DOI 10.34132/mspc2025.01.06.35

Євгеній Худолій

ОЦІНКА РИЗИКІВ ТА ПЕРЕВАГ ВІД ПОЄДНАННЯ ПРИНЦИПІВ ZERO TRUST ТА ТЕХНОЛОГІЇ БЛОКЧЕЙН ДЛЯ ЗАХИСТУ ДАНИХ У БАГАТОХМАРНИХ СЕРЕДОВИЩАХ

Тези представляють теоретико-методологічний аналіз інтеграції моделі нульової довіри (Zero Trust) з блокчейн-технологіями як потенційного чинника посилення кібербезпеки багатохмарних середовищ. Zero Trust виступає інструментом модернізації безпеки, що базується на суворій автентифікації, мінімізації прав доступу та постійному моніторингу. Поєднання Zero Trust із децентралізованими рішеннями блокчейну забезпечує високий рівень надійності, прозорості та незмінності даних. Робота аналізує поточні виклики, переваги та обмеження такого підходу, а також підкреслює перспективи майбутніх досліджень. Особливу увагу приділено розумінню того, як ці підходи можуть зменшити ризики кібератак, забезпечити захист важливої інформації та сприяти розвитку цифрової трансформації. Тези формують основу для подальших досліджень у сфері кібербезпеки.

Ключові слова: *кібербезпека, нульова довіра, блокчейн, багатохмарне середовище, контроль доступу, смарт-контракти*

У нинішню цифрову епоху поширення кіберзагроз стало серйозною проблемою для окремих людей, компаній і урядів. Кіберзагрози залишаються першорядною проблемою у всьому світі, оскільки організації будь-якого розміру та сектору стикаються зі збільшенням кількості та якості кібератак. Для ефективної протидії кіберзагрозам фахівці дедалі частіше впроваджують сучасні підходи, серед яких концепція нульової довіри (Zero Trust), технології блокчейн та багатохмарні середовища, які відіграють важливу роль у побудові стійкої інфраструктури Концепція нульової довіри, що базується на принципі «нікому не довіряй, завжди перевіряй», набула критичного значення в умовах розвитку кіберзагроз, особливо у багатохмарних середовищах [1]. Технологія блокчейн є децентралізованою, незмінною, та пропонує нові можливості для забезпечення довіри та прозорості в розподілених системах [2].

Зі зростанням потреби в надійних рішеннях для захисту розподіленої інфраструктури від кіберзагроз з'являється необхідність дослідження поєднання принципів нульової довіри та технології блокчейн у багатохмарних середовищах. Принципи нульової довіри, зокрема суворий контроль доступу та постійна верифікація, є особливо актуальними в умовах багатохмарних рішень, де взаємодіють різноманітні хмарні провайдери. Водночас блокчейн може забезпечити децентралізовані механізми управління ідентифікацією, контролем доступу та цілісністю даних, що підсилює ефективність підходу нульової довіри. Інтеграція цих технологій дозволяє значно підвищити рівень безпеки у багатохмарних середовищах.

Актуальність дослідження нових рішень у сфері кіберзахисту зумовлена зростаючою частотою кібератака на хмарні сервіси, нові виклики які виникають під час керування безпекою в багатохмарних середовищах, де використовуються декілька хмарних провайдерів. Наявні підходи до захисту часто не відповідають сучасним загрозам і обмежують гнучкість роботи хмарної інфраструктури. У контексті поєднання принципів нульової довіри, а саме суворий контроль доступу та постійна перевірка ідентичності, з децентралізованими можливостями блокчейну, зокрема керування ідентифікацією та забезпечення цілісності даних, відкриває нові перспективи розвитку у сфері безпеки для хмарних середовищ. Така інтеграція може підвищити рівень безпеки, зміцнити довіру до обробки даних і допомогти відповідати встановленим стандартам.

Дослідження спрямоване на ретельний огляд поточного стану досліджень у цій сфері, зокрема для виявлення основних проблем і недоліків наявних рішень, оцінки можливостей, які блокчейн-технології пропонують для посилення захисту багатохмарних середовищ, побудованих відповідно до принципів нульової довіри. Це закладає основу для пошуку нових підходів до керування безпекою в багатохмарних середовищах, поєднуючи інноваційні технології з перевіреними методами.

