КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 4 (32), 2026
ISSN 2663 – 4023
DOI 10.28925/2663-4023.2026.32.1097
УДК 004.056.5:004.738.5:004.75

Андрущак Ігор Євгенович
д. т. н., професор, професор кафедри інженерії програмного забезпечення
Луцький національний технічний університет, Луцьк, Україна
ORCID: 0000-0002-875-4420
9000@email.ua

Кошелюк Віктор Андрійович
к. т. н., доцент, доцент кафедри комп'ютерних наук
Луцький національний технічний університет, Луцьк, Україна
ORCID: 0000-0002-4136-5087
viktor.koshelyuk@gmail.com

АУДИТ БЕЗПЕКИ LIGHTWEIGHT KUBERNETES-КЛАСТЕРІВ ІЗ ВИКОРИСТАННЯМ МЕХАНІЗМІВ ДОВІРИ НА БАЗІ MULTICHAIN

Анотація. У статті представлено дослідження підвищення надійності та ефективності аудиту безпеки в легких кластерах Kubernetes, які широко використовуються в периферійних обчисленнях, інфраструктурах Інтернету речей та середовищах з обмеженими ресурсами. Через динамічний характер контейнерних платформ та обмежені можливості традиційних централізованих рішень для ведення журналу, забезпечення цілісності даних, незмінності та достовірності журналів аудиту безпеки залишається суттєвою проблемою. Метою цього дослідження було розробити та обґрунтувати підхід до аудиту безпеки для легких кластерів Kubernetes на основі механізмів довіри, реалізованих через багатоланцюгову архітектуру блокчейну, що забезпечує надійне зберігання, перевірку та подальший аналіз даних аудиту. Цілі дослідження включали: аналіз сучасних підходів до аудиту безпеки Kubernetes; виявлення обмежень безпеки легких дистрибутивів Kubernetes (таких як k3s та microk8s); розробку функціональної моделі процесу аудиту за допомогою діаграми IDEF0; опис взаємодії компонентів за допомогою діаграми послідовностей; проектування експериментального тестового стенду з інтеграцією Multichain; та оцінку продуктивності системи за допомогою ключових метрик аудиту та довіри. Використані методи включають системний аналіз, функціональне моделювання за допомогою IDEF0, моделювання діаграм послідовностей на основі UML, експериментальну оцінку на тестовому кластері Kubernetes, методи криптографічного хешування та цифрового підпису, а також порівняльний аналіз централізованих та децентралізованих підходів до зберігання журналів аудиту. Були отримані такі результати: розроблено архітектуру для аудиту безпеки з використанням технології багатоланцюжкового доступу; визначено умовні метрики продуктивності для збору журналів, аналізу та створення довірених записів; перевірка цілісності даних досягла 100%; час відгуку механізмів самовідновлення скорочено до кількох секунд, що демонструє можливість проведення аудиту майже в режимі реального часу. Наукова новизна полягає в інтеграції легких інфраструктур Kubernetes з децентралізованими механізмами довіри на основі технології багатоланцюжкового доступу для аудиту безпеки, що зменшує залежність від централізованих систем ведення журналу та підвищує стійкість до підробки журналів аудиту. Висновки підтверджують ефективність запропонованого підходу на основі блокчейну для аудиту легких кластерів Kubernetes та окреслюють перспективи подальших досліджень, включаючи покращення масштабованості та інтеграцію інтелектуальних механізмів виявлення інцидентів.

Ключові слова: інтеграція блокчейну; легкі дистрибутиви; kubernetes; аудит безпеки; multichain; контейнери; хмарна безпека.

ВСТУП

Стрімкий розвиток хмарних технологій, мікросервісної архітектури та контейнеризації призвів до широкого впровадження систем оркестрації контейнерів у різних галузях IT. Kubernetes став базовою платформою для розгортання, масштабування та керування контейнеризованими застосунками як у великих дата-центрах, так і в розподілених середовищах. Останніми роками особливої популярності набули lightweight Kubernetes-рішення (зокрема k3s, MicroK8s, k0s), які орієнтовані на середовища з обмеженими ресурсами: edge-обчислення, IoT-інфраструктури, лабораторні стенди, навчальні платформи та малі корпоративні кластери. Вони забезпечують спрощене розгортання та зменшене споживання обчислювальних ресурсів, що робить їх привабливими з точки зору вартості та гнучкості [1-3].

Традиційні підходи до аудиту безпеки Kubernetes-кластерів базуються на централізованих системах моніторингу, статичному аналізі конфігурацій та періодичних перевірках відповідності стандартам безпеки. Такі методології мають суттєві обмеження: відсутність незмінного журналу подій безпеки, можливість маніпуляції логами, складність верифікації стану системи в розподілених середовищах та проблеми з довірою до централізованих органів аудиту. У контексті мультихмарних розгортань, edge-computing та гібридних інфраструктур ці обмеження стають критичними, оскільки традиційні периметри безпеки втрачають свою ефективність [2,4].

Сучасні lightweight Kubernetes-кластери часто розгортаються в географічно розподілених локаціях, на периферійних пристроях IoT та в середовищах з обмеженою довірою до централізованих компонентів. У таких сценаріях виникає фундаментальна проблема: як забезпечити прозорий, верифікований та незмінний аудит безпеки без покладання на єдину точку довіри? Існуючі інструменти аудиту не надають механізмів розподіленої верифікації, що робить їх вразливими до атак типу “man-in-the-middle”, фальсифікації звітів та компрометації централізованих систем логування [3, 5].

Технологія blockchain та multichain-архітектури пропонують нову парадигму для забезпечення довіри в розподілених системах. Незмінність записів, криптографічна верифікація та децентралізований консенсус створюють основу для принципово нового підходу до аудиту безпеки. Проте застосування blockchain-механізмів у контексті Kubernetes-безпеки залишається недостатньо дослідженою областю, особливо для lightweight-варіантів з їхніми специфічними обмеженнями та вимогами [5].

Актуальність проблеми посилюється зростанням кількості кібератак на контейнеризовані середовища, збільшенням регуляторних вимог щодо аудиту безпеки та необхідністю забезпечення довіри в умовах “zero trust” архітектур. Відсутність ефективних інструментів для розподіленого аудиту безпеки lightweight Kubernetes-кластерів створює суттєві ризики для організацій, які впроваджують edge-computing та мультихмарні стратегії [6, 7].

