УДК 004.056

ВИКОРИСТАННЯ БЛОКЧЕЙН-ТЕХНОЛОГІЙ ДЛЯ ПІДВИЩЕННЯ ДОВІРИ В АУДИТІ ТА АКРЕДИТАЦІЇ ІНФОРМАЦІЙНИХ СИСТЕМ

Назарій ДМИТРІВ[1], Валерія БАЛАЦЬКА[2]

1. Приватний вищий навчальний заклад «Європейський університет»,м. Київ

2. Львівський державний університет безпеки життєдіяльності

Досліджено можливості використання блокчейн-технологій у процесах аудиту, ліцензування та акредитації ін-формаційних систем. Запропоновано концепцію цифрового аудиту з використанням permissioned blockchain для забез-печення прозорості, незмінності та відтворюваності результатів перевірки. Розглянуто підходи до підвищення довіри між акредитуючими органами, розробниками та користувачами систем.

Ключові слова: *блокчейн, аудит, акредитація, КСЗІ, довіра, ліцензування, цифровий контроль, ризик-менеджмент..*

The potential of blockchain technologies in auditing, licensing, and accreditation of information systems is explored. A concept of digital audit using a permissioned blockchain is proposed to ensure transparency, immutability, and traceability of verification results. The approach enhances trust among accreditation authorities, system developers, and end users.

Keywords: *blockchain, audit, accreditation, ISPS, trust, licensing, digital control, risk management*

Розвиток цифрового врядування, розширення електронних сервісів та інтеграція державних реєстрів вимагають підвищення рівня довіри до процесів аудиту, ліцензування та акредитації інформаційних систем. У традиційній моделі перевірки ефективність і достовірність результатів залежать від суб'єктивних чинників – компетентності експертів, якості підготовленої документації, людського контролю та адміністративного впливу [1]. Такий підхід формує ризики фальсифікації результатів, вибіркового ставлення, конфлікту інтересів і неузгодженості між акредитуючими органами, що особливо небезпечно для державних систем, які обробляють критичні дані.

Блокчейн-технології відкривають можливість усунення цих проблем шляхом створення незмінного децентралізованого реєстру аудиторських дій, у якому кожен запис фіксується як транзакція з часовою міткою та криптографічним підписом [2]. У такій моделі жоден учасник не має можливості самостійно змінювати чи видаляти дані перевірки, що забезпечує прозорість і відтворюваність кожного етапу контролю. Такий підхід підвищує рівень цифрової довіри, дозволяє автоматично перевіряти достовірність звітів і запобігає маніпуляціям під час акредитації.

Запропонована модель системи блокчейн-аудиту побудована на основі permissioned blockchain, де кожен вузол належить визначеному суб'єкту процесу: акредитуючому органу, розробнику, власнику інформаційної системи, незалежному аудитору та державному регулятору. Усі вузли взаємодіють у режимі контрольованого консенсусу, який гарантує узгоджене збереження результатів. Кожен етап перевірки – від тестування ефе-

ктивності КСЗІ до оцінки політик безпеки – фіксується у блокчейні, формуючи ланцюг довіри (chain of trust) [3].

Для підвищення об'єктивності пропонується використати математичну модель інтегрального індексу довіри (Trust Index), що враховує результати попередніх аудитів і вагомість виявлених невідповідностей:

$$T_{sys} = \alpha A_{rep} + \beta A_{comp} + \gamma A_{risk},$$

де A_{rep} – рівень репутаційної надійності аудитора, A_{comp} – середня оцінка відповідності стандартам, A_{risk} – показник ризиковості системи; α, β, γ – вагові коефіцієнти *(α+β+γ=1)*.

Якщо $T_{sys} \geq 0,8$, система визнається такою, що заслуговує довіри й може бути акредитована; при $0,6 \leq T_{sys} < 0,8$ – потрібні додаткові перевірки; нижче *0,6* – акредитація неможлива. Така формалізація мінімізує вплив людського чинника та перетворює процес аудиту на цифрово підтверджувану процедуру, що відповідає принципам ISO/IEC 17065:2022 і вимогам GDPR щодо контролю обробки персональних даних [4].

