КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 4 (32), 2026
ISSN 2663 – 4023
DOI 10.28925/2663-4023.2026.32.1136
УДК 004.056.5

Балацька Валерія Сергіївна
доктор філософії,
старший викладач кафедри управління інформаційною безпекою,
Львівський державний університет безпеки життєдіяльності, Львів, Україна
ORCID: 0000-0002-6262-6792
v.balatska@ldubgd.edu.ua

БЛОКЧЕЙН-ОРІЄНТОВАНИЙ ПІДХІД ДО ЗАБЕЗПЕЧЕННЯ ПРОСТЕЖУВАНОСТІ ТА ПЕРЕВІРЮВАНОСТІ ВИКОНАННЯ ПОЛІТИК КСЗІ

Анотація. У статті запропоновано блокчейн-орієнтований підхід до забезпечення простежуваності та перевірюваності виконання політик інформаційної безпеки в комплексних системах захисту інформації (КСЗІ). Актуальність зумовлена тим, що у практиці КСЗІ дотримання політик часто підтверджується журналами подій і звітами, які можуть бути змінені або вилучені, що знижує доказовість аудиту та ускладнює незалежну перевірку. Підхід ґрунтується на фіксації у permissioned-блокчейні лише криптографічних «якорів» (хеш-значень) подій виконання політик, без перенесення повних логів у розподілений реєстр, що мінімізує накладні витрати та ризики розкриття конфіденційних даних. Запропоновано архітектуру, яка включає модуль збору й нормалізації подій, хеш-агрегатор із пакетуванням записів, смартконтракт реєстрації якорів та модуль аудиторської верифікації. Практичний прототип реалізовано як сервіс прикладної логіки, що інтегрується з системою журналювання та взаємодіє зі смартконтрактом через API. Експериментальну перевірку проведено на модельних сценаріях (контроль доступу, зміна ролей, спроби несанкціонованих дій, обробка інцидентів) із подальшою імітацією підміни, видалення та перестановки подій у локальних журналах. Оцінювання виконано за показниками затримки фіксації якоря, пропускної здатності пакетування, частки успішних транзакцій, а також часу аудиторської перевірки для різних обсягів логів. Показано, що запропонований механізм забезпечує виявлення маніпуляцій шляхом невідповідності локально обчислених хешів ончейн-записам, підтримує відтворюваний ланцюг доказів для ключових політик КСЗІ та підвищує прозорість аудиту без довіреної третьої сторони. Обговорено обмеження підходу (вибір критичних подій, керування ключами, політика ретенції) і наведено рекомендації щодо інтеграції з SIEM та вимогами ISO/IEC 27001. Результати можуть бути використані під час проєктування та модернізації КСЗІ для державних інформаційних систем і об’єктів критичної інфраструктури. Запропонований підхід може слугувати основою для автоматизованого формування актів аудиту та незмінних доказів відповідності регламентам КСЗІ організації загалом.

Ключові слова: КСЗІ; політики інформаційної безпеки; аудит; простежуваність; перевірюваність; блокчейн; permissioned blockchain; смартконтракт; хеш-якір; журналювання подій; SIEM; ISO/IEC 27001.

ВСТУП

В умовах інтенсивної цифровізації процесів управління, надання електронних послуг та масштабування розподілених інформаційних систем зростає критичність забезпечення конфіденційності, цілісності та доступності даних [1]. Для державних органів, суб’єктів господарювання, закладів освіти та об’єктів критичної інфраструктури порушення цих властивостей призводить не лише до фінансових втрат, але й до зниження довіри, правових ризиків та зупинок ключових процесів. В Україні інструментом комплексного впорядкування заходів захисту виступає комплексна система захисту інформації (КСЗІ) [2], що визначає організаційні та технічні вимоги до

створення захищеного інформаційного середовища відповідно до нормативних документів у сфері технічного та криптографічного захисту інформації.

Попри наявність нормативної бази та практик аудиту, у багатьох організаціях зберігається системна проблема: політики інформаційної безпеки та регламенти КСЗІ часто мають декларативний характер, тоді як підтвердження їх фактичного виконання спирається на журнали подій [3], звіти адміністраторів та результати періодичних перевірок. Такі джерела доказів є вразливими до маніпуляцій [4], зокрема коригування записів, вилучення фрагментів журналів або ретроспективної «нормалізації» даних перед аудитом. У результаті виникає розрив між формальною відповідністю політикам та реальним виконанням контрольних процедур, що знижує доказовість аудиту і ускладнює незалежну верифікацію дотримання вимог у межах КСЗІ.

Особливої ваги набуває питання перевірюваності виконання політик у контексті відповідності міжнародним і галузевим стандартам (ISO/IEC 27001, NIST SP 800-53) [5], які висувають вимоги до керованості контролів, журналювання, моніторингу, розслідування інцидентів та формування надійних аудиторських слідів [6]. Зростання частки віддаленого доступу, використання хмарних сервісів і мікросервісних архітектур підсилює динамічність інфраструктури: конфігурації та доступи змінюються швидко, а доказова база виконання політик повинна формуватися безперервно, з можливістю подальшої перевірки без залучення «довіреної третьої сторони».

