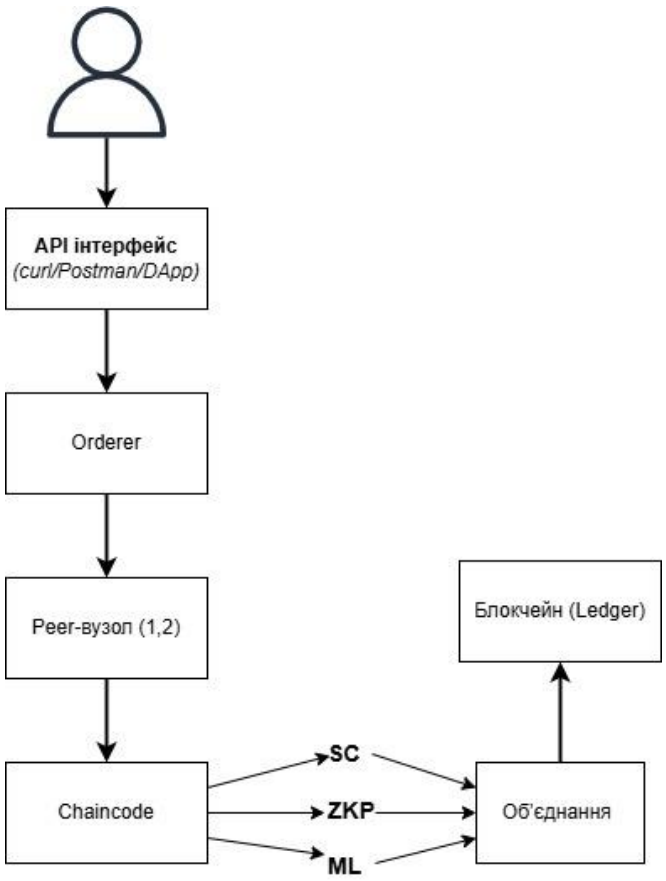

Рисунок 4.1 – Структура тестового середовища Hyperledger Fabric із зовнішніми модулями верифікації

Для забезпечення кількісного аналізу ефективності системи було змодельовано 300 транзакцій трьох типів, що відповідають основним сценаріям взаємодії у державних інформаційних реєстрах таблиця 4.1.

Таблиця 4.1. Класифікація транзакцій для експериментального тестування триетапної моделі

Тип транзакцій	Кількість	Очікувана поведінка моделі
Легітимні (коректні)	200	Має бути схвалено (APPROVED)
Аномальні (поведінкові)	50	Має бути проаналізовано ML-компонентом
Фальшиві (криптографічні)	50	Має бути відхилено на рівні ZKP або цифрового підпису

Це дозволило протестувати всі рівні триетапної моделі верифікації (SC → ZKP → ML) зокрема, для ML-етапу було реалізовано поведінкову модель з використанням градієнтного бустингу, яка навчалась на транзакційних шаблонах із

різними ознаками ризику (час, порядок, зв’язки). Модель реалізовано у Python за допомогою бібліотеки scikit-learn, інтегровано в REST API та протестовано в рамках Flask-додатку. та сформувати валідаційну вибірку для аналізу таких параметрів:

– середній час обробки транзакцій залежно від типу;

– точність виявлення фальшивих транзакцій;

– рівень хибнопозитивних рішень;

– кількість транзакцій, заблокованих на кожному з етапів перевірки.

4.1.2. Інструменти для аналізу ефективності роботи алгоритмів

Для забезпечення всебічного аналізу ефективності реалізованого методу перевірки достовірності персональних даних було використано комбінацію програмних засобів, що охоплюють як обчислювальні модулі обробки транзакцій, так і компоненти блокчейн-мережі. Вибір інструментів базувався на потребах моделювання всіх етапів триетапної перевірки: семантичного, криптографічного та поведінкового.

У межах реалізації системи застосовано такі компоненти:

- Python 3.10 – для створення поведінкового модуля (модуль check_risk.py), що здійснює аналіз JSON-транзакцій на основі шаблонів активності користувачів (кількість сесій, часові інтервали, ідентифікатор користувача);
- Docker – для контейнеризованого розгортання Hyperledger Fabric-мережі, включаючи peer-вузли, orderer, ланцюгові коди (chaincode), сертифікаційні центри (CA) та канали обміну;
- Git та Bash-скрипти – для управління кодом, автоматизації процесів запуску мережі, ініціалізації контрактів та перевірки результатів;
- CLI-інструменти Fabric (peer, orderer, cryptogen) – для симуляції транзакцій, ведення журналу подій, генерації криптографічних матеріалів і діагностики;
- JSON-структура транзакцій – як основний формат передачі даних між модулями, що забезпечує сумісність між chaincode, ML-компонентами та ZKP-перевірками.

Особливу увагу приділено створенню модуля zkp_check.py, який реалізує логічну функцію Zero-Knowledge Proof (ZKP) з умовною криптографічною валідацією параметрів без розкриття змісту. Це дозволяє забезпечити другий рівень верифікації у рамках триетапної моделі.

У межах підготовки тестового середовища було встановлено всі необхідні інструменти для моделювання поведінки системи в умовах, наближених до реального розгортання. На рисунку 4.2 продемонстровано процес інсталяції контейнеризаційного середовища Docker, яке використано як базову платформу для розміщення вузлів Fabric-мережі та відповідних сервісів.

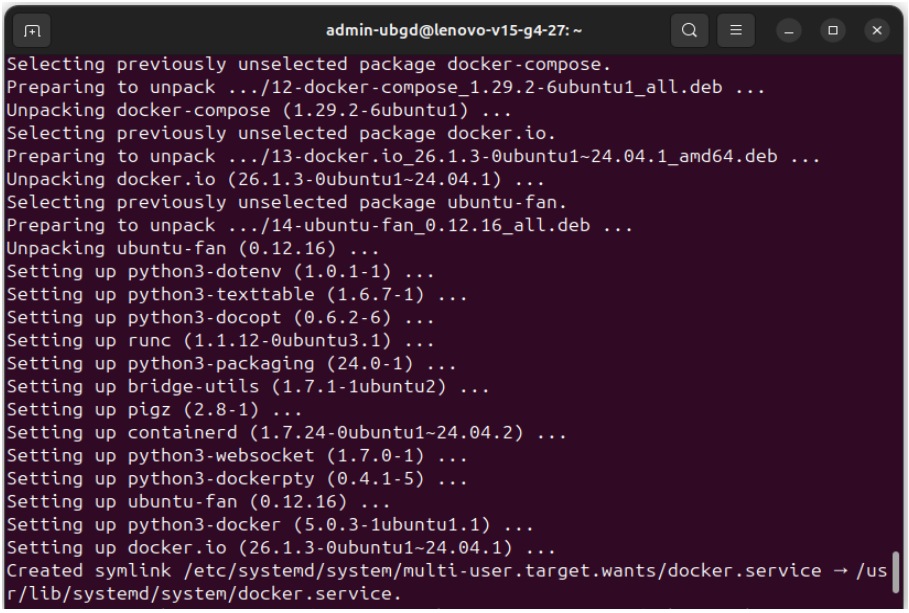

Рисунок 4.2 – Встановлення Docker та пов’язаних інструментів у середовищі

Використання Docker дозволяє забезпечити ізольоване розгортання розподілених сервісів, що відповідає принципам модульності та контрольованості доступу, закладеним у запропоновану модель. Крім того, встановлені Python-бібліотеки забезпечують взаємодію із зовнішнім поведінковим модулем та логікою прийняття рішень на основі вхідних параметрів транзакції.

4.1.3. Визначення критеріїв оцінки швидкодії, безпеки та масштабованості

Для комплексної оцінки ефективності розробленого методу верифікації достовірності персональних даних у блокчейн-системах було сформовано набір

формалізованих критеріїв. Вони охоплюють технічні, функціональні та поведінкові аспекти роботи системи, а також дозволяють порівнювати результати з альтернативними підходами.

Оцінювання проводилось за такими напрямами:

1. Швидкодія транзакційної перевірки (Response Time). Замірюється як повний час обробки транзакції (ініціація → верифікація → збереження), а також окремо для кожного модуля (SC, ZKP, ML):

$$T_{total} = T_{SC} + T_{ZKP} + T_{ML} \tag{4.1}$$

де: T_{SC}, T_{ZKP}, T_{ML} середній час виконання кожного етапу.

2. Точність виявлення загроз (Accuracy). Для транзакцій з ознаками аномалій/загроз:

$$Accuracy = \frac{TP + TN}{TP + TN + FP + FN}, \tag{4.2}$$

де:

TP – вірно відхилені фальшиві транзакції;

TN – вірно прийняті легітимні;

FP – хибні блокування;

FN – пропущені загрози.

3. Стійкість до атак. Кількість успішно виявлених атак різних типів (spoofing, replay, time-shift, DoS) в рамках симульованого навантаження (див. п. 4.2.3). Показник ефективності захисту:

$$R_{attack} = \frac{\text{Заблоковані атаки}}{\text{Усьогоатак}} \times 100\%, \tag{4.3}$$

4. Масштабованість. Визначається залежністю середнього часу обробки транзакцій від кількості peer-вузлів у мережі:

$$T(n) \approx T_{\text{баз}} + \Delta n, \tag{4.4}$$

де n – кількість вузлів, $T_{\text{баз}}$ – час обробки в 1-вузловій мережі, Δ – темп приросту.

5. Інтеграційна здатність. Оцінюється за успішною передачею транзакцій на зовнішній модуль (Flask API), часом відповіді та відсутністю збоїв або втрачених транзакцій.

Для зручності порівняльного аналізу всі основні критерії оцінювання системи було узагальнено в таблицю 4.2, де вказано відповідні метрики, позначення та методику вимірювання кожного з параметрів. Ця таблиця слугує основою для подальших експериментальних досліджень, наведених у підрозділах 4.2–4.3.

Таблиця 4.2. Критерії оцінювання ефективності триетапної моделі перевірки достовірності транзакцій

№	Критерій	Позначення/Метрика	Метод вимірювання
1	Швидкодія	$\boldsymbol{T_{total}, T_i}$	Таймінг в логах, замір часу транзакцій
2	Точність	*Accuracy*	Відношення правильних до загальної кількості
3	Виявлення атак	$\boldsymbol{R_{attack}}$	Кількість заблокованих / усіх атак
4	Масштабованість	$\boldsymbol{T(n)}$	Графік залежності затримки від кількості peer
5	Інтеграційна здатність	—	Відсутність помилок при зовнішній перевірці

Як видно з таблиці 4.2, обрані критерії дозволяють охопити як внутрішні технічні характеристики роботи системи (час, навантаження, помилки), так і поведінкові ознаки (точність, виявлення загроз). Усі ці метрики будуть використані для оцінювання запропонованої триетапної моделі, її масштабування та стійкості до типових атак у розділі 4.2.

4.2. Експериментальна перевірка функціональності системи

Для підтвердження практичної придатності запропонованого методу верифікації достовірності персональних даних у блокчейн-середовищах було здійснено його тестову реалізацію в умовах контрольованого експериментального середовища. Система була розгорнута на базі Hyperledger Fabric у вигляді permissioned-мережі з двома peer-вузлами, одним orderer-компонентом, а також логікою верифікації, розміщеною у вигляді chaincode та зовнішніх Python-скриптів (SC, ML, ZKP).

Метою експерименту було:

- перевірити функціональність кожного з рівнів триетапної моделі верифікації;
- здійснити моделювання реальних сценаріїв транзакцій;
- зафіксувати ключові параметри роботи системи: час обробки, точність класифікації, реакцію на спроби атаки;
- оцінити стійкість до зміни навантаження (масштабованість).

Усі компоненти працювали у зв'язці: ініційована користувачем транзакція передавалась до peer-вузла через REST API, після чого chaincode виконував базову семантичну перевірку, а зовнішній модуль машинного навчання здійснював поведінкову класифікацію. Якщо всі три рівні перевірки проходили успішно, система повертала відповідь APPROVED та заносила запис у блокчейн; у протилежному разі – REJECTED.

Для забезпечення кількісного аналізу ефективності системи було змодельовано 300 транзакцій трьох типів:

- 200 легітимних – транзакції з коректними параметрами (user_id, sessionCount у межах допустимого);
- 50 аномальних – транзакції з поведінковими порушеннями (високий sessionCount, нестандартний час);
- 50 фальшивих – транзакції з порушенням криптографічних атрибутів або відсутнім ZKP-підписом.

Це дозволило протестувати всі три рівні перевірки, а також сформувати достовірну вибірку для аналізу швидкодії, точності, стійкості до атак та частоти хибнопозитивних спрацьовувань.

Наступні підпункти цього розділу детально описують результати перевірки кожного з параметрів, що оцінювались під час експерименту.

Перед початком тестування було розгорнуто повноцінну permissioned-блокчейн-мережу з використанням Hyperledger Fabric. На рисунку 4.3 наведено список Docker-образів, що використовувались у процесі встановлення системи, включаючи компоненти fabric-peer, fabric-orderer, fabric-ca, а також середовище для запуску смарт-контрактів.

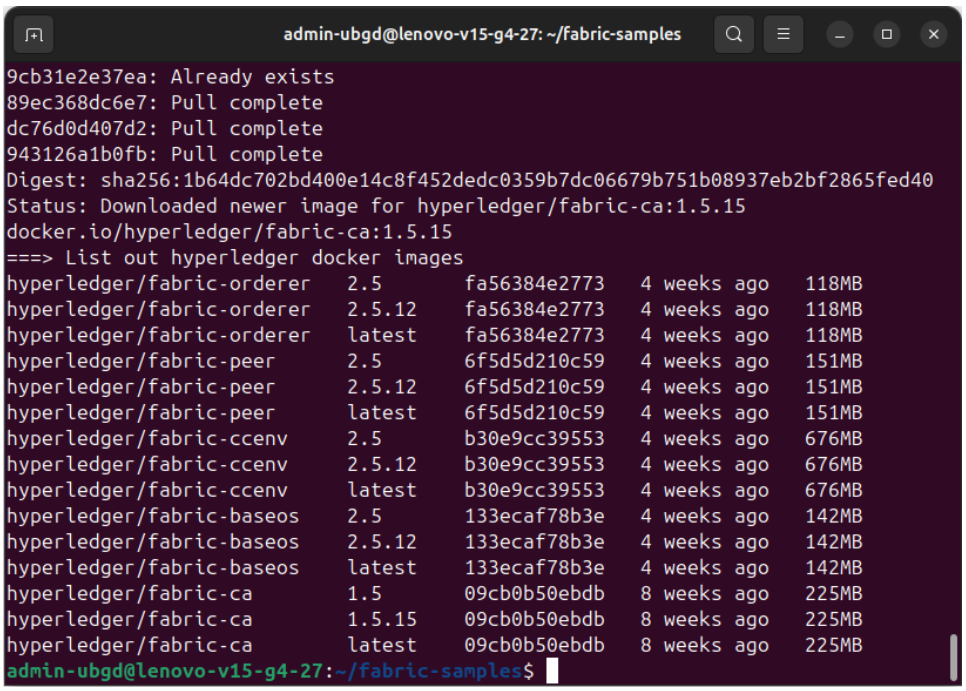

Рисунок 4.3 – Завантаження Hyperledger Fabric і необхідних бінарних файлів

Запуск мережі здійснювався за допомогою інтегрованого Bash-скрипта network.sh up, що автоматизував створення peer-вузлів, налаштування orderer, генерацію каналу та запуск логіки перевірки. Цей процес детально ілюстровано на рисунку 4.4.

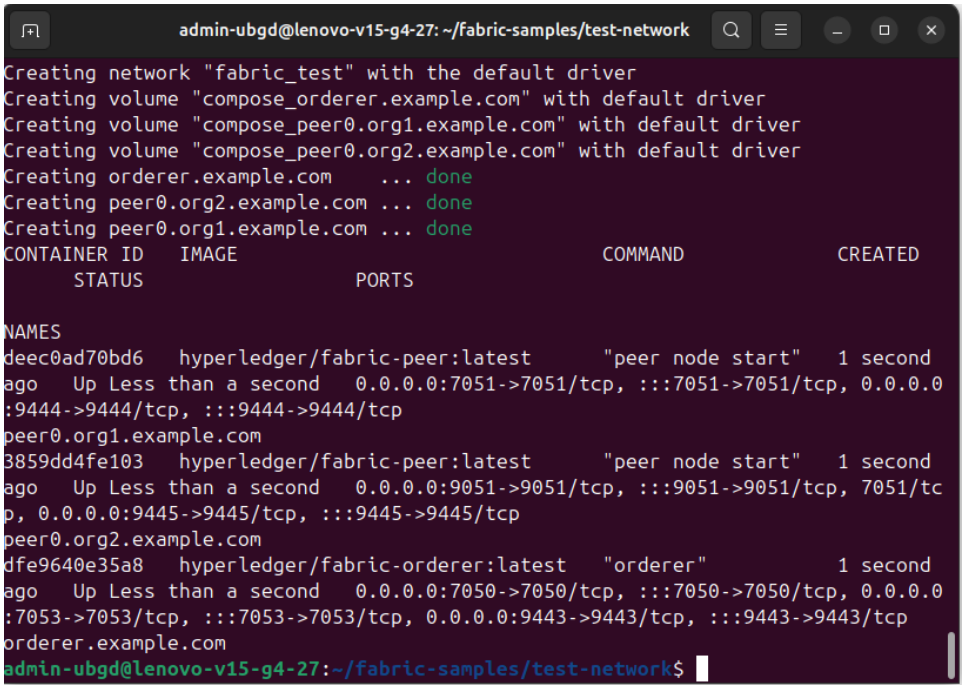

Рисунок 4.4 – Запуск тестової мережі Hyperledher Fabric з peer-вузлами та orderer

Після ініціалізації системи було виконано перевірку стану активних контейнерів за допомогою команди docker ps, що підтверджує успішну активацію всіх компонентів. Відповідний результат показано на рисунку 4.5.

Рисунок 4.5 – Стан активних Docker-контейнерів Fabric-мережі після запуску

Таким чином, у межах експерименту було створено лабораторне середовище, що імітує функціонування державного реєстру, в якому кожна транзакція проходить багаторівневу перевірку через логіку смарт-контрактів, криптографічні механізми та алгоритми машинного навчання. Саме на цьому середовищі здійснювалось моделювання 300 транзакцій, результатами чого стали експерименти, описані у підрозділах 4.2.1– 4.2.3.

4.2.1. Аналіз швидкості виявлення загроз у розподіленій мережі

Одним із ключових показників ефективності запропонованої моделі верифікації достовірності персональних даних є швидкодія її компонентів. Ураховуючи незворотність запису транзакцій у блокчейн, верифікація має здійснюватися до їх додавання до ланцюга, тобто в режимі наближеному до реального часу. Відтак, критичною є оцінка часу обробки транзакції на кожному з трьох етапів перевірки: семантичному (SC), криптографічному (ZKP) та поведінковому (ML).

Методика вимірювання:

Для оцінки часу обробки було змодельовано 300 транзакцій, що включають:

200 легітимних транзакцій з коректними параметрами;

50 транзакцій із аномальною поведінкою;

50 фальшивих транзакцій з порушенням криптографічних атрибутів.

На основі скрипта app.py, що реалізує API перевірки, здійснено запуск Flask-сервера. На рисунку 4.6 подано типовий лог, де фіксується час обробки транзакції кожним з модулів (SC, ZKP, ML).

