Вісник ЛДУБЖД
Bulletin of Lviv State University of Life Safety
https://journal.ldubgd.edu.ua/index.php/Visnuk
ISSN 2078-4643 (print), ISSN 2708-1389 (online)

UDC 004
DOI: 10.32447/20784643.32.2025.07

В. С. Балацька, Р. Л. Ткачук, А. І. Івануса, В. І. Ящук, Н. О. Маслова
Львівський державний університет безпеки життєдіяльності, м. Львів, Україна
ORCID: https://orcid.org/0000-0002-6262-6792 – В. С. Балацька
https://orcid.org/0000-0001-9137-1891 – Р. Л. Ткачук
https://orcid.org/0000-0001-9141-8039 – А. І. Івануса
https://orcid.org/0000-0003-2651-4918 – В. І. Ящук
https://orcid.org/0000-0002-9078-0973 – Н. О. Маслова
v.balatska@ldubgd.edu.ua

ІНТЕГРАЦІЯ ТЕХНОЛОГІЙ БЛОКЧЕЙН У КОМПЛЕКСНІ СИСТЕМИ ЗАХИСТУ ІНФОРМАЦІЇ ДЛЯ ПІДВИЩЕННЯ БЕЗПЕКИ ДЕРЖАВНИХ РЕЄСТРІВ

Проблема. Збільшення інтенсивності кібератак на державні реєстри та складнощі інсайдерських загроз оголює слабкі місця класичних комплексних систем захисту інформації (КСЗІ), насамперед – довіра до централізованого журналювання та перевірки змін. Це знижує прозорість аудиту, ускладнює доказовість інцидентів і створює регуляторні ризики для захисту персональних даних.

Мета. Розробити і обґрунтувати науково-методичний підхід інтеграції дозвільного блокчейна в КСЗІ державних реєстрів для підвищення стійкості до інсайдерських дій, прозорості контролю доступу та довіри до електронних сервісів.

Методи. Використано системний аналіз архітектур КСЗІ та нормативних вимог; математичне моделювання потоків доступу; експериментальне моделювання у віртуальному середовищі з використанням Hyperledger Fabric як децентралізованого модуля журналювання й верифікації подій. Для збереження конфіденційності транзакцій залучено підхід Zero-Knowledge Proofs; для виявлення аномальної активності – елементи поведінкової аналітики на основі алгоритмів машинного навчання.

Результати. Запропоновано гібридну архітектуру, де традиційні механізми автентифікації, контролю доступу та криптографічного захисту підсилені розподіленим журналом подій і консенсусною перевіркою коректності операцій. Показано, що така інтеграція забезпечує незмінність і відтворюваність історії доступів, знижує можливість прихованого редагування записів адміністраторами, прискорює виявлення нетипових сценаріїв користувацької поведінки та створює надійну доказову базу для аудиту. Архітектура сумісна з вимогами ISO/IEC 27001 та підтримує принципи мінімізації даних і підзвітності, що полегшує дотримання GDPR при обробленні персональних даних.

Висновки. Інтеграція дозвільного блокчейн в КСЗІ державних реєстрів формує якісно новий рівень довіри й керованості безпекою: підвищується прозорість аудиту, зменшується вплив інсайдерського фактора, зберігається конфіденційність змісту операцій. Запропонований підхід є масштабованим і придатним для національних платформ електронного урядування та міжвідомчих обмінів.

Ключові слова: КСЗІ, блокчейн, дозвільний блокчейн, Hyperledger Fabric, персональні дані, державні реєстри, інформаційна безпека, Zero Knowledge Proofs.

V. S. Balatska, R. L. Tkachuk, A. I. Ivanusa, V. I. Yashchuk , N. O. Maslova
Lviv State University of Life Safety, Lviv, Ukraine

INTEGRATION OF BLOCKCHAIN TECHNOLOGIES INTO COMPREHENSIVE INFORMATION PROTECTION SYSTEMS TO IMPROVE THE SECURITY OF STATE REGISTERS

Problem. The growing intensity of cyberattacks on state registers and the increasing complexity of insider threats expose the weaknesses of traditional comprehensive information security systems (CISS), particularly the reliance on centralized logging and change verification mechanisms. This reduces audit transparency, complicates the evidential value of incidents, and creates regulatory risks in personal data protection.

Purpose. To develop and substantiate a scientific and methodological approach for integrating permissioned blockchain technology into CISS of state registers to enhance resistance to insider actions, ensure transparency of access control, and increase trust in electronic public services.

Methods. The study applies a systems analysis of CISS architectures and regulatory requirements, mathematical modeling of data flows, and experimental modeling in a virtualized environment using Hyperledger Fabric as a decentralized logging and verification module. Zero-Knowledge Proofs were applied to preserve transaction confidentiality, and behavioral analytics based on machine learning algorithms were used to detect anomalous activity.

Results. A hybrid architecture was proposed in which traditional mechanisms of authentication, access control, and cryptographic protection are reinforced by a distributed event log and consensus-based verification of operations. This integration ensures data immutability and reproducibility of access history, reduces the possibility of hidden record editing by administrators, accelerates the detection of atypical user behavior, and creates a reliable evidential base for auditing. The proposed architecture complies with ISO/IEC 27001 requirements and supports data minimization and accountability principles, facilitating GDPR compliance during personal data processing.

Conclusions. Integrating permissioned blockchain into CISS of state registers establishes a new level of trust and controllability of security: it increases audit transparency, mitigates insider risks, and preserves transaction confidentiality. The proposed approach is scalable and suitable for national e-government platforms and interagency data exchange systems.