Модель нульової довіри базується на перевірці кожного запиту, незалежно від його джерела, і припусканні загроз як ззовні, так і всередині мережі. Ключовими елементами є принцип найменших привілеїв, мікросегментація, безперервний моніторинг та готовність до інцидентів. У багатохмарних середовищах впровадження цієї моделі ускладнюється через різноманітність інструментів і політик різних провайдерів, недостатню видимість ресурсів, проблеми сумісності API та високу ймовірність помилок конфігурації. Додатковим викликом є модель спільної відповідальності, коли обов'язки розподіляються між

провайдером і клієнтом. Змінна природа багатохмарних середовищ, зокрема використання безсерверних функцій та мікросервісів, ускладнює впровадження сталих правил безпеки, а керування доступом на кількох платформах створює додаткове навантаження на команди [3].

На практиці спостерігається зростання впровадження принципів нульової довіри в різних організаціях по всьому світу, особливо завдяки таким рішенням, як Zero Trust Network Access, що поступово витісняють VPN. Ринок безпекових технологій продовжує розвиватися, адже традиційні моделі безпеки виявляються недостатньо стійкими до нових типів загроз. Проте існуючі підходи все ще мають обмеження, що стимулює пошук інноваційних рішень, серед яких інтеграція блокчейну виглядає перспективним напрямом.

Технологія блокчейн як розподілений реєстр забезпечує незмінність даних за допомогою криптографічного хешування, консенсусних механізмів і смарт-контрактів. Блокчейн дозволяє гарантувати цілісність інформації, підвищувати стійкість до атак на централізовані системи та автоматизувати політики доступу без потреби у довірених посередниках. Дана технологія дозволяє створювати журнали аудиту й автоматизувати управління даними в хмарі, зберігаючи всю історію про операції в одному місці. Завдяки таким властивостям блокчейн може відігравати важливу роль у компенсації деяких обмежень моделі нульової довіри в багатохмарних середовищах, одночасно значно підвищуючи безпеку таких середовищ [4].

Інтеграція принципів нульової довіри та блокчейну в багатохмарних середовищах відкриває значні можливості для підвищення рівня безпеки, надійності та стійкості хмарної інфраструктури. Поєднання безперервної перевірки доступу та децентралізованої довіри дозволяє зменшити площу атаки, обмежуючи можливість бокового переміщення зловмисників, а також підвищує ефективність виявлення загроз завдяки безперервному моніторингу та незмінним журналам аудиту. Керування ідентифікацією стає більш гнучким, що зменшує ризики викрадення облікових даних, а цілісність і прозорість даних зміцнюють довіру між усіма учасниками системи. Водночас спрощується керування політиками безпеки та полегшується дотримання безпекових вимог, що особливо актуально в умовах взаємодії з численними сторонніми провайдерами [5].

Разом із цим впровадження комбінованого підходу нульової довіри та блокчейну супроводжується низкою викликів. Це, зокрема, складність інтеграції й управління двома технологіями на різних хмарних платформах, потенційні проблеми з продуктивністю та масштабованістю блокчейн-інфраструктури, а також підвищення витрат на ресурси. Додатковим викликом є те, що нормативно-правове регулювання блокчейн-рішень перебуває на стадії формування, а впровадження потребує спеціалізованих знань у двох складних доменах. Окрему увагу слід приділяти правильному проєктуванню смарт-контрактів, оскільки помилки на цьому етапі можуть створити нові вразливості.

Порівняння традиційного підходу до безпеки, моделі нульової довіри та її комбінації з блокчейн-технологіями у багатохмарних середовищах дозволяє окреслити ключові відмінності між ними. Таблиця 1 узагальнює основні характеристики кожного підходу, підкреслюючи особливості управління доступом, захисту даних, стійкості до загроз, масштабованості та відповідності нормативним вимогам. Такий огляд допомагає сформувати цілісне бачення сильних сторін і обмежень кожної моделі в умовах сучасних багатохмарних архітектур [6].

Таблиця 1.

Порівняння традиційної безпеки, нульової довіри та нульової довіри з блокчейном у багатохмарних середовищах

Характеристика	Традиційна безпека	Нульова довіра	Нульова довіра та Блокчейн
Модель довіри	Неявна довіра всередині периметра	Нікому не довіряй, завжди перевіряй	Децентралізована довіра, підкріплена криптографією
Верифікація ідентичності	Одноразова аутентифікація при вході до мережі	Постійна верифікація кожного запиту на доступ	Децентралізована та постійна верифікація
Механізми забезпечення цілісності даних	Зазвичай централізовані журнали та системи контролю	Безперервний моніторинг та перевірка цілісності	Незмінні аудиторські журнали в блокчейні, криптографічне забезпечення цілісності даних
Аудит	Залежить від централізованих систем аудиту	Постійний моніторинг та аналіз поведінки	Прозорий та незмінний аудит усіх дій в блокчейні
Проблеми масштабованості	Може виникати при зростанні інфраструктури	Потенційні накладні витрати на постійну верифікацію	Проблеми масштабованості блокчейну, необхідність оптимізації
Складність керування	Залежить від розміру та складності інфраструктури	Може бути складною в гетерогенних середовищах	Додаткова складність інтеграції та управління блокчейном
Стійкість до єдиної точки відмови	Залежить від архітектури	Підвищена стійкість завдяки розподіленому контролю	Висока стійкість до єдиної точки відмови завдяки децентралізації блокчейну

