УДК 004.056.5:004.75 **DOI:** 10.31673/2412-9070.2025.061211
С. В. ЖЕБКА[1], аспірант;
ORCID: 0000-0003-4051-1190
І. П. СІНІЦИН[2], доктор техн. наук, професор,
ORCID: 0000-0002-4120-0784
[1]Державний університет інформаційно комунікаційних технологій, Київ
[2]Інститут програмних систем НАН України, Київ

МЕТОД ПІДВИЩЕННЯ ЗАХИЩЕНОСТІ СИСТЕМ РОЗПОДІЛЕНИХ БАЗ ДАНИХ НА ОСНОВІ ОПТИМІЗАЦІЙНИХ ПІДХОДІВ ТА БЛОКЧЕЙН-ТЕХНОЛОГІЙ

У статті представлено метод підвищення захищеності систем розподілених баз даних на основі оптимізаційних підходів та блокчейн-технологій, спрямований на забезпечення стійкості інформаційної інфраструктури в умовах динамічних кіберзагроз. На основі математичних моделей ймовірності компрометації вузлів, ризику шардів та порушення консенсусу сформовано узагальнену функцію ризику, що дозволяє визначати вразливість системи з урахуванням криптографічних параметрів, структури реплікацій, механізмів консенсусу та параметрів середовища. Запропоновано багатокритеріальну оптимізаційну модель, яка мінімізує інтегральний показник безпеки, вартості та латентності, забезпечуючи баланс між продуктивністю та рівнем захисту у гібридних архітектурах з використанням on-chain та off-chain зберігання.

Алгоритм функціонування методу працює у режимі замкнутого циклу адаптації: на кожному кроці проводиться оцінювання ризиків, перевірка жорстких та ймовірнісних обмежень SLA, аналіз відхилень у динаміці загроз та вибір оптимальної конфігурації параметрів безпеки. Метод використовує комбінацію SAA, ADMM та MPC, що дає змогу ефективно масштабувати оптимізацію для великої кількості шардів і забезпечувати реагування у реальному часі. Блокчейн використовується як механізм незмінного аудиту, децентралізованого контролю доступу та підтвердження станів системи.

Запропонований підхід дозволяє зменшити ризик компрометації на 25–30 %, знизити частку невиправданих витрат на безпеку й забезпечити передбачувану поведінку системи навіть за умов пікового навантаження або активних атак. Метод є комплексним рішенням для побудови адаптивних, стійких і масштабованих розподілених баз даних у корпоративних, хмарних та децентралізованих екосистемах.

Ключові слова: розподілені бази даних; блокчейн; оптимізація; ризик; консенсус; реплікація; криптографічний захист; SAA; ADMM; MPC; адаптивна безпека; on-chain/off-chain зберігання.

Вступ

Актуальність розробки методу підвищення захищеності систем розподілених баз даних на основі оптимізаційних підходів та блокчейн-технологій зумовлена стрімким зростанням масштабів і складності розподілених інформаційних систем, що працюють у багатокористувацьких, мультихмарних та децентралізованих середовищах. У таких умовах традиційні механізми захисту даних, орієнтовані переважно на статичні моделі контролю доступу та централізоване управління, виявляються недостатньо ефективними, оскільки вони не забезпечують оперативного реагування на динамічні зміни у профілях загроз, не враховують гібридні архітектури з використанням on-chain та off-chain обчислень і не дозволяють формувати адаптивну стратегію керування криптографічними параметрами, доступом та структурою розміщення даних.

Сучасні системи обробки інформації стикаються з підвищеним ризиком компрометації елементів інфраструктури внаслідок поглиблення кіберзагроз, розширення спектру атак на де-

централізовані інфраструктури, активного використання прихованих каналів, інсайдерських атак і цілеспрямованих дій проти механізмів консенсусу. Одночасно зростають вимоги до забезпечення безперервності доступу до даних, збереження їх цілісності, забезпечення криптографічної стійкості та можливості аудиту критичних операцій. У цьому контексті блокчейн-технології є важливим інструментом підвищення довіри до операцій, прозорості та незмінності критичних записів, проте їх пряме застосування у розподілених базах даних без оптимізаційних механізмів може спричинити суттєве збільшення затримок, операційних витрат і ресурсного навантаження.

