DOI 10.31891/2307-5732-2024-331-47
УДК 004.65.056.53(045)

САЛІЄВА ОЛЬГА
Вінницький національний технічний університет
https://orcid.org/0000-0003-2388-7321
e-mail: salieva8257@gmail.com
ГРИЦАК АНАТОЛІЙ
Вінницький національний технічний університет
https://orcid.org/0000-0002-0776-9889
e-mail: grytsak.a.v@gmail.com
БІЛОУС ВІТАЛІЙ
Вінницький національний технічний університет
https://orcid.org/0009-0001-2350-1583
e-mail: vitalii.bilous@vntu.edu.ua
ІВАНЮК ТАРАС
Вінницький національний технічний університет
e-mail: ivanuk-taras@ukr.net

УДОСКОНАЛЕННЯ СИСТЕМИ ЗАХИСТУ БАЗ ДАНИХ ВІД НЕСАНКЦІОНОВАНОЇ МОДИФІКАЦІЇ НА ОСНОВІ ТЕХНОЛОГІЙ БЛОКЧЕЙН ТА АЛГОРИТМУ КОНСЕНСУСУ PROOF-OF-WORK

У сучасному цифровому світі спостерігається активне використання баз даних, актуальність захисту яких зростає з кожним днем. Адже бази даних можуть містити широкий спектр конфіденційної інформації (персональної, фінансової, державної, комерційної та ін.), неправомірний доступ до якої призведе до незворотних негативних наслідків, включаючи матеріальні збитки, репутаційні втрати та навіть юридичні проблеми. Крім того, з кожним днем зростає кількість та складність кібератак. Зловмисники застосовують різні методи для отримання несанкціонованого доступу до баз даних, наприклад, такі як використання: вразливостей програмного забезпечення, методів соціальної інженерії, атаки грубої сили і т. п. Тому важливе місце посідає проблема підвищення захищеності баз даних від несанкціонованої модифікації. У зв'язку із цим, у роботі пропонується вирішення даного питання шляхом використання технології блокчейн в поєднанні з алгоритмом консенсусу Proof-Of-Work, що забезпечує безпеку та цілісність системи, а також допомагає запобігти шахрайству та зловживанням за рахунок застосування криптографічних методів для захисту блокчейна від несанкціонованого доступу та змін. Також варто зазначити, що алгоритм Proof-of-Work має ряд й інших переваг, зокрема, таких як: децентралізація, прозорість, незмінність даних після їх додавання. Таким чином, для досягнення мети було проаналізовано предметну область, досліджено відомі методи на яких базується робота систем захисту баз даних, створено архітектуру та алгоритм роботи модулю захисту, що надає змогу децентралізовано зберігати дані та, відповідно, підвищити рівень їх захищеності за рахунок використання спеціального протоколу консенсусу для узгодження вмісту реєстру, а також криптографічних алгоритмів хешування та електронних цифрових підписів для забезпечення цілісності транзакції передачі параметрів.

Ключові слова: база даних, технологія блокчейн, алгоритм консенсусу, Proof-of-work, криптографічний алгоритм хешування, цифровий підпис.

SALIIEVA OLHA, HRYTSAK ANATOLIY, BILOUS VITALII, IVANIUK TARAS
Vinnytsia National Technical University

IMPROVEMENT OF DATABASE PROTECTION SYSTEM FROM UNAUTHORIZED MODIFICATION BASED ON BLOCKCHAIN TECHNOLOGY AND PROOF-OF-WORK CONSENSUS ALGORITHM