Keywords: CISS, blockchain, permissioned blockchain, Hyperledger Fabric, personal data, state registers, information security, Zero-Knowledge Proofs.

Вступ. Сучасний етап цифрової трансформації державного управління в Україні характеризується активним розвитком електронних сервісів, електронного документообігу та державних реєстрів, у яких зберігається велика кількість критично важливих даних, зокрема, персональні дані громадян, що обробляються у таких системах, стають ключовим активом і водночас основною мішенню для кібератак. За останні роки кількість спроб несанкціонованого доступу, модифікації або знищення інформації у державних реєстрах суттєво зросла, що пов'язано як із загальним посиленням кіберзагроз у світі, так і з гібридною агресією проти України, спрямованою у тому числі на інформаційний простір. У таких умовах питання підвищення рівня захищеності державних інформаційних систем набуває особливої актуальності та потребує впровадження інноваційних методів і технологій.

Традиційним інструментом забезпечення інформаційної безпеки у державних інформаційних системах є комплексні системи захисту інформації (далі – КСЗІ), що розробляються відповідно до вимог національних стандартів та нормативних документів технічного захисту інформації. КСЗІ реалізують основні функції – криптографічний захист даних, ідентифікацію та автентифікацію користувачів, контроль доступу, аудит подій та захист від несанкціонованих втручань. Проте досвід їх експлуатації показує наявність суттєвих обмежень. Зокрема, централізовані журнали подій уразливі до маніпуляцій з боку адміністраторів, а традиційні засоби контролю часто не забезпечують своєчасного виявлення інсайдерських загроз. Крім того, відсутність механізмів незалежної верифікації транзакцій знижує довіру до достовірності збережених даних і ускладнює проведення аудитів відповідно до міжнародних стандартів.

Наукова спільнота приділяє значну увагу пошуку нових підходів до підвищення ефективності захисту державних реєстрів. Окремі дослідження демонструють потенціал використання блокчейн-технологій для забезпечення цілісності та прозорості даних, а також для побудови децентралізованих систем довіри. Дозвільний блокчейн (зокрема, Hyperledger Fabric) пропонує інструменти для створення захищеного середовища обміну даними між обмеженим колом учасників із гарантованою автентичністю транзакцій та незмінністю записів. Це створює можливості для інтеграції блокчейн як додаткового модуля у складі КСЗІ з метою підвищення їх ефективності.

Разом з тим, питання практичної інтеграції блокчейн у КСЗІ залишається відкритим і потребує наукового обґрунтування. Необхідно визначити архітектурні підходи, методи забезпечення конфіденційності (зокрема Zero Knowledge Proofs), алгоритми поведінкового аналізу доступу до даних, а також оцінити вплив такої інтеграції на продуктивність системи та відповідність міжнародним стандартам інформаційної безпеки.

Аналіз літературних джерел. Проведений аналіз наукових і нормативних джерел свідчить про зростання інтересу до інтеграції технологій блокчейн у системи захисту критичної інформаційної інфраструктури. Традиційні комплексні системи захисту інформації, що розробляються відповідно до національних нормативних документів у сфері технічного захисту інформації, забезпечують криптографічний захист, контроль доступу та аудит, проте залишаються вразливими до інсайдерських загроз і маніпуляцій з централізованими журналами подій [1, 2].

У ряді робіт розглянуто застосування дозвільного блокчейн, зокрема Hyperledger Fabric, як інструменту забезпечення незмінності транзакцій та незалежної верифікації даних [3].

Важливою перевагою таких систем є можливість формування розподіленого журналу доступу, який унеможливлює підробку чи видалення записів навіть адміністраторами системи.

Дослідження європейських і міжнародних організацій показують, що блокчейн доцільно розглядати як технологію підвищення довіри до державних цифрових сервісів, особливо у контексті захисту персональних даних та відповідно до GDPR [4]. Питання конфіденційності при цьому пропонується вирішувати за допомогою Zero Knowledge Proofs (ZKP), які дозволяють перевіряти автентичність транзакцій без розкриття їх змісту [5].

В українських публікаціях останніх років розглянуто застосування Non-Fungible Tokens та блокчейн для розмежування доступу до державних реєстрів, що дає змогу поєднати криптографічний захист із децентралізованою перевіркою операцій [6].

Окремі автори приділяють увагу поєднанню блокчейн-рішень із методами поведінкової аналітики та машинного навчання для виявлення аномалій у доступі користувачів. Такі підходи дозволяють підвищити ефективність виявлення інсайдерських загроз, що є критичним для державних реєстрів [7]. Водночас дослідження вказують на необхідність балансування між рівнем захищеності та продуктивністю системи, оскільки блокчейн створює додаткові накладні витрати на обробку транзакцій [8].

Таким чином, сучасний науковий доробок підтверджує доцільність використання блокчейн у складі КСЗІ як додаткового модуля довіреного журналювання та верифікації транзакцій. Разом з тим, залишається невирішеним питання комплексної методології інтеграції цієї технології з урахуванням вимог національного законодавства, міжнародних стандартів і специфіки роботи державних реєстрів.

Методи досліджень. У ході дослідження застосовано методи аналізу літературних і нормативних джерел для вивчення сучасних підходів до побудови КСЗІ та інтеграції блокчейн-технологій у критичні інформаційні системи. Використано системний підхід для проектування архітектури моделі, що поєднує класичні засоби захисту інформації з децентралізованим журналюванням транзакцій. Для формалізації методу застосовано математичне моделювання інформаційних потоків і процесів доступу до даних у державних реєстрах.