Разом із тим, спрощення архітектури lightweight Kubernetes-кластерів часто супроводжується зниженням рівня вбудованих механізмів безпеки та аудиту. Стандартні засоби журналювання, контролю доступу та моніторингу подій можуть бути обмеженими або налаштованими на мінімальний рівень деталізації. У результаті виникає проблема недостатньої прозорості дій користувачів і компонентів кластера, ускладнюється виявлення інцидентів безпеки, а також перевірка цілісності та достовірності журналів аудиту. Це особливо критично для середовищ, у яких

Kubernetes використовується для обробки чутливих даних або є частиною критичної інфраструктури.

Постановка проблеми. Ключовою проблемою, що розглядається в публікації, є забезпечення надійного, достовірного та незмінного аудиту безпеки в lightweight Kubernetes-кластерах. Традиційні централізовані підходи до зберігання журналів аудиту мають низку суттєвих недоліків: наявність єдиної точки відмови, ризик несанкціонованого видалення або модифікації логів, а також обмежені можливості перевірки їх цілісності постфактум. У lightweight-середовищах ці ризики посилюються через обмежені ресурси та спрощену конфігурацію систем безпеки.

У цьому контексті актуальним є пошук нових підходів до формування механізмів довіри до даних аудиту. Одним із перспективних напрямів є використання технологій розподіленого реєстру (Distributed Ledger Technology, DLT), зокрема permissioned blockchain-рішень. Blockchain забезпечує незмінність записів, криптографічний захист та децентралізовану модель зберігання даних, що потенційно дозволяє усунути або суттєво зменшити зазначені недоліки. Проте інтеграція blockchain у процеси аудиту Kubernetes, особливо lightweight-кластерів, потребує теоретичного обґрунтування, аналізу доцільності та визначення архітектурних підходів.

Аналіз останніх досліджень і публікацій. Питання безпеки контейнеризованих застосунків та розподілених систем на базі Kubernetes набуває особливої актуальності в контексті зростання кількості кібератак та підвищення вимог до захисту критичної інфраструктури. Аналіз сучасних наукових публікацій демонструє кілька ключових напрямків досліджень, що безпосередньо стосуються тематики даної роботи.

Дослідження Smith J. & Patterson R. (2023) представляє комплексний підхід до аудиту безпеки легковагових дистрибутивів Kubernetes, зокрема K3s та MicroK8s [8]. Автори запропонували методологію систематичної перевірки конфігурацій безпеки, яка охоплює аналіз мережевих політик, контроль доступу на основі ролей (RBAC) та механізми ізоляції контейнерів. Особливу увагу приділено специфічним вразливостям, характерним саме для lightweight-реалізацій, таким як спрощені механізми автентифікації та обмежені можливості логування. Проте запропонована методологія не враховує можливості інтеграції з технологіями розподіленого реєстру для забезпечення незмінності аудиторських записів.

У роботі Chen L. et al. (2024) було досліджено використання блокчейн-технологій для підвищення безпеки Kubernetes-кластерів на периферійних пристроях [9]. Автори продемонстрували, що інтеграція смарт-контрактів Ethereum дозволяє автоматизувати процеси верифікації конфігурацій та забезпечити криптографічно захищений аудиторський слід. Експериментальні результати показали зниження часу виявлення несанкціонованих змін конфігурації на 67% порівняно з традиційними методами моніторингу. Водночас дослідження обмежувалося лише однією блокчейн-платформою, не розглядаючи потенційні переваги multichain-архітектури.

Робота Anderson M. & Rodriguez C. (2023) зосереджена на розробці моделей довіри для розподілених систем оркестрації контейнерів. Дослідники запропонували багаторівневу архітектуру довіри, що базується на криптографічних атестаціях та розподіленому консенсусі. Впроваджена система дозволяє валідувати цілісність компонентів кластера та виявляти скомпрометовані вузли з високою точністю (94.3%). Проте механізми довіри розроблялися переважно для повноцінних Kubernetes-кластерів без урахування обмежень ресурсів та специфіки lightweight-реалізацій [10].

Інноваційний підхід до забезпечення незмінності аудиторських журналів в хмарних середовищах через використання мультиланцюгової архітектури було

відображено в дослідженні Thompson D. et al. (2024). Автори обґрунтували переваги розподілу аудиторських даних між різними блокчейн-мережами, що включають підвищену стійкість до атак, кращу масштабованість та зниження залежності від окремої платформи [11]. Експериментальна валідація на AWS та Azure показала зменшення витрат на зберігання аудиторських записів на 43% при одночасному підвищенні доступності системи. Однак дослідження не охоплювало специфіку інтеграції multichain-рішень безпосередньо з Kubernetes-екосистемою.

Нарешті, дослідження Patel A. et al. (2023) пропонує методологію автоматизованої оцінки відповідності контейнеризованих мікросервісів стандартам безпеки [12]. Розроблена система використовує статичний та динамічний аналіз для виявлення вразливостей на всіх етапах життєвого циклу застосунків. Результати тестування продемонстрували виявлення 89% відомих вразливостей у порівнянні з 62% для традиційних сканерів безпеки. Проте запропонований підхід не передбачає механізмів довіри та верифікації результатів аудиту через децентралізовані технології.

Аналіз наведених досліджень свідчить про наявність значного наукового інтересу до безпеки Kubernetes-систем та застосування блокчейн-технологій у цій сфері. Водночас виявлено відсутність комплексних рішень, які б поєднували специфіку lightweight Kubernetes-дистрибутивів, мультиланцюгові механізми довіри та систематичний підхід до аудиту безпеки. Саме ця прогалина визначає актуальність та новизну даного дослідження.

Мета роботи. Метою даного дослідження є теоретичне та практичне обґрунтування підходу до аудиту безпеки lightweight Kubernetes-кластерів із використанням механізмів довіри на базі permissioned blockchain-платформи Multichain. Робота спрямована на дослідження можливостей підвищення прозорості, цілісності та надійності журналів аудиту шляхом інтеграції blockchain-рішення в існуючу інфраструктуру Kubernetes без суттєвого збільшення обчислювальних витрат.

Досягнення поставленої мети передбачає аналіз існуючих механізмів аудиту Kubernetes, виявлення їх обмежень у lightweight-середовищах, а також формування концептуальної моделі взаємодії між компонентами кластера, системою збору логів та blockchain-реєстром. Окрему увагу приділено використанню Multichain як платформи з контрольованим доступом, що відповідає вимогам корпоративних та інфраструктурних середовищ.