У цьому контексті перспективним є застосування блокчейн-орієнтованих механізмів для побудови перевірюваного аудиторського сліду [7]. Проте пряме перенесення журналів у блокчейн є практично недоцільним [8] через обсяги даних, накладні витрати та ризики витоку чутливої інформації. Тому актуальним є підхід, що передбачає фіксацію у розподіленому реєстрі не первинних журналів, а криптографічних «якорів» [9] подій виконання політик (хеш-значень і доказів цілісності), які забезпечують незмінність, часову прив’язку та незалежну верифікацію.

Метою дослідження є наукове обґрунтування, розроблення та експериментальна перевірка блокчейн-орієнтованого підходу до забезпечення простежуваності й перевірюваності виконання політик інформаційної безпеки в КСЗІ шляхом фіксації криптографічних «якорів» (хеш-значень) аудиторських подій у permissioned-блокчейні та побудови процедур незалежної верифікації цілісності й повноти аудиторського сліду без розкриття змісту журналів [10].

Постановка проблеми. Сучасні організації експлуатують розподілені інформаційні системи з великою кількістю сервісів, користувачів і каналів доступу, що зумовлює підвищені вимоги до керованості заходів захисту та доказовості їх виконання. У межах комплексної системи захисту інформації (КСЗІ) політики інформаційної безпеки визначають правила доступу, обробки даних, журналювання, реагування на інциденти та інші контрольні процедури. Проте на практиці підтвердження дотримання політик переважно базується на локальних журналах подій, звітах адміністраторів або результатах періодичних перевірок. Такі джерела аудиторських доказів не забезпечують криптографічно гарантованої незмінності: записи можуть бути відредаговані, вилучені або «очищені» перед аудитом, а також втрачені внаслідок збоїв чи компрометації системи журналювання. Як наслідок, виникає розрив між декларативною відповідністю політикам та фактичним виконанням контролів КСЗІ, що знижує об’єктивність аудиту [11], ускладнює розслідування інцидентів і формування довіри до результатів перевірки.

Додатковим чинником є динамічність сучасних інфраструктур: використання хмарних сервісів, контейнеризації та віддаленого доступу призводить до частих змін конфігурацій, ролей і прав, які повинні бути простежуваними у часі та перевірюваними

незалежною стороною [12]. Вимоги стандартів ISO/IEC 27001 і NIST SP 800-53 підсилюють потребу в надійному аудиторському сліді, що підтверджує цілісність і повноту журналювання для критичних подій. Водночас пряме зберігання повних журналів у блокчейні є недоцільним через обсяги даних, накладні витрати та ризики розкриття конфіденційної інформації [13].

Отже, науково-практичною проблемою є відсутність у КСЗІ уніфікованого механізму, який би забезпечував простежуваність і криптографічно перевірювану незмінність виконання політик шляхом фіксації лише необхідних доказів (криптографічних якорів) та підтримував незалежну верифікацію аудитором без довіреної третьої сторони [14].

Аналіз останніх досліджень і публікацій. Упродовж останніх років у фокусі досліджень з інформаційної безпеки суттєво посилився акцент на доказовості (evidence) виконання контролів та політик, а не лише на їх формальному описі. У стандартизованих підходах до управління ІБ ключовими стають вимоги до журналювання, моніторингу, розслідування інцидентів і збереження доказів, що прямо відображено у сучасних версіях міжнародних нормативів та каталогів контролів. Зокрема, ISO/IEC 27001:2022 виносить логування в окремий технологічний контроль і трактує його як основу для виявлення та розслідування інцидентів. Каталог контролів NIST SP 800-53 Rev.5 деталізує вимоги до аудиту (група AU), охоплюючи генерацію, захист, аналіз, кореляцію та реагування на відмови процесу логування, що формує рамку для перевірюваного аудиторського сліду. Окремо NIST у документі з планування кіберлог-менеджменту підкреслює організаційну необхідність побудови керованої програми логування як основи моніторингу та аудиту. Європейські рекомендації ENISA також акцентують, що журнали мають охоплювати релевантні події (спроби доступу, адміністративні дії, зміни конфігурацій) і мати визначену політику ретенції як доказ для моніторингу та форензики.

Паралельно розвиваються технічні підходи до підвищення цілісності журналів: хеш-ланцюги, деревоподібні структури агрегування (Merkle/Hash trees) [15], цифрові підписи та WORM-практики. Такі рішення зменшують ризик підміни логів, однак часто залишаються залежними від довіреної інфраструктури або адміністратора, що обмежує незалежну перевірку. Саме тому помітною тенденцією є застосування permissioned-блокчейнів як “реєстру доказів” для журналів і аудиту. У роботі B. Putz та співавт. [16] запропоновано інфраструктуру аудиту логів, де в блокчейні зберігаються докази цілісності, а не повні журнали, що підсилює незмінність без опори на третю сторону. Схожі ідеї розвиваються у сучасних блокчейн-орієнтованих системах керування журналами для хмарних середовищ (зокрема BCALS) [17], де блокчейн використовується для підвищення довіри до аудиторських логів, а також у роботах про масштабоване мережеве логування з блокчейн-фіксацією. Додатково, дослідження з тампер-евідент логування пропонують ефективні хеш-дерева та часові конструкції для великих обсягів подій, що є важливим для практичного “якоріння” подій політик КСЗІ.