In today's digital world, there is an active use of databases, and the relevance of protecting them is growing every day. After all, databases can contain a wide range of confidential information (personal, financial, government, commercial, etc.), unauthorized access to which will lead to irreversible negative consequences, including material damage, reputational losses, and even legal problems. In addition, the number and complexity of cyberattacks is growing every day. Attackers use various methods to gain unauthorized access to databases, such as the use of software vulnerabilities, social engineering methods, brute force attacks, etc. Therefore, the problem of increasing the security of databases against unauthorized modification is of great importance. In this regard, this paper proposes to address this issue by using blockchain technology in combination with the Proof-Of-Work consensus algorithm, which ensures the security and integrity of the system, and helps prevent fraud and abuse by using cryptographic methods to protect the blockchain from unauthorized access and modification. It is also worth noting that the Proof-of-Work algorithm has a number of other advantages, such as decentralization, transparency, and data immutability after it is added. Thus, to achieve the goal, the subject area was analyzed, the known methods on which the operation of database security systems is based were investigated, the architecture and algorithm of the security module were created, which allows for decentralized data storage and, accordingly, increases the level of their security by using a special consensus protocol to coordinate the contents of the registry, as well as cryptographic hashing algorithms and electronic digital signatures to ensure the integrity of the parameter transfer transaction.

Keywords: database, blockchain technology, consensus algorithm, Proof-of-work, cryptographic hashing algorithm, digital signature.

Вступ

Постановка задачі. На цей день бази даних (БД) є одним з найважливіших ресурсів для будь-якої сфери суспільної діяльності. Вони зумовили необхідність вдосконалення їхнього захисту. Адже з кожним роком зростає не тільки кількість БД, але й збільшується кількість нових кіберзагроз та вразливостей БД до атак.

Для підвищення захищеності БД використовують різні методи, зокрема [1]:

– вбудовані засоби контролю даних;
– забезпечення цілісності зв'язків таблиць;
– організація спільного використання об'єктів БД в мережі;
– захист паролем;
– шифрування;
– розділення прав доступу до об'єктів БД;
– захист полів і записів таблиць БД.

Проте зазначені методи не вирішують повною мірою проблему неправомірної модифікації даних, що зберігаються у БД. Тому варто звернути увагу на можливість застосування в системі захисту БД технологій Blockchain у поєднанні із Proof-of-work (PoW), що сприятиме підвищенню рівня захищеності БД за рахунок створення децентралізованого реєстру взаємодій з базою даних, інформація якого зберігається як на сервері, так і на вузлах мережі блокчейну.

Для досягнення поставленої мети необхідно провести аналіз предметної області; дослідити відомі методи на яких базується робота систем захисту БД; розробити покращений алгоритм роботи модуля захисту БД; здійснити програмну реалізацію блокчейну та алгоритму консенсусу Proof-of-Work; провести тестування розробленого модуля захисту БД, оцінити його ефективність.

Аналіз основних публікацій

З кожним роком спостерігається все більш швидке зростання ризиків безпеки БД. Це пов'язано з розвитком інформаційних технологій, появою нових способів атак та збільшенням обсягу даних, які зберігаються в БД. Тому даній тематиці присвячено багато робіт. Так, у роботі [2] автор систематизував загрози і вразливості характерні для БД. У роботі [3] надається короткий огляд вразливостей, пропонується певний набір правил і дій, які можуть знизити ризики, пов'язані з порушенням конфіденційності, доступності та цілісності даних. Автори праці [4] у своїй публікації особливу увагу приділяють основам управління безпекою БД та технологіям, які підтримують її впровадження. У [5] розглянуто різні способи розширення ланцюга аутентифікації користувача БД. У свою чергу, в роботі [6] проблема захисту БД розглянута з точки зору безпеки розроблених додатків, підключених до БД. У цій статті описано 20 різновидів загроз безпеці БД, які створюються через веб-сайти та обговорено можливі засоби їх усунення. Дослідженню різноманітних загроз захищеності БД і технологій забезпечення безпеки БД присвячено роботу [7].

