

УДК 004.056

ІНТЕГРАЦІЯ БЛОКЧЕЙН-ТЕХНОЛОГІЙ У СИСТЕМИ КОМПЛЕКСНОГО ЗАХИСТУ ІНФОРМАЦІЇ

Валерія БАЛАЦЬКА¹, Андрій ІВАНУСА¹, Василь ПОБЕРЕЖНИК²

1. Львівський державний університет безпеки життєдіяльності

2. Національний університет «Львівська політехніка»

Розглянуто інтеграцію блокчейн-технологій у структуру КСЗІ як інноваційний підхід до підвищення довіри, прозорості та стійкості інформаційних систем. Запропоновано гібридну модель на основі permissioned blockchain, яка дозволяє забезпечити простежуваність подій і зменшити ризики внутрішніх порушень. Проаналізовано практичні переваги та напрями впровадження.

Ключові слова: блокчейн, КСЗІ, довіра, permissioned blockchain, консенсус, ризик, кібербезпека, аутентифікація.

The paper investigates blockchain technology integration into complex information security systems (ISPS) as an innovative approach to enhance trust, transparency, and resilience. A hybrid permissioned blockchain model is proposed, ensuring event traceability and reducing insider risks. Practical advantages and implementation prospects in critical information infrastructures are discussed.

Keywords: blockchain, ISPS, trust, permissioned blockchain, consensus, risk, cybersecurity, authentication.

Сучасна цифрова екосистема, у якій взаємодіють державні, комерційні та освітні структури, функціонує в умовах постійного зростання обсягів даних, кількості користувачів і кіберзагроз. Глобальні тенденції цифрової трансформації – електронне врядування, хмарні сервіси, смарт-контракти, електронна ідентифікація – вимагають не лише технічних, а й концептуально нових підходів до забезпечення безпеки інформації. Водночас посилюються загрози внутрішніх інсайдерів, які мають легітимний доступ до ресурсів і здатні змінювати або видаляти критичні дані.

Класичні системи комплексного захисту інформації (КСЗІ), побудовані на централізованих принципах, уже не відповідають вимогам прозорості та довіри, оскільки значна частина інцидентів виникає не через технічні, а через організаційні та поведінкові фактори [1]. У таких умовах актуальним є створення середовища цифрової довіри, де автентичність і достовірність операцій підтверджуються не адміністраторами, а алгоритмами [2]. Одним із найбільш ефективних підходів є впровадження блокчейн-технологій у структуру КСЗІ, що дозволяє забезпечити незмінність журналів подій, децентралізований аудит, стійкість до внутрішніх маніпуляцій [3] і повну простежуваність життєвого циклу даних.

Блокчейн виступає як архітектура колективного контролю, у якій довіра до системи не потребує довіри до її окремих учасників. На відміну від централізованих баз даних, де єдина точка відмови створює ризики

втрата або спотворення інформації, блокчейн забезпечує консенсусне підтвердження подій між усіма вузлами мережі. Це формує нову парадигму безпеки – розподілену довіру, яка не залежить від людини чи організації, а підтримується математичними та криптографічними механізмами.

Використання *permissioned blockchain* забезпечує контрольований доступ, автентифікацію вузлів і гнучке управління ролями, що критично важливо для державних або корпоративних інформаційних систем, де відкриті публічні мережі неприйнятні. Такі мережі дозволяють застосовувати каналну сегментацію – кожен підрозділ або служба має власний канал транзакцій, який може перевірятися незалежно, зберігаючи при цьому загальний консенсус.

Запропонована модель інтеграції блокчейн в КСЗІ базується на трьохрівневій архітектурі, яка включає:

1. Ідентифікаційний рівень – управління ключами, сертифікатами, криптографічними токенами доступу та реєстрами користувачів.
2. Транзакційний рівень – децентралізований аудит і збереження подій у вигляді блоків із підписами та часовими мітками.
3. Аналітичний рівень – математичне оцінювання довіри, поведінковий аналіз і прогнозування ризиків на основі функції довіри.