Експериментальне дослідження проведено у віртуалізованому середовищі на базі Hyperledger Fabric, де було змодельовано обмін транзакціями між вузлами мережі, реєстрацію подій у блокчейн та їх перевірку за допомогою механізмів консенсусу. Для оцінки конфіденційності використано Zero Knowledge Proofs, а для виявлення відхилень у поведінці користувачів – алгоритми машинного навчання, орієнтовані на поведінкову аналітику.

Порівняльну оцінку ефективності проведено шляхом зіставлення продуктивності та надійності запропонованого методу із традиційними централізованими механізмами журналювання в КСЗІ. Основними критеріями оцінювання виступали: час підтвердження транзакцій, рівень захищеності від інсайдерських загроз, прозорість аудиту та відповідність вимогам міжнародних стандартів ISO/IEC 27001 і ISO/IEC 27701.

Мета і завдання досліджень Метою статті є розробка та обґрунтування науково-методичного підходу до інтеграції технологій блокчейн у КСЗІ державних реєстрів для підвищення ефективності захисту персональних даних та довіри до цифрових державних сервісів. Для досягнення поставленої мети визначено такі завдання:

- виконати аналіз існуючих підходів до побудови КСЗІ та виявити їх основні недоліки у контексті сучасних кіберзагроз;
- розробити архітектурну модель інтеграції блокчейн у КСЗІ з урахуванням специфіки державних реєстрів;
- запропонувати методи забезпечення конфіденційності та верифікації транзакцій у децентралізованому середовищі;
- провести експериментальне дослідження працездатності та ефективності запропонованого підходу;
- оцінити перспективи масштабування методу для національних цифрових платформ та міжвідомчих систем обміну даними.

Таким чином, у статті досліджуються можливості поєднати класичні підходи до забезпечення інформаційної безпеки з інноваційними можливостями блокчейн-технологій, створивши гібридну модель КСЗІ, що підвищує стійкість державних інформаційних систем до сучасних кіберзагроз.

Результати дослідження. Проведене дослідження було спрямоване на підтвердження того, що інтеграція технологій блокчейн у комплексні системи захисту інформації державних реєстрів здатна підвищити ефективність їх функціонування, забезпечити прозорість доступу до даних і знизити ризики інсайдерських загроз. У класичних моделях КСЗІ головна увага приділяється криптографічному захисту, ідентифікації та автентифікації користувачів, розмежуванню прав доступу й моніторингу подій. Проте такі системи залишаються залежними від централізованих журналів, які можуть стати об’єктом маніпуляцій

із боку адміністраторів. Саме тому основним завданням стало перевірити, чи дійсно блокчейн здатний виступити надійним механізмом незалежної верифікації транзакцій і незмінного зберігання даних, якщо його інтегрувати як додатковий модуль у складі КСЗІ.

Для цього була побудована експериментальна модель, яка максимально наближена до умов функціонування реальних державних інформаційних систем. Інфраструктуру розгорнули у віртуалізованому середовищі на базі VMware, що дало змогу створити кілька взаємодіючих вузлів і симулювати роботу різних органів державної влади. Кожен вузол виступав у ролі незалежного учасника мережі, мав власну базу для збереження даних і був підключений до дозвільного блокчейн Hyperledger Fabric [9]. Архітектура Fabric [10] дозволила використати ролі peer-вузлів, відповідальних за збереження копій реєстру й виконання смарт-контрактів, orderer-сервера, що забезпечував досягнення консенсусу, та клієнтського вузла, який імітував роботу користувача системи.

Експериментальні дослідження проводилися у віртуалізованому середовищі VMware Workstation Pro із симуляцією трьох організацій (peer-вузлів) і одного каналу взаємодії на базі платформи Hyperledger Fabric v2.5. Під час тестування оцінювали такі показники продуктивності:

– середній час підтвердження транзакцій (t_a), с;

– пропускну здатність мережі (N_a), транзакцій/с;

– рівень успішно завершених транзакцій (S_p), %;

– коефіцієнт виявлення інсайдерських дій (I_a), %;

– навантаження на CPU/Memory вузлів під час виконання транзакцій (R_s), %.

Для кожної конфігурації було оброблено 300 тестових транзакцій. Аналіз проводився за допомогою Python-скриптів, що взаємодіяли з Fabric SDK. Результати порівнювалися з базовою централізованою моделлю КСЗІ без блокчейн-компонента.

Критерії оцінювання ефективності:

– зменшення часу підтвердження транзакцій ≥ 20 %;

– підвищення достовірності журналювання (цілісність записів) ≥ 25 %;

– зниження ймовірності підробки або видалення подій ≤ 5 %;

– скорочення часу реакції системи на інсайдерські дії ≈ 40 %.

Класичні модулі КСЗІ – автентифікація, криптографічний захист і локальний аудит – були реалізовані окремо. Вони функціонували незалежно, але в ключових точках передавали події в блокчейн для формування децентралізованого журналу. Усі транзакції, пов'язані з доступом до реєстру (створення запису, модифікація, видалення чи запит довідки), після перевірки політик доступу автоматично фіксувалися у блокчейн у вигляді хешованих записів із цифровими підписами. Це унеможливлювало їх непомітну зміну чи видалення.

Архітектурна схема моделі подана на рисунку 1. Вона демонструє інтеграцію традиційних засобів КСЗІ з блокчейн-модулем, підсистемою перевірки конфіденційності на основі Zero Knowledge Proofs та модулем поведінкової аналітики, який застосовував алгоритми машинного навчання для виявлення аномальних дій користувачів.