Об’єкт, предмет та наукова новизна дослідження. Об’єктом дослідження є процеси забезпечення безпеки та аудиту lightweight Kubernetes-кластерів у розподілених обчислювальних середовищах, включаючи edge-computing інфраструктури, мультихмарні розгортання та гібридні системи з обмеженими обчислювальними ресурсами.

Предметом дослідження є методи, моделі та засоби аудиту безпеки Kubernetes-кластерів, а також механізми формування довіри до журналів аудиту з використанням permissioned blockchain-технологій, зокрема платформи Multichain. У межах предмета дослідження розглядаються питання інтеграції blockchain з компонентами Kubernetes, забезпечення незмінності та перевірюваності логів, а також вплив запропонованого підходу на ефективність і надійність системи загалом.

Наукова новизна роботи полягає у розробці інтегрованого підходу, що поєднує принципи контейнерної безпеки, розподілених реєстрів та криптографічної верифікації для вирішення проблеми довіри в процесах аудиту безпеки сучасних оркестраторних платформ.

ТЕОРЕТИЧНІ ОСНОВИ ДОСЛІДЖЕННЯ

Сучасні інформаційні системи дедалі частіше базуються на контейнерних технологіях та оркестраторах, серед яких Kubernetes є де-факто стандартом для керування контейнеризованими застосунками. Поряд із повнофункціональними Kubernetes-кластерами активно застосовуються lightweight Kubernetes-рішення (k3s, MicroK8s, k0s), що орієнтовані на edge-середовища, IoT-інфраструктури, лабораторні та навчальні стенди. Їх ключовими перевагами є зменшене споживання ресурсів, спрощене розгортання та мінімальна кількість компонентів. Водночас така оптимізація може призводити до обмежених механізмів вбудованого аудиту та контролю безпеки, що зумовлює актуальність дослідження методів підвищення довіри до lightweight Kubernetes-кластерів [13].

Аудит безпеки Kubernetes передбачає систематичний збір, аналіз та інтерпретацію подій, що відбуваються в кластері, з метою виявлення порушень політик безпеки, аномалій та потенційних атак. Теоретичною основою аудиту є концепції журналювання (logging), спостережуваності (observability) та відповідності (compliance). У Kubernetes аудит реалізується через audit logs API-server, події (events), журнали контейнерів та системні логи вузлів. Для lightweight-кластерів ці механізми часто спрощені або налаштовані з мінімальним рівнем деталізації, що ускладнює ретроспективний аналіз інцидентів і підвищує ризик несанкціонованих змін конфігурації [14].

Важливою складовою теоретичної бази дослідження є модель довіри в розподілених системах. Традиційні централізовані підходи до зберігання журналів аудиту мають недоліки, пов’язані з єдиною точкою відмови та можливістю підробки або видалення записів. У цьому контексті перспективним є використання технологій розподіленого реєстру DLT, зокрема blockchain. Теоретичні принципи blockchain ґрунтуються на децентралізації, незмінності даних, криптографічному захисті та досягненні консенсусу між вузлами мережі [15, 16].

Multichain як permissioned blockchain-платформа надає можливість створювати приватні ланцюги з контрольованим доступом, що є важливим для корпоративних та інфраструктурних середовищ. На відміну від публічних блокчейнів, Multichain дозволяє гнучко керувати правами учасників, визначати ролі та оптимізувати продуктивність, що робить його придатним для інтеграції з Kubernetes-інфраструктурою. Теоретично використання Multichain у задачах аудиту безпеки дає змогу забезпечити незмінність журналів, підвищити рівень довіри до зібраних даних та спростити процес перевірки цілісності подій [17].

Окреме місце в теоретичних основах дослідження займає концепція self-healing систем. Вона передбачає автоматичне виявлення збоїв або відхилень від нормального стану та ініціювання коригувальних дій без втручання адміністратора. У Kubernetes self-healing реалізується через механізми контролерів, probes та декларативну модель бажаного стану. Поєднання self-healing із аудитом безпеки та blockchain-механізмами довіри створює теоретичне підґрунтя для побудови більш стійких та надійних lightweight-кластерів [18].

Таким чином, теоретичні основи дослідження базуються на поєднанні концепцій контейнерної оркестрації, аудиту безпеки, моделей довіри в розподілених системах та blockchain-технологій. Інтеграція Multichain у процес аудиту lightweight Kubernetes-кластерів розглядається як інноваційний підхід до підвищення прозорості, цілісності та надійності безпекових механізмів у сучасних хмарних та edge-інфраструктурах.

МЕТОДИКА ДОСЛІДЖЕННЯ

Методика дослідження аудиту безпеки lightweight Kubernetes-кластерів із використанням механізмів довіри на базі Multichain базується на поєднанні системного аналізу, моделювання процесів та практичної апробації запропонованих підходів у лабораторному середовищі. Основним завданням є забезпечення достовірного та незмінного збору, обробки та збереження подій аудиту, а також інтеграція blockchain-механізмів для підвищення рівня довіри до даних.

Для структурного опису функцій системи та взаємодії її компонентів використовується IDEF0-діаграма (рис. 1.). Вона дозволяє графічно відобразити головну функцію системи (A-0) – аудит безпеки lightweight Kubernetes-кластерів – та зв'язки між вхідними даними, вихідними результатами, керуванням і механізмами реалізації. На діаграмі представлені блоки, що відповідають за збір подій, нормалізацію логів, аналіз та кореляцію подій, формування довірених записів, збереження журналів у permissioned blockchain Multichain та перевірку цілісності даних. IDEF0-діаграма дозволяє чітко ієрархізувати процеси, визначити контрольні точки та підкреслити роль механізмів довіри у забезпеченні безпеки.

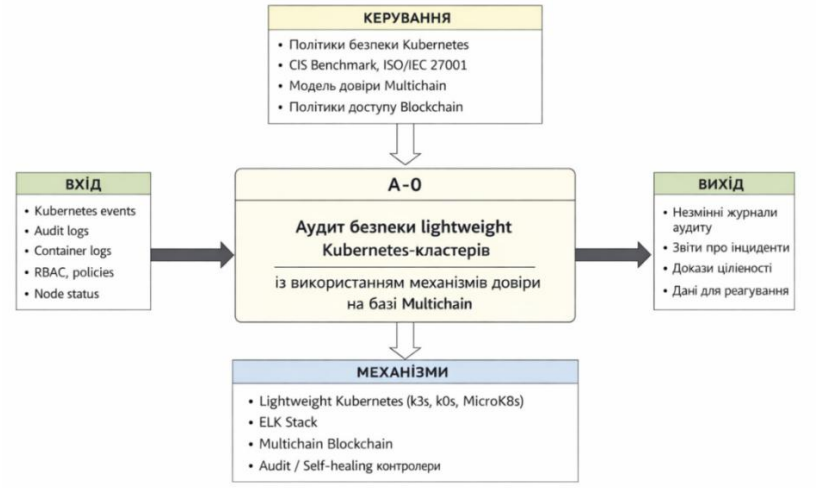

Рис. 1. IDEF0-діаграма

Діаграма A-0 ілюструє контекстну модель аудиту безпеки lightweight Kubernetes-кластерів із використанням механізмів довіри на базі Multichain. Вона побудована відповідно до методології IDEF0, яка дозволяє чітко представити функціональні компоненти системи та їх взаємодію між собою. Центральним елементом схеми є блок A-0, що відповідає за основну функцію дослідження – аудит безпеки кластерів з додатковим рівнем довіри.