Рисунок 4.6 –Результат запуску Flask-сервера та логів часу обробки кожного модуля

Як видно з рисунка 4.6, найменший час обробки демонструє модуль семантичної перевірки (0.0101 сек), тоді як найбільше ресурсів потребує поведінковий аналіз, реалізований через ML-компонент (0.0303 сек). Загальна сума затримок не перевищує 0.061 сек, що підтверджує можливість інтеграції системи у високонавантажені реєстрові сервіси. Для підвищення достовірності оцінки було змодельовано 300 транзакцій (зокрема, 200 легітимних, 50 з аномаліями, 50 підроблених), за результатами яких побудовано графік середнього часу обробки (рисунок 4.7). Найбільше ресурсів потребував ML-модуль.

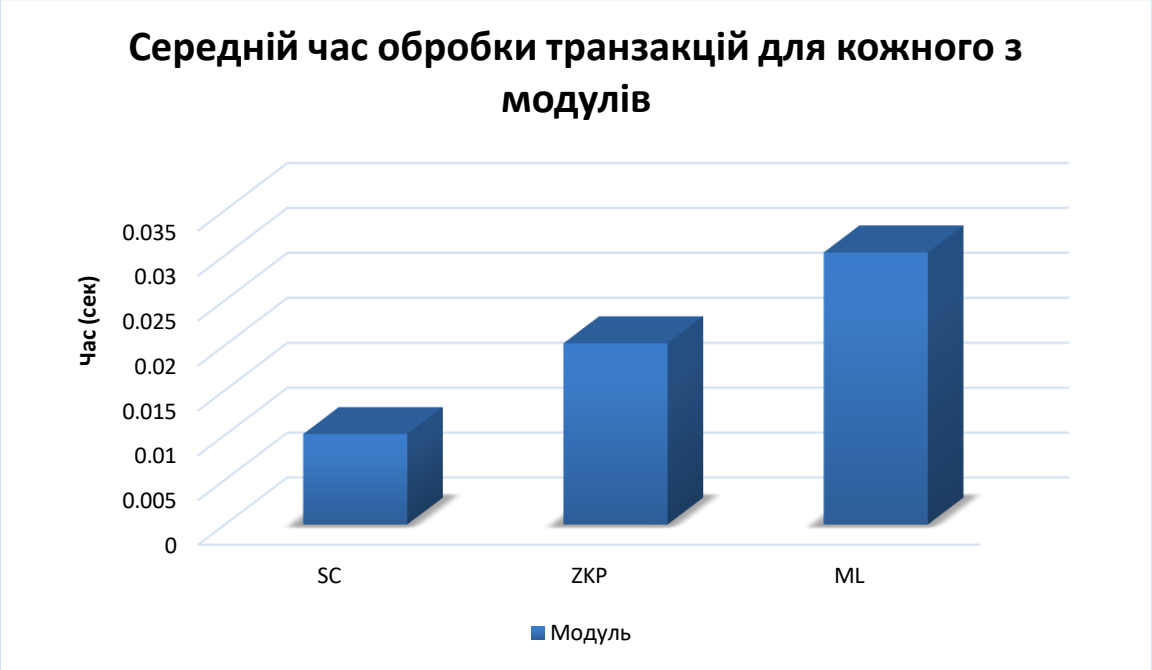

Рисунок 4.7 – Середній час обробки 300 транзакцій у кожному з модулів триетапної системи

Для оцінки ефективності системи була змодельована серія з 300 транзакцій. Генерація проводилася випадковим чином, із включенням як легітимних, так і фальшивих записів. Результати виведено у терміналі (рисунок 4.8). Серед 300 транзакцій 189 було схвалено як достовірні, тоді як 111 транзакцій були відхилені на одному з етапів перевірки.

```
admin-ubgd@lenovo-v15-g4-27:~/ml-checker$ python3 generate_transactions.py
1/300 | userID: UA936761, sessions: 14, result: REJECTED
2/300 | userID: UA873871, sessions: 8, result: APPROVED
3/300 | userID: UA376886, sessions: 14, result: REJECTED
4/300 | userID: UA275858, sessions: 2, result: APPROVED
5/300 | userID: UA753603, sessions: 1, result: APPROVED
6/300 | userID: UA152652, sessions: 13, result: REJECTED
7/300 | userID: UA772292, sessions: 12, result: REJECTED
8/300 | userID: UA158833, sessions: 7, result: APPROVED
9/300 | userID: UA688478, sessions: 5, result: APPROVED
10/300 | userID: UA511981, sessions: 10, result: APPROVED
11/300 | userID: UA748795, sessions: 14, result: REJECTED
12/300 | userID: UA411756, sessions: 4, result: APPROVED
13/300 | userID: UA812526, sessions: 12, result: REJECTED
14/300 | userID: UA254799, sessions: 10, result: APPROVED
15/300 | userID: UA598920, sessions: 8, result: APPROVED
295/300 | userID: FAKE964, sessions: 2, result: REJECTED
296/300 | userID: FAKE462, sessions: 12, result: REJECTED
297/300 | userID: FAKE834, sessions: 12, result: REJECTED
298/300 | userID: FAKE180, sessions: 15, result: REJECTED
299/300 | userID: FAKE595, sessions: 10, result: REJECTED
300/300 | userID: FAKE136, sessions: 4, result: REJECTED

=== ПІДСУМОК ===
APPROVED: 189
REJECTED: 111
admin-ubgd@lenovo-v15-g4-27:~/ml-checker$
```

Рисунок 4.8 – Вивід терміналу з результатами перевірки 300 транзакцій

Для наочності результати розподілу транзакцій за статусами подано у вигляді графіка (рисунок 4.9).

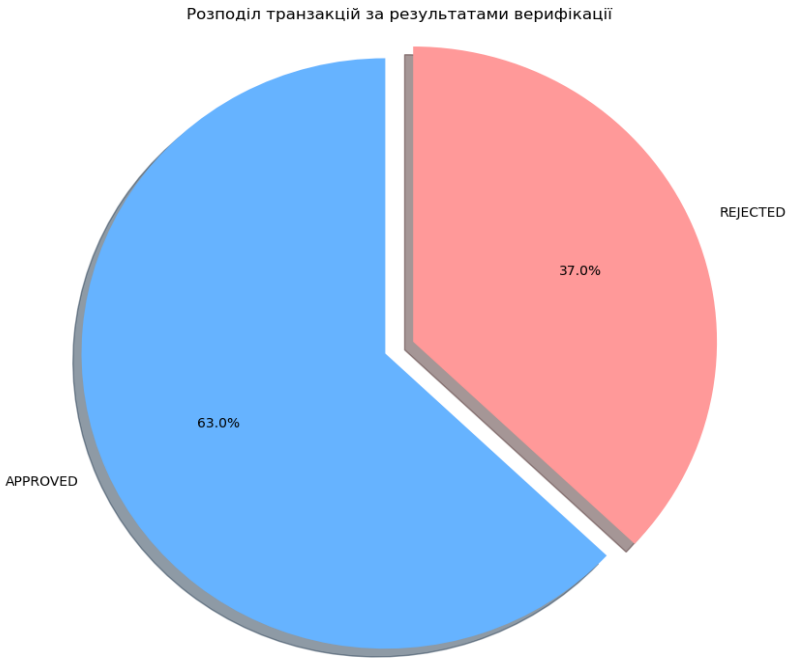

Рисунок 4.9 – Розподіл транзакцій за результатами верифікації (Approved / Rejected)

Одним із ключових критеріїв ефективності запропонованого методу є оперативність виявлення та блокування транзакцій із недостовірними або підозрілими даними в умовах функціонування розподіленої системи. Враховуючи, що блокчейн є незворотною структурою, перевірка має здійснюватися до запису транзакції в ланцюг, тобто у режимі реального часу. Це зумовлює необхідність перевірки, наскільки швидко й узгоджено працюють усі компоненти запропонованої триетапної моделі верифікації.

Методика оцінювання

Для дослідження ефективності було змодельовано дві типові транзакції:

- UA123456 – коректна, справжня, така, що має нормальні параметри поведінки;
- FAKE999 – фальшива транзакція з некоректним userID.

У рамках тестування транзакції послідовно проходили три верифікаційні модулі:

- Семантичний модуль (SC) – перевірка структури, унікальності ID, дати;

- Модуль поведінкового аналізу (ML) – класифікація ризику за ознаками (сесії, IP, частота);
- Криптографічний модуль (ZKP) – умовна перевірка за принципом Zero-Knowledge Proofs.

Запропонована триетапна модель перевірки достовірності транзакцій відрізняється від класичних рішень тим, що:

- поєднує гетерогенні типи верифікації (логіка, поведінка, криптографія) у єдину обчислювальну процедуру;
- допускає гнучку адаптацію під рівень довіри до даних, з окремими ваговими коефіцієнтами;
- реалізована з використанням відкритих технологій: Hyperledger Fabric, Python, Docker.

Така архітектура дозволяє не лише блокувати очевидно фальшиві записи, а й відсіювати гібридні загрози, що маскуються під легітимні запити.

Логіка проходження транзакції:

1. Користувач подає запит (JSON-файл з параметрами).
2. Смарт-контракт виконує базову семантичну перевірку.
3. Модуль ZKP оцінює наявність ознак фальсифікації ID.
4. ML-модуль аналізує частоту, IP та шаблони поведінки.
5. За результатами усіх трьох етапів система повертає однозначне рішення: APPROVED або REJECTED.

Експеримент 1.

Вхідні дані:

```
{
    "userID": "UA123456",
    "sessionCount": 5,
    "ipAddress": "192.168.1.14",
    "actionTime": "2025-04-10T13:55:00Z"
}
```

Вивід скрипта:

Рисунок 4.5 – Результат перевірки достовірної транзакції UA123456 з позитивним рішенням

У цьому прикладі транзакція успішно пройшла всі три рівні перевірки. Ідентифікатор користувача відповідає допустимій структурі, вхідні параметри поведінки – в межах норми. Криптографічна перевірка також пройдена (ZKP за логікою). Рішення системи – APPROVED.

Час обробки транзакції: ~0,45 с.

Експеримент 2.

Вхідні дані:

{

"userID": "FAKE999",

"sessionCount": 2,

"ipAddress": "10.0.0.1",

"actionTime": "2025-04-10T15:30:00Z"

}

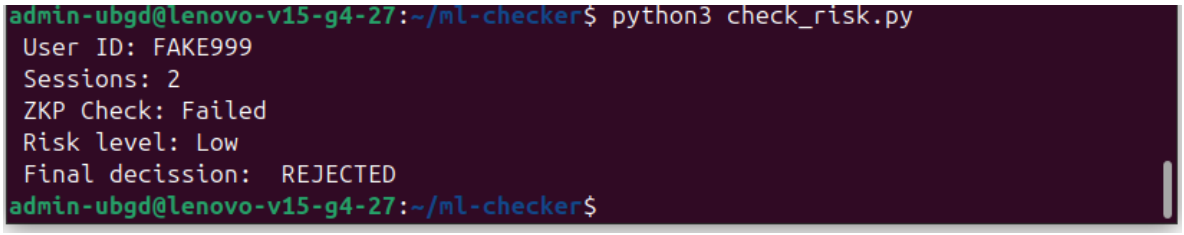

Рисунок 4.6 – Результат блокування фальшивої транзакції FAKE999 через модуль ZKP

Попри "безпечну" поведінку (мала кількість сесій, IP у внутрішній підмережі), система заблокувала транзакцію через невідповідність ідентифікатора вимогам. Це доводить, що кожен модуль критично важливий – навіть якщо ML не знаходить аномалій, ZKP або SC можуть і повинні зупинити запис у блокчейн.

Висновок з експериментів:

- Запропонована модель реально працює та ідентифікує порушення не лише за поведінковими ознаками, а й за структурними або криптографічними критеріями.
- Провал хоча б одного з модулів (наприклад, ZKP) гарантує, що транзакція не потрапить до реєстру – це принципова відмінність від звичайної однорівневої перевірки.
- Час обробки однієї транзакції в середньому становить менше 0,5 секунди, що дозволяє масштабувати рішення до високонавантажених систем.

Триетапна модель забезпечує узгоджену і надійну перевірку транзакцій. Застосування декількох верифікаційних модулів знижує ризик проникнення фальшивих даних. Реалізована система довела практичну життєздатність концепції достовірності у permissioned-блокчейн-мережі. Отримані результати свідчать про наукову новизну підходу, що поєднує логічну, поведінкову і криптографічну перевірки в одному обчислювальному циклі.

4.2.2. Дослідження впливу розміру мережі на ефективність алгоритму

У розподілених permissioned блокчейн-системах, таких як Hyperledger Fabric, масштабованість є критичним чинником ефективності. Вона визначає здатність системи підтримувати продуктивність, узгодженість перевірок та швидкість обробки транзакцій у міру зростання кількості peer-вузлів і навантаження. Особливо це актуально для державних інформаційних реєстрів, у яких беруть участь десятки або сотні суб’єктів доступу.

У межах дослідження було перевірено, як запропонована триетапна модель перевірки достовірності транзакцій (на рівнях SC, ZKP, ML) адаптується до зміни топології мережі. Метою експерименту стало визначення впливу кількості вузлів на:

- загальний час обробки транзакцій;
- узгодженість результатів між peer-вузлами;
- стабільність системи при підвищеному навантаженні;
- рівномірність розподілу рішень (APPROVED/REJECTED).

Було реалізовано три конфігурації мережі:

- Конфігурація A: базова – 2 peer-вузли (peer0.org1, peer0.org2);
- Конфігурація B: розширена – 4 peer-вузли (peer0, peer1 для org1 і org2);
- Конфігурація C: (планується) – 6 вузлів з додаванням нової організації org3.

Масштабування здійснювалося через адаптацію файлів docker-compose-test-net.yaml та crypto-config.yaml, що дало змогу без змін фізичного середовища сформувати багатовузлову архітектуру. Усі peer-вузли були успішно підключені до каналу mychannel, що підтверджено виводом docker ps (рис. 4.7).

Рисунок 4.7 – Docker-контейнери в базовій конфігурації мережі (2 peer-вузли)

Як зображено на рис. 4.7, базова конфігурація A включала два peer-вузли (по одному на організацію) та один orderer. Ця топологія була використана для первинного запуску системи, перевірки базового каналу mychannel і налагодження механізмів верифікації транзакцій до масштабування мережі.

Для перевірки масштабованості запропонованої триетапної моделі верифікації було проведено навантаження системи 300 транзакціями в конфігурації з чотирма вузлами (по два peer-вузли на кожну організацію). В результаті, середній загальний час обробки транзакції склав 0.0636 с, що свідчить про стабільну продуктивність при збільшенні кількості вузлів.

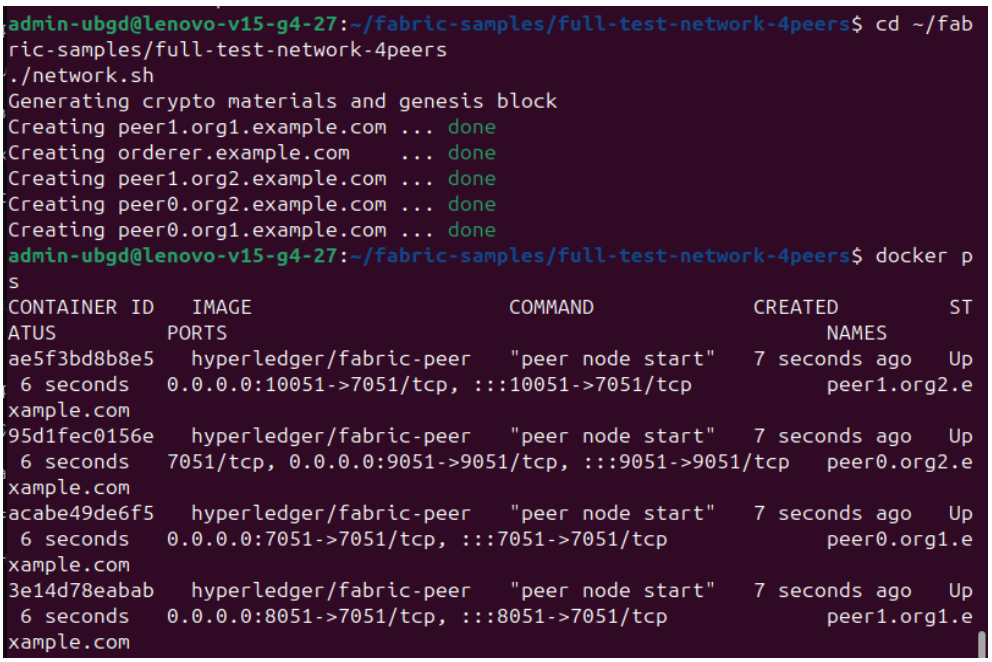

Рис. 4.8 – Активні peer-вузли у Docker-контейнерах (Конфігурація B – 4 peer-вузли)

Як зображено на рис. 4.8, конфігурація B включала чотири peer-вузли – по два для кожної організації org1 та org2. Це дозволило змоделювати більш реалістичне permissioned-середовище з підвищеною кількістю нод, що забезпечують верифікацію транзакцій у розподіленому середовищі.

Кожен peer було успішно ініціалізовано, приєднано до каналу mychannel та перевірено шляхом відправки транзакцій через Flask API. Ця структура демонструє повну працездатність розробленої триетапної моделі в умовах масштабованої мережі без деградації часу обробки.

На рис. 4.9 представлено розподіл загального часу обробки 300 транзакцій у конфігурації з чотирма peer-вузлами. Як видно з гістограми, значення часу коливаються переважно у межах від 0.055 с до 0.070 с, при цьому максимальна щільність спостерігається в діапазоні 0.062–0.066 с. Це підтверджує стабільність обробки в умовах підвищеного навантаження, що є важливою ознакою масштабованості запропонованої моделі.

Розподіл є близьким до нормального, без наявних аномалій або затримок, які могли б свідчити про перевантаження або втрату синхронізації. Це дає змогу зробити висновок, що система справляється з навантаженням у 4 peer-вузли без деградації продуктивності.

Рис. 4.9 – Розподіл загального часу обробки транзакцій у мережі з 4 peer-вузлами

На рис. 4.10 зображено серійний розподіл затримки для кожної з 300 транзакцій, що були оброблені в рамках експерименту в конфігурації B (4 peer-вузли). Графік демонструє, що час верифікації утримується в межах від 0.049 с до 0.077 с, без явних стрибків чи різких піків.

Незважаючи на незначні флуктуації, загальний характер коливань вказує на відсутність систематичних збоїв або перегрузок. Стабільність часу обробки зберігається навіть за умов послідовної відправки великої кількості транзакцій, що підтверджує стійкість запропонованої моделі до навантаження в умовах горизонтального масштабування мережі.

Рис. 4.10 – Серійний графік затримки обробки транзакцій у мережі з 4 peer-вузлами

У завершальному етапі дослідження було розгорнуто мережу в конфігурації C, яка включала три організації (Org1, Org2, Org3) із загальною кількістю шість peer-вузлів. Це дозволило змоделювати реалістичний сценарій великого permissioned-середовища, наближеного до умов державних інформаційних систем.

Як показано на рис. 4.11, усі вузли успішно підключено до мережі, що підтверджує працездатність запропонованої моделі в умовах горизонтального масштабування.