Мета статті. Метою статті є наукове обґрунтування та розроблення блокчейн-орієнтованого підходу до забезпечення простежуваності й перевірюваності виконання політик інформаційної безпеки в комплексній системі захисту інформації (КСЗІ) шляхом фіксації криптографічних «якорів» аудиторських подій у permissioned-блокчейні та формування процедур незалежної верифікації цілісності й повноти аудиторського сліду без розкриття змісту журналів.

Основними завданнями статті виступають:

1. Проаналізувати обмеження традиційних механізмів журналювання та аудиту в КСЗІ щодо забезпечення доказовості виконання політик.

2. Визначити вимоги до простежуваності та перевірюваності виконання політик КСЗІ з урахуванням положень ISO/IEC 27001 та NIST SP 800-53.
3. Обґрунтувати концепцію застосування permissioned-блокчейну для формування незмінного аудиторського сліду на основі криптографічного «якоріння» подій.
4. Розробити модель події виконання політики (структуру атрибутів), механізм нормалізації та алгоритм хеш-агрегації (зокрема пакетування/дерева хешів) для мінімізації ончейн-даних.
5. Спроєктувати та описати архітектуру прототипу, що включає модуль збору подій, сервіс обчислення якорів, смартконтракт реєстрації якорів і модуль аудиторської верифікації.
6. Реалізувати прототип інтеграції з системою журналювання/моніторингу (SIEM або централізоване логування) та забезпечити обмін даними через API.
7. Провести експериментальну перевірку на модельних сценаріях КСЗІ (контроль доступу, зміна ролей, несанкціоновані дії, інциденти) з імітацією модифікації та вилучення логів.
8. Оцінити ефективність підходу за показниками затримки фіксації якоря, пропускної здатності, частки успішних транзакцій і часу аудиторської перевірки, а також сформувати рекомендації щодо практичного впровадження в організаціях різного типу.

РЕЗУЛЬТАТИ ДОСЛІДЖЕНЬ

Концепція блокчейн-орієнтованого забезпечення простежуваності та перевірюваності виконання політик КСЗІ.

Запропонований підхід розв’язує одну з найпроблемніших практичних задач у межах комплексної системи захисту інформації (КСЗІ): забезпечення доказовості того, що вимоги політик інформаційної безпеки не лише задекларовані, а й виконувалися у визначений період часу. У типовому середовищі КСЗІ контроль виконання політик підтверджується переважно системними журналами, звітами адміністраторів, витягами з SIEM та протоколами перевірок. Однак такі артефакти аудиту залишаються уразливими до маніпуляцій: записи можуть бути модифіковані, вилучені або «нормалізовані» ретроспективно перед аудитом, особливо у випадку інсайдерських загроз або компрометації адміністративних облікових записів. Це створює розрив між формальною відповідністю політикам і фактичним станом безпеки, знижує достовірність висновків аудиту та ускладнює розслідування інцидентів.

У межах дослідження запропоновано блокчейн-орієнтований підхід, який формує перевірюваний аудиторський слід на основі криптографічного «якоріння» (anchoring) подій виконання політик. Принциповим є те, що блокчейн не використовується як сховище первинних журналів. Натомість у permissioned-блокчейн фіксуються криптографічні докази цілісності (агреговані хеш-значення) для пакетів подій, що мають найбільшу аудитну цінність. Первинні журнали при цьому зберігаються у внутрішній інфраструктурі (локальні журнали, централізоване лог-сховище, SIEM), а блокчейн виконує роль незмінного реєстру доказів, який унеможливлює непомітну підміну або вилучення подій.

Оскільки доказовість у КСЗІ має бути пов’язана з конкретними політиками, у дослідженні виконано відбір класів подій, що підлягають якорінню, з урахуванням їх критичності для контролю доступу, управління привілеями, керування конфігураціями, безперервності журналювання та реагування на інциденти [18]. Цей відбір

систематизовано в таблиці 1, яка відображає відповідність між політиками КСЗІ, класами подій та їх аудитною значущістю.

Таблиця 1

Критичні події для якоріння за політиками КСЗІ та аудитними контролями

Політика КСЗІ	Клас подій, що якоряться	Приклади подій	Аудиторська цінність
Контроль доступу	Автентифікація/ авторизація	login success/fail, MFA, lockout	підтвердження виконання вимог доступу та ідентифікації
Управління привілеями	Зміна ролей/прав	grant/revoke role, group change, privilege escalation	доказ коректності адміністрування та мінімізації привілеїв
Журналювання та моніторинг	Зміни конфігурацій логування	log policy change, agent stop/start, sink unreachable	доказ неперервності та повноти журналювання
Керування конфігураціями	Критичні зміни налаштувань	firewall rule change, VPN config, TLS settings	простежуваність змін та відтворюваність стану
Реагування на інциденти	Події інцидентів і дій реагування	alert, isolate host, ticket close	доказ реагування, часових меж і коригувальних дій

Запропонована концепція забезпечує два практично значущі ефекти. По-перше, вона підвищує цілісність аудиту: навіть за умови компрометації лог-сховища зловмисник не може непомітно привести журнали у «бажаний» стан без порушення відповідності ончейн-якорям. По-друге, вона створює механізм незалежної верифікації: аудитор здатний перевірити достовірність вибірки подій без потреби довіряти адміністратору або одному централізованому компоненту.