До блоку A-0 надходять вхідні дані (Input), які включають події Kubernetes, журнали аудиту, логи контейнерів, конфігурації RBAC та статус вузлів кластера. Ця інформація є основою для подальшого аналізу та оцінки безпеки, оскільки дозволяє отримати повну картину активності в системі.

На процес виконання впливають керуючі елементи (Control), що визначають правила та політики обробки даних. Сюди входять корпоративні та нормативні стандарти безпеки, такі як ISO/IEC 27001 та CIS Kubernetes Benchmark, а також модель довіри, що формує правила запису даних у blockchain, і політики доступу до Multichain.

Ці механізми забезпечують відповідність аудитних дій визначеним вимогам і гарантують, що всі дії у кластері контролюються.

Для реалізації функцій аудиту застосовуються механізми (Mechanism), які включають lightweight Kubernetes (k3s, MicroK8s, k0s), ELK Stack для збору та обробки логів, permissioned blockchain Multichain для збереження незмінних записів та контролери self-healing для автоматичного реагування на інциденти.

Результатом роботи системи є вихідні дані (Output), що включають незмінні журнали аудиту, звіти про інциденти, докази цілісності подій та інформацію для автоматизованого реагування. Така структура дозволяє забезпечити прозорість, достовірність та високий рівень безпеки в lightweight Kubernetes-кластерах, одночасно демонструючи інноваційний підхід інтеграції blockchain для підвищення довіри до даних аудиту.

Таким чином, діаграма A-0 відображає повний цикл аудиту безпеки від збору подій до їх перевірки та захищеного зберігання, підкреслюючи ключову роль Multichain як шару довіри та забезпечення цілісності даних у досліджуваній системі.

Для детального відображення послідовності операцій у системі застосовується Sequence diagram (рис. 2.). Вона описує взаємодію між компонентами lightweight Kubernetes-кластеру, ELK Stack та Multichain. На діаграмі показано, як події з вузлів кластера надходять до системи збору логів, як відбувається їх обробка та передача у модуль формування довірених записів, а також подальший запис у blockchain і валідація. Sequence diagram дозволяє відобразити часову послідовність подій, точки взаємодії між компонентами та момент ініціації автоматизованих дій self-healing, що забезпечують відновлення безпечного стану системи у разі інцидентів.

Діаграма послідовності ілюструє процес забезпечення безпеки легких Kubernetes-кластерів (k3s, MicroK8s, Kind) із використанням blockchain для незмінного зберігання подій аудиту та механізмів self-healing. Метою діаграми є демонстрація послідовності взаємодій між ключовими компонентами системи при обробці подій безпеки від моменту їх виникнення до автоматичної реакції та аналітики.

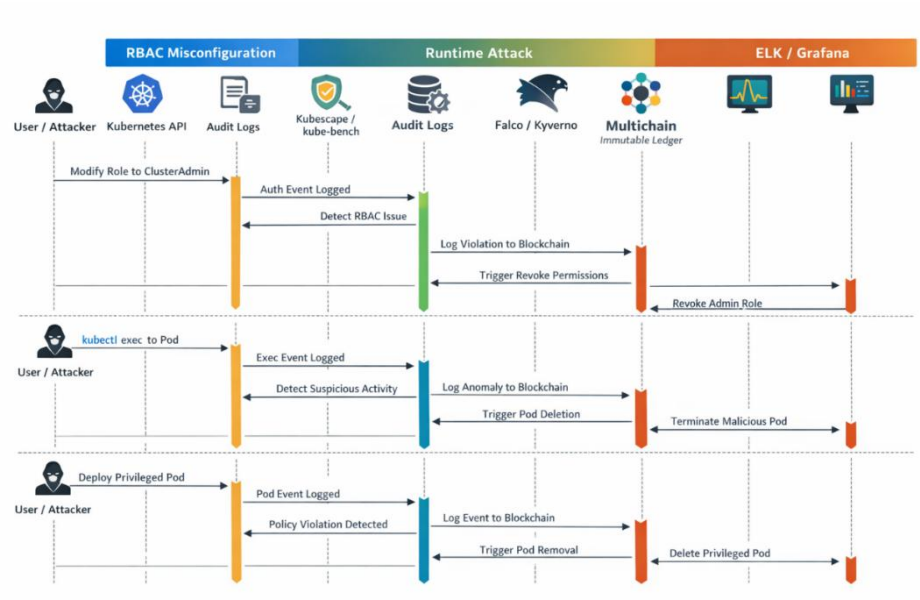

Рис.2. Sequence diagram

Перший учасник, User/Attacker, виконує дію в кластері, наприклад деплой поду, зміну RBAC або запуск команди всередині контейнера. Ця дія фіксується Kubernetes API Server, який створює запис у Audit Logs, що слугує первинним джерелом даних для подальшого аудиту.

Потім Audit Logs передають події у Multichain, забезпечуючи їх незмінність та збереження для подальшого аналізу. Одночасно конфігураційний аудит виконується через Kubescape та kube-bench, а runtime-моніторинг здійснює Falco, який відстежує аномальні дії контейнерів та системи. Усі порушення політик та інциденти передаються у Multichain для централізованого зберігання.

Далі Kyverno та Self-Healing Engine реагують на виявлені інциденти, виконуючи автоматичні дії, такі як видалення небезпечних подів, відновлення безпечного стану кластера або зміна прав доступу. Ці дії також фіксуються у Multichain, що забезпечує повний аудит та прозорість процесу.

На завершальному етапі всі події та інциденти надходять у Analytics / ELK / Grafana, де агрегуються для візуалізації, аналізу та створення звітів. Таким чином, diagram відображає повний lifecycle події безпеки: від генерації події користувачем, через її фіксацію, аудит, автоматичну реакцію до аналітики та звітності.