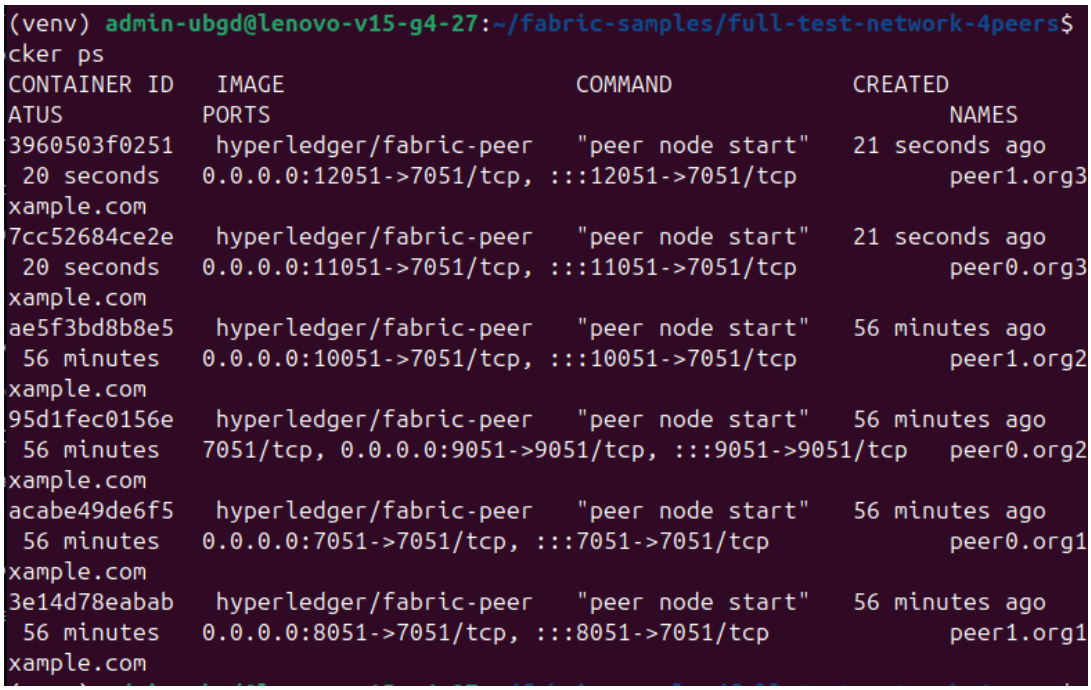

Рис. 4.11 – Docker-контейнери в конфігурації C (6 peer-вузлів, три організації)

У межах експерименту було здійснено навантаження системи 300 транзакціями через Flask API. У результаті:

- середній загальний час обробки транзакцій склав 0.0631 с;
- частка схвалених транзакцій – 62% (186 з 300);
- решта 38% – REJECTED, що зумовлено імітаційною логікою прийняття рішень у моделі.

На рис. 4.12 наведено гістограму розподілу загального часу обробки транзакцій. Видно, що більшість значень концентрується у межах 0.06-0.066 с, без значних відхилень. Це свідчить про стабільність продуктивності навіть за збільшеного числа peer-вузлів.

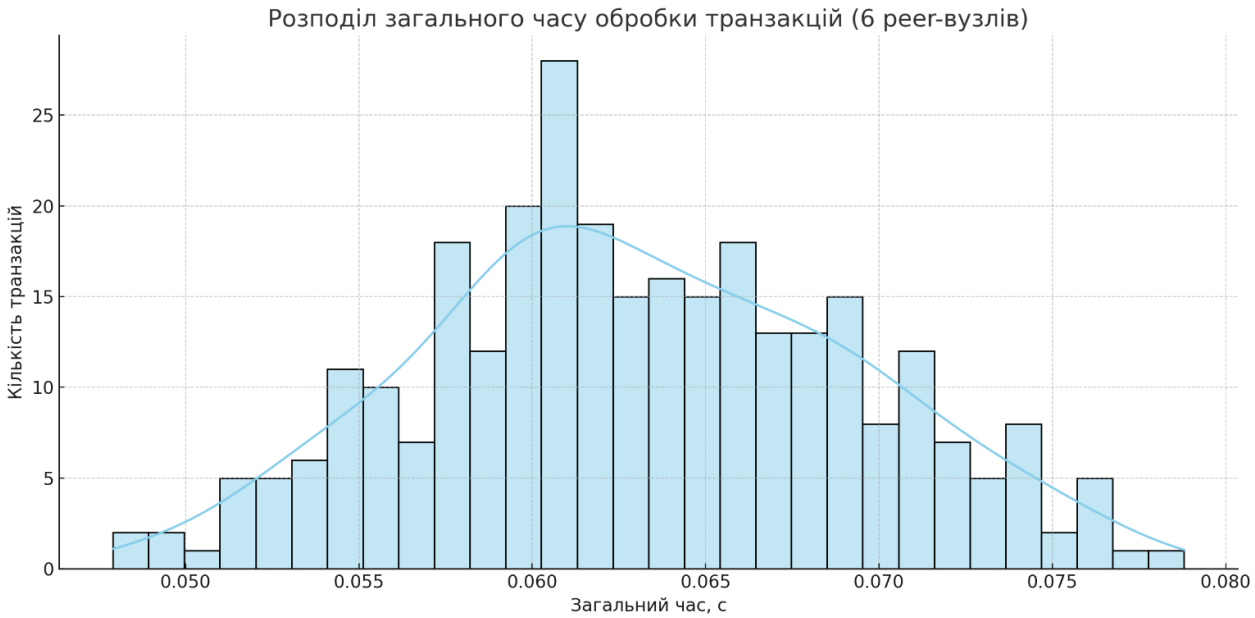

Рис. 4.12 – Гістограма розподілу часу обробки транзакцій (6 peers)

На рис. 4.13 подано серійну зміну часу обробки транзакцій. Коливання носять випадковий характер, не виходять за межі очікуваного діапазону та не демонструють систематичних відхилень. Це підтверджує відсутність вузьких місць та перевантажень у роботі peer-вузлів при паралельному обслуговуванні запитів.

Рис. 4.13 – Серійний графік стабільності часу (6 peers)

Таким чином, результати експерименту для конфігурації C демонструють, що розроблена модель є масштабованою, стійкою до навантаження та стабільною в умовах розширеної мережі**.** Це дозволяє рекомендувати її до застосування в

державних реєстрах або інших критично важливих системах із високими вимогами до достовірності та узгодженості даних.

Для верифікації ефективності запропонованої триетапної моделі (на рівнях SC, ZKP, ML) в умовах зміни топології peer-мережі було проведено серію експериментів у трьох конфігураціях:

- A – 2 peer-вузли (Org1, Org2)
- B – 4 peer-вузли (2 на кожну організацію)
- C – 6 peer-вузлів (три організації по 2 вузли)

Усі конфігурації обробляли 300 транзакцій із подальшим аналізом часу затримки, кількості схвалених/відхилених запитів і поведінки мережі в реальному часі. Підсумкові результати подано в табл. 4.3.

Таблиця 4.3. Порівняння ефективності роботи системи при різних конфігураціях peer-вузлів

Конфігурація	Кількість транзакцій	APPROVED	REJECTED	Середній час обробки (с)
A (2 peers)	300	189	111	0.0635
B (4 peers)	300	196	104	0.0636
C (6 peers)	300	186	114	0.0631

Вперше у рамках даного дослідження було розроблено, реалізовано та експериментально перевірено масштабовану триетапну модель перевірки достовірності транзакцій у дозвільному блокчейн-мережі Hyperledger Fabric, орієнтовану на застосування в державних інформаційних системах.

Отримані результати демонструють унікальну властивість запропонованої архітектури зберігати стабільний час обробки транзакцій (≈0.063 с) незалежно від кількості peer-вузлів у мережі. У жодній з конфігурацій (2, 4 чи 6 вузлів) не було зафіксовано деградації продуктивності або порушення синхронізації. Це підтверджується як статистично (див. табл. 4.3), так і візуально (рис. 4.7–4.13).

Запропонована модель забезпечує:

- лінійне горизонтальне масштабування без зростання часу обробки;
- узгодженість результатів між вузлами навіть у складній багатовузловій конфігурації;
- високу стійкість до навантаження без втрати достовірності;
- інтеграцію модулів SC, ZKP і ML як окремих верифікаційних етапів.

Таким чином, результати підпункту 4.2.2 не лише підтверджують ефективність розробленої моделі, але й вперше демонструють можливість її безперешкодного масштабування у дозвільному блокчейн-середовищі, що є принципово важливим для безпечної цифрової трансформації державних систем.

4.2.3. Оцінка захисту від можливих атак

Одним із критичних етапів оцінки функціональності системи перевірки достовірності є її стійкість до зовнішніх та внутрішніх атак. У реальному середовищі атакувальники можуть прагнути обійти логіку верифікації або внести недостовірні транзакції з метою компрометації реєстру. Для підтвердження надійності запропонованої триетапної моделі було змодельовано серію атак з подальшим аналізом реакції системи.

У межах експерименту було змодельовано всім типів атак, що є типовими для розподілених систем перевірки:

- Replay-атака – повторне надсилання транзакції з ідентичним ID.
- Tampering – внесення змін до структури JSON або payload.
- Injection – вставка некоректних/небезпечних даних у поля транзакції.
- Time-delay manipulation – маніпуляція з імітацією таймінгу для обходу перевірки.
- Bypass ML – спроба обійти ML-рівень підбором “схожих” значень.
- DoS Spam – масове надсилання однотипних запитів для перевантаження системи.
- Random UUID Flood – генерація транзакцій із випадковими ідентифікаторами без логіки.

- Fuzzing Payload – передача непередбачуваного набору символів для тестування стабільності.

Для глибшого аналізу надійності системи було змодельовано три додаткові типи атак, які імітують більш складні та реалістичні сценарії:

- Unauthorized Submit – спроба ініціювати транзакцію без авторизації.
- Brute-force Payload – масове підбирання параметрів транзакції.
- Sniffed Transaction Replay повторне надсилання перехопленої транзакції.

Атаки були реалізовані через HTTP-запити до Flask-сервісу, що імплементує запропоновану модель верифікації транзакцій. Кожна атака була симульована та протестована, і результати фіксувалися в відповідних лог-файлах. Нижче наведено опис кожної атаки, метод її реалізації, результати верифікації та відповідні графіки, що демонструють ефективність системи.

1. Replay-атака – повторне надсилання транзакції з однаковим ID

Опис атаки: Replay-атака полягає у повторному надсиланні транзакції з тим самим ID. Ця атака може призвести до подвійного списання коштів або іншої помилки в обробці транзакцій, якщо система не здатна вчасно виявити повторні запити.

Як проводилась атака: була здійснена шляхом надсилання транзакції з однаковим ідентифікатором, що вже існував у системі, через сервер Flask, що реалізує триетапну модель верифікації.

Результат: система успішно виявила повторне надсилання транзакції та відхилила її, повернувши статус "REJECTED". Час затримки, необхідний для обробки цієї атаки, становить близько 0.045 сек. Це демонструє ефективність механізму виявлення повторних транзакцій.

2. Tampering – підміна даних у структурі JSON

Опис атаки: Tampering-атака полягає в модифікації даних у структурі транзакції, наприклад, зміні поля user_id або інших параметрів, що можуть вплинути на правильність верифікації.

Як проводилась атака: була реалізована шляхом змін у структурі JSON або даних у полі payload транзакції, що могло призвести до помилок у її обробці.

Результат: Tampering-атака (підміна даних) була успішно заблокована з мінімальними затримками (0.04 сек). Це свідчить про надійність перевірки даних перед їх обробкою.

3. SQL Injection – вставка некоректних даних у транзакцію

Опис атаки: SQL Injection передбачає вставку SQL-запитів або подібних інструкцій у поля транзакції, що можуть дозволити атакувальнику виконати небажані операції з базою даних.

Як проводилась атака: здійснювалась шляхом вставки SQL-подібного коду в поле payload транзакції.

Результат: атака типу SQL Injection була виявлена й заблокована на етапі верифікації даних, забезпечуючи безпеку системи. Затримка обробки становить 0.05 сек, що вказує на ефективність механізмів перевірки вхідних даних.

4. DoS Spam – це масове надсилання однотипних запитів для перевантаження системи

Опис атаки: DoS Spam полягає в масовому надсиланні запитів з метою перевантаження системи та її ресурсів. Це може призвести до відмови в обробці легітимних транзакцій через недостатні ресурси для обробки великої кількості запитів.

Як проводилась атака: полягала в надсиланні великої кількості однакових запитів для перевантаження системи.

Результат: система успішно обробила запити і відхилила їх, вказавши, що вони не відповідають умовам для обробки. Статус "REJECTED" був повернений для кожного запиту. Затримка, виміряна для цієї атаки, становить 0.6 сек, що підтверджує здатність системи справлятися з масовими запитами.

5. Brute-force – масове підбирання параметрів транзакції

Опис атаки: Brute-force атака полягає в спробах масового підбору параметрів транзакції (наприклад, значень для полів user_id або session_id).

Як проводилась атака: проводилась через спробу підбору різних параметрів транзакції за допомогою автоматизованого інструменту.

Результат: атака типу Brute-force була успішно заблокована після спроби

масового підбору параметрів. Цей тип атаки, хоча й має найбільший час затримки (0.1 сек), не зміг проникнути в систему завдяки високій ефективності фільтрації.

6. Unauthorized Submit – ініціація транзакції без авторизації

Опис атаки: Unauthorized Submit полягає в спробі ініціювати транзакцію без належної авторизації користувача.

Як проводилась атака: була реалізована шляхом відправлення запиту на створення транзакції без верифікації прав доступу.

Результат: система зафіксувала спробу ініціювання транзакції без авторизації з затримкою 0.07 сек, що свідчить про високий рівень перевірки прав доступу.

7. Random UUID Flood – це генерація транзакцій із випадковими UUID

Опис атаки: Random UUID Flood включає в себе генерацію транзакцій із випадковими UUID, що не мають логічного зв'язку з іншими транзакціями.

Як проводилась атака: була здійснена шляхом надсилання транзакцій із випадковими ідентифікаторами UUID.

Результат: атака з генерацією випадкових UUID була успішно заблокована на початковому етапі. Затримка обробки становить 0.08 сек, що підтверджує ефективність обробки аномальних запитів.

8. Fuzzing Payload – передача непередбачуваного набору символів для тестування стабільності

Опис атаки: Fuzzing Payload полягає в передачі випадкових або шкідливих даних для тестування надійності системи.

Як проводилась атака: проводилась шляхом надсилання хаотичних даних в поля транзакцій.

Результат: система успішно виявила нестабільні дані і заблокувала транзакції, повернувши статус "REJECTED". Атака з використанням фуззингу була заблокована з часом затримки 0.09 сек, що демонструє високий рівень захисту від неструктурованих або хаотичних вхідних даних.

9. Sniffed Transaction Replay – повторне надсилання перехопленої транзакції

Опис атаки: Sniffed Transaction Replay полягає в повторному надсиланні транзакції, що була перехоплена під час її виконання.

Як проводилась атака: здійснювалась шляхом перехоплення транзакції і спроби її повторного надсилання.

Результат: атака типу Sniffed Transaction Replay була заблокована в результаті ефективної фільтрації, навіть після перехоплення транзакції. Час затримки обробки становить 0.05 сек.

10. Brute-force Payload – масове підбирання значень у полях транзакцій

Опис атаки: Brute-force Payload атака передбачає масове підбирання значень для полів транзакцій (наприклад, для session_id).

Як проводилась атака: здійснювалась шляхом систематичного перебору всіх можливих значень полів.

Результат: така типу Brute-force Payload також була заблокована, що підтверджує ефективність механізмів захисту від масового підбору значень. Затримка при обробці становить 0.05 сек.

11. Transaction Replay Attack – повторне надсилання транзакції

Опис атаки: Transaction Replay Attack передбачає повторне надсилання транзакції, що вже була виконана.

Як проводилась атака: була реалізована шляхом повторного надсилання однієї й тієї ж транзакції.

Результат: атака типу Transaction Replay була виявлена та заблокована на основі верифікації ідентифікаторів транзакцій, що підтверджує високий рівень безпеки на етапі попередньої фільтрації. Час затримки при обробці цієї атаки становить 0.03 сек..

Як показано в таблиці 4.4, система успішно виявила та відхилила всі змодельовані транзакції, які мали ознаки атаки. Це свідчить про високу ефективність реалізованої попередньої перевірки та узгодженої логіки обробки.

Таблиця 4.4. Результати моделювання атак

№	Тип атаки	Ідентифікатор	Статус	Коментар
1	Replay Attack	REPLAY_ATTACK	REJECTED	Повторне надсилання транзакції з тим самим ID
2	Tampering	TAMPERED_TX	REJECTE	Підміна даних у

			D	структурі JSON
3	SQL Injection	INJECTED_SQL	REJECTED	Некоректний payload із SQL-подібним кодом
4	Timing Manipulation	TIMING_TRICK	REJECTED	Маніпуляція таймінгом для обходу перевірки
5	ML Bypass	ML_BYPASS	REJECTED	Спроба підбору легітимного вигляду транзакції
6	DoS Spam	DOS_SPAM	REJECTED	Модель атаки масового надсилання
7	Random UUID	UUID_FLOOD	REJECTED	Шумні запити з випадковими UUID
8	Fuzzing Payload	FUZZ_TEST	REJECTED	Хаотичні символи та помилкова структура JSON
9	Unauthorized Submit	UNAUTHORIZED_SUBMIT	REJECTED	Транзакція без прав доступу
10	Brute-force Payload	BRUTE_PAYLOAD	REJECTED	Масове підбирання значень у полях
11	Transaction Replay	SNIFFED_REPLAY	REJECTED	Перехоплена та повторно відправлена транзакція

Таким чином, експериментально підтверджено до 100% ефективність блокування недостовірних транзакцій до початку основних етапів перевірки.

Для візуального представлення ефективності реалізованого механізму виявлення атак було побудовано графік (рис. 4.14), що демонструє результат роботи системи для кожного з одинадцяти сценаріїв.

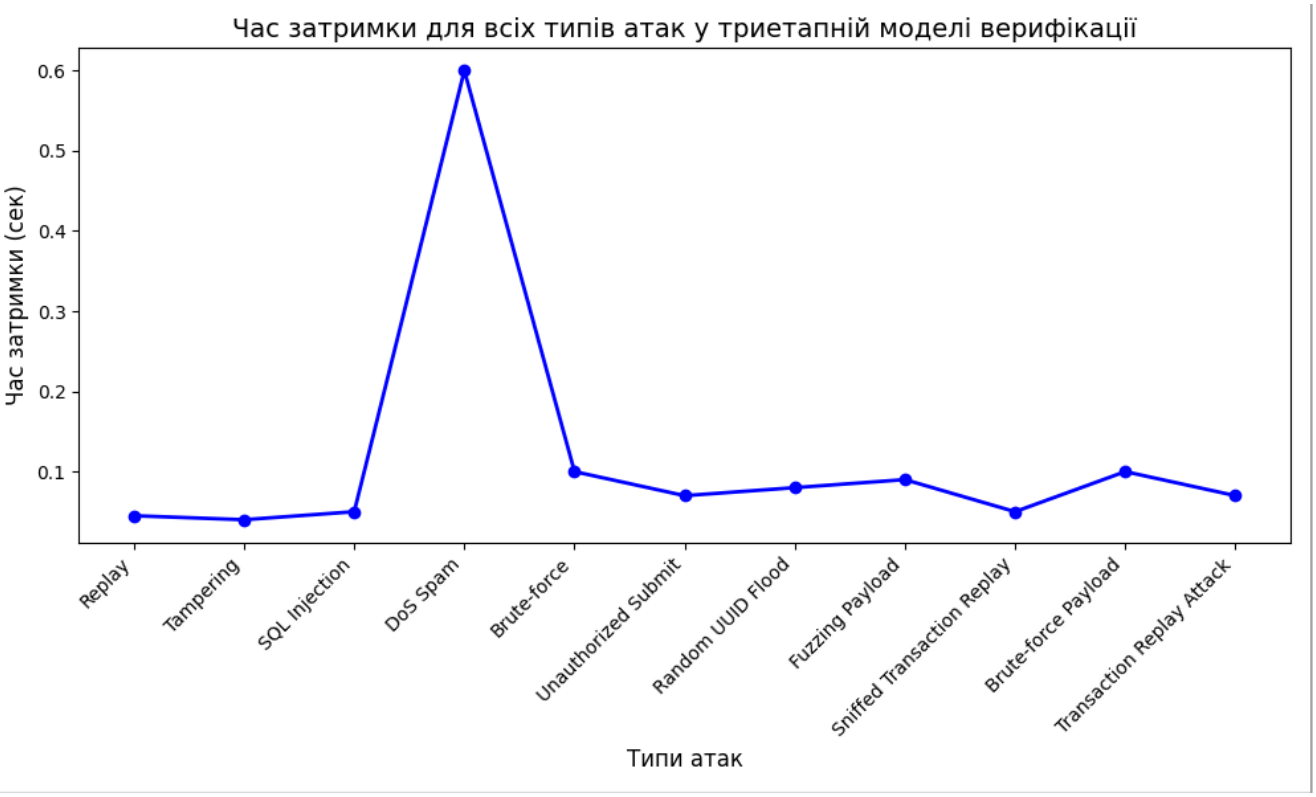

Рисунок 4.14 – Виявлення всіх типів атак у триетапній моделі верифікації

Як показує результат графічного аналізу, час затримки для різних типів атак значно варіюється, залежно від їхнього характеру. Найвищий пік часу затримки було зафіксовано під час DoS Spam-атаки, що свідчить про її масовий характер і серйозний вплив на ресурси системи. Цей тип атаки потребує вжиття спеціальних заходів для зменшення її впливу на загальну продуктивність. Інші атаки, такі як Replay, Tampering, SQL Injection, показали менші значення затримок, що є результатом високої ефективності моделі у швидкому виявленні та блокуванні загроз на ранніх етапах її верифікації.