Архітектура рішення та потік формування доказів. Архітектуру блокчейн-орієнтованого аудиторського сліду наведено на рисунку 1. Вона спроєктована з урахуванням типових практик побудови КСЗІ: події генеруються багатьма джерелами; логування та моніторинг реалізуються через SIEM або централізований збір журналів; аудит здійснюється періодично і, як правило, на основі вибірок [19]. У такій системі важливо зберегти сумісність із наявними процесами, не створюючи надлишкового навантаження та не виносячи конфіденційні дані за межі контрольованого периметра.

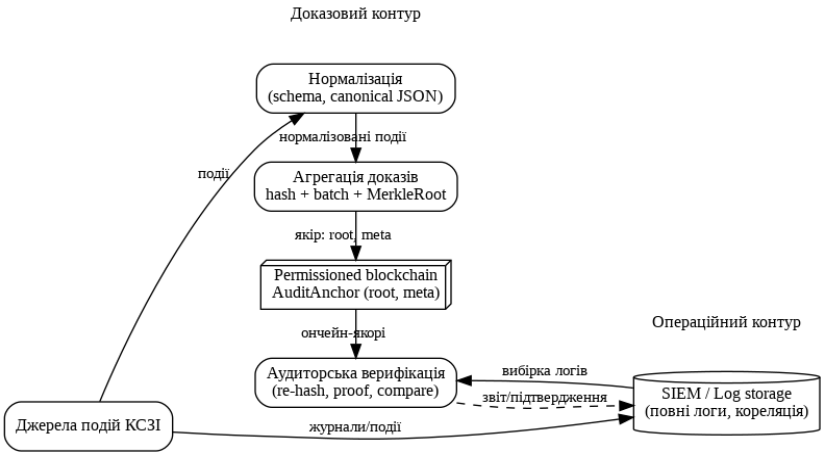

Рис. 1 – Архітектурна модель блокчейн-орієнтованого аудиторського сліду виконання політик КСЗІ

Згідно з рисунком 1, рішення включає такі функціональні компоненти:

- джерела подій КСЗІ (контроль доступу, сервери застосунків, мережеві засоби захисту, системи керування конфігураціями, агенти журналювання, SIEM);
- модуль збору та нормалізації подій, який приводить записи до уніфікованої структури, забезпечує узгоджені часові мітки та застосовує детерміновану серіалізацію. Даний етап є критичним, оскільки будь-яка неоднозначність представлення події створює ризики некоректної верифікації;
- хеш-агрегатор (Anchor Builder), який обчислює хеші подій, виконує пакетування і формує агрегований доказ цілісності (наприклад, Merkle root). Пакетування необхідне для масштабованості та керування накладними витратами;
- permissioned-блокчейн зі смартконтрактом AuditAnchor, який приймає агрегований доказ та метадані пакета (інтервал часу, кількість подій, ідентифікатор політики/джерела) і незмінно фіксує їх;
- модуль аудиторської верифікації, який повторно обчислює докази для заданих подій/вибірок і порівнює їх з ончейн-якорями, формуючи об’єктивний висновок щодо цілісності й повноти.

Архітектура передбачає два взаємодоповнювальні контури: оперативний (кореляція та реагування в SIEM) і доказовий (формування й перевірка якорів). Це принципово важливо для КСЗІ: SIEM забезпечує детекцію та аналіз, тоді як блокчейн-реєстр доказів забезпечує незмінність і перевірюваність критичних подій.

Модель події виконання політики та механізм вибіркової верифікації. Для того щоб криптографічні докази коректно відображали виконання політик КСЗІ, введено формалізовану модель події виконання політики [20]. Кожна подія представлена кортежем:

$$e_i = \langle policy\_id, control\_id, subject, object, action, result, timestamp, source, context \rangle$$

де $policy\_id$ пов’язує подію з політикою КСЗІ; $control\_id$ (опційно) відображає прив’язку до контрольної вимоги/домена; $subject$ та $object$ визначають суб’єкт і ресурс; $action$ описує дію; $result$ – результат виконання; $timestamp$ – час; $source$ – джерело; $context$ – додаткові атрибути (IP, session_id, device_id, параметри конфігурації тощо). Для забезпечення відтворюваності застосовується детермінована серіалізація $Serialize(e_i)$ (наприклад, canonical JSON), після чого обчислюється хеш:

$$h_i = H(Serialize(e_i))$$

Далі хеші групуються у пакет P_k за правилом пакетування (за N подій або часовим інтервалом), а для пакета будується Merkle-дерево з коренем:

$$root_k = MerkleRoot(P_k)$$

У блокчейн фіксується самеroo $root_k$ (а не набір h_i), що радикально скорочує обсяг ончейн-даних і забезпечує масштабованість. Водночас використання Merkle-дерева дозволяє виконувати вибіркову перевірку: щоб довести наявність і незмінність конкретної події, достатньо надати її хеш h_i та Merkle proof (шлях у дереві). Принцип вибіркової верифікації наведено на рисунку 2.