Формалізований рівень довіри вузла і у момент часу t визначається як $T_i(t) = \alpha P_i(t) + \beta H_i(t) + \gamma S_i(t)$, де $P_i(t)$ – ймовірність коректної поведінки; $H_i(t)$ – показник історичної надійності; $S_i(t)$ – ступінь узгодженості дій із сусідніми вузлами; α, β, γ – вагові коефіцієнти, що описують вплив кожного параметра ($\alpha + \beta + \gamma = 1$).

Для моделювання ризику використовується експоненційна функція:

$$R_i(t) = 1 - e^{(-\lambda(T(crit) - T_i(t)))},$$

де λ – коефіцієнт чутливості системи, $T(crit)$ – критичне значення довіри, за яким система переходить у режим посиленого контролю. Таким чином, навіть незначне падіння довіри викликає нелінійне зростання ризику, що дає змогу оперативно реагувати на потенційні загрози.

Ймовірність несанкціонованої модифікації даних у блокчейн описується виразом $P(mod) = (1 - p)^n$, де p – ймовірність правильного підтвердження транзакції одним вузлом, n – кількість вузлів у консенсусній групі. Для систем із 10 вузлами при $p=0,85$ ймовірність успішної підміни даних становить лише 0,0002, що практично унеможливило компрометацію журналів аудиту. Моделювання виконано на тестовому середовищі Hyperledger Fabric з використанням алгоритмів RAFT і PBFT. Результати показали, що впровадження блокчейн скорочує час виявлення аномалій на 25-30 %, зменшує кількість помилкових сповіщень на 18% і повністю усуває можливість редагування журналів подій без колективного підтвердження.

Особливу увагу приділено організаційному аспекту інтеграції, який полягає у розподілі функцій контролю між підсистемами [4]. Це дозволяє знизити залежність від людського чинника, автоматизувати управління

політиками безпеки та створити «пояснювану КСЗІ» (Explainable Security), де кожне рішення має формалізоване математичне обґрунтування.

Впровадження блокчейн-технологій у державні інформаційні системи України сприятиме реалізації принципів Zero Trust Architecture [5] – архітектури «нульової довіри», що базується на постійній перевірці кожної дії користувача. Крім того, поєднання блокчейн з алгоритмами штучного інтелекту дозволить створювати самонавчальні системи кіберзахисту, які динамічно адаптуються до змін середовища, зберігаючи відповідність міжнародним стандартам ISO/IEC 27001, 27701 та вимогам GDPR. З практичного погляду, така модель може бути впроваджена у вітчизняних реєстрах, зокрема у системах електронних сервісів «Дія», кадастрових реєстрах, медичних базах, банківських сервісах, де важливо довести незмінність транзакцій і зберегти довіру користувачів. Вона також може стати базою для створення універсальної платформи перевірки подій безпеки, здатної інтегрувати різні державні КСЗІ у спільний довірчий простір.

Підсумовуючи, слід зазначити, що інтеграція блокчейн в архітектуру КСЗІ є не просто технологічним трендом, а стратегічним напрямом розвитку національної інформаційної безпеки. Така синергія математичного моделювання, децентралізованої довіри та автоматизованого аудиту формує нову парадигму – «безпека через довіру», яка має потенціал стати основою майбутніх державних і корпоративних систем кіберзахисту.

Література

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. Balatska V., Opirskyy I. Blockchain as a tool for transparency and protection of government registries // Ukrainian Scientific Journal of Information Security. – 2024. – Vol. 30(2). – P. 221–230. DOI: <https://doi.org/10.18372/2225-5036.30.19211>
3. Балацька В., Ткачук Р., Маслоva Н. Еволюція КСЗІ та інтеграція блокчейн-технологій у кіберзахисті державних інформаційних систем України // Кібербезпека: освіта, наука, техніка. – 2025. – № 2(30). – С. 316–332. DOI: <https://doi.org/10.28925/2663-4023.2025.30.975>
4. Opirskiy I., Poberezhnyk V., Balatska V. Method for Ensuring Data Integrity and Authenticity Based on Blockchain Technology Integration / I. Opirskiy, V. Poberezhnyk, V. Balatska // DECaT'2025: Digital Economy Concepts and Technologies, April 4, 2025, Kyiv. CEUR Workshop Proceedings 3800, pp. 70-80. URL: <https://ceur-ws.org/Vol-4029/>
5. 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>