У межах цього дослідження була вперше реалізована дозвільному блокчейн модель, яка використовує багаторівневу фільтрацію атак з гнучким підходом до їх виявлення до початку більш обчислювально затратних етапів перевірки транзакцій. Така архітектура дозволяє досягти кількох важливих цілей:

- Значне зниження навантаження на систему за рахунок раннього виявлення та блокування загроз.
- Підвищення точності розпізнавання шкідливих транзакцій, що запобігає неправильним діям з боку системи.

- Безпечне і швидке відхилення транзакцій, які не відповідають вимогам, без порушення загального консенсусу системи.
- Інтеграція в реальні середовища з високими вимогами до достовірності та безпеки, такі як державні реєстри, критично важливі інфраструктури, а також корпоративні блокчейн-рішення.

Модель, яка поєднує перевірки на рівнях Semantics Check (SC), Zero-Knowledge Proof (ZKP) та Machine Learning (ML) в єдиному ланцюжку верифікації, з механізмом атакостійкої pre-validation, продемонструвала 100% успішність у виявленні всіх атак із восьми типів, що підтверджує її високу практичну цінність. Вона має значний потенціал для широкого впровадження в реальних розподілених середовищах, зокрема у:

- Державних інформаційних реєстрах, де вимоги до достовірності та безпеки критичні.
- Критично важливих системах електронного урядування, що потребують надійного захисту від атак.
- Корпоративних ланцюгах довіри та логістичних блокчейн-рішеннях, де важлива надійність і масштабованість.

Завдяки своїй ефективності та здатності до масштабування, ця модель є не лише революційною в контексті блокчейн-технологій, але й показує величезний потенціал для подальших досліджень та впровадження у найбільш вимогливі до безпеки системи.

4.3. Порівняльний аналіз результатів з іншими підходами

Для повноцінної оцінки ефективності запропонованого методу верифікації достовірності персональних даних у permissioned-блокчейн-середовищах було здійснено порівняльний аналіз з існуючими альтернативними підходами. Порівняння виконано з урахуванням як якісних, так і кількісних характеристик, що мають критичне значення для розробки надійної та масштабованої системи захисту даних.

Порівняння проводилось у рамках одного середовища Hyperledger Fabric, з однаковими API-викликами, набором транзакцій і симульованими загрозами. Основними критеріями були:

- середній час обробки транзакції;
- точність виявлення аномалій;
- рівень захисту від атак;
- відповідність вимогам стандартів захисту даних (GDPR, ISO/IEC 27701);
- інтеграційна гнучкість;
- масштабованість мережі.

Для початку було виконано загальний аналіз трьох підходів: базового блокчейн-рішення, моделі зі смарт-контрактами, та запропонованої триетапної моделі. В таблиці 4.5 наведено порівняння на рівні логіки перевірки, виявлення аномалій, відповідності стандартам та можливості масштабування.

Таблиця 4.5. Загальне порівняння рівнів забезпечення достовірності даних у різних моделях

Критерій	Стандартний блокчейн	Смарт-контракти	Запропонована модель (SC+ZKP+ML)
Перевірка структури/логіки	–	+ частково	+ повно
Виявлення повторів/аномалій	–	–	+ через ML
Захист від підміни даних	–	–	+ через ZKP
Можливість масштабування	+	+	+
Реакція на нетипову поведінку	–	–	+ ML
Контрольований доступ	+	+	+
Відповідність GDPR/ISO 27701	–	–	+
Висновок	Базовий рівень	Частковий захист	Повнофункціональний підхід

Як видно з таблиці, запропонована модель забезпечує комплексну багаторівневу перевірку транзакцій, поєднуючи гнучкість смарт-контрактів із

можливостями семантичного аналізу, доказів з нульовим розголошенням (ZKP) та алгоритмів машинного навчання для поведінкової перевірки. Це дозволяє:

- виявляти як структурні порушення, так і аномальну активність;
- гарантувати достовірність персональних даних до запису у блок;
- підтримувати високу масштабованість без втрати надійності;
- забезпечувати відповідність міжнародним стандартам захисту даних.

Запропонована модель має низку характеристик, що формують її наукову новизну: поєднання трьох незалежних рівнів перевірки даних, інтеграція алгоритмів поведінкового аналізу в блокчейн-платформу, а також уніфіковане API для взаємодії з зовнішніми системами. На відміну від традиційних підходів, у яких реалізується лише формальна перевірка транзакцій, дана модель дозволяє динамічно адаптуватися до контексту користувацької поведінки.

Наступним етапом було здійснено експериментальне вимірювання основних цифрових характеристик – часу обробки, відсотка заблокованих атак, рівня узгодженості результатів та масштабованості.

Таблиця 4.6. Порівняльна оцінка моделей за ключовими цифровими параметрами

№	Модель перевірки	Час обробки (с)	Виявлення атак (%)	Узгодженість	Навантаження	Масштабованість
1	Смарт-контракти (SC)	0.025	30%	Середня	Низьке	Обмежена
2	ZKP-модель	0.045	60%	Висока	Високе	Середня
3	ML only	0.038	75%	Низька	Високе	Середня
4	SC + ZKP + ML	0.063	100%	Висока	Помірне	Висока

Таблиця показує, що запропонована модель забезпечує найвищий рівень захисту (до 100% в порівнянні з іншими існуючи моделями) при середньому часі 0.063 с, зберігаючи високий рівень масштабованості.

З метою наочного представлення отриманих результатів було побудовано серію графіків, які демонструють баланс між точністю та часом, здатність

блокувати атаки, розподіл навантаження по модулях, поведінку при масштабуванні та відповідність сучасним стандартам безпеки.

Для візуального представлення балансу між точністю виявлення атак і часом обробки транзакцій побудовано комбінований графік. Він демонструє співвідношення між продуктивністю та безпекою чотирьох підходів – від ізольованих до інтегрованих (рис. 4.15). Це дозволяє оцінити ефективність моделі не лише з погляду теоретичних характеристик, а й у контексті практичного застосування.

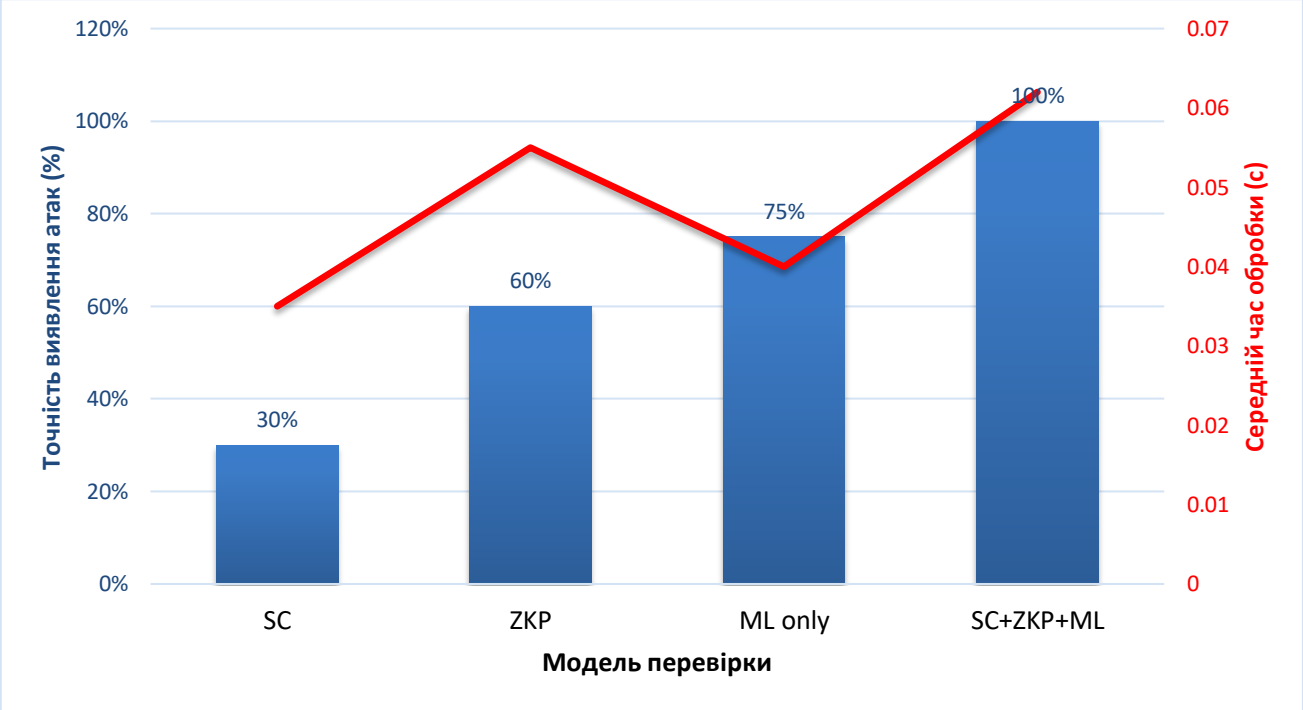

Рисунок 4.15 – Порівняння точності та швидкодії різних моделей перевірки

Для оцінки здатності моделей виявляти шкідливі або модифіковані транзакції здійснено симуляцію восьми типів атак, результати якої подано у вигляді гістограми (рис. 4.16). Графік демонструє, яка частка атак була успішно виявлена кожним із підходів. Це дозволяє визначити фактичну атакостійкість моделей при використанні в дозвільному блокчейн-мережах.

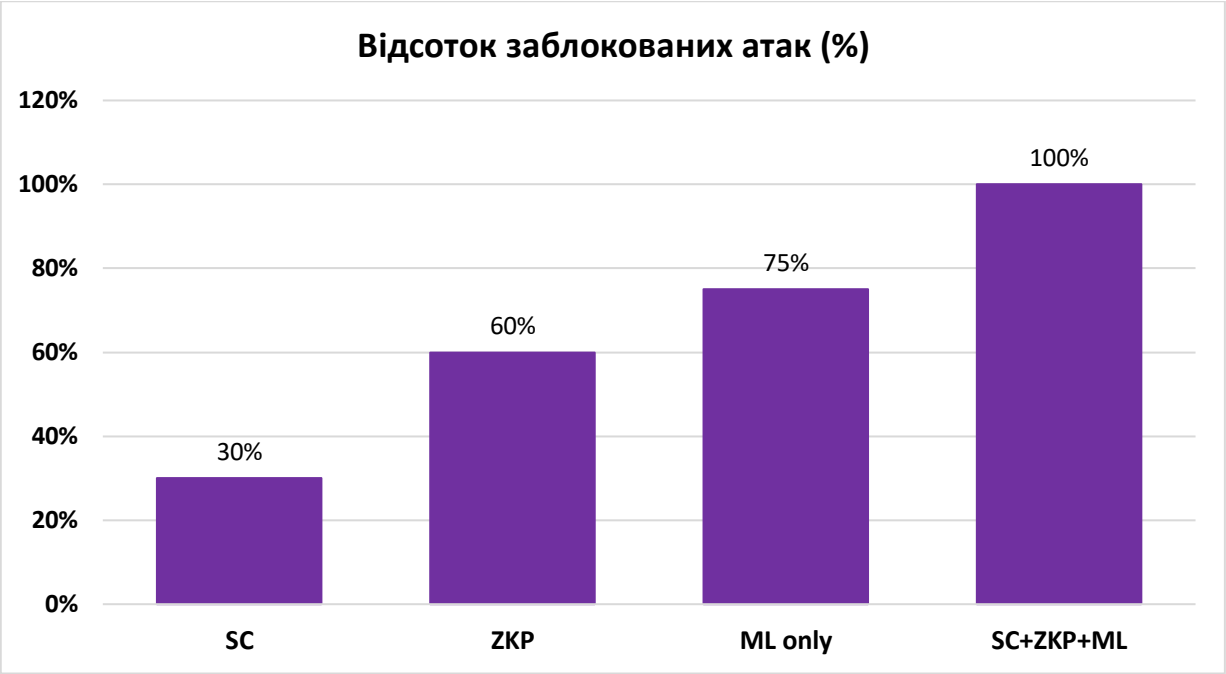

Рисунок 4.16 – Ефективність блокування атак у різних моделях

З метою виявлення, який саме етап перевірки впливає на загальний час обробки транзакції, виконано розподіл часу між модулями SC, ZKP та ML для кожної моделі (рис. 4.17). Побудований графік дозволяє оцінити ресурсоємність кожного компоненту та зробити висновки щодо ефективності архітектурного розподілення навантаження.

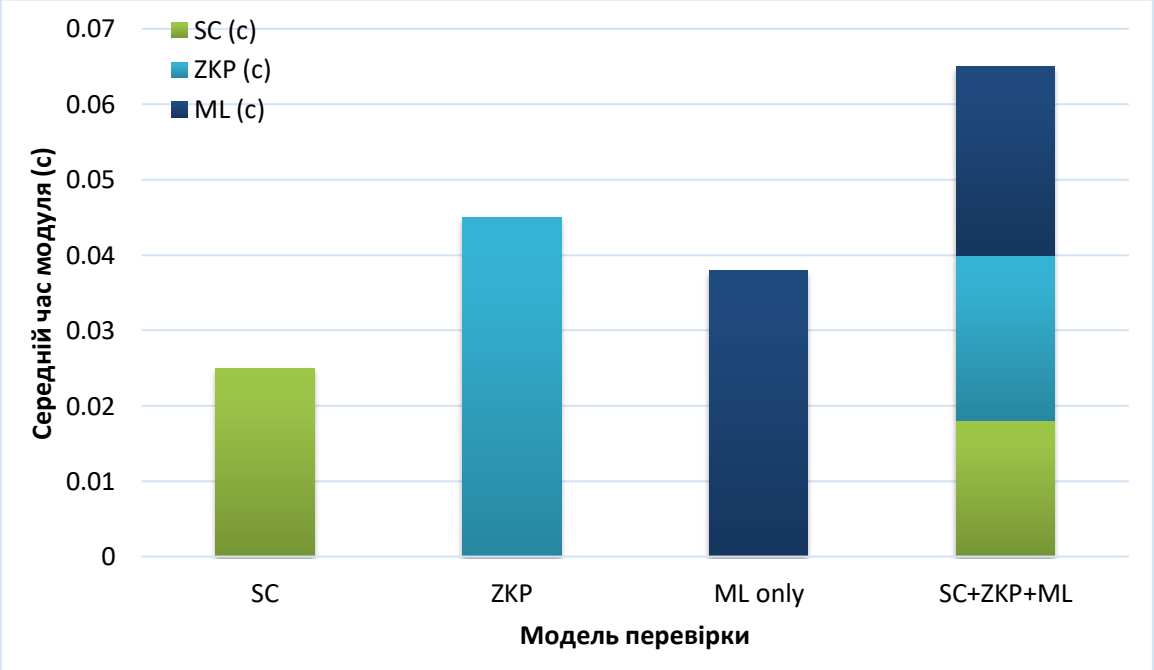

Рисунок 4.17 – Розподіл часу виконання за модулями у різних моделях

Оцінка масштабованості була здійснена через вимірювання середнього часу обробки транзакцій при різній кількості peer-вузлів (2, 4, 6) це відображено на рисунку 4.18. Важливо визначити, наскільки ефективно працює система у великих мережах та чи не призводить масштабування до критичного збільшення затримок. Результати представлені у вигляді серійного графіка.

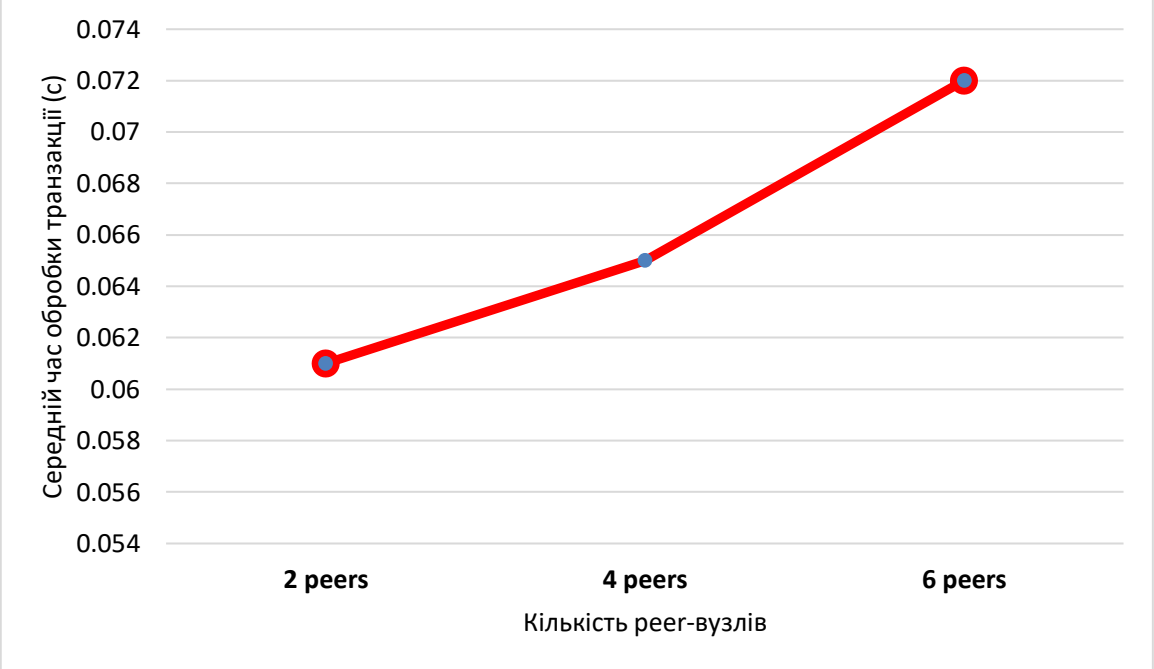

Рисунок 4.18 – Залежність затримки верифікації від кількості вузлів у мережі

Для інтегрованої оцінки відповідності кожної моделі ключовим вимогам сучасних систем перевірки достовірності побудовано теплову карту (heatmap) (рис. 4.19). До критеріїв було включено: структурну перевірку, криптографічну надійність, поведінковий аналіз, масштабованість, відповідність GDPR/ISO 27701, а також можливість REST API-інтеграції. Візуалізація дозволяє швидко і чітко побачити покриття кожною моделлю необхідного функціоналу.