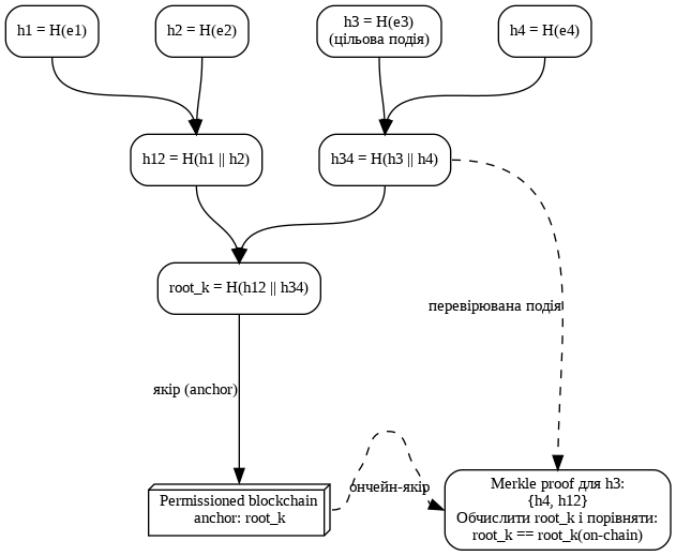

Рис. 2 – Формування Merkle-доказу для вибіркової верифікації події та порівняння з ончейн-якорем

Рисунок 2 відображає ключову для аудиту властивість: аудитор може перевірити конкретну подію або вибірку подій без доступу до всього масиву журналів. Це зменшує ризики розкриття чутливих даних і водночас підсилює доказовість, оскільки будь-яка модифікація події або вилучення запису порушує відповідність доказу ончейн-якорю.

Для уніфікації реалізації запропоновано алгоритм формування якорів і реєстрації в смартконтракті, наведений у алгоритмі 1.

Алгоритм 1 – Пакетування подій та фіксація якоря в блокчейні (псевдокод)

1. Прийняти потік подій E із джерел КСЗІ.
2. Для кожної події e виконати нормалізацію: $e' = Normalize(e)$.
3. Детерміновано серіалізувати подію: $s = Serialize(e')$.
4. Обчислити хеш події: $h = H(s)$ та додати h у буфер пакета P.
5. Якщо виконано умову пакетування (досягнуто N подій або минув інтервал Δt), побудувати Merkle-дерево для P та обчислити $root = MerkleRoot(P)$.
6. Сформувати метадані пакета: $meta = \{source, policy\_id, t\_start, t\_end, |P|\}$.
7. Викликати смартконтракт: $AuditAnchor.addAnchor(root, meta)$ і зафіксувати транзакцію.
8. Зберегти локально P, $meta$ та структури для формування Merkle proof; очистити буфер P та продовжити обробку.

Прототип, сценарії експерименту та виявлення маніпуляцій. Практичну перевірку підходу виконано на прототипі, який реалізує повний цикл «подія → якоріння → верифікація». Прототип включав сервіс прийому подій (інтеграція з журналюванням через API або лог-стрім), компонент нормалізації, агрегатор доказів (пакетування та MerkleRoot), клієнт взаємодії зі смартконтрактом та модуль аудиторської перевірки. Важливо, що прототип розроблено з урахуванням розмежування ролей: компонент, який підписує транзакції у блокчейн, працює у контрольованому середовищі, що мінімізує ризик компрометації ключів підпису.

Експерименти проведено на наборі сценаріїв, що відповідають типовим процесам КСЗІ і відображені у таблиці 1:

- контроль доступу: успішні та неуспішні входи, MFA-події, блокування акаунтів;

- управління привілеями: надання/відкликання ролей, зміни членства у групах доступу, ескалація привілеїв;
- керування конфігураціями: зміни правил міжмережевого екрану, VPN-налаштувань, параметрів TLS, зміни ACL;
- безперервність журналювання: зупинка/запуск агентів логування, зміни політики збору подій, недоступність лог-сховища;
- інциденти та реагування: алерти, створення інциденту, ізоляція вузла, завершення інциденту з фіксацією дій.

Для оцінки здатності підходу виявляти втручання у журнали застосовано імітації, характерні для інсайдерських загроз або компрометації системи логування: (а) видалення підмножини записів у журналі; (б) підміна атрибутів подій (зміна результату, суб'єкта, параметрів конфігурації); (в) перестановка подій, що порушує часову послідовність; (г) часткове «відновлення» журналу із фрагментами, які виглядають коректно з погляду формату. У кожному випадку верифікація призводила до розбіжності: або змінювався хеш події h_i або неможливо було відновити Merkle proof відповідно до ончейн-кореня $root_k$. Практично це означає, що аудитору достатньо отримати вибірку подій і відповідні докази (як на рисунку 2), щоб об'єктивно встановити наявність/відсутність маніпуляцій.

Оцінювання ефективності: вплив режиму якоріння на накладні витрати. Для обґрунтування практичності підходу виконано оцінювання впливу режимів якоріння на накладні витрати системи. Аналіз здійснювався за показниками: (1) затримка фіксації якоря (від появи події до появи $root_k$ у блокчейні); (2) кількість транзакцій у блокчейні; (3) час аудиторської перевірки вибірки; (4) чутливість до росту інтенсивності подій. Узагальнені результати для різних режимів якоріння наведено в таблиці 2.