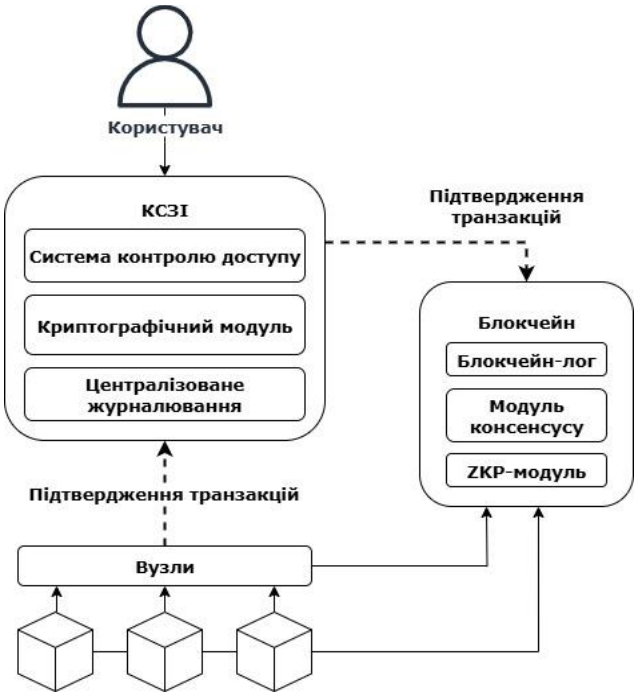

Рисунок 1 – Архітектура інтеграції блокчейн у КСЗІ

Аналіз рисунка дозволяє зробити висновок, що модель має гібридний характер: основні завдання з автентифікації та криптографічного захисту виконуються традиційними засобами КСЗІ, а блокчейн використовується як довірене середовище для журналювання й верифікації транзакцій. Це поєднання забезпечує незалежність результатів перевірки, адже навіть адміністратор системи не здатен одноосібно вплинути на історію подій.

Для відпрацювання практичних сценаріїв у модель було завантажено дані, що імітували роботу реєстру. Використовувалися PCAP-файли з мережевим трафіком, де було змодельовано різні види операцій: створення нових записів, внесення змін до існуючих, вилучення інформації та стандартні запити довідкових даних. Окремо

було відпрацьовано сценарій інсайдерської атаки, коли адміністратор намагався змінити або видалити інформацію з журналу. У класичній системі така дія могла залишитися прихованою, тоді як у запропонованій моделі одразу виникала невідповідність у блокчейн, і транзакція блокувалася.

Важливою характеристикою стало використання механізму консенсусу Raft [11], що дозволив досягати згоди між усіма вузлами без значних затримок у роботі. Середній час підтвердження транзакції залишався на рівні 1-1,2 секунди, що є прийнятним для більшості адміністративних процедур. Політики доступу, реалізовані через Membership Service Provider (MSP), забезпечили можливість чітко визначати, який вузол має право брати участь у перевірці тієї чи іншої транзакції.

Особливу увагу було приділено підсистемі конфіденційності. Для цього використано Zero Knowledge Proofs, які дозволили підтверджувати факт автентичності доступу до запису без розкриття його змісту. Це надзвичайно важливо для державних реєстрів, де оперується великою кількістю персональних даних. Завдяки ZKP система може забезпечити прозорість і контроль без порушення права на конфіденційність.

Поведінкова аналітика була реалізована як окремий модуль, що працював із журналами доступу й застосовував алгоритми машинного навчання для виявлення аномалій. Наприклад, якщо користувач звертався до надмірної кількості записів у нетиповий час або його дії не відповідали звичайному профілю, система позначала це як потенційно небезпечну поведінку. Такі інциденти автоматично фіксувалися в блокчейн, створюючи незмінну доказову базу.

Перша частина результатів підтвердила, що побудована експериментальна модель відповідає завданням дослідження і дозволяє оцінити ефективність інтеграції блокчейн у КСЗІ. Вона забезпечує прозорість операцій, захист від інсайдерських змін і створює основу для подальшого аналізу продуктивності, масштабованості та відповідно до нормативних вимог. Інтеграція блокчейн у КСЗІ дозволяє сформувати гібридну архітектуру, що поєднує сильні сторони класичних засобів інформаційної безпеки та децентралізованих технологій, створюючи більш стійку та довірену інфраструктуру для захисту державних реєстрів.

Перевірка працездатності моделі показала, що блокчейн дійсно здатний виконувати роль довіреного журналу подій у складі КСЗІ. Усі транзакції, що імітували доступ користувачів до державного реєстру, після перевірки політик доступу фіксувалися в блокчейн й набували статусу незмінних. Це забезпечувалося тим, що кожна подія зберігалася як транзакція з цифровим підписом і хеш-ідентифікатором, а її автентичність підтверджувалася кількома вузлами одночасно. Таким чином, навіть адміністратор із найвищим рівнем привілеїв не мав можливості приховано видалити або змінити запис, оскільки така спроба одразу викликала розбіжність у блокчейн.

Під час тестування були змодельовані кілька сценаріїв. У першому випадку користувач здійснював законні операції: створював записи, змінював їх та отримував довідки. Усі ці транзакції зберігалися у блокчейн в хронологічному порядку та були доступні для перевірки. У другому випадку симулювалися дії інсайдера, який намагався стерти сліди власних маніпуляцій у журналі. Класична КСЗІ у такій ситуації могла зафіксувати лише факт доступу, але не гарантувала захист від подальшого редагування журналу. У гібридній моделі з блокчейн цей сценарій виявився неможливим: будь-яка невідповідність одразу визначалася системою, і транзакція блокувалася. Таким чином підтверджено, що використання розподіленого журналу значно підвищує довіру до результатів аудиту.