Виділення невирішених раніше частин загальної проблеми

Система захисту БД – це комплекс заходів (фізичних, адміністративних, технологічних), які спрямовані на запобігання несанкціонованому доступу, використанню, розголошенню або модифікації даних. Найпоширенішими системами захисту БД є Acra-database-protection-suite [8], Imperva Secure Sphere Data Security [9], McAfee Vulnerability Manager for Databases [10], які надають послуги щодо захисту БД із централізованим типом зберігання даних, проте не забезпечують захищеності від несанкціонованої модифікації особами, які мають безпосередній доступ до взаємодії з БД. Тому у роботі пропонується вирішити дану проблему за рахунок поєднання технологій Blockchain та PoW, механізм роботи яких гарантує, що розподілені реєстри є точними копіями, і це в свою чергу знижує ризик зміни інформації в БД та забезпечує підвищення її захищеності від несанкціонованої модифікації. Крім того, для забезпечення цілісності транзакції передачі параметрів застосовуватиметься криптографічний алгоритм хешування SHA256 та електронний цифровий підпис.

Формулювання цілі статті. Метою дослідження є удосконалення системи захисту БД від несанкціонованої модифікації на основі технології блокчейн та алгоритму консенсусу PoW.

Основна частина

Вдосконалення системи захисту БД від несанкціонованої модифікації

Розробимо децентралізовану однорангову блокчейн-мережу, яка позбавлятиме окремих учасників чи груп учасників можливості контролювати базову інфраструктуру та дестабілізувати роботу системи. Усі учасники мережі (фізичні особи, державні структури, організації і т. п.) матимуть рівні права та підключатимуться до неї за одними й тими же протоколами. По суті, запропонована система захисту БД записуватиме хронологічний порядок проведення транзакцій з усіма вузлами мережі, що визнали дійсність транзакцій за допомогою обраної моделі консенсусу. У результаті отримаємо транзакції, що не підлягають відміні та децентралізовано узгоджені всіма учасниками мережі.

Вузли запропонованої блокчейн-мережі використовують спеціальний протокол консенсусу PoW для узгодження вмісту реєстру. Криптографічний алгоритми хешування SHA256 гарантує, що будь-яка зміна вхідних даних транзакції, навіть незначна, приведе до появи іншого значення хешу в результатах розрахунків, що вказує на ймовірність компрометації вхідних даних транзакції. Використання електронного цифрового підпису надасть гарантію того, що транзакції здійснюються легітимними відправниками

На основі використання вищезазначених технологій, розробимо модуль захисту БД, який повинен взаємодіяти з будь-якими змінами в БД та своєчасно передавати вхідні дані.

Модуль реалізуємо у вигляді серверної та клієнтської частин. Серверна частина модулю захисту представляє собою програмний продукт, який складається з шести блоків: криптографічного блоку, блоку взаємодії з БД, блоку взаємодії з вузлами мережі блокчейн, блок вирішення проблем при отримані результатів

клієнтських обчислень, блок консенсусу (PoW). Архітектуру розробленого модулю захисту БД відображено на рис. 1.