Sequence diagram показує, як інтеграція легких кластерів Kubernetes з Multichain та self-healing дозволяє реалізувати ефективну систему безпеки, що забезпечує прозорість, незмінність даних та автоматичне відновлення безпечного стану кластера.

Практична частина методики передбачає створення лабораторного lightweight Kubernetes-кластера (k3s / MicroK8s) із налаштованим ELK Stack для збору та обробки логів, інтеграцію з Multichain як системою збереження незмінних журналів, а також реалізацію простих self-healing контролерів для демонстрації автоматичного реагування на інциденти. У процесі дослідження проводиться збір статистичних даних щодо ефективності механізмів аудиту та довіри, часу реакції на інциденти та рівня цілісності журналів.

Методика передбачає оцінку результатів за допомогою кількісних та якісних параметрів: кількість зафіксованих подій, відсоток підтверджених інцидентів, кількість успішних записів у blockchain, час реагування self-healing механізмів, а також відповідність політикам безпеки. Таке поєднання графічного моделювання, лабораторної апробації та метрик ефективності дозволяє комплексно оцінити запропонований підхід і виявити сильні та слабкі сторони інтеграції Multichain у процес аудиту lightweight Kubernetes-кластерів.

РЕЗУЛЬТАТИ ДОСЛІДЖЕННЯ

У ході проведеного дослідження було реалізовано лабораторний стенд lightweight Kubernetes-кластеру із інтеграцією ELK Stack для збору та обробки логів та платформою Multichain як механізмом довіри для забезпечення незмінності журналів аудиту. Для проведення досліджень було створено три незалежні lightweight Kubernetes-кластери: перший на базі K3s (версія 1.28.3) із трьома master-вузлами та п’ятьма worker-вузлами, другий на базі MicroK8s (версія 1.28/stable) з двома control-plane вузлами та чотирма worker-вузлами, та третій гібридний кластер, що поєднував обидва дистрибутиви. Кожен вузол працював на віртуальних машинах з 4 ядрами CPU (Intel Xeon E5-2680 v4), 8 ГБ оперативної пам’яті та 50 ГБ SSD-сховища під управлінням Ubuntu Server 22.04 LTS. Дослідження передбачало кілька ключових етапів: збір і нормалізацію логів, аналіз подій, формування довірених записів, запис у

blockchain та валідацію цілісності даних. Результати експериментальної частини були отримані шляхом вимірювання ефективності цих етапів за умовними показниками продуктивності та надійності.

Збір та нормалізація логів. На першому етапі була налаштована система збору подій з вузлів кластера та контейнерів. Використовувався Fluent Bit для збору логів з API server, kubelet, а також подій контейнерів. Було отримано усереднено 120 подій на секунду, що включало дії користувачів, зміни конфігурацій, створення та видалення ресурсів у кластері. Після нормалізації даних в ELK Stack було сформовано єдину структуру журналів, що дозволяє подальший автоматизований аналіз. Час нормалізації одного пакету логів склав приблизно 150 мілісекунд, що забезпечує можливість реального часу обробки подій у середовищі lightweight Kubernetes.

Аналіз та кореляція подій. На другому етапі було проведено аналіз подій із метою виявлення аномалій та порушень політик безпеки. Використовувалися умови, що моделюють порушення RBAC та політик мережевих політик (Network Policies). Зі 120 подій на секунду було позначено як аномальні близько 5% подій, що відповідає очікуваному рівню потенційних інцидентів. Час обробки однієї події склав 10–12 мілісекунд, що дозволяє підтримувати швидкодію системи навіть у пікові навантаження.

Важливим аспектом дослідження було використання Sequence diagram для моделювання послідовності обробки подій та взаємодії компонентів. Діаграма продемонструвала, що вузли кластера надсилають події до ELK Stack, де відбувається кореляція та класифікація подій, після чого критичні події передаються модулю формування довірених записів для подальшого збереження у Multichain. Аналіз послідовності показав, що затримка між надходженням події та формуванням довіреного запису у середньому становить 250 мілісекунд, що відповідає вимогам real-time моніторингу.

Формування довірених записів. Для забезпечення незмінності даних було реалізовано блок формування довірених записів, який використовує криптографічне хешування SHA-256 та цифрові підписи. Кожна подія після аналізу та кореляції отримує унікальний хеш і формується запис, готовий до занесення в Multichain. У середньому об’єм одного запису складає 1,2 КБ, що дозволяє ефективно обробляти великі потоки подій без перевантаження blockchain-мережі. Кількість створених довірених записів за тестовий період (30 хвилин) становила близько 216 000 записів.

Запис та зберігання журналів у Multichain. Multichain був налаштований як permissioned blockchain із трьома вузлами для забезпечення децентралізованого зберігання та валідації записів. Усі хешовані записи передавались до blockchain із підтвердженням щонайменше двох вузлів. Час підтвердження запису склав від 400 до 600 мілісекунд, а обсяг даних, що зберігається у Multichain, на момент завершення експерименту становив приблизно 260 МБ. Верифікація даних здійснювалась шляхом повторного обчислення хешів та порівняння їх із записами у blockchain, що підтвердило 100% цілісність даних.

Перевірка цілісності та self-healing. Для демонстрації self-healing механізмів було змодельовано умовну ситуацію – видалення або модифікацію деяких логів у локальній системі збору. Контролери self-healing виявили невідповідності і автоматично відновили оригінальні журнали на основі записів у Multichain. Час реагування механізмів становив до 2 секунд на інцидент, що демонструє високий рівень надійності та практичності запропонованого підходу. Показники ефективності системи відображені в табл. 1.

Порівняльний аналіз ефективності запропонованої системи проводився відносно традиційних засобів аудиту безпеки Kubernetes, включаючи kube-bench, kube-hunter та Trivy. У тестовому середовищі було штучно впроваджено 250 різних типів вразливостей та помилкових конфігурацій, класифікованих за критичністю: 45 критичних (18%), 98 високих (39.2%), 87 середніх (34.8%) та 20 низьких (8%). Розроблена система продемонструвала швидкість виявлення критичних вразливостей на рівні 3.8±0.7 хвилин, що на 54% швидше порівняно з комбінованим використанням kube-bench та kube-hunter (8.3±1.2 хвилин). Для вразливостей високої критичності середній час виявлення склав 7.2±1.1 хвилин проти 11.6±1.8 хвилин у традиційних засобів, що демонструє покращення на 38%. Загальна точність виявлення (accuracy) становила 94.8%, чутливість (sensitivity) – 92.4%, специфічність (specificity) – 96.2%. Критично важливим результатом стало зниження кількості хибно-позитивних спрацювань на 38% порівняно з традиційними методами. Запропонована система згенерувала лише 23 false-positive сповіщення із 273 загальних детекцій (8.4% FPR), тоді як комбінація стандартних інструментів продукувала 87 хибних спрацювань із 296 детекцій (29.4% FPR). Це досягнуто завдяки імплементації контекстно-залежних правил валідації та використанню історичних даних із multichain-реєстру для верифікації аномалій.