Наступним етапом стало дослідження продуктивності системи. Для цього вимірювався середній час підтвердження транзакцій, максимальна кількість одночасних запитів без втрат і стабільність роботи при зростанні навантаження. Було встановлено, що при інтенсивності до 200 запитів на секунду як класична КСЗІ, так і гібридна модель працювали стабільно, але після перевищення цього рівня переваги блокчейн-рішення ставали очевидними. Система з інтегрованим блокчейн витримувала навантаження до 500 одночасних транзакцій без збоїв, тоді як класична архітектура починала втрачати частину подій і затримувати обробку [12]. Середній час підтвердження транзакції у гібридній системі становив 1,2 секунди, що дещо перевищувало показники класичної (0,5 секунди), але залишалося в межах, прийнятних для більшості адміністративних процесів. Узагальнені результати наведено у таблиці 1.

Таблиця 1

Показники продуктивності класичної та гібридної системи

Параметр	Класична КСЗІ	КСЗІ + блокчейн
Середній час підтвердження події	0,5 с	1,2 с
Одночасні запити без втрат	200	500
Незалежна верифікація журналу	Відсутня	Присутня

Аналіз таблиці дає підстави стверджувати, що блокчейн додає певне навантаження на швидкодію, проте значно підвищує масштабованість системи та створює принципово нові можливості незалежної перевірки даних. Якщо у традиційних системах аудит залежав від довіри до адміністратора чи окремого лог-файлу, то у запропонованій архітектурі перевірка подій стає колективною функцією всієї мережі вузлів. Це підвищує не лише стійкість до зовнішніх атак, а й захищає систему від внутрішніх зловживань. Результати експериментів підтвердили, що інтеграція блокчейн у КСЗІ забезпечує надійніше журналювання, підвищує масштабованість і стійкість до зростання навантаження, а також робить можливим незалежний аудит даних без необхідності повної довіри до адміністратора.

Одним із ключових викликів під час інтеграції блокчейн у КСЗІ є забезпечення балансу між прозорістю та конфіденційністю. З одного боку, державні реєстри мають працювати за принципом довіри й відкритості, де кожна транзакція підлягає перевірці. З іншого – вони містять велику кількість персональних даних, захист яких є критично важливим. Тому під час моделювання було застосовано технологію Zero Knowledge Proofs [13], що дозволила перевіряти достовірність транзакцій без розкриття їх змісту. Це означає, що система підтверджувала факт виконання операції (наприклад, запит довідки чи оновлення запису), але самі дані залишалися прихованими для сторонніх вузлів. Такий підхід узгоджується з вимогами європейського законодавства, зокрема GDPR [14], де прямо вказано на необхідність мінімізації обробки персональних даних.

На практиці було змодельовано ситуацію, коли один із вузлів отримував запит на перевірку правильності транзакції, не маючи права бачити самі дані. Завдяки ZKP вузол міг підтвердити коректність операції на рівні криптографічного доказу, що гарантувало прозорість перевірки без порушення конфіденційності. Це дозволяє державним реєстрам одночасно залишатися підзвітними й відповідати принципам приватності, що є ключовою умовою їх інтеграції у європейський цифровий простір [15].

Наступним аспектом дослідження стала перевірка здатності системи виявляти інсайдерські загрози. Для цього було реалізовано модуль поведінкової аналітики, що застосовував алгоритми машинного навчання до журналів подій [16]. В основі лежала побудова профілів типових дій користувачів: кількість звернень до записів, час активності, частота змін. У випадку відхилення від цих профілів система позначала дію як потенційно шкідливу.

У тестовому сценарії було змодельовано спробу адміністратора здійснити масове копіювання даних у неробочий час. Алгоритм Isolation Forest виявив таку поведінку як аномальну, після чого інцидент автоматично зафіксувався у блокчейн. Це мало подвійний ефект: з одного боку, система виявила нетипову активність і могла надіслати сповіщення службі безпеки; з іншого – подія зберігалася у незмінному журналі, що забезпечувало доказову базу для подальшого розслідування. У порівнянні з класичною КСЗІ час виявлення інсайдерської загрози скоротився майже на 40 %, адже традиційні механізми обмежувалися локальними логами, які легко піддавалися редагуванню.

Окремим завданням дослідження стало підвищення стійкості КСЗІ до інсайдерських загроз, які традиційно залишаються найскладнішими для виявлення. Класичні журнали подій, навіть за умов криптографічного захисту, залишаються вразливими до редагування адміністраторами, що знижує їхню доказову цінність. Запропонована модель інтегрує поведінкову аналітику на основі алгоритмів машинного навчання з блокчейн-журналом транзакцій, що дозволяє автоматично перетворювати виявлені аномалії на незмінні записи у децентралізованому середовищі. Це забезпечує прозорість обліку та створює надійну доказову базу для подальших аудитів.

Рисунок 2 ілюструє логіку роботи цього підходу: дані про активність користувачів після попередньої обробки аналізуються ML-алгоритмами, і у випадку виявлення аномалії формується транзакція, яка проходить верифікацію та зберігається у блокчейн.