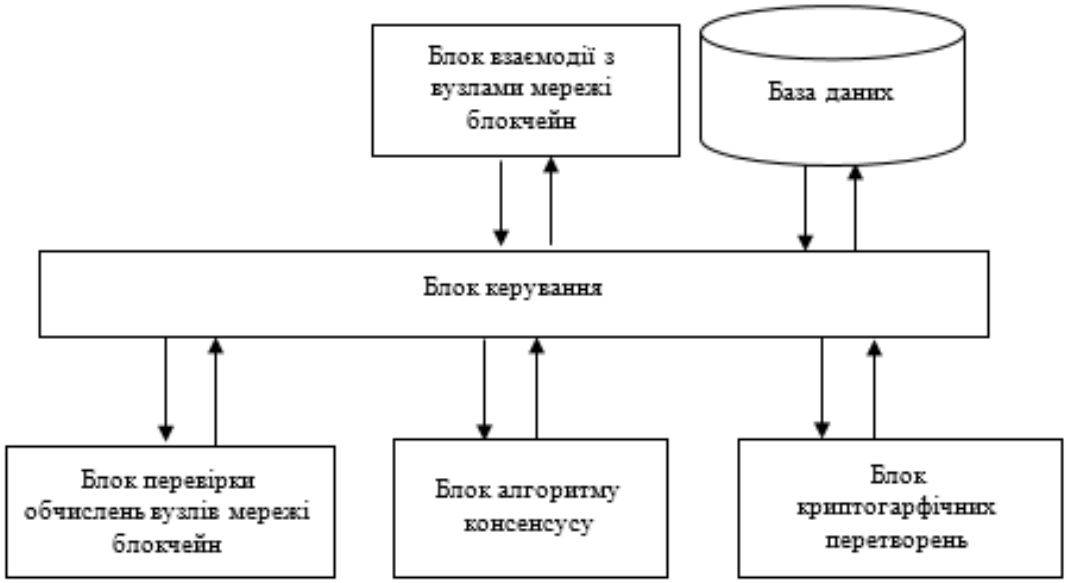

Рис. 1. Алгоритм роботи серверної частини модулю захисту

Криптографічний блок представляє собою функцію, яка спрямована на перетворення вхідних даних, а саме: хешу БД, часової мітки, хешу попереднього блоку в наступний блок. Результат роботи криптографічного блоку передається на клієнтську частину для оброблення за вибраним алгоритмом консенсусу Proof-Of-Work.

Блок взаємодії з БД являє собою функцію, яка реагує на кожне нове підключення. Оскільки підключення відбувається лише тоді, коли йде допис у БД, то блок отримує нове значення хешу БД, і відправляє його у криптографічний блок.

Блок взаємодії з вузлами мережі блокчейн створений для взаємодії серверної частини з децентралізованими вузлами, для обробки та створення блоків. Даний блок отримує інформацію для обробки за допомогою обраного алгоритму консенсусу Proof-Of-Work та відправляє її на сервер для додавання у блокчейн. Також вузол мережі зберігає на своїй стороні актуальну версію блокчейну.

Оскільки клієнтська частина може застосовуватись на засобах з різними обчислювальними потужностями, то виникає проблема у знаходженні єдиного правильного варіанту обчислення алгоритму консенсусу для блока. Розв’язанню даного питання сприяє блок вирішення проблем при отриманні даних від децентралізованих вузлів блокчейну.

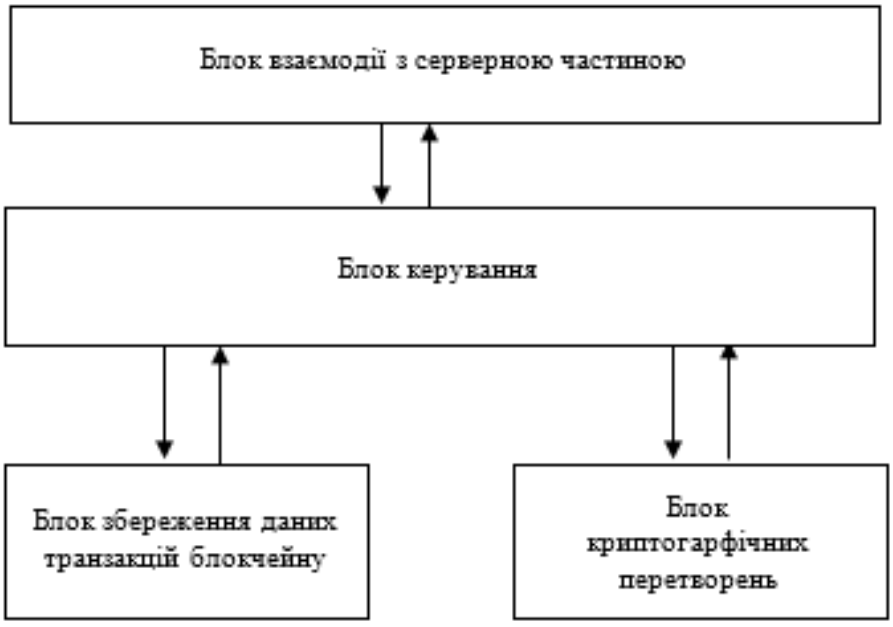

Рис. 2. Алгоритм роботи клієнтського модулю захисту

Блок консенсусу реалізований для підтвердження достеменності результатів обробки блоків клієнтами децентралізованої мережі блокчейн.