Таблиця 2

Узагальнені результати експерименту для різних режимів якоріння подій

Режим	Розмір пакета	Транзакцій у блокчейн	Затримка фіксації якоря	Час аудиторської перевірки вибірки
Без пакетування	1 подія	дуже висока	мінімальна для 1 події, але швидке перевантаження мережі	низький для одиничних подій, високий для великих масивів
Пакетування за N	N = 100	значно менше	керована, залежить від швидкості накопичення	середній, стабільний для вибірок
Пакетування за часом	Δt = 60 с	низька	залежить від інтервалу Δt	середній/низький, залежить від обсягу пакета

Дані таблиці 2 демонструють закономірність: при якорінні кожної події окремою транзакцією блокчейн швидко стає вузьким місцем, що робить підхід непридатним для середовищ з високою інтенсивністю логів. Натомість пакетування (за N або Δt) зменшує кількість транзакцій на порядки, зберігаючи можливість вибіркової верифікації завдяки Merkle-доказам. Компроміс полягає у збільшенні затримки фіксації якоря, однак ця затримка є керованою та може бути налаштована відповідно до критичності політики. Для найкритичніших подій (наприклад, ескалація привілеїв або зміни політик журналювання) доцільно застосовувати окремий профіль пакетування (менший N або коротший Δt), що може бути відображено в регламенті журналювання як елемент політик КСЗІ.

Практичні аспекти впровадження в КСЗІ та узгодження з аудитом. Запропонований механізм є найбільш ефективним у поєднанні з існуючими практиками моніторингу: SIEM зберігає функцію кореляції та детекції, а блокчейн-орієнтований компонент

підсилює доказовість журналів і забезпечує перевірюваність ключових подій. Для процедур аудиту КСЗІ це означає можливість переходу від суто документального контролю до контролю, який має криптографічно підтверджуваний аудиторський слід. При цьому важливо розмежувати, що блокчейн не «підміняє» журнали; він гарантує, що журнали, на які спирається аудит, не були непомітно змінені в межах зафіксованих пакетів.

Обмеження підходу є керованими і мають бути формально враховані у політиках КСЗІ. По-перше, необхідно забезпечити керування ключами підпису транзакцій (використання HSM/TPM, розмежування доступів, контрольна процедура ротації) [21]. По-друге, критичною є синхронізація часу (NTP з контролем), оскільки часові мітки визначають межі пакетів та відтворюваність доказів. По-третє, потрібна узгоджена політика ретенції локальних журналів: блокчейн забезпечує доказ незмінності, але деталі інцидентів відновлюються з первинних записів. Саме тому якоріння доцільно включати як частину політики журналювання КСЗІ разом із вимогами до зберігання, доступу та процедури надання вибірок аудитору.

ВИСНОВКИ

У роботі обґрунтовано блокчейн-орієнтований підхід до забезпечення простежуваності та перевірюваності виконання політик КСЗІ на основі криптографічного якоріння аудитно-значущих подій. Показано, що традиційні практики аудиту, які спираються переважно на централізовані журнали та звіти, не гарантують незмінності доказової бази за наявності інсайдерських загроз або компрометації компонентів логування; запропонований підхід усуває цю вразливість шляхом фіксації агрегованих доказів цілісності в permissioned-блокчейні без перенесення повних логів ончейн.

Розроблено архітектурну модель рішення з розділенням на операційний (SIEM/лог-сховище) і доказовий (нормалізація, агрегація, AuditAnchor, верифікація) контури, що забезпечує сумісність із типовою інфраструктурою КСЗІ та мінімізує накладні витрати. Введено формалізовану подієву модель виконання політики та механізм вибіркової перевірки на основі Merkle-доказів, що дозволяє аудитору підтверджувати цілісність конкретних подій або вибірок шляхом порівняння з ончейн-якорем $root_k$. Експериментально підтверджено, що спроби видалення, підміни або перестановки подій у локальних журналах виявляються як невідповідність сформованих доказів зафіксованим у блокчейні якорям.

Показано, що масштабованість досягається завдяки пакетуванню подій (за кількістю або часовим інтервалом), яке зменшує кількість транзакцій у блокчейні при збереженні перевірюваності через Merkle-пути. Отримані результати дозволяють сформулювати практичні рекомендації щодо впровадження підходу в межах політик КСЗІ: визначення переліку подій для якоріння (зокрема для контролю доступу, керування привілеями, журналювання, змін конфігурацій та реагування на інциденти), вибір режиму пакетування відповідно до критичності контролів, а також регламентація керування ключами підпису, синхронізації часу та ретенції первинних журналів.

Подальші дослідження доцільно спрямувати на автоматизоване зіставлення контролів політик КСЗІ з подіями телеметрії (policy-to-event mapping), адаптивний вибір параметрів пакетування залежно від ризик-профілю, а також формалізацію процедур незалежного аудиту для різних організаційних сценаріїв (державні реєстри, критична інфраструктура, хмарні середовища).