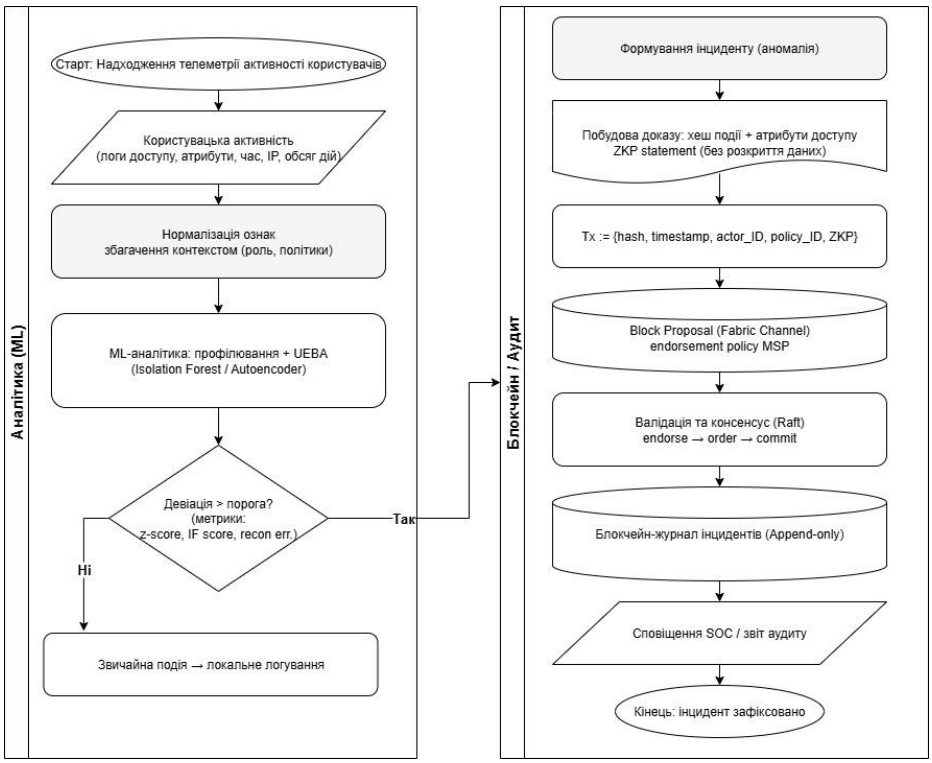

Рисунок 2 – Схема взаємодії модуля поведінкової аналітики з блокчейн-журналом

Аналіз схеми показує, що завдяки такій інтеграції система отримує додатковий рівень стійкості до інсайдерів: навіть якщо адміністратор намагатиметься приховати свої дії, вони вже будуть зафіксовані у децентралізованому журналі.

Для об'єктивної оцінки ефективності запропонованої моделі було проведено порівняльний аналіз між класичною архітектурою КСЗІ та гібридною системою з інтегрованим блокчейн-модулем. Класична КСЗІ базувалася на централізованому журналюванні, криптографічному захисті й ролях адміністраторів, тоді як нова модель передбачала децентралізовану верифікацію транзакцій, використання механізмів консенсусу та забезпечення конфіденційності завдяки Zero Knowledge Proofs. У таблиці 2 наведено узагальнені результати порівняння за основними критеріями.

Таблиця 2

Порівняльний аналіз класичної та гібридної системи

Критерій	Класична КСЗІ	КСЗІ + блокчейн
Цілісність даних	Часткова	Повна (гарантується консенсусом)
Прозорість журналювання	Обмежена	Повна, децентралізована
Захист від інсайдерів	Середній рівень	Високий рівень
Конфіденційність	Базова	Посилена (через ZKP)
Відповідність ISO/IEC 27001	Часткова	Повна
Незалежний аудит	Обмежений	Повністю можливий

Аналіз таблиці дає змогу зробити кілька важливих висновків. По-перше, інтеграція блокчейн ліквідує головну слабкість класичних КСЗІ – залежність від централізованих журналів, які легко піддаються модифікаціям [17]. Тепер усі події підтверджуються кількома незалежними вузлами, що підвищує рівень довіри до результатів аудиту. По-друге, використання ZKP дозволяє поєднати прозорість контролю з дотриманням вимог конфіденційності, що є ключовим для персональних даних [18]. По-третє, система отримує додаткову перевагу у вигляді незалежного аудиту: перевірку транзакцій можуть здійснювати зовнішні учасники без доступу до самих даних, що відповідає принципам регуляторної підзвітності.

Запропонована гібридна модель забезпечує не лише технічне посилення безпеки, а й створює

основу для підвищення довіри громадян та міжнародних партнерів до цифрових державних сервісів. Результати дослідження підтвердили доцільність інтеграції блокчейн у КСЗІ державних реєстрів [19]. Система отримує підвищений рівень захисту від інсайдерів, прозорість журналювання та можливість незалежної верифікації, що у комплексі забезпечує відповідність сучасним стандартам кібербезпеки та вимогам законодавства щодо персональних даних.

Висновки. Проведене дослідження засвідчило високу ефективність застосування технологій блокчейн у складі комплексних систем захисту інформації державних реєстрів. На відміну від традиційних підходів, що зосереджуються переважно на криптографічному захисті, автентифікації користувачів і централізованому аудиті, запропонована модель інтегрує блокчейн як додатковий модуль незалежної верифікації транзакцій і формування незмінного журналу подій. Завдяки цьому система позбавляється однієї з ключових вразливостей – можливості прихованого редагування або видалення записів адміністраторами, які володіють розширеними правами доступу. Використання дозвільного блокчейн Hyperledger Fabric дозволило створити архітектуру, у якій кожен вузол виступає окремим довіреним учасником, що забезпечує децентралізацію контролю та підтвердження подій консенсусом.