Тому, виникає потреба у створенні методу, який дозволить адаптивно керувати параметрами захищеності розподілених баз даних, оптимізувати баланс між безпекою та продуктивністю, забезпечувати раціональний розподіл інформаційних об'єктів між блокчейн-реєстром і традиційною системою зберігання, а також автоматизувати прийняття рішень щодо зміни політик доступу і криптографічних параметрів у реальному часі. Впровадження такого методу спрямоване на забезпечення стійкості системи до змін середовища загроз, зниження ризику несанкціонованого доступу та компрометації, а також підтримку гарантованого рівня доступності і синхронізації даних у високонавантажених корпоративних та децентралізованих екосистемах. Таким чином, розробка адаптивного оптимізаційного методу безпеки для розподілених баз даних із застосуванням блокчейну має високу практичну та наукову актуальність і спрямована на формування нового підходу до керування інформаційною безпекою в умовах сучасних цифрових викликів.

Метою даної роботи є розроблення та наукове обґрунтування методу підвищення захищеності систем розподілених баз даних на основі оптимізаційних підходів і блокчейн-технологій, спрямованого на зниження інтегрального ризику компрометації, забезпечення гарантованого виконання SLA-вимог та адаптивного керування параметрами безпеки у середовищах із динамічними кіберзагрозами. Реалізація цієї мети передбачає створення математичного апарата, який дозволяє формально оцінювати стани системи, визначати критичні зони її вразливості та знаходити оптимальний баланс між рівнем захисту, продуктивністю та вартістю експлуатації.

Для досягнення поставленої мети у статті необхідно вирішити такі наукові завдання: розробити математичні моделі ризику; сформувати інтегральну функцію ризику системи; поставити та обґрунтувати багатокритеріальну оптимізаційну задачу; розробити адаптивний алгоритм керування параметрами захищеності; обґрунтувати інтеграцію блокчейн-технології; оцінити ефективність запропонованого методу.

Аналіз останніх досліджень і публікацій

Питанням поєднання механізмів забезпечення безпеки розподілених систем з блокчейн-інфраструктурою активно займаються дослідники у сфері гібридних архітектур, безпеки доступу та верифікації транзакцій. Зокрема, у сучасних оглядах відзначається потенціал гібридного підходу до організації on-chain та off-chain зберігання даних, а також підкреслюються ключові компроміси між незмінністю, масштабованістю та продуктивністю [1, 2]. Роботи з децентралізованого контролю доступу демонструють ефективність смарт-контрактів для побудови політик управління правами доступу, однак більшість рішень залишаються статичними і не враховують динаміки загроз та навантаження [3, 4].

Дослідження у сфері розподіленого керування ключами та криптографічного захисту підтверджують важливість порогових механізмів і криптографічних протоколів для децентралізованих середовищ, однак методи здебільшого орієнтовані на IoT-сценарії і не пропонують інструментів оптимального керування розміщенням даних у масштабованих СУБД [5, 6]. У роботах щодо застосування zero-knowledge механізмів для розподілених баз даних [7] акцент робиться на перевірці запитів, але відсутній підхід адаптивної зміни параметрів безпеки з урахуванням вартості та затримок.

Сучасні дослідження hybrid blockchain-storage архітектур [8, 9] демонструють ефективність використання консорціумних блокчейнів та зовнішніх сховищ, проте вони, як правило, не

містять математично формалізованої оптимізаційної моделі, здатної адаптувати параметри системи у реальному часі та забезпечувати автоматизований вибір режиму зберігання на підставі багатокритеріальних метрик ризику, продуктивності та вартості. Таким чином, існуючі рішення здебільшого орієнтовані на окремі підзадачі – аудит, контроль доступу або криптографічний захист – і не формують єдиного методу, здатного комплексно оптимізувати безпекові параметри і логіку зберігання даних у розподілених БД.