У свою чергу, клієнтська частина модулю захисту складається з блоків керування, криптографічних перетворень за обраним алгоритмом консенсусу, блоку взаємодії з серверною частиною, блоку збереження кожної транзакції у вузлі блокчейну (рис. 2).

Структура блоку криптографічних перетворень на клієнтській частині аналогічна відповідному блоку на серверній частині.

Блок взаємодії з серверною частиною відповідає за обмін інформацією та отримання нових значень для обробки і відправки на сервер для утворення блокчейну.

Блок збереження даних транзакцій блокчейну відповідає за збереження блоків, послідовність яких і створює блокчейн.

Розробка алгоритму роботи підсистеми методу захисту БД від несанкціонованих модифікацій.

Модуль захисту БД реалізовано для забезпечення децентралізованого збереження даних, завдяки чому підвищується захищеність БД, адже метадані та хеш суми внесених даних у інформаційно-комунікаційну систему зберігаються на вузлах мережі блокчейну.

Робота модулю захисту БД складається з наступних кроків (рис. 3).

Крок 1. Інформаційно-комунікаційна система відслідковує дію користувача і вносить дані у БД.

Крок 2. Модуль захисту реагує на звернення інформаційно-комунікаційної системи на створення запису у БД.

Крок 3. Модуль захисту ініціалізує створення нового блоку, який має:

– індекс новоствореного блоку шляхом збільшення значення довжини блокчейну на одиницю. Використання даного параметру вирішує проблему сумісності результатів обробки блоків на вузлах з різною швидкодією обчислювальних засобів;

– значення часової мітки, застосування якої визначає час, коли модуль захисту ініціалізував створення блоку з точністю до хвилини;

– хеш-суму введених даних, яка забезпечує швидкодію у перевірці запису у БД інформаційно-комунікаційної системи на цілісність та відповідність даних введених користувачем;

– ініціалізацію перемінної для взаємодії з вузлами мережі.

Крок 3.1. Генерація значення консенсусу $proof$ за обраним алгоритмом Proof-of-Work. Даний параметр буде відправлено для обчислення на вузли мережі, і він є доказом виконаної роботи.

Крок 3.2. Отримання хеш-суми попереднього блоку $previous\_hash$, що гарантує незмінність блоків.

Крок 4. Вузол мережі блокчейну отримує транзакцію, зчитуючи структуру блоку і його параметри.

Крок 4.1. Вузол мережі блокчейну ініціалізує застосування алгоритму консенсусу Proof-of-Work, та після необхідних криптографічних перетворень отримує значення параметру блоку $proof$ і оновлює даний параметр.

Крок 4.2. Вузол мережі блокчейну, на якому було виконано обчислення блоку, зберігає локальну копію блоку, до якого, за необхідністю, можливо звернутись для перевірки цілісності.

Крок 4.3. Вузол мережі блокчейну відправляє оновлений блок на сервер.

Крок 5. Серверна частина модулю захисту отримує результати обчислень блоків вузлами мережі.

Крок 5.1. При отриманні блоку серверна частина перевіряє параметр блоку $index$.

У разі, якщо значення параметру $index$ відповідає значенню довжині блокчейну, або є меншим, то блок вважається не актуальним і не вноситься у блокчейн, виконується повернення до кроку 5.

Якщо значення параметру $index$ більше за довжину блокчейну на одиницю, то даний блок вважається актуальним, виконується перехід до кроку 5.2.

Крок 5.2. Серверна частина модулю зчитує значення параметру $proof$ та обчислює його правильність.