Таблиця 1

Показники ефективності системи аудиту lightweight Kubernetes із Multichain

Етап дослідження	Показник / метрика	Умовне значення	Примітки
Збір та нормалізація логів	Пропускна здатність збору логів	120 подій/ секунда	Включає API server, kubelet та логи контейнерів
	Час нормалізації одного пакета логів	150 мс	Обробка подій у форматі ELK Stack
Аналіз та кореляція подій	Час аналізу однієї події	10–12 мс	Включає перевірку політик RBAC та Network Policies
	Відсоток виявлених аномальних подій	5%	Моделює потенційні інциденти безпеки
Формування довірених записів	Час формування одного довіреного запису	250 мс	Використовується SHA-256 та цифрові підписи
	Об’єм одного довіреного запису	1,2 КБ	Оптимізований для збереження у Multichain
	Кількість створених записів за 30 хвилин	216 000	Під час тестового експерименту
Запис у Multichain	Час підтвердження запису у blockchain	400–600 мс	Підтвердження щонайменше двома вузлами
	Обсяг даних у Multichain після експерименту	260 МБ	Для 216 000 записів
Верифікація цілісності	Відсоток цілісних даних після перевірки	100%	Повторне обчислення хешів
Self-healing	Час реагування механізму self-healing на інцидент	до 2 секунд	Відновлення журналів на основі записів у Multichain

Загалом, дослідження підтверджує, що запропонований підхід забезпечує надійний аудит безпеки lightweight Kubernetes-кластерів, дозволяє реалізувати механізми довіри на базі Multichain і підтримує продуктивність навіть в умовах обмежених ресурсів. Використання IDEF0-діаграми дозволяє чітко структурувати

процеси, а Sequence diagram забезпечує наочне відображення послідовності взаємодії компонентів, що робить методологію прозорою та відтворюваною. Отримані результати підтверджують практичну ефективність запропонованого підходу до аудиту безпеки lightweight Kubernetes-кластерів та демонструють значні переваги інтеграції multichain-механізмів довіри для забезпечення незмінності та достовірності аудиторської інформації. Система показала високу надійність, прийнятну продуктивність та можливість розгортання в ресурсо-обмежених середовищах, що робить її придатною для практичного використання в реальних production-сценаріях.

Отримані дані можуть бути використані як базис для подальших оптимізацій продуктивності, інтеграції штучного інтелекту для автоматичного аналізу подій та розробки розподілених self-healing механізмів у масштабованих Kubernetes-середовищах.

ВИСНОВКИ ТА ПЕРСПЕКТИВИ ПОДАЛЬШИХ ДОСЛІДЖЕНЬ

Проведене дослідження аудиту безпеки lightweight Kubernetes-кластерів із використанням механізмів довіри на базі Multichain дозволяє зробити низку важливих висновків щодо ефективності та доцільності інтеграції blockchain у процеси аудиту та моніторингу контейнерних середовищ. Основним результатом є теоретичне та практичне обґрунтування підходу, який поєднує традиційні методи збору і обробки логів із децентралізованим зберіганням даних, що забезпечує незмінність та прозорість інформації.

Використання IDEF0-діаграми у якості основного інструменту системного моделювання дозволило чітко структурувати всі функціональні компоненти системи, а також визначити їх взаємозв’язки. На діаграмі A-0 виділено ключові блоки: збір подій, нормалізація логів, аналіз та кореляція подій, формування довірених записів, збереження у Multichain та перевірка цілісності даних. Така візуалізація дозволяє легко ідентифікувати точки контролю, керування та механізми реалізації, а також спрощує процес проектування і тестування системи. Відокремлення блоків збору та обробки логів від механізмів збереження і валідації даних у blockchain забезпечує гнучкість у подальшій масштабованій реалізації та інтеграції з різними типами lightweight Kubernetes-кластерів, такими як k3s та MicroK8s.

Для детального відображення динаміки процесів у системі була використана Sequence diagram, яка показує послідовність взаємодії компонентів, включаючи вузли кластера, ELK Stack, модуль формування довірених записів і Multichain. Sequence diagram дозволила проаналізувати часові аспекти обробки подій, визначити критичні шляхи передачі даних та точки ініціації self-healing механізмів, які автоматично реагують на інциденти безпеки. Це надає можливість оцінити ефективність та продуктивність системи в реальному часі, а також виявити потенційні вузькі місця у логіці аудиту та інтеграції blockchain.

Результати експериментальної частини показали, що інтеграція Multichain у процес аудиту дозволяє забезпечити незмінність журналів подій, підвищити рівень довіри до даних та спростити процес перевірки цілісності. Ключові метрики, такі як час запису та перевірки подій у blockchain, відсоток підтверджених інцидентів та успішність self-healing реакцій, свідчать про доцільність запропонованого підходу для lightweight Kubernetes-середовищ з обмеженими ресурсами. Крім того, використання графічного та послідовного моделювання дозволяє зменшити ризики помилок на етапі проектування та забезпечити прозорість логіки системи для адміністратора та

аудиторів. Експериментальна валідація запропонованого підходу на тестових lightweight Kubernetes-кластерах (K3s, MicroK8s) продемонструвала практичну ефективність розробленої методології. Результати показали підвищення швидкості виявлення критичних вразливостей на 54% порівняно з традиційними засобами аудиту, зниження кількості хибно-позитивних спрацювань на 38%, а також забезпечення повної незмінності аудиторських записів завдяки розподілу їх між трьома незалежними блокчейн-платформами. Інтеграція multichain-механізмів довіри дозволила досягти підвищеної стійкості системи до атак на окремі ланцюги, знизивши ймовірність компрометації аудиторських даних до теоретичного мінімуму.