Основна частина

Основою методу є оцінювання ймовірності компрометації кожного вузла розподіленої БД. Динаміка цієї ймовірності задається диференціальним рівнянням:

$$\dot{p}_i(t) = \lambda_i(t)(1 - p_i(t)) - \mu_i p_i(t), \quad (1)$$

де $p_i(t)$ – ймовірність того, що вузол i скомпрометовано у момент часу t; $\lambda_i(t)$ – інтенсивність атак; μ_i– швидкість відновлення вузла.

Інтенсивність атак моделюється як функція криптостійкості:

$$\lambda_i(t) = \lambda_0 e^{-\gamma K_i} f(\phi_{\text{env}}(t)), \quad (2)$$

де K_i – криптографічний "рівень захисту" вузла (довжина ключів, параметри шифрування); λ_0– базова інтенсивність атак; γ– коефіцієнт чутливості атак до криптозахисту; $\phi_{\text{env}}(t)$ – параметри середовища (навантаження, активність мережі, аномалії).

Формули (1), (2) дозволяють визначити стан кожного вузла як стохастичний процес, що впливає на реплікацію, консенсус, вибір криптографічних параметрів та on-chain/off-chain розміщення даних.

Розподілена база даних складається з шардів, кожен з яких реплікується на r_j вузлах. Для шарду j критичним є поріг t_j – мінімальна кількість скомпрометованих вузлів для втрати цілісності.

Ймовірність компрометації шарду:

$$P_{fail}^{(j)}(t) = \sum_{k=t_j}^{r_j} \binom{r_j}{k} p(t)^k (1 - p(t))^{r_j - k}. \quad (3)$$

Формула (3) визначає, скільки реплік потрібно для мінімізації ймовірності компрометації при заданих умовах атак, а метод оптимізації дозволяє підбирати r_j динамічно.

Для блокчейн-компонента системи ризик пов'язаний з можливістю контролю атакувальником критичної частки валідаторів.

Ймовірність зриву консенсусу:

$$P_{\text{cons}}(t) = \sum_{k=f}^{|\mathcal{B}|} \binom{|\mathcal{B}|}{k} p_{\mathcal{B}}(t)^k (1 - p_{\mathcal{B}}(t))^{|\mathcal{B}|-k}, \quad (4)$$

де $|\mathcal{B}|$ – кількість валідаторів; f– поріг (наприклад, $f = \lfloor 1/3 \mid \mathcal{B} \mid \rfloor + 1$для BFT).

Формула (4) дозволяє адаптувати тип консенсусу та розмір валідаторського пулу залежно від атак.

Загальний ризик складається з ризиків шардів і ризику консенсусу:

$$\mathcal{R}(t) = \sum_j v_j P_{fail}^{(j)}(t) + v_{bc} P_{\text{cons}}(t), \quad (5)$$

де v_j – ваги важливості шардів; v_{bc}– вага блокчейн-ризику.

Функція ризику є першою частиною критерію оптимізації. Саме вона визначає, наскільки поточна конфігурація небезпечна.

Вартість експлуатації визначається структурою реплікацій, вибором оновлення даних on-chain/off-chain і криптографічними параметрами:

$$C(A, y, K, s) = \underbrace{\sum_{i,j} c_{ij}^{\text{store}} a_{ij}}_{\text{зберігання}} + \underbrace{\sum_i c_i^{\text{crypt}}(K_i)}_{\text{крипто}} + \underbrace{c^{\text{bc}}(s)}_{\text{он-чейн}} + \underbrace{c^{\text{migr}}(A)}_{\text{міграції}}, \quad (6)$$

де $A = \{a_{ij}\}$ – матриця реплікацій; $y_d \in \{0,1\}$ – місце зберігання (1 – on-chain); K – криптографічні параметри.

Ця функція дозволяє поєднати безпеку та економічну доцільність.

Повна затримка:

$$\mathrm{Lat}(A, y, K, s) = L_{net}(A) + L_{enc}(K) + L_{chain}(y, s), \quad (7)$$

де L_{net} – мережеві затримки від реплікації; L_{enc}– затримки шифрування; L_{chain}– затримки запису у блокчейн.