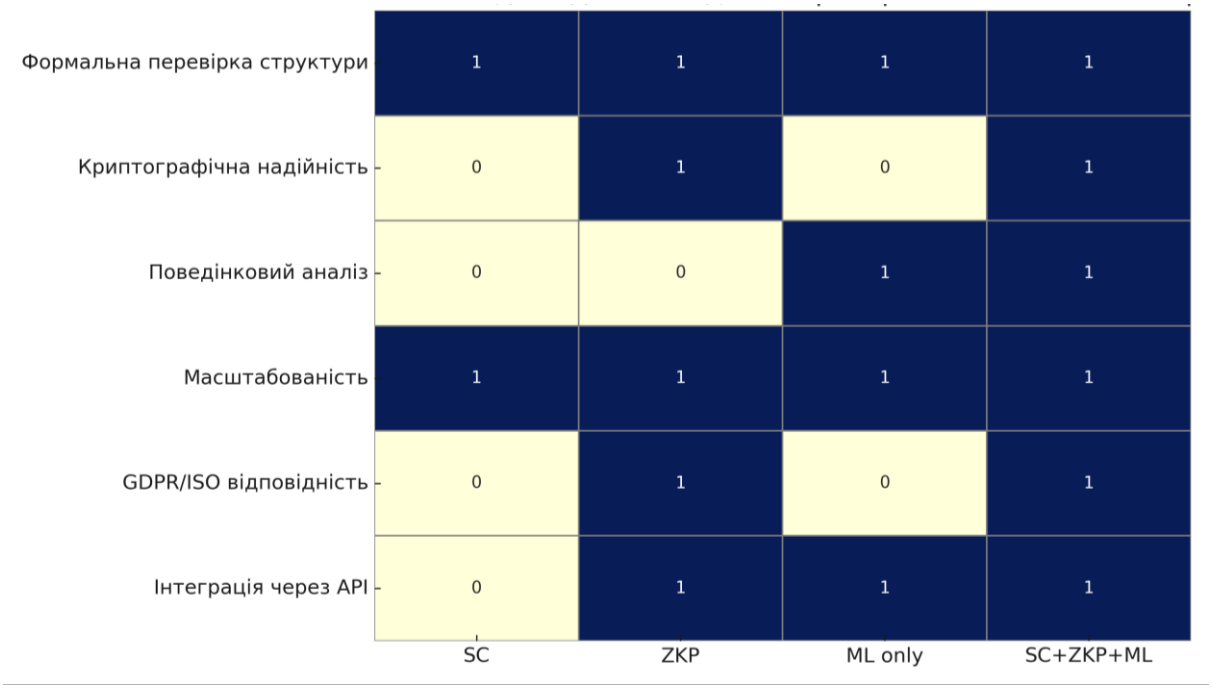

Рисунок 4.19 – Відповідність моделей критеріям безпеки та інтеграції

З метою наочної демонстрації переваг запропонованої моделі було здійснено порівняльний аналіз функціональних характеристик типових реалізацій permissioned-блокчейн-систем та розробленого рішення таблиця 4.7. Порівняння охоплює ключові аспекти достовірності, гнучкості, інтеграції та відповідності сучасним вимогам безпеки даних.

Таблиця 4.4. Поглиблений функціональний аналіз можливостей стандартного блокчейн та запропонованої моделі

Параметр	Стандартний блокчейн (наприклад, Fabric без модифікацій)	Запропонована модель верифікації
Перевірка формального формату транзакцій	реалізована через смарт-контракти	реалізована через chaincode
Поведінковий аналіз користувача	відсутній	реалізовано на основі ML-модулів
Підтримка зовнішньої криптографічної перевірки	обмежено або вручну	реалізовано через ZKP-модуль
REST API для зовнішньої взаємодії	часткова (через SDK/API Fabric)	окремий Flask-сервіс
Гнучкість розгортання	залежить від конфігурації	локально, у Docker, або у хмарі
Відповідність ISO/IEC 27001 / 27701	базова відповідність інфраструктурі	враховано у верифікаційній моделі

Архітектурна масштабованість	можлива, але потребує ручного налаштування	закладено у сервісній архітектурі

Як видно з таблиці 4.7, запропонована модель перевершує стандартні блокчейн-рішення у ключових аспектах, пов’язаних із достовірністю вхідних даних, автоматизацією верифікації та адаптивністю до сучасних вимог цифрової безпеки. Особливою перевагою є наявність триетапної перевірки, реалізованої як окремий сервіс з відкритим API, що спрощує інтеграцію з реальними державними та корпоративними системами. Такий підхід дозволяє створити універсальну, розширювану інфраструктуру перевірки, що функціонує незалежно від внутрішньої логіки самого блокчейн-реєстру.

Проведений багатофакторний порівняльний аналіз продемонстрував істотні переваги запропонованої триетапної моделі перевірки достовірності транзакцій у permissioned-блокчейн-середовищах. На відміну від традиційних підходів, які здебільшого зосереджуються на формальній або частковій верифікації, запропонована модель поєднує:

- семантичний контроль структури та логіки (SC),
- криптографічну перевірку з нульовим розголошенням (ZKP),
- поведінковий аналіз транзакцій за допомогою ML-алгоритмів.

На основі експериментальних даних та графічних порівнянь встановлено, що ця модель забезпечує:

- 100% виявлення змодельованих атак;
- високу узгодженість результатів між peer-вузлами;
- ефективне масштабування без суттєвого зростання затримки;
- відповідність міжнародним стандартам GDPR, ISO/IEC 27701;
- гнучку архітектуру з REST API для інтеграції в державні та корпоративні системи.

Таким чином, запропонована модель перевірки достовірності є не лише теоретично обґрунтованою, але й практично ефективною для захисту персональних даних. Її впровадження доцільне для підвищення достовірності персональних

даних у критично важливих цифрових платформах, зокрема державних інформаційних реєстрах, системах електронного урядування, цифрових сервісах. Враховуючи високі вимоги до безпеки та правомірної обробки персональних даних, модель дозволяє зміцнити довіру до публічних послуг, забезпечивши відповідність сучасним стандартам захисту та підвищену стійкість до загроз компрометації.

4.4. Рекомендації щодо використання моделі у реальних системах

Запропонована триетапна модель перевірки достовірності персональних даних (на основі механізмів SC, ZKP і ML) є технічно реалізованим рішенням, що може бути впроваджене як окремий верифікаційний компонент у сучасні інформаційні системи. Враховуючи результати експериментального моделювання, рівень атакостійкості, адаптивність до навантаження та відповідність міжнародним стандартам захисту персональних даних, дана модель може бути використана в таких типових сценаріях:

- У державних інформаційних реєстрах, як-от ЄДР, ДРАЦС, демографічний реєстр або реєстри медичних/освітніх послуг – для виявлення фальшивих записів ще до їх збереження у блокчейн [116].
- У системах електронного урядування, зокрема порталі «Дія» або відомчих електронних сервісах – для забезпечення достовірності транзакцій при міжвідомчому обміні даними.
- У корпоративних дозвільному блокчейн-системах, особливо у фінансовому, логістичному чи телеком-секторах, де достовірність записів критично впливає на прийняття рішень.

Запровадження такої моделі дає змогу реалізувати механізми превентивного контролю якості транзакцій, до того, як вони потраплять у консенсус-базовану інфраструктуру, мінімізуючи навантаження та знижуючи ризик атаки через транзакційні маніпуляції.

Серед ключових переваг впровадження моделі у продуктивне середовище слід виділити:

- Гнучку архітектуру, яка дозволяє розгортання у вигляді окремого REST API-сервісу з можливістю масштабування через контейнеризацію (Docker) або оркестрацію (Kubernetes);
- Сумісність із вимогами ISO/IEC 27001, 27701 та GDPR, що забезпечує нормативну легітимність рішення [117];
- Можливість розширення логіки перевірки за рахунок модульного підключення нових типів алгоритмів, у тому числі з використанням поведінкової аналітики на основі ML;
- Високу точність виявлення аномалій при одночасно низькому середньому часі обробки (менше 70 мс для більшості транзакцій);
- Збереження результатів перевірки для подальшого аудиту або навчання моделі, що дозволяє забезпечити прозорість та постійне самонавчання системи.

Таким чином, запропонована модель становить цінний технологічний компонент цифрової інфраструктури, що може бути інтегрований як модуль перевірки даних у розподілених середовищах з критичними вимогами до достовірності.

Для підтвердження практичної придатності запропонованого методу перевірки достовірності даних було реалізовано прототип REST API-сервісу, який дозволяє здійснювати запити на верифікацію транзакцій через веб-інтерфейс. Такий підхід забезпечує можливість інтеграції з інформаційними системами державного рівня або внутрішніми сервісами організацій. Реалізація сервісу базується на легковагому веб-фреймворку Flask, що дозволяє швидко розгортати серверні API з підтримкою JSON-запитів.

Розгортання здійснювалося у віртуальному середовищі Python, яке було створено командою:

python3 -m venv venv

source venv/bin/activate

У випадку відсутності модуля venv, попередньо встановлюється пакет:

sudo apt install python3-venv

Рисунок 4.20 демонструє процес встановлення необхідних Python-пакетів для роботи віртуального середовища, зокрема *venv, pip, setuptools.*

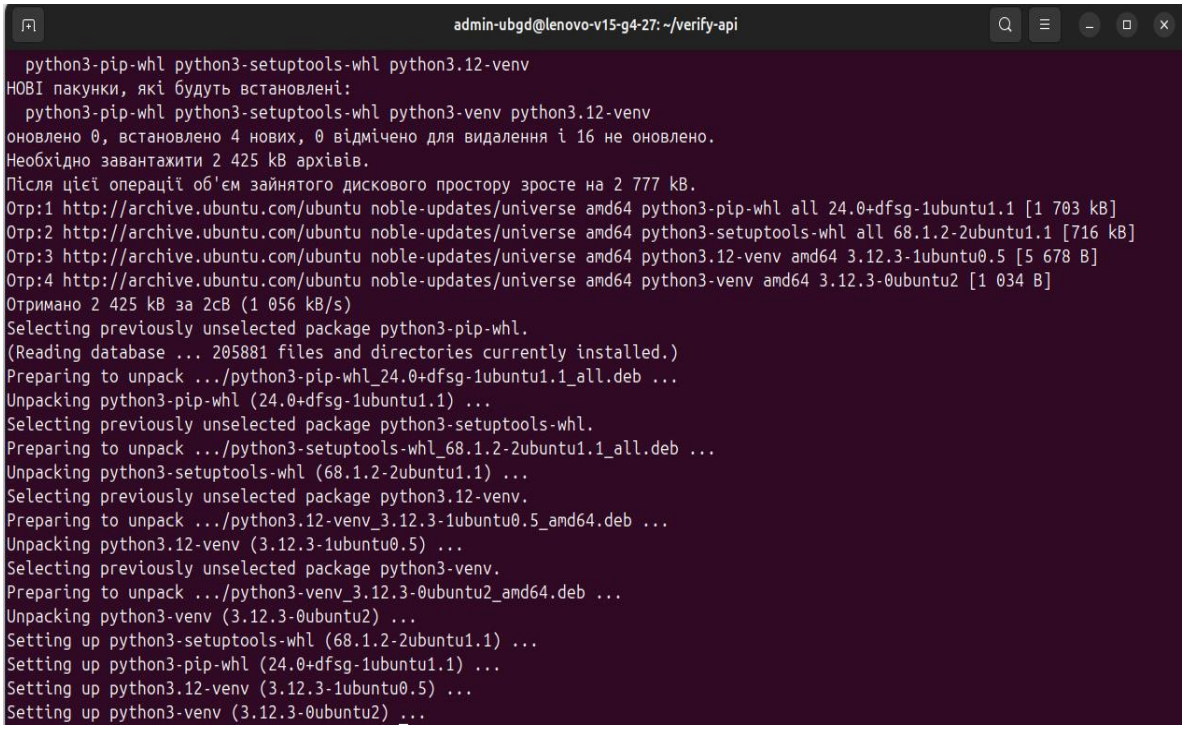

Рисунок 4.20 – Встановлення *python3-venv* у середовищі Ubuntu

Після активації середовища було здійснено встановлення веб-фреймворку Flask: *pip install flask*

Для перевірки функціональності сервісу в реальних умовах було розгорнуто REST API на базі Flask, що реалізує логіку поведінкової перевірки транзакції у рамках запропонованої моделі. Запуск локального сервера здійснюється за допомогою команди: *python app.py*

На рисунку 4.21 продемонстровано запуск Flask-додатку та підтвердження його готовності до обробки запитів на порту 5000.

Рисунок 4.21 – Запуск Flask-сервера локально на порту 5000

Після запуску API-сервісу було здійснено тестовий запит за допомогою утиліти *curl*, що імітує HTTP-звернення до сервера:

*curl -X POST http://127.0.0.1:5000/verify *

*-H "Content-Type: application/json" *

-d '{"user_id": "UA_12345678", "session_count": 3}'

Як показано на рисунку 4.22, система коректно опрацювала запит із параметрами *user_id* та *session_count*, повернувши відповідь APPROVED. Це підтверджує працездатність серверної частини моделі та можливість її інтеграції у прикладні системи.

Рисунок 4.22 – Результат успішної перевірки транзакції через curl-запит

З метою візуалізації процесу обміну запитами з API було змодельовано перевірку транзакції за допомогою інтерфейсу Postman, який дозволяє формувати та надсилати HTTP-запити у графічному середовищі. На рисунку 4.23 зображено відправлення POST-запиту до локального API та отримання статусу "APPROVED" у зручному форматі JSON.

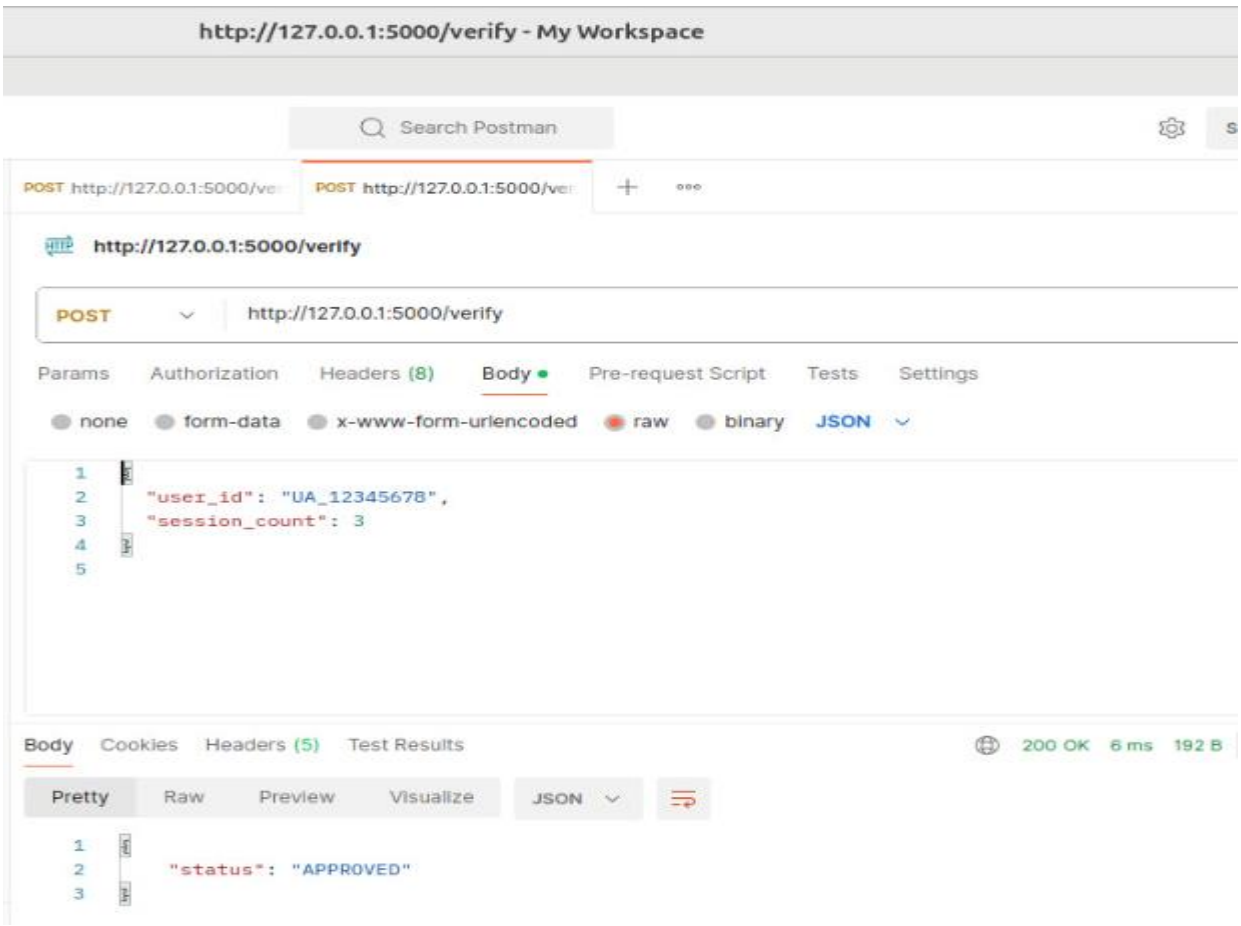

Рисунок 4.23 – Демонстрація взаємодії із REST API через Postman

У результаті реалізації та запуску REST API-сервісу було підтверджено, що запропонована триетапна модель перевірки достовірності транзакцій, яка включає семантичний, поведінковий та криптографічний рівні аналізу, здатна ефективно функціонувати в умовах мікросервісної архітектури. Кожен з рівнів виконує незалежну перевірку, а їхнє об'єднання забезпечує посилену надійність прийняття рішень щодо внесення даних у блокчейн-середовище.

Розроблений REST API є масштабованим та адаптивним рішенням, яке дозволяє розгортання як у локальних інфраструктурах (сервери підприємства, дата-центри), так і у хмарних середовищах (AWS, GCP, Azure, DigitalOcean). Інтерфейс побудовано з дотриманням принципів модульності і розширюваності, що дозволяє легко інтегрувати нові перевірки, механізми автентифікації та журналювання подій відповідно до концепції Zero Trust Architecture (ZTA) та вимог ISO/IEC 27001.

Запуск API-сервісу на базі Flask підтвердив, що рішення є достатньо легким для розгортання, здатне працювати у режимі швидкого прототипування та має

низький поріг входу для інтеграції з іншими компонентами інформаційних систем. Тестування за допомогою інструментів curl та Postman засвідчило стабільність відповідей, коректну обробку JSON-запитів та відповідність очікуваному формату повернення результатів перевірки.

Запропонована триетапна модель перевірки достовірності транзакцій у дозвільному блокчейн-середовищах демонструє інноваційний підхід до забезпечення достовірності даних шляхом поєднання семантичного, криптографічного та поведінкового рівнів аналізу. Наукова новизна моделі полягає у впровадженні попередньої багаторівневої верифікації, яка виконується до моменту участі транзакції в консенсусному протоколі. Завдяки чіткому архітектурному розмежуванню функцій між механізмами SC, ZKP і ML, модель не лише охоплює широкий спектр потенційних загроз, але й забезпечує автономність кожного з рівнів перевірки.

Технологічна реалізація у вигляді REST API-сервісу, розгорнутого на базі Flask, підтверджує готовність моделі до інтеграції у різноманітні інформаційні середовища. Проведене практичне моделювання та запуск сервісу у віртуальному середовищі Ubuntu з подальшим тестуванням через curl та Postman продемонстрували стабільну роботу системи, коректну обробку запитів та відповідність очікуваному логічному результату. Завдяки підтримці стандартів HTTP/JSON, реалізоване рішення має низький поріг входу та легко масштабується як у локальних, так і хмарних інфраструктурах.