Порівняльний аналіз демонструє, що інтеграція принципів нульової довіри з блокчейн-технологіями відкриває новий рівень захисту й прозорості для багатохмарних середовищ, водночас створюючи виклики.

Отже, інтеграція безпеки з нульовою довірою з технологією блокчейн в багатохмарних середовищах є одним із перспективних напрямків створення сучасних розподілених інфраструктур з вищим рівнем безпеки. Однак, попри те, що ця комбінація може дати величезні переваги, такі як покращена безпека, краща цілісність даних і легша відповідність нормам, слід враховувати такі проблеми, як масштабованість, проблеми з продуктивністю та складність інтеграції. Подальші дослідження знадобляться для створення потужних і застосовних рішень, здатних задовольнити зростаючі вимоги організацій щодо безпеки їх багатохмарних розгортань.

References

1. Nguyen H., Sharma R., Patel S. Zero trust security architectures for multi-cloud environments: Implementation. ResearchGate. 2025. Retrieved from: https://www.researchgate.net/publication/390493182_Zero_Trust_Security_Architectures_for_Multi_Cloud_Environments_Implementation_Strategies_and_Measurable_Outcomes.
2. Zhao X., Rahman S., Martinez L. Leveraging towards access control, identity management, and security in multi-cloud systems, information. MDPI. 2024. Retrieved from: https://www.mdpi.com/2624-800X/4/4/47.
3. Wang Y., Alavi M. Zero trust architecture in multi-cloud environments: A security perspective, ResearchGate. 2025. Retrieved from: https://www.researchgate.net/publication/387902626_Zero_Trust_Architecture_in_Multi-cloud_Environments_A_Security_Perspective.
4. Singh P., Kaur R. The use of blockchain for identity and access management (IAM) in multi-cloud systems. ResearchGate. 2024. Retrieved from:, https://www.researchgate.net/publication/382541839_The_Use_of_Blockchain_for_Identity_and_Access_Management_IAM_in_Multi-cloud.
5. Jadhav R. Zero Trust: The absolute solution to cloud security challenges. AccuKnox Blog. 2024. Retrieved from: https://www.accuknox.com/blog/zero-trust-cloud-security-future.
6. The impact of blockchain on cloud security / Cloud Security Alliance (CSA). CSA Blog. 2023. Retrieved from: https://cloudsecurityalliance.org/blog/2023/10/03/the-impact-of-blockchain-on-cloud-security.

DOI 10.34132/mspc2025.01.06.35

Yevhenii Khudolii

ASSESSMENT OF RISKS AND BENEFITS OF COMBINING ZERO TRUST PRINCIPLES AND BLOCKCHAIN TECHNOLOGY FOR DATA PROTECTION IN MULTI-CLOUD ENVIRONMENTS

The theses present a theoretical and methodological analysis of integrating the Zero Trust model with blockchain technologies as a potential factor for enhancing cybersecurity in multi-cloud environments. Zero Trust serves as a security modernization tool based on strict authentication, minimal access rights, and continuous monitoring. Combining Zero Trust with decentralized blockchain solutions ensures a high level of reliability, transparency, and data immutability. The work analyzes current challenges, advantages, and limitations of this approach, while also highlighting future research prospects. Special attention is given to understanding how these approaches can reduce cyberattack risks, protect important information, and support the development of digital transformation. The theses provide a foundation for further studies in the field of cybersecurity.

Key words: *cybersecurity, zero trust, blockchain, multicloud environment, access control, smart contracts*

Відомості про автора / Information about the Author

Худолій Євгеній, магістр з комп'ютерної інженерії Чорноморського національного університету імені Петра Могили, м. Миколаїв, Україна. E-mail: hudoliy.e@gmail.com, orcid: https://orcid.org/0009-0006-0852-9795.

Yevhenii Khudolii, Master of Computer Engineering, Petro Mohyla Black Sea National University, Mykolaiv, Ukraine. E-mail: hudoliy.e@gmail.com, orcid: https://orcid.org/0009-0006-0852-9795.

Стаття отримана редакцією 20.05.2025.