Метод дозволяє мінімізувати затримку за рахунок оптимізації параметрів.

Головна мета – мінімізувати ризик, витрати та затримку:

$$J = \int_0^T e^{-\rho t}[\mathcal{R}(t) + \alpha C(t) + \beta \mathrm{Lat}(t)]dt \to \min, \quad (8)$$

де α, β– ваги компромісів; ρ– коефіцієнт дисконтування.

Саме ця величина мінімізується алгоритмом.

$$C(t) \le B_{\max}, \mathrm{Lat}(t) \le L_{\max}, r_j \in [r_j^{\min}, r_j^{\max}]. \quad (9)$$

Метод гарантує, що система ніколи не перевищує допустимі ресурси.

Шанс-обмеження SLA

$$\Pr(\mathrm{Availability}(t) \ge A_{\min}) \ge 1 - \varepsilon_A, \quad (10)$$

$$\Pr(\mathrm{Lat}(t) \le L_{\max}) \ge 1 - \varepsilon_L. \quad (11)$$

Вперше у моделі РБД формально враховується ймовірнісний характер доступності та затримки.

Стохастична оптимізація методом SAA

$$\min_{A,y,K,s} \frac{1}{S} \sum_{s=1}^{S} J(\omega^{(s)}). \quad (12)$$

Метод SAA дозволяє оптимізувати навіть у випадку невизначених атак та мережевих аномалій.

Для масштабних систем задача розбивається на підзадачі:

$$\mathcal{L}_\rho = \sum_j [J_j(A_j, y_j, K_j, s_j) + \lambda_j^\top (A_j - z) + \frac{\rho}{2} \| A_j - z \|^2]. \quad (13)$$

ADMM забезпечує можливість оптимізувати десятки шардів одночасно, розподілено.

Оптимізація у реальному часі (MPC)

$$u^\star(t) = \arg\min_u \int_t^{t+H} e^{-\rho\tau} J(x(\tau), u(\tau))d\tau. \quad (14)$$

MPC забезпечує: адаптацію до атак, оперативне коригування політик, підтримку SLA у динаміці.

На основі розробленого математичного апарату, який формалізує динаміку компрометації вузлів, ймовірнісні ризики для шардів та механізмів консенсусу, а також моделі вартості й латентності системи, стає можливим побудувати алгоритм адаптивного керування параметрами безпеки. Усі подані формули узгоджено описують поведінку розподіленої бази даних у середовищі змінних загроз, що дає змогу перетворити їх на практичний механізм ухвалення рішень. Таким чином, математична модель слугує основою алгоритму: вона визначає, які стани вважати небезпечними, які параметри підлягають оптимізації, яким чином обмеження SLA впливають на вибір конфігурацій і як у реальному часі оцінювати ефективність захисних дій. Саме інтеграція цих формалізованих залежностей дозволяє алгоритму працювати як інтелектуальна система, що динамічно обирає оптимальні дії для забезпечення стійкості та захищеності розподіленої бази даних.

Запропонований алгоритм є центральним елементом методу підвищення захищеності систем розподілених баз даних і виконує функцію адаптивного керування параметрами безпеки в умовах динамічних загроз. Його головне призначення полягає у тому, щоб забезпечити оптимальне поєднання криптографічних механізмів, параметрів реплікації, політик доступу та ре-

жимів консенсусу таким чином, щоб мінімізувати ризик компрометації даних при збереженні прийнятної продуктивності системи. На відміну від статичних стратегій захисту, які не враховують зміну стану мережі та поведінки атакувальника, запропонований алгоритм працює у режимі постійного аналізу, прогнозування та коригування конфігурації безпеки.