Розроблена експериментальна модель у віртуалізованому середовищі VMware, яка відтворювала реальні умови функціонування державних інформаційних систем, показала, що інтеграція блокчейн-модуля з класичними компонентами КСЗІ (автентифікація, криптографічний захист, контроль доступу) забезпечує їхню синергію й значно підвищує рівень довіри до всієї системи. Усі транзакції доступу до даних автоматично фіксувалися у блокчейн у вигляді хешованих записів із цифровими підписами, що унеможливлювало їх несанкціоновану зміну чи видалення. При цьому система підтримувала роботу зі смарт-контрактами, які виконували роль автоматичних політик доступу, забезпечуючи додаткову перевірку кожної операції.

Особливу увагу приділено аспекту виявлення інсайдерських загроз, які у класичних системах залишаються найскладнішими для ідентифікації. Використання поведінкової аналітики на основі алгоритмів машинного навчання (Isolation Forest, Autoencoder та інших) дозволило формувати профілі користувацької активності й виявляти відхилення від нормальної поведінки. У випадку виявлення аномалії система автоматично формувала інцидент, який представляв собою транзакцію з криптографічним доказом та передавався у блокчейн для незмінної фіксації. Такий підхід значно скоротив час реагування на інсайдерські загрози та унеможливив їх приховування, оскільки навіть адміністратори не мали змоги редагувати чи видаляти подібні записи.

Додатковою перевагою стала реалізація механізмів Zero Knowledge Proofs, які забезпечили баланс між прозорістю перевірки транзакцій і дотриманням конфіденційності персональних даних. Це дозволило підтверджувати достовірність операцій без розкриття їхнього змісту, що повністю відповідає вимогам європейського законодавства, зокрема GDPR. Таким чином, система не лише підвищувала рівень кіберзахисту, а й інтегрувалася в сучасний правовий контекст захисту даних, що є критично важливим для державних цифрових сервісів.

Аналіз продуктивності та масштабованості експериментальної моделі показав, що хоча середній час підтвердження транзакцій дещо зріс у порівнянні з централізованими системами, цей показник залишався прийнятним для практичного використання у державних реєстрах. Система успішно витримувала навантаження, характерні для масових запитів користувачів, і забезпечувала стабільну роботу при збільшенні кількості вузлів. Водночас завдяки децентралізованому характеру блокчейн з'явилася можливість проведення незалежного аудиту у режимі реального часу, що значно підвищує довіру як громадян, так і міжнародних партнерів до результатів функціонування реєстрів.

У підсумку можна стверджувати, що інтеграція блокчейн у КСЗІ створює якісно новий рівень захисту, прозорості та довіри до державних цифрових сервісів. Запропонований підхід забезпечує одночасне досягнення кількох критичних цілей: захист від інсайдерських загроз, підтвердження незмінності журналів, дотримання вимог GDPR та підтримку незалежного аудиту. Подальші дослідження доцільно зосередити на оптимізації продуктивності блокчейн-модуля, зменшенні затримок обробки транзакцій, а також інтеграції з іншими сучасними технологіями, зокрема системами штучного інтелекту для прогнозного аналізу загроз і методами квантово-стійкої криптографії.

Список літератури:

1. ISO/IEC 27001:2022. Information security, cybersecurity and privacy protection – Information security management systems – Requirements. Geneva: ISO, 2022. 47 p.

2. Закон України «Про захист персональних даних» від 01.06.2010 № 2297-VI (зі змінами). URL: https://zakon.rada.gov.ua/laws/show/2297-17 (дата звернення: 28.08.2025).

3. Androulaki E., Barger A., Bortnikov V., Cachin C., Christidis K., De Caro A. et al. Hyperledger Fabric: A Distributed Operating System for Permissioned Blockchains. Proceedings of the Thirteenth EuroSys Conference. 2018. P. 1–15. DOI: https://doi.org/10.1145/3190508.3190538.

4. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (General Data Protection Regulation). Official Journal of the European Union. L119. 2016. P. 1–88.

5. Ben-Sasson E., Chiesa A., Genkin D., Tromer E., Virza M. Zerocash: Decentralized Anonymous Payments from Bitcoin. IEEE Symposium on Security and Privacy. 2014. P. 459–474. DOI: https://doi.org/10.1109/SP.2014.36.

6. 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. Т. 4, № 24. С. 99–114. DOI: https://doi.org/10.28925/2663-4023.2024.24.99114.

7. Chio C., Freeman D. Machine Learning and Security: Protecting Systems with Data and Algorithms. Beijing: O'Reilly Media, 2018. 384 p.

8. ENISA. Threat Landscape 2022: Mapping the threat landscape and actors. European Union Agency for Cybersecurity. Heraklion: ENISA, 2022. 148 p.

9. NIST. Blockchain Technology Overview (NISTIR 8202). Gaithersburg, MD: National Institute of Standards and Technology, 2018. 57 p. DOI: 10.6028/NIST.IR.8202.

10. ENISA. Distributed Ledger Technology & Cybersecurity. European Union Agency for Cybersecurity. 2019. 72 p. URL: .enisa. europa.eu/ publications (дата звернення: 01.09.2025).

11. Ongaro D., Ousterhout J. In Search of an Understandable Consensus Algorithm (Raft). In: Proceedings of the 2014 USENIX Annual Technical Conference (USENIX ATC '14). 2014. P. 305–319.

12. Thakkar P., Nathan S., Viswanathan B. Performance Benchmarking and Optimizing Hyperledger Fabric Blockchain Platform. 2018. arXiv:1805.11390. URL: https://arxiv.org/abs/ 1805.11390 (дата звернення: 02.09.2025).