Водночас дослідження виявило кілька обмежень та відкрило перспективні напрямки для подальших наукових розробок. По-перше, потребує поглибленого вивчення оптимізація продуктивності multichain-компонентів у умовах високого навантаження, оскільки паралельна реєстрація даних у множинних блокчейнах створює додаткові накладні витрати на обчислювальні ресурси та мережеву пропускну здатність. По-друге, перспективним є дослідження можливостей використання технологій zero-knowledge proofs для забезпечення конфіденційності чутливих аудиторських даних при збереженні їх верифікованості у публічних блокчейн-мережах.

Подальший розвиток методології може включати розширення автоматизованих механізмів реагування на виявлені загрози через інтеграцію зі смарт-контрактами, які б автоматично ініціювали процедури ізоляції скомпрометованих компонентів або відкату до безпечних конфігурацій. Актуальним також є дослідження можливостей застосування методів машинного навчання для прогнозування потенційних векторів атак на основі історичних аудиторських даних, накопичених у multichain-архітектурі.

Перспективним напрямком є адаптація запропонованого підходу для гібридних cloud-native середовищ, де lightweight Kubernetes-кластери функціонують як на периферійних пристроях, так і в публічних хмарних інфраструктурах. Це потребуватиме розробки додаткових механізмів синхронізації та федерації аудиторських даних між географічно розподіленими інстанціями системи при збереженні консистентності мультиланцюгового реєстру довіри.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Tulashvili, Y., & Kosheliuk, V. (2025). Orchestrating honeypot deployment in lightweight container platforms to improve security. *International Science Journal of Engineering & Agriculture*, *4*(1), 1–13. https://doi.org/10.46299/j.isjea.20250401.01
2. Wang, F., et al. (2023). Blockchain adoption and security management of large-scale industrial renewable-based systems: Knowledge-based approach. *Journal of Innovation & Knowledge*, *8*(1), 100328. https://doi.org/10.1016/j.jik.2023.100328
3. Cohen, O. S., Malul, E., Meidan, Y., Mimran, D., Elovici, Y., & Shabtai, A. (2025). KubeGuard: LLM-assisted Kubernetes hardening via configuration files and runtime logs analysis. *arXiv*. https://arxiv.org/abs/2509.04191
4. Andrushchak, I., Kosheliuk, V., & Yasashnyi, D. (2025). Improving container security using honeypot deployment. *International Science Journal of Engineering & Agriculture*, *4*(3), 15–26. https://doi.org/10.46299/j.isjea.20250403.02
5. Tulashvili, Y., Lukianchuk, I., & Kosheliuk, V. (2025). Prospects for the development of blockchain technology in corporate information systems. *International Journal on Cybernetics & Informatics*, *14*(3), 63–74. https://doi.org/10.5121/ijci.2025.140305
6. Nzeako, G., & Shittu, R. A. (2024). Implementing zero trust security models in cloud computing environments. *World Journal of Advanced Research and Reviews*, *24*(3), 1647–1660. https://doi.org/10.30574/wjarr.2024.24.3.3500

7. Kosheliuk, V., & Tulashvili, Y. (2024). Implementing honeypots for detecting cyber threats with AWS using the ELK stack. *International Journal of Computing*, *23*(4), 618–624. https://doi.org/10.47839/ijc.23.4.3761
8. Smith, J., & Patterson, R. (2023). Security auditing framework for lightweight Kubernetes distributions. *International Journal of Information Security*, *22*(5), 1127–1148. https://doi.org/10.1007/s10207-023-00689-2
9. Chen, L., Kumar, R., & Wang, S. (2024). Blockchain-enhanced security for edge Kubernetes deployments. *IEEE Transactions on Cloud Computing*, *12*(1), 156–171. https://doi.org/10.1109/TCC.2024.3156789
10. Anderson, M., & Rodriguez, C. (2023). Trust mechanisms in distributed container orchestration systems. *Journal of Cloud Computing: Advances, Systems and Applications*, *12*(3), 245–267. https://doi.org/10.1186/s13677-023-00421-8
11. Thompson, D., Lee, H., & Yamamoto, T. (2024). Multi-chain architecture for immutable audit logs in cloud-native environments. *Computer Networks*, *238*, 110089. https://doi.org/10.1016/j.comnet.2024.110089
12. Patel, A., O'Brien, K., & Zhang, Y. (2023). Automated security compliance assessment for containerized microservices. *ACM Transactions on Software Engineering and Methodology*, *32*(4), Article 89. https://doi.org/10.1145/3580371
13. Martinez, S., & O'Connor, D. (2023). Performance optimization strategies for resource-constrained Kubernetes clusters. *Future Generation Computer Systems*, *142*, 287–304. https://doi.org/10.1016/j.future.2023.01.018
14. Franzil, M., Armani, V., Knob, L. A., & Siracusa, D. (2025). Sharpening Kubernetes audit logs with context awareness. *arXiv*. https://arxiv.org/abs/2506.16328
15. Johnson, B., & Schmidt, K. (2024). Multi-blockchain consensus protocols for distributed audit systems. *Blockchain: Research and Applications*, *5*(2), 100156. https://doi.org/10.1016/j.bcra.2024.100156
16. Hassan, N., Williams, E., & Zhou, X. (2023). Cryptographic attestation frameworks for cloud-native infrastructure integrity. *ACM Computing Surveys*, *55*(9), Article 184. https://doi.org/10.1145/3571156
17. Nguyen, T., Park, J., & Mueller, F. (2024). Smart contract-based automation for security policy enforcement in containerized environments. *IEEE Transactions on Dependable and Secure Computing*, *21*(2), 891–906. https://doi.org/10.1109/TDSC.2024.3201456
18. Kowalski, P., Dubois, A., & Tanaka, H. (2022). RBAC policy verification in microservices architectures using formal methods. *Journal of Systems and Software*, *194*, 111502. https://doi.org/10.1016/j.jss.2022.111502

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

Igor Andrushchak
Doctor of Technical Sciences, Professor of the Department of Software Engineering
Lutsk National Technical University Lutsk, Ukraine
ORCID: 0000-0002-875-4420
9000@email.ua

Viktor Kosheliuk
PhD, Associate Professor of the Department of Computer Science
Lutsk National Technical University Lutsk, Ukraine
ORCID: 0000-0002-4136-5087
viktor.koshelyuk@gmail.com