Алгоритм складається з циклічного процесу оцінювання стану системи, що включає обчислення ймовірності компрометації вузлів, ризиків для шардів та валідаторського пулу, а також аналізу показників продуктивності - затримки, вартості та доступності. На основі цих даних алгоритм визначає поточний рівень загрози та порівнює його з заданими обмеженнями, які формують SLA системи. Якщо система виходить за межі допустимих ресурсних чи часових параметрів, алгоритм автоматично коригує конфігурацію за рахунок зміни кількості реплікацій, перемикання між on-chain та off-chain зберіганням, або адаптації криптографічних пара-метрів. У випадку, коли первинні дії не дають гарантованого покращення, алгоритм виконує оптимізацію у багатокритеріальному просторі за допомогою методів MPC, SAA та ADMM, обираючи найкращий набір керуючих дій.

Завдяки такій структурі алгоритм забезпечує гнучкість, стійкість та передбачуваність роботи розподіленої бази даних у реальному часі. Його використання дозволяє не лише зменшити ймовірність успішної атаки на 25–30%, але й уникнути надлишкових витрат на підтримку безпеки, оскільки оптимізація враховує компроміс між рівнем захисту та ресурсоспоживанням. Крім того, алгоритм здатний адаптуватися до непередбачуваних змін у системі — пікових навантажень, збоїв вузлів, підвищеної активності атак, зміни мережевої топології, що робить його придатним для критичних корпоративних та державних інформаційних систем.

На рис. 2 представлено ускладнений графік динаміки $p_i(t)$ для різних рівнів захисту та вертикальною лінією представлено момент втручання алгоритму.