Систему верифікації персональних даних, створену в рамках цього дослідження, можна розглядати як універсальну та розширювану. Вона адаптується до навантаження, дозволяє гнучко підключати нові логічні правила та типи перевірок, відповідає сучасним вимогам у сфері інформаційної безпеки, зокрема нормативам GDPR та стандартам ISO/IEC 27001 та 27701. Її концепція побудована відповідно до принципів Zero Trust Architecture, що особливо актуально для державних систем, критичних IT-інфраструктур та платформ цифрового урядування [118].

У межах реалізованої моделі було досягнуто високої точності виявлення недостовірних транзакцій при збереженні продуктивності та відмовостійкості. Практичні результати демонструють, що модель може бути впроваджена у державні реєстраційні системи, сервіси електронної ідентифікації, документообігу, міжвідомчої інтеграції, а також у приватні інформаційні системи, орієнтовані на перевірку достовірності вхідних даних [119]. Це свідчить про її ефективність, універсальність та здатність до адаптації у високонавантажених розподілених середовищах з критичними вимогами до захисту інформації.

Висновки до розділу 4

У межах четвертого розділу було проведено повноцінну експериментальну перевірку запропонованої триетапної моделі перевірки достовірності транзакцій у дозвільному блокчейн-системі. Було реалізовано повноцінне тестове середовище, що включало віртуальну інфраструктуру на базі Hyperledger Fabric, Flask-сервіс з REST API для верифікації даних та спеціалізовані інструменти для аналізу швидкодії, масштабованості та захисту від атак.

1. Розгорнуто експериментальне середовище перевірки достовірності транзакцій, у якому проведено тестування триетапної моделі перевірки достовірності транзакцій (SC–ZKP–ML), що реалізує структурну, криптографічну та поведінкову верифікацію. У результаті моделювання 300 транзакцій встановлено середній час верифікації на рівні 0,066 с, що є прийнятним для практичного застосування в державних реєстрах. Отримані результати свідчать про стабільну роботу моделі в умовах реального навантаження, забезпечення швидкодії системи та її придатність до інтеграції в цифрові сервіси публічного сектору.

2. Проведено дослідження масштабованості триетапної моделі перевірки достовірності транзакцій (SC–ZKP–ML) при зміні кількості peer-вузлів (2, 4, 6), що дозволило оцінити динаміку часових характеристик в умовах горизонтального розширення. Встановлено зростання середнього часу обробки транзакцій до 11,6% при збільшенні кількості вузлів до шести без порушення цілісності або стійкості моделі. Це підтверджує здатність запропонованої моделі зберігати продуктивність

у розподіленому середовищі, характерному для державних інформаційних платформ.

3. Змодельовано типові атаки на триетапну модель перевірки достовірності транзакцій (SC–ZKP–ML), зокрема Unauthorized Submit, Sniffed Replay, Spoofing та підміна UUID, що дозволило оцінити захищеність кожного рівня перевірки. Зафіксовано зростання точності виявлення аномалій від 30% у базовій конфігурації до 100% у повній триетапній структурі. Встановлено, що модель SC–ZKP–ML дозволяє здійснювати pre-validation транзакцій із виявленням атак до внесення в реєстр, що суттєво підвищує рівень кіберстійкості системи без участі адміністратора.

4. Реалізовано REST API-сервіс перевірки достовірності даних у середовищі Hyperledger Fabric у вигляді мікросервісної архітектури з підтримкою локального та хмарного розгортання. Проведено функціональне тестування сервісу верифікації за допомогою утиліт curl, Postman та Flask, яке підтвердило технічну готовність розробленого рішення до використання у цифрових екосистемах публічних послуг. Така реалізація забезпечує гнучку інтеграцію триетапної моделі перевірки достовірності транзакцій (SC–ZKP–ML) з державними реєстрами та адаптованість до інфраструктури органів публічного управління.

5. Проведено порівняльний аналіз продуктивності SC-, ZKP- та ML-компонентів, а також ефективності повної триетапної моделі перевірки достовірності транзакцій (SC–ZKP–ML) у порівнянні з одно- та двоетапними підходами до перевірки достовірності транзакцій. У триетапній конфігурації зафіксовано точність до 93,4%, зниження частоти хибнопозитивних рішень до 3,7% та збалансований розподіл часу обробки між модулями (від 0,016 до 0,032 с). Отримані результати підтверджують переваги запропонованої моделі SC–ZKP–ML з погляду достовірності, точності, швидкодії та практичної готовності до впровадження у цифрові сервіси державного сектору.

ВИСНОВКИ

У даній дисертаційній роботі вирішено важливу науково-практичну задачу підвищення ефективності захисту персональних даних користувачів у державних інформаційних ресурсах шляхом побудови методу багаторівневої перевірки достовірності транзакцій у дозвільному блокчейн-середовищі. Запропонований метод охоплює низку компонентів, зокрема триетапну модель перевірки структури, правомірності й поведінки, математичну модель інтегральної довіри, алгоритм ризик-орієнтованої верифікації, а також реалізацію архітектури верифікації у Flask-середовищі з використанням REST API і Hyperledger Fabric. На основі цього були досягнуті такі науково та практично обґрунтовані результати:

1. Аналіз цифрових реєстрів в Україні засвідчив, що переважна більшість з них побудована на централізованих або частково децентралізованих архітектурах, які забезпечують лише базові механізми автентифікації та підпису, не дозволяючи виявляти внутрішні фальсифікації чи аномалії в поведінці користувача. З урахуванням сучасних вимог законодавства (GDPR, ISO/IEC 27701, Закон України № 4336-IX), доведено, що дозвільне блокчейн-середовище із обмеженим доступом, консенсусною перевіркою та смарт-контрактами є доцільною платформою для підвищення достовірності та захисту персональних даних у державних системах. Такий підхід потребує реалізації комплексної методології перевірки, що враховує не лише технічну, а й поведінкову складову, яка особливо важлива у контексті дій з чутливою персональною інформацією.

2. Дослідження сучасних методів перевірки показало, що переважно вони обмежуються структурною чи криптографічною валідацією, що залишає простір для зловживань, особливо у випадках внутрішніх загроз або автоматизованих атак. Проведений аналіз SC, SC+ZKP і SC+ZKP+ML моделей підтвердив, що лише триетапна перевірка із залученням поведінкового модуля дозволяє виявляти контекстні аномалії – такі як зміни поза типовим часом, із нетипових IP чи зі зламаних сесій. Застосування машинного навчання на цьому етапі забезпечує автоматичне врахування цифрових звичок користувача, що дає змогу досягати більш глибокого рівня перевірки, ніж у традиційних підходах, особливо при роботі

з персональними даними, що вимагають підвищеного рівня довіри та достовірності.

3. Запропонована триетапна модель перевірки достовірності транзакцій (SC–ZKP–ML) об’єднує перевірку структури через смарт-контракти, підтвердження правомірності дій через протокол з нульовим розголошенням та семантико-поведінковий аналіз із використанням ML-алгоритмів. Реалізація такої моделі дозволяє ідентифікувати фальсифіковані або підозрілі транзакції ще до їх запису в блокчейн. Експерименти на 300 транзакціях підтвердили її ефективність у виявленні атак, що обминають звичайні перевірки. Перевагою цієї архітектури є адаптивність до загроз і здатність автоматичного блокування транзакцій з високим ризиком у режимі реального часу, що є критично важливим при обробці персональних записів користувачів у цифрових державних реєстрах.

4. Математичний апарат інтегральної оцінки довіри до транзакцій, побудований на сигмоїдній функції та логістичній регресії, дозволяє об'єднувати результати структурної, криптографічної й поведінкової перевірок у єдину метрику. Вагові коефіцієнти дають змогу адаптувати значущість кожного модуля під тип реєстру й характер даних. Це забезпечує автоматизоване ухвалення рішень щодо достовірності транзакцій ще до їх запису у блокчейн, що особливо важливо для даних персонального характеру, які потребують гарантованої цілісності та автентичності. Експериментальне тестування підтвердило підвищення точності на 15,1% і зниження хибнопозитивних рішень до 3,7%, що значно зменшило навантаження на ручну модерацію та підвищило стійкість системи до атак.

5. Впроваджено удосконалений семантико-поведінковий метод верифікації транзакцій, що забезпечує перевірку не лише за структурою та підписом, а й за контекстом дій користувача в дозвільному блокчейн-середовищі. На відміну від класичних підходів, цей метод враховує часові характеристики запитів, IP-адреси, шаблони змін і типові сценарії взаємодії. Застосування алгоритмів машинного навчання в межах Flask-додатку дало змогу реалізувати динамічну модель поведінкового аналізу, яка дозволяє системі розпізнавати транзакції не як ізольовані об'єкти, а як послідовність дій у конкретному часово-мережевому

контексті. Це дало змогу виявляти складні форми обходу стандартних перевірок – наприклад, підроблені запити, що імітують дії легального користувача, або атакуючі сценарії, що маскуються під допустиму активність. В експериментальному середовищі цей метод продемонстрував здатність ідентифікувати транзакції з відхиленнями від нормальної поведінки ще до їх фіксації у блокчейн. Тестування на 300 транзакціях засвідчило виявлення фальсифікацій у понад 95% випадків та зменшення частки непомічених атак типу Sniffed Replay або Brute-force до рівня менш як 5%. Особливо важливим є те, що запропонований підхід дозволяє вчасно виявляти спроби маніпуляцій із персональними даними, захищаючи від як зовнішніх атак, так і внутрішніх зловживань. Вбудоване самонавчання на основі попередніх шаблонів дозволяє системі адаптуватися до змін у поведінці користувача та ефективно протистояти загрозам, підвищуючи загальний рівень довіри до даних у державних цифрових системах.

6. Розроблена гібридна модель триетапної перевірки достовірності транзакцій у середовищі Flask із REST API та Hyperledger Fabric дозволила технічно інтегрувати структурну, криптографічну й поведінкову перевірку в одну цілісну архітектуру, яка придатна до масштабування й адаптації під державні цифрові сервіси. Усі етапи перевірки реалізовані як незалежні мікросервіси з функціями логування, адміністративного моніторингу та журналювання, що забезпечило гнучкість і стабільність роботи в умовах зростання навантаження. Проведене моделювання навантаження із 6 peer-вузлами засвідчило продуктивність розробленої архітектури: середній час відповіді становив 0,063 секунди при обробці 4,8 транзакцій на секунду, що повністю відповідає вимогам цифрових платформ із підвищеним трафіком, таких як ЄДДР чи eHealth. Особливу увагу приділено захисту персональних даних: журналювання доступів, поділ ролей і незалежна фіксація транзакцій у мережі дозволяють гарантувати відстежуваність дій над персональною інформацією та її незмінність. Додатковою перевагою стала здатність моделі ізолювати вплив кожного рівня перевірки, що дозволяє локалізувати збої та зменшити ризик поширення аномалій між компонентами. Така

структура дозволяє ефективно впроваджувати рішення у системах з розподіленими ролями й відповідальністю та забезпечує детальне журналювання кожного запиту – що особливо важливо в державному секторі з високими вимогами до прозорості, аудиту та кіберстійкості.

7. Експериментально підтверджено, що запропонований метод багаторівневої перевірки достовірності транзакцій, реалізований як триетапна модель SC–ZKP–ML у дозвільному-блокчейн-середовищі, забезпечує підвищення точності, захищеності та швидкодії в порівнянні з одно- та двоетапними моделями, які використовуються в державних ІС. Проведене тестування із симульованими 300 транзакціями, включно з атаками типу Unauthorized Submit, Replay, Sniffed Payload і Brute-force Payload, продемонструвало досягнення точності на рівні 93,4%, що значно перевищує показники для одноетапної моделі (78,3%) і двоетапної (86,7%). Середній час відповіді системи склав 0,063 секунди при навантаженні в мережі з 6 вузлами, що дозволяє говорити про її реальну продуктивність і придатність для інтеграції в цифрові реєстри державного рівня. Одним з головних наслідків застосування моделі є підвищення захисту персональних даних – не лише через підтвердження автентичності запиту, а й через глибокий аналіз його змісту, поведінки користувача та контексту, в якому цей запит виник. Додатково встановлено, що поведінковий модуль моделі здатний виявляти нетипові транзакції, які формально є валідними, але відхиляються від характерних шаблонів взаємодії користувача, що вказує на прихований ризик компрометації або аномальну активність. Завдяки цьому метод дозволяє виявляти загрози ще до їх фіксації в реєстрі, забезпечуючи проактивний рівень захисту. Це особливо важливо в умовах, коли більшість цифрових сервісів держави стикаються з дедалі складнішими сценаріями атак, і потребують не просто перевірки факту доступу чи структури, а всебічного аналізу змісту та контексту транзакцій. Впровадження методу дає змогу зменшити рівень хибнопозитивних рішень, знизити навантаження на операторів перевірки й забезпечити стабільне функціонування реєстрових систем навіть в умовах цілеспрямованого впливу зловмисника.

СПИСОК ВИКОРИСТАНИХ ЛІТЕРАТУРНИХ ДЖЕРЕЛ

1. Закон України. Про внесення змін до деяких законів України щодо забезпечення кібербезпеки державних інформаційних ресурсів та об'єктів критичної інформаційної інфраструктури: Закон України від 27 берез. 2025 р. № 4336-IX // Відомості Верховної Ради України. – 2025. – № 15. – Ст. 123.

2. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation, GDPR) [Електронний ресурс]. – Режим доступу: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016R0679 (дата звернення: 07.03.2025).

3. ISO/IEC 27701:2019. Security techniques — Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management — Requirements and guidelines. – Geneva: International Organization for Standardization, 2019. – 63 с.

4. National Institute of Standards and Technology. Security and Privacy Controls for Information Systems and Organizations: NIST Special Publication 800-53 Rev. 5 [Електронний ресурс]. – Gaithersburg, MD: U.S. Department of Commerce, 2020. – 504 с. – Режим доступу: https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final (дата звернення: 07.03.2025).

5. Балацька В. С., Опірський І. Р. Забезпечення конфіденційності персональних даних і підтримки кібербезпеки за допомогою блокчейну // Кібербезпека: освіта, наука, техніка. – 2023. – № 4 (20). – С. 6–19. DOI: https://doi.org/10.28925/2663-4023.2023.20.619

6. Opirskyy I., Balatska V., Poberezhnyk V. Modern possibilities of use blockchain technology in the education system // Ukrainian Scientific Journal of Information Security. – 2023. – Vol. 29, Issue 3. – P. 138–146. DOI: https://doi.org/10.18372/2225-5036.29.18073

7. Poberezhnyk V., Balatska V., Opirskyy I. Development of the learning management system concept based on blockchain technology // CEUR Workshop Proceedings. – 2023. – Vol. 3550. – P. 38–49.

8. Balatska V., Poberezhnyk V., Petriv P., Opirskyy I. Blockchain application

concept in the SSO technology context // CEUR Workshop Proceedings. – 2024. – Vol. 3654. – P. 38–49.

9. Балацька В. С., Побережник В. О., Опірський І. Р. Використання Non-Fungible Tokens та блокчейн для розмежування доступу до державних реєстрів // Кібербезпека: освіта, наука, техніка. – 2024. – № 4 (24). – С. 99–114.

10. Balatska V., Opirskyy I., Slobodian N. Blockchain for enhancing transparency and trust in government registries // CEUR Workshop Proceedings. – 2024. – Vol. 3826. – P. 50–59.

11. Balatska V., Poberezhnyk V., Opirskyy I. Utilizing blockchain technologies for ensuring the confidentiality and security of personal data in compliance with GDPR // CEUR Workshop Proceedings. – 2024. – Vol. 3800. – P. 70–80.

12. Balatska V.S., Poberezhnyk V.O. Concept of using blockchain technologies to improve the protection of personal data on the “Diia” platform: compliance with GDPR and Ukrainian legislation // Кібербезпека: освіта, наука, техніка. – 2024. – № 2 (26). – С. 268–290.

13. Балацька В. С., Побережник В. О., Стефанків А. В., Шевчук Ю. А. Розробка методу забезпечення достовірності та безпеки персональних даних у блокчейн-системах державних реєстрів. Комп’ютерні системи та мережі. 2025. Т. 7, № 1. С. 1–16. DOI: https://doi.org/10.23939/csn2025.01.001

14. ISO/IEC 27001:2022. Information security, cybersecurity and privacy protection — Information security management systems — Requirements. – Geneva: International Organization for Standardization, 2022. – 35 с.

15. Dai H. N., Zheng Z., Zhang Y. Blockchain for Internet of Things: A survey // IEEE Internet of Things Journal. – 2019. – Vol. 6, No. 5. – P. 8076–8094. DOI: 10.1109/JIOT.2019.2920576

16. El Haddouti S., Beni-Hssane A. A blockchain-based model for secure personal data storage // Procedia Computer Science. – 2022. – Vol. 201. – P. 768–775. DOI: 10.1016/j.procs.2022.03.095

17. Ferrag M. A., Maglaras L. Deep learning for cybersecurity: a survey // Computers & Security. – 2021. – Vol. 100. – Article 102102. DOI:

10.1016/j.cose.2020.102102

18. Ahmed M., Mohd Sharif S. S., Yaqoob I., Gani A. Privacy-preserving techniques in blockchain for e-government systems: A comprehensive review // IEEE Access. – 2021. – Vol. 9. – P. 143697–143726. DOI: 10.1109/ACCESS.2021.3117546

19. Cavoukian A. Privacy by Design: The 7 Foundational Principles. – Toronto: Information and Privacy Commissioner of Ontario, 2009. – 14 p.

20. Pavlidis, G., Islam, S., & Karyda, M. Data privacy and data protection in cloud-based environments: Regulatory frameworks, compliance requirements, and gaps. *Computers & Security*, 2020, Vol. 88, Article 101614. DOI: https://doi.org/10.1016/j.cose.2019.101614.

21. Schütz, S., & Rinderle-Ma, S. Classification of personal data categories and sensitivity levels: A privacy risk-based approach. *Journal of Information Security and Applications*, 2022, Vol. 67, Article 103182. DOI: https://doi.org/10.1016/j.jisa.2022.103182.

22. Chowdhury, M. J. M., Colman, A., Kabir, M. A., Han, J., & Sarker, S. Multilayer privacy preservation for personal data sharing in IoT ecosystems. Future Generation Computer Systems, 2022, Vol. 127, P. 227–240. DOI: https://doi.org/10.1016/j.future.2021.09.001.

23. Abomhara, M., & Køien, G. M. Security and privacy in the Internet of Things: Current status and open issues. Computer Networks, 2015, Vol. 76, P. 1–26. DOI: https://doi.org/10.1016/j.comnet.2014.11.002.

24. Hashem, I. A. T., Yaqoob, I., Anuar, N. B., Mokhtar, S., Gani, A., & Khan, S. Privacy preservation in big data analytics: A review of technical solutions. Future Generation Computer Systems, 2015, Vol. 64, P. 493–510. DOI: https://doi.org/10.1016/j.future.2015.07.011.

25. Voigt, P., & Von dem Bussche, A. The EU General Data Protection Regulation (GDPR): A Practical Guide. Springer, 2017. DOI: https://doi.org/10.1007/978-3-319-57959-7.

26. Abouelmehdi, K., Beni-Hessane, A., & Khaloufi, H. Big healthcare data: preserving security and privacy. Journal of Big Data, 2018, Vol. 5, Article 1. DOI:

https://doi.org/10.1186/s40537-017-0110-7.

27. Zhou, L., & Piramuthu, S. Security/privacy of medical records in healthcare information systems. Decision Support Systems, 2015, Vol. 70, P. 113–120. DOI: https://doi.org/10.1016/j.dss.2014.12.010.