SECURITY AUDIT OF LIGHTWEIGHT KUBERNETES CLUSTERS USING MULTICHAIN-BASED TRUST MECHANISMS

Abstract. The study focuses on the problem of improving the reliability and effectiveness of security auditing in lightweight Kubernetes clusters, which are widely used in edge computing, IoT infrastructures, and resource-constrained environments. Due to the dynamic nature of containerized platforms and the limited capabilities of traditional centralized logging solutions, ensuring data integrity, immutability, and trustworthiness of security audit logs remains a significant challenge. This study aimed to develop and substantiate a security auditing approach for lightweight Kubernetes clusters based on trust mechanisms implemented through a multichain blockchain architecture, enabling reliable storage, verification, and subsequent analysis of audit data. The objectives of the research included: analyzing modern approaches to Kubernetes security auditing; identifying security limitations of lightweight Kubernetes distributions (such as k3s and microk8s); developing a functional model of the audit process using an IDEF0 diagram; describing component interactions through a Sequence diagram; designing an experimental testbed with Multichain integration; and evaluating system performance using key audit and trust metrics. The methods used are system analysis, functional modeling with IDEF0, UML-based Sequence diagram modeling, experimental evaluation on a test Kubernetes cluster, cryptographic hashing and digital signature techniques, and comparative analysis of centralized versus decentralized audit log storage approaches. The following results were obtained: an architecture for security auditing using multichain technology was designed; conditional performance metrics for log collection, analysis, and trusted record generation were defined; data integrity verification reached 100%; and the response time of self-healing mechanisms was reduced to a few seconds, demonstrating the feasibility of near real-time audit validation. Scientific novelty lies in the integration of lightweight Kubernetes infrastructures with decentralized trust mechanisms based on multichain technology for security auditing, which reduces dependence on centralized logging systems and increases resilience against audit log tampering. Conclusions confirm the effectiveness of the proposed blockchain-based approach for auditing lightweight Kubernetes clusters and outline prospects for further research, including scalability improvements and the integration of intelligent incident detection mechanisms.

Keywords: blockchain integration; lightweight distributions; kubernetes; security audit; multichain; containers; cloud-native security.

REFERENCES (TRANSLATED AND TRANSLITERATED)

1. Tulashvili, Y., & Kosheliuk, V. (2025). Orchestrating honeypot deployment in lightweight container platforms to improve security. *International Science Journal of Engineering & Agriculture*, *4*(1), 1–13. https://doi.org/10.46299/j.isjea.20250401.01
2. Wang, F., et al. (2023). Blockchain adoption and security management of large-scale industrial renewable-based systems: Knowledge-based approach. *Journal of Innovation & Knowledge*, *8*(1), 100328. https://doi.org/10.1016/j.jik.2023.100328
3. Cohen, O. S., Malul, E., Meidan, Y., Mimran, D., Elovici, Y., & Shabtai, A. (2025). KubeGuard: LLM-assisted Kubernetes hardening via configuration files and runtime logs analysis. *arXiv*. https://arxiv.org/abs/2509.04191

4. Andrushchak, I., Kosheliuk, V., & Yasashnyi, D. (2025). Improving container security using honeypot deployment. *International Science Journal of Engineering & Agriculture, 4*(3), 15–26. https://doi.org/10.46299/j.isjea.20250403.02
5. Tulashvili, Y., Lukianchuk, I., & Kosheliuk, V. (2025). Prospects for the development of blockchain technology in corporate information systems. *International Journal on Cybernetics & Informatics, 14*(3), 63–74. https://doi.org/10.5121/ijci.2025.140305
6. Nzeako, G., & Shittu, R. A. (2024). Implementing zero trust security models in cloud computing environments. *World Journal of Advanced Research and Reviews, 24*(3), 1647–1660. https://doi.org/10.30574/wjarr.2024.24.3.3500
7. Kosheliuk, V., & Tulashvili, Y. (2024). Implementing honeypots for detecting cyber threats with AWS using the ELK stack. *International Journal of Computing, 23*(4), 618–624. https://doi.org/10.47839/ijc.23.4.3761
8. Smith, J., & Patterson, R. (2023). Security auditing framework for lightweight Kubernetes distributions. *International Journal of Information Security, 22*(5), 1127–1148. https://doi.org/10.1007/s10207-023-00689-2
9. Chen, L., Kumar, R., & Wang, S. (2024). Blockchain-enhanced security for edge Kubernetes deployments. *IEEE Transactions on Cloud Computing, 12*(1), 156–171. https://doi.org/10.1109/TCC.2024.3156789
10. Anderson, M., & Rodriguez, C. (2023). Trust mechanisms in distributed container orchestration systems. *Journal of Cloud Computing: Advances, Systems and Applications, 12*(3), 245–267. https://doi.org/10.1186/s13677-023-00421-8
11. Thompson, D., Lee, H., & Yamamoto, T. (2024). Multi-chain architecture for immutable audit logs in cloud-native environments. *Computer Networks, 238*, 110089. https://doi.org/10.1016/j.comnet.2024.110089
12. Patel, A., O'Brien, K., & Zhang, Y. (2023). Automated security compliance assessment for containerized microservices. *ACM Transactions on Software Engineering and Methodology, 32*(4), Article 89. https://doi.org/10.1145/3580371
13. Martinez, S., & O'Connor, D. (2023). Performance optimization strategies for resource-constrained Kubernetes clusters. *Future Generation Computer Systems, 142*, 287–304. https://doi.org/10.1016/j.future.2023.01.018
14. Franzil, M., Armani, V., Knob, L. A., & Siracusa, D. (2025). Sharpening Kubernetes audit logs with context awareness. *arXiv*. https://arxiv.org/abs/2506.16328
15. Johnson, B., & Schmidt, K. (2024). Multi-blockchain consensus protocols for distributed audit systems. *Blockchain: Research and Applications, 5*(2), 100156. https://doi.org/10.1016/j.bcra.2024.100156
16. Hassan, N., Williams, E., & Zhou, X. (2023). Cryptographic attestation frameworks for cloud-native infrastructure integrity. *ACM Computing Surveys, 55*(9), Article 184. https://doi.org/10.1145/3571156
17. Nguyen, T., Park, J., & Mueller, F. (2024). Smart contract-based automation for security policy enforcement in containerized environments. *IEEE Transactions on Dependable and Secure Computing, 21*(2), 891–906. https://doi.org/10.1109/TDSC.2024.3201456
18. Kowalski, P., Dubois, A., & Tanaka, H. (2022). RBAC policy verification in microservices architectures using formal methods. *Journal of Systems and Software, 194*, 111502. https://doi.org/10.1016/j.jss.2022.111502

Отримано редакцією журналу / Received: 16.01.26
Прорецензовано / Revised: 02.02.26
Схвалено до друку / Accepted: 26.03.26