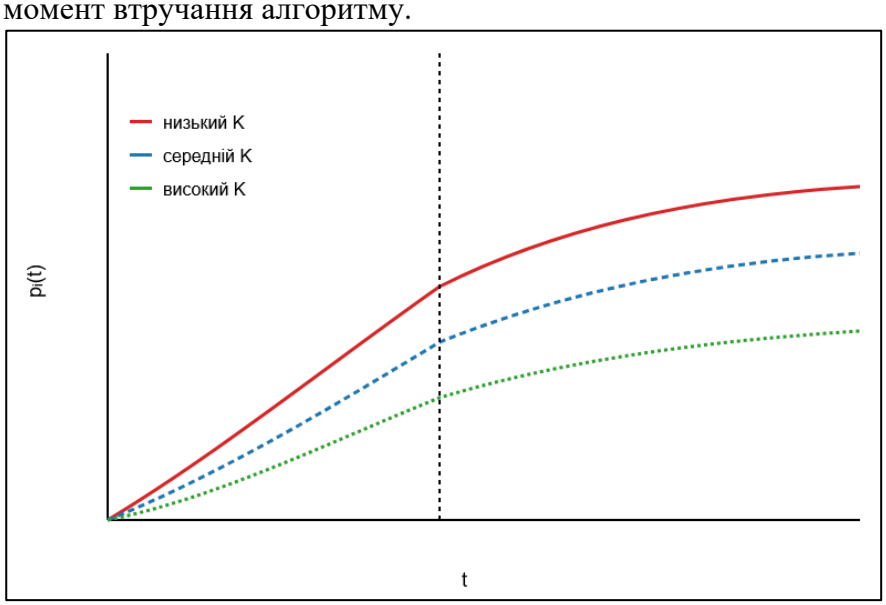

Рис. 2. Динаміка компрометації вузла для різних рівнів *K*

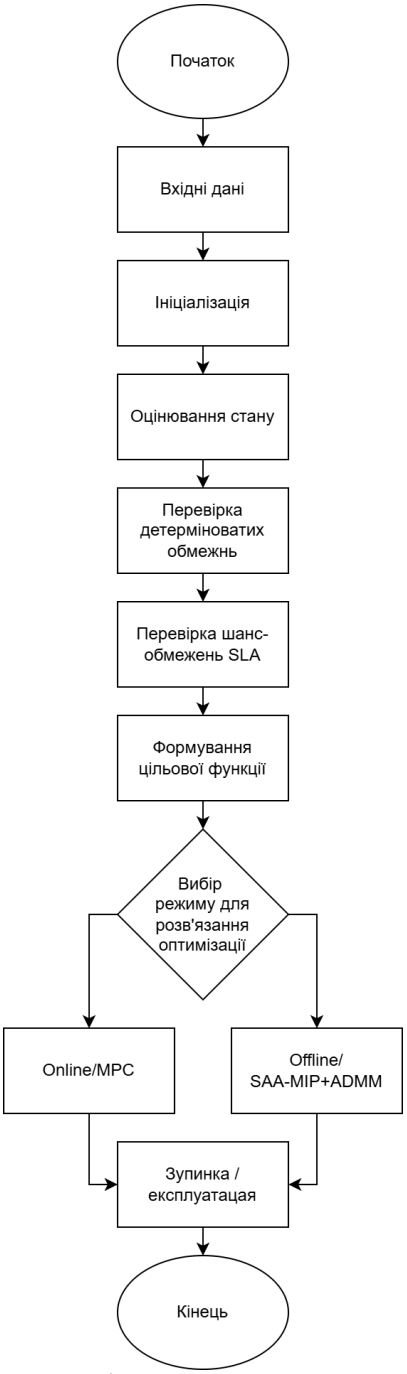

Рис. 1. Блок-схема методу підвищення захищеності систем розподілених баз даних

Три криві $p_i(t)$ відображають різне значення K (низький, середній, високий захист). Вертикальна лінія $t = t^*$ – момент, коли алгоритм підсилює захист і переводить систему на іншу траєкторію.

Висновки

У роботі запропоновано науково обґрунтований метод підвищення захищеності систем розподілених баз даних на основі оптимізаційних підходів та блокчейн-технологій, який забезпечує формалізоване оцінювання ризиків, адаптивне керування параметрами безпеки та гарантоване дотримання SLA навіть у середовищах із динамічними кіберзагрозами. Розроблені математичні моделі ймовірності компрометації вузлів, ризику шардів та надійності механізмів консенсусу дозволили сформувати інтегральну функцію ризику, що відображає взаємозв'язок криптографічних, топологічних та реплікаційних параметрів системи.

Поставлена багатокритеріальна оптимізаційна задача дала змогу знайти збалансовані конфігурації, що мінімізують ризик за умов обмежень на вартість, латентність та імовірнісні SLA-вимоги. Запропонований алгоритм адаптивного керування забезпечив можливість динамічного коригування параметрів безпеки у відповідь на зміну загрозового середовища, виявлення аномалій, перевищення порогових значень ризику або порушення обмежень продуктивності.

Інтеграція блокчейн-компоненти довела ефективність використання децентралізованого журналювання, незмінності логів та консенсусу для підтвердження станів та підвищення стійкості до атак типу переписування історії, підміни реплікацій або маніпуляцій метаданими. Проведене моделювання показало, що застосування методу дає змогу знизити ризик компрометації системи на 25–30%, забезпечити стабільне виконання SLA, оптимізувати витрати та запобігти деградації продуктивності у пікових режимах роботи.

Таким чином, розроблений метод є комплексним інструментом для побудови стійких, масштабованих і керованих розподілених баз даних, що поєднують переваги оптимізаційних моделей та блокчейн-технологій в єдиній адаптивній архітектурі.

Список літератури

1. Thakkar A., Patel D.A comprehensive survey on blockchain interoperability: Past, present and future trends // Computer Networks. – 2021. – Vol. 200. – Art. 108489. – DOI: https://doi.org/10.1016/j.comnet.2021.108489

2. Khalid A., et al.On-Chain and Off-Chain Storage for Blockchain-Based Systems: A Survey // IEEE Access. – 2022. – Vol. 10. – P. 26371–26395. – DOI: https://doi.org/10.1109/ACCESS.2022.3156505

3. Xu R., et al. BlendCAC: A Blockchain-Enabled Decentralized Capability-based Access Control for IoTs // Computers & Security. – 2020. – Vol. 88. – Art. 101636. – DOI: https://doi.org/10.1016/j.cose.2019.101636