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. International Organization for Standardization. (2022). *ISO/IEC 27001: Information security, cybersecurity and privacy protection—Information security management systems—Requirements.* ISO.
2. International Organization for Standardization. (2022). *ISO/IEC 27002: Information security, cybersecurity and privacy protection—Information security controls.* ISO.
3. Scarfone, K. A., & Souppaya, M. P. (2023). *Cybersecurity log management planning guide* (NIST Special Publication 800-92 Rev. 1, IPD). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-92r1.ipd
4. Koisser, D., & Sadeghi, A.-R. (2023). Accountability of things: Large-scale tamper-evident logging for smart devices. *arXiv*. https://doi.org/10.48550/arXiv.2308.05557
5. Joint Task Force. (2020). *Security and privacy controls for information systems and organizations* (NIST Special Publication 800-53 Rev. 5). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-53r5
6. Rose, S., Borchert, O., Mitchell, S., & Connelly, S. (2020). *Zero trust architecture* (NIST Special Publication 800-207). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-207
7. Putz, B., Menges, F., & Pernul, G. (2019). A secure and auditable logging infrastructure based on a permissioned blockchain. *Computers & Security*, 101602. https://doi.org/10.1016/j.cose.2019.101602
8. Ali, A., Khan, A., Ahmed, M., & Jeon, G. (2022). BCALS: Blockchain-based secure log management system for cloud computing. *Transactions on Emerging Telecommunications Technologies*. https://doi.org/10.1002/ett.4272
9. Rakib, M. H., Hossain, S., Jahan, M., & Kabir, U. (2022). A blockchain-enabled scalable network log management system. *Journal of Computer Science, 18*(6), 496–508. https://doi.org/10.3844/jcssp.2022.496.508
10. Faccia, A., & Petratos, P. (2022). Is permissioned blockchain the key to support external audit? *Journal of Open Innovation: Technology, Market, and Complexity, 8*(3), 156.
11. Balatska, V. S., Tkachuk, R., & Maslova, N. (2025). Evolution of complex information security systems and integration of blockchain technologies in cybersecurity of government information systems of Ukraine. *Cybersecurity: Education, Science, Technique, 2*(30), 316–332. https://doi.org/10.28925/2663-4023.2025.30.975
12. Balatska, V. S., Ivanusa, A. I., & Panovyk, U. M. (2025). Method of integration of information security policies, standards, and protocols in building information security systems in organizations. *Cybersecurity: Education, Science, Technique, 3*(31), 283–297. https://doi.org/10.28925/2663-4023.2025.31.1021
13. Balatska, V. S., & Dmytriv, N. (2025). Inter-organizational exchange of confidential personal data based on permissioned blockchain. *Cybersecurity: Education, Science, Technique, 2*(29), 178–193. https://doi.org/10.28925/2663-4023.2025.29.875
14. European Union Agency for Cybersecurity. (2025). *Technical implementation guidance on cybersecurity risk management measures* (Version 1.0). https://doi.org/10.2824/2702548
15. Liu, Z., et al. (2023). Dynamic data integrity auditing based on hierarchical Merkle hash tree in cloud storage. *Electronics, 12*(3), 717. https://doi.org/10.3390/electronics12030717
16. Du, R., et al. (2025). Certificateless data integrity auditing with sparse Merkle trees for the cloud-edge environment. *Scientific Reports, 15*, 14041. https://doi.org/10.1038/s41598-025-14041-9
17. Zhou, H., et al. (2025). Certificate-based multi-copy cloud storage auditing scheme supporting data dynamics. *Computers & Security*, 104096. https://doi.org/10.1016/j.cose.2024.104096
18. Balatska, V. S., Poberezhnyk, V. V., & Opirskyi, I. R. (2024). Use of non-fungible tokens and blockchain for access control to government registries. *Cybersecurity: Education, Science, Technique, 4*(24), 99–114. https://doi.org/10.28925/2663-4023.2024.24.99114
19. 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. https://doi.org/10.18372/2225-5036.30.19211
20. Punia, A., et al. (2024). A systematic review on blockchain-based access control systems in cloud environment. *EURASIP Journal on Information Security*, 18. https://doi.org/10.1186/s13677-024-00697-7
21. Yaqub, N., et al. (2025). Blockchain-enabled policy-based access control mechanism. *PeerJ Computer Science*, e2647. https://doi.org/10.7717/peerj-cs.2647

КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 4 (32), 2026
ISSN 2663 – 4023

Valeriia Balatska
PhD, Senior Lecturer of the Department of Information Security Management,
Lviv State University of Life Safety, Lviv, Ukraine
ORCID: 0000-0002-6262-6792
v.balatska@ldubgd.edu.ua

BLOCKCHAIN-ORIENTED APPROACH TO ENSURING TRACEABILITY AND VERIFIABILITY OF ISMS POLICY ENFORCEMENT

Abstract. This paper proposes a blockchain-oriented approach to ensuring the traceability and verifiability of information security policy enforcement within integrated information security management systems (ISMS). The relevance of the study is driven by the fact that, in practical ISMS deployments, compliance with security policies is commonly confirmed through event logs and reports that may be altered or deleted, thereby reducing the evidentiary value of audits and complicating independent verification. The proposed approach is based on recording only cryptographic "anchors" (hash values) of policy enforcement events in a permissioned blockchain, rather than storing complete logs in a distributed ledger. This design minimizes system overhead and mitigates the risk of sensitive data disclosure. An architecture is introduced that comprises an event collection and normalization module, a hash aggregator with batch packaging, a smart contract for anchor registration, and an audit verification module. A practical prototype was implemented as an application-level service integrated with an existing logging system and interacting with the smart contract via an API. Experimental evaluation was conducted using modeled scenarios, including access control enforcement, role changes, unauthorized action attempts, and incident handling, followed by simulated log tampering through deletion, substitution, and reordering of events in local logs. The evaluation considered anchor registration latency, batching throughput, successful transaction ratio, and auditor verification time for varying log volumes. The results demonstrate that the proposed mechanism reliably detects log manipulation through inconsistencies between locally computed hashes and on-chain records, supports a reproducible chain of evidence for critical ISMS policies, and enhances audit transparency without relying on a trusted third party. The paper also discusses limitations of the approach, including the selection of critical events, key management, and data retention policies, and provides recommendations for integration with SIEM platforms and alignment with ISO/IEC 27001 requirements. The obtained results can be applied in the design and modernization of ISMS for government information systems and critical infrastructure facilities. The proposed approach may serve as a foundation for automated generation of audit reports and immutable evidence of compliance with organizational ISMS regulations.