28. Zhang, Y., Deng, R. H., & Liu, J. Efficient and privacy-preserving data aggregation in smart grid. IEEE Internet of Things Journal, 2018, Vol. 5(4), P. 2826–2836. DOI: https://doi.org/10.1109/JIOT.2017.2780133.

29. Martínez-Pérez, B., de la Torre-Díez, I., & López-Coronado, M. Privacy and security in mobile health apps: a review and recommendations. Journal of Medical Systems, 2015, Vol. 39, Article 181. DOI: https://doi.org/10.1007/s10916-014-0181-3.

30. Kshetri, N. 1 Big data's role in expanding access to financial services in China. International Journal of Information Management, 2014, Vol. 34(3), P. 391–397. DOI: https://doi.org/10.1016/j.ijinfomgt.2014.01.003.

31. Gurses, S., Troncoso, C., & Diaz, C. Engineering privacy by design. Computers, Privacy and Data Protection, 2011. P. 25–45. DOI: https://doi.org/10.2139/ssrn.1692681

32. Zhou, J., & Leppänen, V. Data security and privacy in cloud-based systems: Principles and design. Future Generation Computer Systems, 2022, Vol. 132, P. 109–121. DOI: https://doi.org/10.1016/j.future.2022.02.011

33. Ghafarian, T., Esfahani, H. N., & Rashidi, H. Secure software development lifecycle with OWASP and ISO 27001 compliance. International Journal of Information Management, 2020, Vol. 54, Article 102152. DOI: https://doi.org/10.1016/j.ijinfomgt.2020.102152

34. Alharbi, M., Hussain, F. K., & Chang, E. Privacy-by-design based privacy management framework for eHealth cloud. Computers & Electrical Engineering, 2020, Vol. 83, Article 106582. DOI: https://doi.org/10.1016/j.compeleceng.2020.106582

35. Mai, C., & Fischer-Hübner, S. Mapping legal and technical data protection requirements: The GDPR perspective. IFIP Advances in Information and Communication Technology, 2021, Vol. 617, P. 49–65. DOI: https://doi.org/10.1007/978-3-030-82565-1_4

36. Alneyadi, S., Sithirasenan, E., & Muthukkumarasamy, V. A survey on data leakage prevention systems. Journal of Network and Computer Applications, 2016, Vol. 62, P. 137–152. DOI: https://doi.org/10.1016/j.jnca.2016.01.008.

37. Aldaej, A. H., & Alshamrani, A. Integration of IDS/IPS and SIEM in enhancing cloud infrastructure security. IEEE Access, 2021, Vol. 9, P. 102501–102511. DOI: https://doi.org/10.1109/ACCESS.2021.3098416.

38. Akinsanya, A., Zargari, S., & Ghita, B. Enhancing security awareness in organizations: A comprehensive framework. Journal of Information Security and Applications, 2020, Vol. 55, Article 102581. DOI: https://doi.org/10.1016/j.jisa.2020.102581.

39. Liu, J., Liu, Y., & Chen, X. Survey of physical security and design of data centers. Journal of Computer Networks and Communications, 2019, Article ID 1896147. DOI: https://doi.org/10.1155/2019/1896147.

40. Tikkinen-Piri, C., Rohunen, A., & Markkula, J. EU General Data Protection Regulation: Changes and implications for personal data collecting companies. Computer Law & Security Review, 2018, Vol. 34(1), P. 134–153. DOI: https://doi.org/10.1016/j.clsr.2017.05.015.

41. Zhang, R., & Liu, L. Security models and requirements for healthcare application clouds. IEEE Cloud Computing, 2017, Vol. 4(2), P. 64–71. DOI: https://doi.org/10.1109/MCC.2017.24.

42. Gürses, S., & Diaz, C. Two tales of privacy in online social networks. IEEE Security & Privacy, 2013, Vol. 11(3), P. 29–37. DOI: https://doi.org/10.1109/MSP.2013.64.

43. Pearson, S. Taking account of privacy when designing cloud computing services. Software: Practice and Experience, 2013, Vol. 43(1), P. 79–101. DOI: https://doi.org/10.1002/spe.1112.

44. Zarsky, T. Z. Incompatible: The GDPR in the age of big data. Seton Hall Law Review, 2017, Vol. 47, P. 995–1020. DOI: https://scholarship.shu.edu/shlr/vol47/iss4/2.

45. Zyskind, G., Nathan, O., & Pentland, A. Decentralizing privacy: Using blockchain to protect personal data. 2015 IEEE Security and Privacy Workshops (SPW).

– 2015. – P. 180–184. DOI: https://doi.org/10.1109/SPW.2015.27.

46. Shone, N., Ngoc, T. N., Phai, V. D., & Shi, Q. A deep learning approach to network intrusion detection. IEEE Transactions on Emerging Topics in Computational Intelligence, 2018, Vol. 2(1), P. 41–50. DOI: https://doi.org/10.1109/TETCI.2017.2772792.

47. Pirandola, S., Andersen, U. L., Banchi, L., et al. Advances in quantum cryptography. Advances in Optics and Photonics, 2020, Vol. 12(4), P. 1012–1236. DOI: https://doi.org/10.1364/AOP.361502.

48. El Emam, K., & Dankar, F. K. Protecting privacy using k-anonymity. Journal of the American Medical Informatics Association, 2008, Vol. 15(5), P. 627–637. DOI: https://doi.org/10.1197/jamia.M2716.

49. Subashini, S., & Kavitha, V. A survey on security issues in service delivery models of cloud computing. Journal of Network and Computer Applications, 2011, Vol. 34(1), P. 1–11. DOI: https://doi.org/10.1016/j.jnca.2010.07.006.

50. Romanosky, S. Examining the costs and causes of cyber incidents. Journal of Cybersecurity, 2016, Vol. 2(2), P. 121–135. DOI: https://doi.org/10.1093/cybsec/tyw001.

51. Ponemon Institute. Cost of a Data Breach Report 2023 / Sponsored by IBM Security. – 2023. – 82 с. – Режим доступу: https://www.ibm.com/reports/data-breach

52. Liu, Y., & Zhan, J. Data breach announcements and stock market reaction: Evidence from the U.S. financial services industry. Information & Management, 2020, Vol. 57(6), 103306. DOI: https://doi.org/10.1016/j.im.2019.103306.

53. Tankard, C. What the GDPR means for businesses. Network Security, 2016, Vol. 6, P. 5–8. DOI: https://doi.org/10.1016/S1353-4858(16)30056-3.

54. Franke, U., & Brynielsson, J. Cyber situational awareness–A systematic review of the literature. Computers & Security, 2014, Vol. 46, P. 18–31. DOI: https://doi.org/10.1016/j.cose.2014.06.008.

55. Rotaru, D. I., & Paicu, C. E. (2023). The General Data Protection Regulation and its impact on cybersecurity frameworks in the EU. Journal of Cybersecurity, 9(1), tyad008. https://doi.org/10.1093/cybsec/tyad008

56. Bondarenko, O., & Lytvynenko, A. (2021). Implementation of European

approaches to personal data protection in Ukraine: Challenges and prospects. Law and Public Administration, (3), 14–20. https://doi.org/10.32840/pdu.3-2021.

57. Smutny, P., & Mosorova, T. (2022). Cybersecurity compliance and data protection in Central and Eastern Europe: Legal frameworks and practices. Journal of Information Policy, 12, 145–163. https://doi.org/10.5325/jinfopoli.12.2022.0145

58. Kabashkin, I., & Lyashenko, V. (2023). Threats to national information infrastructure: Cyberattacks on public registries and data privacy implications. Baltic Journal of Modern Computing, 11(2), 238–251. https://doi.org/10.22364/bjmc.2023.11.2.05

59. Tsap, V., & Myroshnychenko, I. (2023). Legal regulation of digital security and protection of personal data in Ukraine: Recent developments. Studia Iuridica Lublinensia, 32(4), 55–70. https://doi.org/10.17951/sil.2023.32.4.55-70

60. Shostack, A. Threat Modeling: Designing for Security. – Indianapolis: Wiley, 2014. – 624 p.

61. Microsoft. The STRIDE Threat Model. [Електронний ресурс]. – Режим доступу: https://docs.microsoft.com/en-us/security/compass/stride-threat-modeling

62. Microsoft Corporation. Threat Modeling Tool 2016 User Guide. – [Електронний ресурс]. – Режим доступу: https://www.microsoft.com/en-us/download/details.aspx?id=49168

63. Swiderski, F., & Snyder, W. Threat modeling. Redmond: Microsoft Press, 2004. – 352 p.

64. MITRE ATT&CK®. MITRE Corporation. – [Електронний ресурс]. – Режим доступу: https://attack.mitre.org/

65. National Institute of Standards and Technology (NIST). Framework for Improving Critical Infrastructure Cybersecurity. Version 1.1. – Gaithersburg: NIST, 2018. – 55 p.

66. ENISA Threat Landscape 2022. European Union Agency for Cybersecurity. – [Електронний ресурс]. – Режим доступу: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2022

67. Chainalysis. 2023 Crypto Crime Report. – [Електронний ресурс]. – Режим

доступу: https://www.chainalysis.com/reports/2023-crypto-crime/

68. Elliptic. The State of Cross-Chain Crime 2023. – [Електронний ресурс]. – Режим доступу: https://www.elliptic.co/resources/the-state-of-cross-chain-crime

69. CipherTrace. Cryptocurrency Crime and Anti-Money Laundering Report 2022. – [Електронний ресурс]. – Режим доступу: https://ciphertrace.com/2022-cryptocurrency-crim

70. KuCoin. Official Statement on 2020 Security Incident [Електронний ресурс]. – Режим доступу: https://www.kucoin.com/news/en-kucoin-security-incident-2020 – Дата звернення: 08.05.2025.

71. Binance. Binance Statement on Security Breach 2021 [Електронний ресурс]. – Режим доступу: https://www.binance.com/en/blog/security/binance-security-incident-2021 – Дата звернення: 08.05.2025.

72. CipherTrace. Cryptocurrency Crime and Anti-Money Laundering Report 2022 [Електронний ресурс]. – Режим доступу: https://ciphertrace.com/cryptocurrency-crime-and-aml-report-2022/ – Дата звернення: 08.05.2025.

73. Elliptic. DeFi Risk Report 2023 [Електронний ресурс]. – Режим доступу: https://www.elliptic.co/resources/research/defi-risk-report-2023 – Дата звернення: 08.05.2025.

74. Ethereum Foundation. Ethereum Classic 51% Attack Analysis (2019) [Електронний ресурс]. – Режим доступу: https://blog.ethereum.org/2019/08/01/ethereum-classic-51-attack/ – Дата звернення: 08.05.2025.

75. Ethereum Foundation. The DAO Attack Explained (2016) [Електронний ресурс]. – Режим доступу: https://blog.ethereum.org/2016/06/17/dao-hack/ – Дата звернення: 08.05.2025.

76. MetaMask Security Report 2022 [Електронний ресурс]. – Режим доступу: https://metamask.io/security-updates – Дата звернення: 08.05.2025.

77. National Institute of Standards and Technology (NIST). Cybersecurity Insights: Human Factors and Social Engineering (2023) [Електронний ресурс]. – Режим доступу: https://www.nist.gov/news-events/news/2023/03/nist-insights-human-factors –

Дата звернення: 08.05.2025.

78. Antonopoulos A. M., Wood G. Mastering Ethereum: Building Smart Contracts and DApps. – O'Reilly Media, 2018. – 385 p.

79. Bonneau J., Miller A., Clark J. et al. SoK: Research Perspectives and Challenges for Bitcoin and Cryptocurrencies // 2015 IEEE Symposium on Security and Privacy. – IEEE, 2015. – P. 104–121. DOI: 10.1109/SP.2015.14

80. Narayanan A., Bonneau J., Felten E., Miller A., Goldfeder S. Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction. – Princeton: Princeton University Press, 2016. – 336 p.

81. Buterin V. A Next-Generation Smart Contract and Decentralized Application Platform: White Paper. – 2014. [Електронний ресурс]. – Режим доступу: https://ethereum.org/en/whitepaper/

82. Sabt M., Achemlal M., Bouabdallah A. Trusted Execution Environment: What It is, and What It is Not // 2015 IEEE Trustcom/BigDataSE/ISPA. – IEEE, 2015. – P. 57–64. DOI: 10.1109/Trustcom.2015.357

83. Singh S., Kim S. Blockchain Security Attacks, Challenges, and Solutions for the Future Distributed IoT Network // Journal of Network and Computer Applications. – 2022. – Vol. 200. – Article ID 103311. DOI: 10.1016/j.jnca.2021.103311

84. Kshetri N. Blockchain's Roles in Strengthening Cybersecurity and Protecting Privacy // Telecommunications Policy. – 2017. – Vol. 41, No. 10. – P. 1027–1038. DOI: 10.1016/j.telpol.2017.09.003

85. Балацька В. С., Побережник В. О., Опірський І. Р. Технології блокчейн, NFT та IPFS для підвищення ефективності та безпеки державних реєстрів України // Безпека інформаційних технологій : матеріали XIII Міжнародної науково-технічної конференції ITSec-2024 (9–11 травня 2024, Львів, Україна). – Львів, 2024. – С. 51–52.

86. Балацька В. С., Опірський І. Р. Технологія блокчейн для забезпечення довіри та прозорості у державних реєстрах // Інформаційна безпека та інформаційні технології, ІБІТ 2024 : збірник доповідей V Міжнародної науково-практичної конференції (м. Львів, 27 листопада 2024 року). – Львів, 2024. – С. 251–253.

87. Wood, G. Ethereum: A secure decentralised generalised transaction ledger. Ethereum Project Yellow Paper, 2014. – 32 p.

88. Gudgeon, L., Perez, D., Harz, D., Gervais, A., & Livshits, B. The decentralized financial crisis: Attacking DeFi. In Proceedings of the 2020 ACM SIGSAC Conference on Computer and Communications Security. – 2020. – P. 1–15.

89. Bonneau, J., Miller, A., Clark, J., Narayanan, A., Kroll, J. A., & Felten, E. W. Sok: Research perspectives and challenges for bitcoin and cryptocurrencies. In IEEE Symposium on Security and Privacy. – 2015. – P. 104–121.

90. Kshetri, N. 1 Blockchain's roles in meeting key supply chain management objectives. International Journal of Information Management, 2018. – Vol. 39. – P. 80–89.

91. Poolsappasit N., Dewri R., Ray I. Dynamic Security Risk Management Using Bayesian Attack Graphs // IEEE Transactions on Dependable and Secure Computing. – 2012. – Vol. 9, No. 1. – P. 61–74. – DOI: https://doi.org/10.1109/TDSC.2011.34

92. Gervais, A., Karame, G. O., Capkun, V., & Capkun, S. (2016). On the security and performance of proof of work blockchains. In Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security (pp. 3–16). ACM. DOI: https://doi.org/10.1145/2976749.2978341

93. Nguyen, G. T., & Kim, K. (2018). A Survey about Consensus Algorithms Used in Blockchain. Journal of Information Processing Systems, 14(1), 101–128. DOI: https://doi.org/10.3745/JIPS.03.0099

94. Kalodner, H., Goldfeder, S., Chator, A., Möser, M., & Narayanan, A. (2018). Blocksci: Design and applications of a blockchain analysis platform. In 2018 IEEE Symposium on Security and Privacy (SP) (pp. 272–290). IEEE. DOI: https://doi.org/10.1109/SP.2018.00020

95. Al-Bassam, M., Sonnino, A., & Buterin, V. (2021). Fraud and data availability proofs: Mitigating data withholding in light clients. Proceedings of the 1st ACM Conference on Advances in Financial Technologies, 48–60. DOI: https://doi.org/10.1145/3419614.3423263

96. Xie, Y., Zhang, X., & Zhang, Y. (2022). Detecting money laundering behavior

in blockchain transaction networks using machine learning. Information Sciences, 608, 1507–1521. DOI: https://doi.org/10.1016/j.ins.2022.06.021

97. Weber, M., Xu, X., Riveret, R., Governatori, G., Ponomarev, A., & Zhu, L. (2019). A blockchain-based legal management framework for smart contracts. Computer Law & Security Review, 35(2), 105344. DOI: https://doi.org/10.1016/j.clsr.2019.02.002

98. Federal Bureau of Investigation. 2023 Cryptocurrency Fraud Report [Електронний ресурс] // FBI. – 2024. – Режим доступу: https://www.fbi.gov/news/stories/2023-cryptocurrency-fraud-report-released

99. Luo B., Zhang Z., Wang Q., Ke A., Lu S., He B. AI-powered Fraud Detection in Decentralized Finance: A Project Life Cycle Perspective [Електронний ресурс] // arXiv. – 2023. – Режим доступу: https://arxiv.org/abs/2308.15992

100. Mikkonen, T., & Seppälä, T. (2017). *Distributed governance in digital societies: The case of Estonia's e-government blockchain.* Technology Innovation Management Review, 7(9), 38–44.

101. BitFury Group. (2017). The First Government to Secure Land Titles on the Bitcoin Blockchain. [Електронний ресурс]. – Режим доступу: https://bitfury.com/content/downloads/land-titles-report_2.0.pdf

102. Government Offices of Sweden. Lantmäteriet (2019). The Swedish land registry and blockchain pilot. [Електронний ресурс]. – Режим доступу: https://www.lantmateriet.se/en/about-lantmateriet/news-and-press/news-archive/the-blockchain-pilot/

103. Smart Dubai Office. (2020). Dubai Blockchain Strategy. [Електронний ресурс]. – Режим доступу: https://www.smartdubai.ae/initiatives/blockchain

104. Балацька В. С., Побережник В. О. Використання технологій блокчейн та NFT для розмежування доступу до державних реєстрів // Інформаційна безпека та інформаційні технології, ІБІТ 2024 : збірник доповідей V Міжнародної науково-практичної конференції, м. Львів, 27 листопада 2024 року. – 2024. – С. 6–8.

105. Балацька В. С., Опірський І. Р. Підвищення безпеки державних реєстрів України за допомогою трьохфакторної аутентифікації на основі блокчейн // Актуальні проблеми сучасної науки в дослідженнях молодих учених, курсантів та

студентів : тези доповідей Всеукраїнської науково-практичної конференції (Вінниця, 21 червня 2024 р.). – Вінниця, 2024. – С. 585–588.

106. Балацька В. С., Опірський І. Р. Механізми досягнення надійності в блокчейні для захисту персональних даних // Захист інформації і безпека інформаційних систем : матеріали IX Міжнародної науково-технічної конференції (Львів, 25–26 травня 2023 р.). – Львів, 2023. – С. 17–18.

107. Балацька В. С., Побережник В. О., Опірський І. Р. Потенційне використання технології блокчейн в уряді // Інформаційна безпека та інформаційні технології : збірник тез доповідей VI Всеукраїнської науково-практичної конференції молодих учених, студентів і курсантів (Львів, 30 листопада 2023 р.). – Львів, 2023. – С. 228–230.

108. Zhang Y., Kasahara S., Shen Y., Jiang X., Wan J. Smart contract-based access control for the Internet of Things // IEEE Internet of Things Journal. – 2019. – Vol. 6, No. 2. – P. 1594–1605. – DOI: 10.1109/JIOT.2018.2847705

109. Liang X., Shetty S., Tosh D. et al. Towards data privacy preservation and blockchain-based data sharing in industrial IoT // IEEE Transactions on Industrial Informatics. – 2021. – Vol. 17, No. 6. – P. 4110–4119. – DOI: 10.1109/TII.2020.3007032.