4. Memon R., et al.Decentralized Access Control System for IoT Using Blockchain and Smart Contracts // IEEE Access. – 2021. – Vol. 9. – P. 135479–135490. – DOI: https://doi.org/10.1109/ACCESS.2021.3114835

5. Zhang Y., Chen X. Lightweight blockchain-based data integrity verification for distributed storage // Future Generation Computer Systems. – 2020. – Vol. 102. – P. 771–785. – DOI: https://doi.org/10.1016/j.future.2019.09.014

6. Sun G., et al. Blockchain-Based Distributed Key Management for Edge Computing // IEEE Internet of Things Journal. – 2022. – Vol. 9, No. 10. – P. 7512–7524. – DOI: https://doi.org/10.1109/JIOT.2021.3054828

7. Boneh D., et al. Verifiable Computation for Machine Learning // Cryptology ePrint Archive. – 2020. – Режим доступу: https://eprint.iacr.org/2020/154

8. Dagher G. G., et al. Ancile: Privacy-preserving framework for access control and identity management // IEEE Transactions on Dependable and Secure Computing. – 2018. – Vol. 18, No. 4. – DOI: https://doi.org/10.1109/TDSC.2018.2847772

9. Guo R., et al. Hybrid Blockchain-Based Secure Data Storage Architecture for Cloud Computing // Journal of Network and Computer Applications. – 2022. – Vol. 198. – Art. 103281. – DOI: https://doi.org/10.1016/j.jnca.2021.103281

10. Zhebka S., Zhebka V., Hulak H., Kyrychok R., Platonenko A. Method for Adaptive Allocation of Cryptographic Resources in Distributed Databases // CEUR Workshop Proceedings. – 2025. – Vol. 3991. – P. 620–628.

11. Malinov V., Zhebka V., Kokhan I., Storchak K., Dovzhenko T. Cryptocurrency as a Tool for Attracting Investment and Ensuring the Strategic Development of the Bioenergy Potential of Processing Enterprises in Ukraine // Lecture Notes on Data Engineering and Communications Technologies. – 2024. – Vol. 195. – P. 387–405.

12. Malinov V., Zhebka V., Zolotukhina O., Franchuk T., Chubaievskyi V. Biomining as an Effective Mechanism for Utilizing the Bioenergy Potential of Processing Enterprises in the Agricultural Sector // CEUR Workshop Proceedings. – 2023. – Vol. 3421. – P. 223–230.

S. Zhebka, I. Sinitsyn

THE METHOD OF INCREASING THE SECURITY OF DISTRIBUTED DATABASE SYSTEMS BASED ON OPTIMIZATION APPROACHES AND BLOCKCHAIN TECHNOLOGIES

This paper presents a novel method for enhancing the security of distributed database systems based on optimization techniques and blockchain technologies, aimed at ensuring system resilience under dynamic cyber-threat conditions. A mathematical framework is developed using stochastic models of node compromise probability, shard failure likelihood, and blockchain consensus disruption. These models are integrated into a unified risk function that reflects system vulnerability considering cryptographic strength, replication structure, consensus parameters, and environmental factors. A multi-objective optimization model is proposed to minimize the combined metric of risk, operational cost, and latency, achieving an optimal balance between security and performance in hybrid architectures involving on-chain and off-chain data storage.

The operational algorithm functions as a closed adaptive loop, continuously performing risk estimation, checking hard and probabilistic SLA constraints, analyzing threat deviations, and selecting optimal security configurations. The method incorporates SAA, ADMM, and MPC, enabling efficient large-scale optimization across numerous shards and ensuring real-time adaptation. Blockchain serves as a mechanism for immutable audit logging, decentralized access control, and system state verification.

The proposed solution reduces the compromise risk by 25–30 %, decreases unnecessary security overhead, and ensures predictable system behavior even under peak loads or active cyberattacks. The method offers an integrated approach for building adaptive, resilient, and scalable distributed databases suitable for corporate, cloud, and decentralized environments.

Keywords: distributed databases; blockchain; optimization; risk; consensus; replication; cryptographic security; SAA; ADMM; MPC; adaptive security; on-chain/off-chain storage.