Якщо отриманий результат підтверджує правильність виконаної роботи, то відбувається перехід до кроку 6. В іншому випадку даний блок відкидається і виконується повернення до кроку 5.

Крок 6. Отриманий блок одержує підтверджений статус за обраним алгоритмом консенсусу Proof-of-Work та алгоритмом вирішення проблеми сумісності результатів обчислень блоків мережі блокчейну.

Крок 6.1. Серверна частина модулю захисту вносить блок до блокчейну, тим самим збільшує його довжину на 1.

Крок 6.2. Серверна частина модулю захисту записує блокчейн у БД модулю захисту.

Після розробки усіх необхідних алгоритмів, здійснено програмну реалізацію блокчейну та алгоритму консенсусу Proof-of-Work, на основі яких протестовано розроблений модуль захисту БД (рис. 4). При цьому було використано бібліотеку для автоматичного тестування unittest та концепцію test case.

Test case – блок тестування, який валідує відповіді на різні набори вхідних даних. Модуль unittest надає базовий клас TestCase, який застосовується для створення нових тестових ітерацій даних, які будуть надіслані функціям для перевірки варіативності та рівня обробки вхідних даних функцій і можливих помилок при роботі модулю захисту [11].

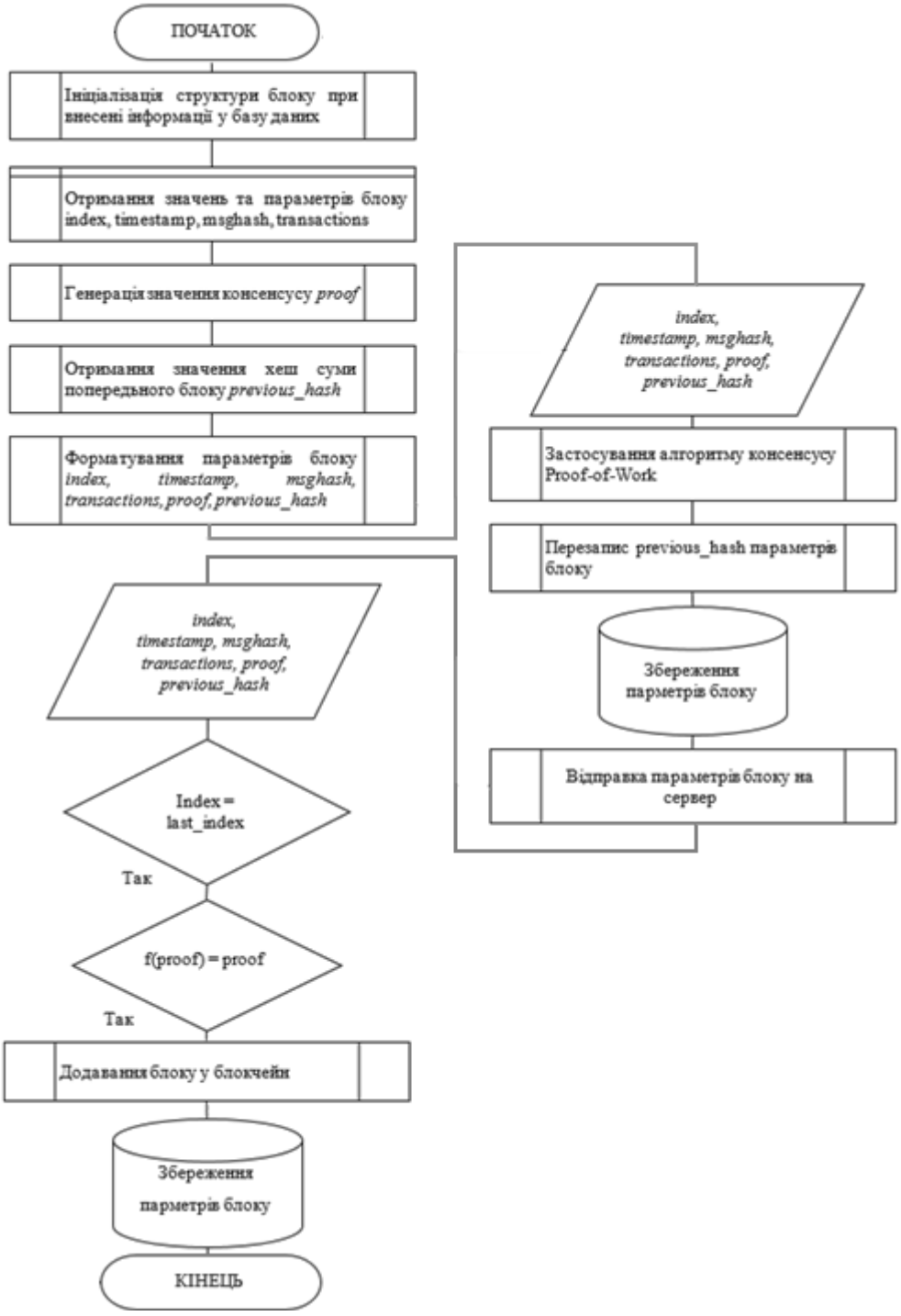

Рис. 3. Узагальнений алгоритм модулю захисту

```
Process finished with exit code 0
Test 4 successfully passed
---------------
Test 3 successfully passed


Ran 4 tests in 5.014s
OK
---------------
Test 1 successfully passed
---------------
Test 2 successfully passed
---------------
```

Рис. 4. Результат тестування обраних функцій модулю захисту

Отриманий результат тестування свідчить про достатній рівень обробки помилок реалізованих функцій модулю захисту.

Порівняльний аналіз розробленої підсистеми захисту БД з існуючими аналогами.