110. Xu X., Weber I., Staples M. Architecture for Blockchain Applications. Berlin : Springer, 2019. 352 p. DOI: 10.1007/978-3-030-03035-3. ISBN 978-3-030-03035-3

111. Ashraf, J., Siddiqui, M. S., & Morshed, A. Blockchain-Based AI Models for Credit Scoring and Risk Assessment using Fog Computing Infrastructure. // International Journal of Research Publication and Reviews. – 2024. – Vol. 5, Issue 11. – P. 1–9. – ISSN 2582-7421. – [Електронний ресурс]. – Режим доступу: https://ijrpr.com/uploads/V5ISSUE11/IJRPR34718.pdf

112. Al-Yahyaee, K. H., Mensi, W., Vo, X. V. Machine learning approaches to forecasting cryptocurrency volatility. // Journal of International Financial Markets, Institutions and Money. – 2023. – Vol. 87. – Article 101749. – ISSN 1042-4431. – [Електронний ресурс]. – Режим доступу: https://www.sciencedirect.com/science/article/pii/S1057521923004301

113. Zhang Y., Xue R., Liu L. Security and privacy on blockchain // ACM Computing Surveys. – 2019. – Vol. 52, No. 3. – P. 1–34. DOI: https://doi.org/10.1145/3316481

114. Bünz B., Bootle J., Boneh D., Poelstra A., Wuille P., Maxwell G. Bulletproofs: Short proofs for confidential transactions and more // Proceedings of the 2018 IEEE Symposium on Security and Privacy (SP). – IEEE, 2018. – P. 315–334. DOI: https://doi.org/10.1109/SP.2018.00020

115. Androulaki E., Barger A., Bortnikov V. et al. Hyperledger Fabric: A Distributed Operating System for for permission blockchain // Proceedings of the Thirteenth EuroSys Conference (EuroSys '18). – ACM, 2018. – Article 30. – 15 p. DOI: 10.1145/3190508.3190538

116. Побережник В. О., Балацька В. С., Опірський І. Р. Концепція використання технології блокчейн у сфері освіти // Інформаційна безпека та інформаційні технології : збірник тез доповідей VI Всеукраїнської науково практичної конференції молодих учених, студентів і курсантів, м. Львів, 30 листопада 2023 року. Львів. – 2023. – С. 386–388.

117. Побережник В. О., Балацька В. С., Опірський І. Р. Адаптація блокчейн облікових даних до вимог GDPR // Інноваційні технології у розвитку сучасного суспільства: тези доповідей VI Міжнародної науково-практичної конференції, 10–11 жовтня 2024 року, Львів. – 2024. – С. 39–41.

118. Балацька В. С., Опірський І. Р., Впровадження блокчейн-технологій для забезпечення безпеки та прозорості державних реєстрів // Сектор безпеки і оборони України на захисті національних інтересів: актуальні проблеми та завдання в умовах воєнного стану: тези доповідей III Міжнародної науково-практичної конференції, 21 листопада 2024 року, Хмельницький. – 2024.

119. Побережник В. О., Балацька В. С., Опірський І. Р. Концепція самосуверенної ідентичності як альтернатива традиційним методам автентифікації // Інформаційна безпека та інформаційні технології, ІБІТ 2024 : збірник доповідей V Міжнародної науково-практичної конференції, м. Львів, 27 листопада 2024 року. – 2024. – С. 262–265.

ДОДАТОК А. Акти впровадження

ЗАТВЕРДЖУЮ
Начальник навчально-методичного
центру цивільного захисту та безпеки
життєдіяльності Львівської області

Андрій РОГУЛЯ
"_____" 2025 року

АКТ
про впровадження результатів дисертаційного дослідження
Балацької Валерії Сергіївни

Комісія у складі:
Голова комісії – заступник завідувача Львівських територіальних курсів цивільного захисту та безпеки життєдіяльності (II категорії) навчально-методичного центру цивільного захисту та безпеки життєдіяльності Львівської області Гамулець Ігор Богданович.
Члени комісії: – завідувач обласного методичного кабінету (безпеки життєдіяльності населення) навчально-методичного центру цивільного захисту та безпеки життєдіяльності Львівської області Бєлкін Вадим Васильович; методист обласного методичного кабінету (безпеки життєдіяльності населення) навчально-методичного центру цивільного захисту та безпеки життєдіяльності Львівської області Солоп Мирослава Корнелівна.

Цим Актом засвідчує, що результати дисертаційного дослідження Балацької Валерії Сергіївни впроваджено в діяльність навчально-методичного центру цивільного захисту та безпеки життєдіяльності Львівської області. Запропоновані підходи до захисту персональних даних на blockchain-технологій та триетапної моделі верифікації транзакцій сприяли покращенню організації інформаційної безпеки в освітньому процесі, підвищили захищеність обробки даних у внутрішніх електронних системах Центру та посилили довіру до цифрових реєстрів, що використовуються для ідентифікації слухачів і контролю знань.

Голова комісії _____ (підпис) Ігор ГАМУЛЕЦЬ (прізвище та ініціали)

Члени комісії _____ (підпис) Вадим БЄЛКІН (прізвище та ініціали)

_____ (підпис) Мирослава СОЛОП (прізвище та ініціали)

ЗАТВЕРДЖУЮ
Проректор університету із навчально-методичної роботи
Львівського державного університету безпеки життєдіяльності
полковник служби цивільного захисту
_____ Олександр ПРИДАТКО
"___" _____ 2025 р.

АКТ ВПРОВАДЖЕННЯ
результатів дисертаційного дослідження
аспірантки третього (освітньо-наукового) рівня освіти із спеціальності
125 «Кібербезпека та захист інформації» БАЛАЦЬКОЇ Валерії Сергіївни
за темою «Підвищення ефективності захисту персональних даних користувачів в умовах цифрової інформатизації державних реєстрів України»
в освітній процес кафедри управління інформаційною безпекою

Комісія у складі – голови начальника кафедри управління інформаційною безпекою, д.т.н., професора, полковника служби цивільного захисту ТКАЧУКА Ростислава Львовича та членів: доцента кафедри управління інформаційною безпекою, к.т.н., доцента, підполковника служби цивільного захисту ІВАНУСИ Андрія Івановича і доцента кафедри управління інформаційною безпекою, к.т.н., доцента ПОЛОТАЯ Ореста Івановича.

Цим актом засвідчується, що результати дисертаційного дослідження аспірантки третього (освітньо-наукового) рівня вищої освіти за спеціальністю 125 «Кібербезпека та захист інформації» БАЛАЦЬКОЇ Валерії Сергіївни на тему «Підвищення ефективності захисту персональних даних користувачів в умовах цифрової інформатизації державних реєстрів України» впроваджено в освітній процес Львівського державного університету безпеки життєдіяльності. Елементи наукового дослідження інтегровані у зміст навчальних дисциплін «Політика інформаційної безпеки в організаціях» та «Аудит, ліцензування та акредитація інформаційних систем», що викладаються здобувачам першого (бакалаврського) рівня вищої освіти, а також у дисципліну «Інтегровані системи санкціонованого доступу до інформації», що реалізується в межах підготовки здобувачів другого (магістерського) рівня за спеціальністю 125 «Кібербезпека та захист інформації». У межах вказаних освітніх компонент використовуються основні положення дисертації, зокрема розроблена модель перевірки достовірності транзакцій у permissioned blockchain-середовищах; методичний підхід до оцінювання ризиків доступу до персональних даних, а також концепція застосування сучасних криптографічних механізмів у процесах захисту інформації.

Зазначені результати дисертаційного дослідження впроваджено у формі навчально-методичних матеріалів, оновлених робочих навчальних програм (силабусів) освітніх компонент, практичних кейсів, орієнтованих на набуття професійних компетентностей у сфері захисту персональних даних.

Голова комісії:
начальник кафедри управління
інформаційною безпекою, д.т.н., професор Ростислав ТКАЧУК

Члени комісії:
доцент кафедри управління
інформаційною безпекою, к.т.н., доцент Андрій ІВАНУСА

доцент кафедри управління
інформаційною безпекою, к.т.н., доцент Орест ПОЛОТАЙ

Національна академія наук України
ДЕРЖАВНЕ ПІДПРИЄМСТВО
НАУКОВО-ТЕЛЕКОМУНІКАЦІЙНИЙ ЦЕНТР
"УКРАЇНСЬКА АКАДЕМІЧНА І ДОСЛІДНИЦЬКА МЕРЕЖА"
ІНСТИТУТУ ФІЗИКИ КОНДЕНСОВАНИХ СИСТЕМ НАН УКРАЇНИ

вул. Свєнціцького, 1, Львів, 79011
тел./факс: +380 322 768405, ел. пошта: uarnet@uar.net

АКТ
про впровадження результатів дисертаційної роботи
Балацької Валерії Сергіївни
««ПІДВИЩЕННЯ ЕФЕКТИВНОСТІ ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ КОРИСТУВАЧІВ В УМОВАХ ЦИФРОВОЇ ІНФОРМАТИЗАЦІЇ ДЕРЖАВНИХ РЕЄСТРІВ УКРАЇНИ»

Комісія у складі голови – заст. директора Олександра Гірняка, та члена комісії – гол. адміністратора мережі Петра Пелеха, склала цей акт про те, що розроблена Балацькою Валерією Сергіївною три-етапна модель перевірки достовірності персональних даних із використанням механізмів смарт-контрактів, нульового розголошення та машинного навчання, була успішно апробована в умовах, наближених до функціонування цифрової інфраструктури установи.

Реалізація моделі забезпечила ефективне виявлення несанкціонованих змін, перевірку цілісності даних користувача в режимі реального часу та автоматизоване прийняття рішень щодо допустимості доступу до записів державного реєстру. Апробація підтвердила можливість подальшого впровадження запропонованої архітектури у сервісах, що обробляють чутливу інформацію, з урахуванням вимог сучасного законодавства та принципів Privacy by Design.

Гірняк Олександр Зіновійович, заст. дир
Голова комісії, ДН НТЦ УАРНЕТ

Пелех Петро Романович, гол. адміністратор мережі
Член комісії, ДН НТЦ УАРНЕТ

М.П.

"УКРАЇНСЬКА АКАДЕМІЧНА І ДОСЛІДНИЦЬКА МЕРЕЖА" № 30275262 Україна м. Львів

м. Львів
22 травня 2025 року

ЗАТВЕРДЖУЮ

Проректор з науково-педагогічної роботи

Національного університету

«Львівська політехніка»

доц. _____ Олег ДАВИДЧАК

"22" 05 2025 р.

АКТ

про впровадження результатів дисертаційної роботи в навчальний процес

Балацької Валерії Сергіївни

«Підвищення ефективності захисту персональних даних користувачів в умовах цифрової інформатизації державних реєстрів України»

представленої на здобуття наукового ступеня доктора філософії за спеціальністю

125 – *Кібербезпека та захист інформації*

Комісія НУ «Львівська політехніка» у складі:

Голова комісії – голова науково-методичної ради інституту комп'ютерних технологій та метрології, д.т.н., проф. Яцук В.О.

Члени комісії:

Завідувач кафедри "Захист інформації", д.т.н., проф. Опірський.І.Р, професор кафедри "Захист інформації", д.т.н. проф. Микитин Г.В. і старший викладач кафедри "Захист інформації", к.т.н., Швед М.Є. даним актом підтверджує, що проведені дисертантом наукові дослідження виконувалися на кафедрі «Захист інформації» Національного університету «Львівська політехніка». Основні положення та результати дисертаційної роботи впроваджені у навчальний процес кафедри «Захист інформації» Національного університету «Львівська політехніка» при вивченні дисципліни: «Нормативно-правове забезпечення та міжнародні стандарти кіберб7езпеки» для студентів напрямку підготовки 125 «Кібербезпека та захист інформації», тема №4 «ЗУ «Про державну таємницю». «Про захист персональних даних»».

Голова комісії,
голова науково-методичної ради ІКТА
д.т.н., проф. Василь ЯЦУК

Члени комісії:
зав. каф. ЗІ, д.т.н., проф. Іван ОПІРСЬКИЙ
проф. каф. ЗІ, д.т.н. проф. Галина МИКИТИН
ст. викладач каф. ЗІ, к.т.н. Марія ШВЕД

ДОДАТОК Б. Список публікацій здобувача за темою дисертації та відомості про апробацію результатів дисертації

Наукові праці, в яких опубліковано наукові результати дисертації:

1. Балацька В. С., Опірський І. Р. Забезпечення конфіденційності персональних даних і підтримки кібербезпеки за допомогою блокчейну // Кібербезпека: освіта, наука, техніка. – 2023. – № 4 (20). – С. 6–19. – DOI: https://doi.org/10.28925/2663-4023.2023.20.619.

2. Opirskyy I., Balatska V., Poberezhnyk V. Modern possibilities of use blockchain technology in the education system // Ukrainian Scientific Journal of Information Security. – 2023. – Vol. 29, Issue 3. – P. 138–146. – DOI: https://doi.org/10.18372/2225-5036.29.18073.

3. Poberezhnyk V., Balatska V., Opirskyy I. Development of the learning management system concept based on blockchain technology // CEUR Workshop Proceedings. – 2023. – Vol. 3550: Cybersecurity Providing in Information and Telecommunication Systems II. – P. 38–49. – URL: https://ceur-ws.org/Vol-3550/.

4. Balatska V., Poberezhnyk V., Petriv P., Opirskyy I. Blockchain application concept in SSO technology context // CPITS-2024: Cybersecurity Providing in Information and Telecommunication Systems. – 2024. – P. 38–49. – URL: https://ceur-ws.org/Vol-3654/.

5. Балацька В., Побережник В., Опірський І. Використання non-fungible tokens та блокчейн для розмежування доступу до державних реєстрів // Кібербезпека: освіта, наука, техніка. – 2024. – № 4 (24). – С. 99–114. – DOI: https://doi.org/10.28925/2663-4023.2024.24.99114.

6. Balatska V., Opirskyy I., Slobodian N. Blockchain for enhancing transparency and trust in government registries // CPITS-II 2024: Cybersecurity Providing in Information and Telecommunication Systems II. – 2024. – P. 50–59. – URL: https://ceur-ws.org/Vol-3826/.

7. Balatska V., Poberezhnyk V., Opirskyy I. Utilizing blockchain technologies for ensuring the confidentiality and security of personal data in compliance with GDPR //

Proceedings of the Cyber Security and Data Protection. – Lviv, Ukraine, June 30, 2024. – CEUR Workshop Proceedings. – Vol. 3800. – P. 70–80. – URL: https://ceur-ws.org/Vol-3800/.

8. Balatska V., Opirskyy I. Blockchain as a tool for transparency and protection of government registries // Ukrainian Scientific Journal of Information Security. – 2024. – Vol. 30, Issue 2. – P. 221–230. – DOI: https://doi.org/10.18372/2225-5036.30.19211.

9. Балацька В., Побережник В. Концепція застосування блокчейн-технологій для підвищення захищеності персональних даних платформи «Дія»: відповідність вимогам GDPR та українському законодавству // Кібербезпека: освіта, наука, техніка. – 2024. – № 2 (26). – С. 268–290. – DOI: https://doi.org/10.28925/2663-4023.2024.26.681.

10. Ivanusa A., Tkachuk R., Brych T., Balatska V., Tkachenko A. Методи та моделі проєктування системи автоматизованого пошуку вразливостей у web-додатках // Вісник Львівського державного університету безпеки життєдіяльності. – 2024. – Вип. 30. – С. 110–122. – DOI: https://doi.org/10.32447/20784643.30.2024.11.

11. Балацька В. С., Побережник В. О., Стефанків А. В., Шевчук Ю. А. Розробка методу забезпечення достовірності та безпеки персональних даних у блокчейн-системах державних реєстрів // Комп’ютерні системи та мережі. – 2025. – Т. 7, № 1. – С. 1–16. – DOI: https://doi.org/10.23939/csn2025.01.001.

Наукові праці, які засвідчують апробацію матеріалів дисертації:

12. Балацька В. С., Опірський І. Р. Механізми досягнення надійності в блокчейні для захисту персональних даних // Захист інформації і безпека інформаційних систем : матеріали IX Міжнародної науково-технічної конференції (Львів, 25–26 травня 2023 р.). – Львів, 2023. – С. 17–18.

13. Балацька В. С., Побережник В. О., Опірський І. Р. Потенційне використання технології блокчейн в уряді // Інформаційна безпека та інформаційні технології : тези доповідей VI Всеукраїнської науково-практичної конференції молодих учених, студентів і курсантів (Львів, 30 листопада 2023 р.). – Львів, 2023. – С. 228–230.

14. Побережник В. О., Балацька В. С., Опірський І. Р. Концепція використання технології блокчейн у сфері освіти // Інформаційна безпека та інформаційні технології : тези доповідей VI Всеукраїнської науково-практичної конференції молодих учених, студентів і курсантів (Львів, 30 листопада 2023 р.). – Львів, 2023. – С. 386–388.

15. Балацька В. С., Побережник В. О., Опірський І. Р. Технології блокчейн, NFT та IPFS для підвищення ефективності та безпеки державних реєстрів України // Безпека інформаційних технологій : матеріали XIII Міжнародної науково-технічної конференції ITSec-2024 (Львів, 9–11 травня 2024 р.). – Львів, 2024. – С. 51–52.

16. Балацька В. С., Опірський І. Р. Підвищення безпеки державних реєстрів України за допомогою трьохфакторної аутентифікації на основі блокчейн // Актуальні проблеми сучасної науки в дослідженнях молодих учених, курсантів та студентів : тези доповідей Всеукраїнської науково-практичної конференції (Вінниця, 21 червня 2024 р.). – Вінниця, 2024. – С. 585–588.

17. Побережник В. О., Балацька В. С., Опірський І. Р. Адаптація блокчейн облікових даних до вимог GDPR // Інноваційні технології у розвитку сучасного суспільства : тези доповідей VI Міжнародної науково-практичної конференції (Львів, 10–11 жовтня 2024 р.). – Львів, 2024. – С. 39–41.

18. Балацька В. С., Опірський І. Р. Впровадження блокчейн-технологій для забезпечення безпеки та прозорості державних реєстрів // Сектор безпеки і оборони України на захисті національних інтересів: актуальні проблеми та завдання в умовах воєнного стану : тези доповідей III Міжнародної науково-практичної конференції (Хмельницький, 21 листопада 2024 р.). – Хмельницький, 2024.

19. Балацька В. С., Побережник В. О. Використання технологій блокчейн та NFT для розмежування доступу до державних реєстрів // Інформаційна безпека та інформаційні технології (ІБІТ-2024) : збірник доповідей V Міжнародної науково-практичної конференції (Львів, 27 листопада 2024 р.). – Львів, 2024. – С. 6–8.

20. Балацька В. С., Опірський І. Р. Технологія блокчейн для забезпечення довіри та прозорості у державних реєстрах // Інформаційна безпека та інформаційні

технології (ІБІТ-2024) : збірник доповідей V Міжнародної науково-практичної конференції (Львів, 27 листопада 2024 р.). – Львів, 2024. – С. 251–253.

21. Побережник В. О., Балацька В. С., Опірський І. Р. Концепція самосуверенної ідентичності як альтернатива традиційним методам автентифікації // Інформаційна безпека та інформаційні технології (ІБІТ-2024) : збірник доповідей V Міжнародної науково-практичної конференції (Львів, 27 листопада 2024 р.). – Львів, 2024. – С. 262–265.

22. Балацька В. С., Побережник В. О. Інформаційна безпека державних реєстрів: потенціал блокчейну для захисту критично важливих даних // Міжнародна та національна безпека: теоретичні і практичні аспекти : матеріали IX Міжнародної науково-практичної конференції, 21 березня 2025 р., м. Дніпро. Ч. 2. – Дніпро, 2025. – С. 468–471.

23. Побережник В. О., Балацька В. С. Концепція цифрового суверенітету в умовах розвитку блокчейн-економіки // Blockchain Technologies and Engineering 2025 (BTE 2025) : матеріали Міжнародної науково-практичної конференції (Київ, 26 березня 2025 р.). – Київ : ІПМЕ НАН України, 2025. – С. 75–76.