Keywords: Integrated information security system (IISS); information security policies; audit; traceability; verifiability; blockchain; permissioned blockchain; smart contract; hash anchor; event logging; SIEM; ISO/IEC 27001.

REFERENCES (TRANSLATED AND TRANSLITERATED)

1. International Organization for Standardization. (2022). *ISO/IEC 27001: Information security, cybersecurity and privacy protection—Information security management systems—Requirements.* ISO.
2. International Organization for Standardization. (2022). *ISO/IEC 27002: Information security, cybersecurity and privacy protection—Information security controls.* ISO.
3. Scarfone, K. A., & Souppaya, M. P. (2023). *Cybersecurity log management planning guide* (NIST Special Publication 800-92 Rev. 1, IPD). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-92r1.ipd
4. Koisser, D., & Sadeghi, A.-R. (2023). Accountability of things: Large-scale tamper-evident logging for smart devices. *arXiv*. https://doi.org/10.48550/arXiv.2308.05557
5. Joint Task Force. (2020). *Security and privacy controls for information systems and organizations* (NIST Special Publication 800-53 Rev. 5). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-53r5

6. Rose, S., Borchert, O., Mitchell, S., & Connelly, S. (2020). *Zero trust architecture* (NIST Special Publication 800-207). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-207
7. Putz, B., Menges, F., & Pernul, G. (2019). A secure and auditable logging infrastructure based on a permissioned blockchain. *Computers & Security*, 101602. https://doi.org/10.1016/j.cose.2019.101602
8. Ali, A., Khan, A., Ahmed, M., & Jeon, G. (2022). BCALS: Blockchain-based secure log management system for cloud computing. *Transactions on Emerging Telecommunications Technologies*. https://doi.org/10.1002/ett.4272
9. Rakib, M. H., Hossain, S., Jahan, M., & Kabir, U. (2022). A blockchain-enabled scalable network log management system. *Journal of Computer Science, 18*(6), 496–508. https://doi.org/10.3844/jcssp.2022.496.508
10. Faccia, A., & Petratos, P. (2022). Is permissioned blockchain the key to support external audit? *Journal of Open Innovation: Technology, Market, and Complexity, 8*(3), 156.
11. Balatska, V. S., Tkachuk, R., & Maslova, N. (2025). Evolution of complex information security systems and integration of blockchain technologies in cybersecurity of government information systems of Ukraine. *Cybersecurity: Education, Science, Technique, 2*(30), 316–332. https://doi.org/10.28925/2663-4023.2025.30.975
12. Balatska, V. S., Ivanusa, A. I., & Panovyk, U. M. (2025). Method of integration of information security policies, standards, and protocols in building information security systems in organizations. *Cybersecurity: Education, Science, Technique, 3*(31), 283–297. https://doi.org/10.28925/2663-4023.2025.31.1021
13. Balatska, V. S., & Dmytriv, N. (2025). Inter-organizational exchange of confidential personal data based on permissioned blockchain. *Cybersecurity: Education, Science, Technique, 2*(29), 178–193. https://doi.org/10.28925/2663-4023.2025.29.875
14. European Union Agency for Cybersecurity. (2025). *Technical implementation guidance on cybersecurity risk management measures* (Version 1.0). https://doi.org/10.2824/2702548
15. Liu, Z., et al. (2023). Dynamic data integrity auditing based on hierarchical Merkle hash tree in cloud storage. *Electronics, 12*(3), 717. https://doi.org/10.3390/electronics12030717
16. Du, R., et al. (2025). Certificateless data integrity auditing with sparse Merkle trees for the cloud-edge environment. *Scientific Reports, 15*, 14041. https://doi.org/10.1038/s41598-025-14041-9
17. Zhou, H., et al. (2025). Certificate-based multi-copy cloud storage auditing scheme supporting data dynamics. *Computers & Security*, 104096. https://doi.org/10.1016/j.cose.2024.104096
18. Balatska, V. S., Poberezhnyk, V. V., & Opirskyi, I. R. (2024). Use of non-fungible tokens and blockchain for access control to government registries. *Cybersecurity: Education, Science, Technique, 4*(24), 99–114. https://doi.org/10.28925/2663-4023.2024.24.99114
19. 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. https://doi.org/10.18372/2225-5036.30.19211
20. Punia, A., et al. (2024). A systematic review on blockchain-based access control systems in cloud environment. *EURASIP Journal on Information Security*, 18. https://doi.org/10.1186/s13677-024-00697-7
21. Yaqub, N., et al. (2025). Blockchain-enabled policy-based access control mechanism. *PeerJ Computer Science*, e2647. https://doi.org/10.7717/peerj-cs.2647

Отримано редакцією журналу / Received: 22.01.26
Прорецензовано / Revised: 15.02.26
Схвалено до друку / Accepted: 26.03.26