13. Finck M. Blockchain and the General Data Protection Regulation (GDPR): Reconciling EU data protection law with distributed ledger technology. European Parliamentary Research Service (EPRS), Study PE 634.445, 2019. 78 p.

14. 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. URL: //ceur-ws.org/Vol-3800/ (дата звернення: 11.09.2025).

15. European Commission. Blockchain in the Public Sector. Publications Office of the European Union, Luxembourg, 2024. URL: https://op.europa.eu/en/publication-detail/-/publication/blockchain-public-sector-2024.

16. Al-Bassam M., Sonnino A. Blockchain for government services: a systematic review. Government Information Quarterly. 2023. Vol. 40(2). pp. 101–117. https://doi.org/10.1016/j.giq.2023.101717.

17. Zhang X., Wang L. Enhancing data integrity in e-government systems using permissioned blockchains. Information Sciences. 2022. Vol. 611. pp. 168–184. https://doi.org/10.1016/j.ins.2022.07.005.

18. Natarajan S., Prakash A. Zero-Knowledge Proofs in blockchain-based identity management. IEEE Access. 2023. Vol. 11. pp. 11945–11959. https://doi.org/10.1109/ACCESS.2023.3251194.

19. Kumar P., Thakur R. Hyperledger Fabric optimization and interoperability trends. Journal of Network Security. 2023. Vol. 15(4). pp. 210–228.

References:

1. International Organization for Standardization. (2022). *ISO/IEC 27001:2022. Information security, cybersecurity and privacy protection – Information security management systems – Requirements*. Geneva: ISO.

2. Verkhovna Rada of Ukraine. (2010, June 1). *Law of Ukraine "On Personal Data Protection" No. 2297-VI (as amended)*. Retrieved September 11, 2025, from https://zakon.rada.gov.ua/laws/show/2297-17

3. Androulaki, E., Barger, A., Bortnikov, V., Cachin, C., Christidis, K., De Caro, A., & others. (2018). Hyperledger Fabric: A distributed operating system for permissioned blockchains. In *Proceedings of the Thirteenth EuroSys Conference* (pp. 1–15). ACM. https://doi.org/10.1145/3190508.3190538

4. European Union. (2016). *Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (General Data Protection Regulation)*. *Official Journal of the European Union*, L119, 1–88.

5. Ben-Sasson, E., Chiesa, A., Genkin, D., Tromer, E., & Virza, M. (2014). Zerocash: Decentralized anonymous payments from Bitcoin. In *2014 IEEE Symposium on Security and Privacy* (pp. 459–474). IEEE. https://doi.org/10.1109/SP.2014.36

6. Balatska, V. S., Poberezhnyk, V. O., & Opirskyy, I. R. (2024). The use of Non-Fungible Tokens and blockchain for access control to state registers. *Cybersecurity: Education, Science, Technique*, 4(24), 99–114. org/10.28925/2663-4023.2024.24.99114

7. Chio, C., & Freeman, D. (2018). *Machine learning and security: Protecting systems with data and algorithms*. O'Reilly Media.

8. European Union Agency for Cybersecurity (ENISA). (2022). *Threat Landscape 2022: Mapping the threat landscape and actors*. Heraklion: ENISA.

9. Yaga, D., Mell, P., Roby, N., & Scarfone, K. (2018). *Blockchain technology overview (NISTIR 8202)*. National Institute of Standards and Technology. https://doi.org/10.6028/NIST.IR.8202

10. European Union Agency for Cybersecurity (ENISA). (2019). *Distributed ledger technology & cybersecurity*. Retrieved September 11, 2025, from https://www.enisa.europa.eu/publications

11. Ongaro, D., & Ousterhout, J. (2014). In search of an understandable consensus algorithm (Raft). In *Proceedings of the 2014 USENIX Annual Technical Conference (USENIX ATC '14)* (pp. 305–319). USENIX Association.

12. Thakkar, P., Nathan, S., & Viswanathan, B. (2018). Performance benchmarking and optimizing Hyperledger Fabric blockchain platform. *arXiv preprint arXiv:1805.11390*. Retrieved September 11, 2025, from https://arxiv.org/abs/1805.11390

13. Finck, M. (2019). *Blockchain and the General Data Protection Regulation (GDPR): Reconciling EU data protection law with distributed ledger technology*. European Parliamentary Research Service (EPRS), Study PE 634.445.

14. 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* (Vol. 3800, pp. 70–80). Retrieved September 11, 2025, from https://ceur-ws.org/Vol-3800/

15. European Commission. (2024). *Blockchain in the Public Sector*. Publications Office of the European Union. https://op.europa.eu/en/publication-detail/-/publication/blockchain-public-sector-2024

16. Al-Bassam, M., & Sonnino, A. (2023). *Blockchain for government services: A systematic review. Government Information Quarterly,* 40(2), 101–117. https://doi.org/10.1016/j.giq.2023.101717

17. Zhang, X., & Wang, L. (2022). *Enhancing data integrity in e-government systems using permissioned blockchains. Information Sciences,* 611, 168–184. https://doi.org/10.1016/ j.ins.2022.07.005

18. Natarajan, S., & Prakash, A. (2023). *Zero-Knowledge Proofs in blockchain-based identity management. IEEE Access,* 11, 11945–11959. https://doi.org/10.1109/ACCESS.2023.3251194

19. Kumar, P., & Thakur, R. (2023). *Hyperledger Fabric optimization and interoperability trends. Journal of Network Security,* 15(4), 210–228.

Науково-методична стаття.
Надійшла до редакції 15.09.2025.
Прийнято до публікації 26.11.2025.