Важливою складовою моделі є створення єдиного децентралізованого реєстру сертифікованих інформаційних систем, який містить структуровані метадані про статус акредитації, дати перевірок, типи впроваджених КСЗІ, чинні сертифікати відповідності, результати аудитів і рівень довіри до системи. Такий реєстр може бути реалізований у форматі permissioned blockchain, де запис здійснюють лише уповноважені органи, а перегляд окремих параметрів можливий для громадськості через відкритий вебінтерфейс. Це забезпечує поєднання прозорості та конфіденційності: відкритими залишаються лише контрольні хеші, дати й статуси акредитації, тоді як внутрішні звіти зберігаються у зашифрованому вигляді.

Використання такого механізму підвищує рівень довіри громадськості до органів контролю у сфері інформаційної безпеки, створює умови для взаємної перевірки між суб'єктами й спрощує процес верифікації сертифікатів. Сторонні аудитори або постачальники послуг можуть підтверджувати дійсність сертифікатів без запитів до центральних баз, що підвищує ефективність контролю в реальному часі.

Інтеграція смарт-контрактів аудиту дає змогу автоматично перевіряти відповідність КСЗІ мінімальним вимогам [5]. Алгоритми контрактів верифікують наявність криптографічних модулів, резервного копіювання, політик доступу, журналювання інцидентів тощо. У разі виявлення невідповідностей смарт-контракт формує цифровий звіт, який додається до блокчейну та може ініціювати повторну оцінку системи. Це частково автоматизує аудит, зменшує вплив людського чинника та скорочує тривалість акредитації з кількох тижнів до кількох днів.

Імітаційне моделювання у середовищі Hyperledger Fabric підтвердило практичну ефективність підходу. Система містила три типи вузлів: регулятор, аудитор і розробник. За результатами експериментів середній час обробки заявки скоротився на 32 %, а кількість логічних помилок у звітно-

сті – на 19 %. Крім того, жоден запис не міг бути змінений без підтвердження більшістю вузлів мережі, що доводить стійкість рішення до внутрішніх маніпуляцій.

Крім технічних переваг, важливими є організаційно-правові аспекти. Чинні нормативні акти (Постанова КМУ № 373, Закон України «Про захист інформації в ІТС») не враховують децентралізованих моделей аудиту. Проте блокчейн може функціонувати як доповнення до чинних процедур експертизи КСЗІ, забезпечуючи цифрову фіксацію дій експертів, незалежну верифікацію рішень і можливість перевірки достовірності сертифікатів у будь-який момент часу.

У перспективі це створить підґрунтя для національного електронного реєстру акредитованих систем, інтегрованого з державними платформами «Дія» та ДССЗЗІ. Такий підхід забезпечить централізоване, але децентралізовано верифіковане зберігання даних, автоматичний моніторинг чинності сертифікатів і контроль термінів їх поновлення.

Впровадження блокчейн-технологій у процеси аудиту, ліцензування та акредитації формує нову модель цифрової довіри, у якій кожна дія має криптографічне підтвердження, а історія змін зберігається у розподіленому середовищі. Це підвищує стійкість до кіберзагроз, достовірність даних і створює основу для реалізації національної стратегії кіберстійкості та гармонізації українських підходів із міжнародними стандартами ISO/IEC 27001, 27701 і 17065.

Література

1. Балацька В. С., Дмитрів Н. Міжорганізаційний обмін конфіденційними персональними даними на основі дозвільного блокчейн // Кібербезпека: освіта, наука, техніка. – 2025. – № 2(29). – С. 178–193. DOI: https://doi.org/10.28925/2663-4023.2025.29.875.

2. 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.

3. Опірський І., Побережник В., Балацька В. Method for Ensuring Data Integrity and Authenticity Based on Blockchain Technology Integration // CEUR Workshop Proceedings: DECaT'2025 – Digital Economy Concepts and Technologies. – Kyiv, 2025. – P. 70–80. URL: https://ceur-ws.org/Vol-4029/.

4. Wang Y., Singh S., Al-Bahadili H. Blockchain-Based Audit Framework for Ensuring Integrity and Trust in Digital Certification Systems // IEEE Access. – 2024. – Vol. 12. – P. 48756–48771. DOI: https://doi.org/10.1109/ACCESS.2024.3456712.

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.