Системи керування БД є складними, вони створюють власний набір ризиків безпеки, деякі з яких подібні до іншого системного програмного забезпечення (наприклад, оновлення, виправлення, надійність пароля тощо), а деякі з них є унікальними для БД (наприклад, загрози від ін'єкції SQL, або експлойти переповнення буфера).

Використовуючи розроблений алгоритм підсистеми захисту БД та існуючі аналоги, виконаємо порівняльний аналіз щодо обраних ознак (табл. 1)

Таблиця 1

Порівняльний аналіз розробленої підсистеми захисту з існуючими аналогами

Система захисту	**Неправомірна модифікація з безпосереднім доступом до БД**	**Шифрування**	**SQL ін'єкція**	**Переповнення буферу обміну**	**Запобігання несанкціонованому доступу до БД із зовнішнього середовища**	**Запобігання несанкціонованій модифікації**
Acra-database-protection-suite [8]					✓	
Imperva SecureSphere Data Security [9]					✓	
McAfee Vulnerability Manager for Databases [10]			✓	✓	✓	
Розроблена підсистема захисту БД	✓	✓			✓	✓

Провівши аналіз існуючих систем та засобів захисту БД наведених у табл. 1 можна зробити висновок, що розроблена підсистема надає послуги щодо захисту БД із децентралізованим типом зберігання даних, виконує їх шифрування та має ряд переваг над існуючими аналогами.

Обговорення результатів та перспективи подальшого розвитку досліджень.

Отримані результати свідчать, що за рахунок використання в системі захисту БД технологій Blockchain у поєднанні із Proof-of-work підвищується захищеність системи захисту БД від несанкціонованої модифікації. Також це відбувається і за рахунок використання криптографічного алгоритму хешування SHA256 та електронного цифрового підпису. Проте подальших досліджень потребує пошук нових шляхів виявлення та запобігання вторгненням в БД інформаційних систем. Зокрема, варто звернути увагу на застосування штучного інтелекту для аналізу поведінки користувачів та виявлення аномалій, що сприятиме вчасному виявленню та нейтралізації загроз модифікації даних.

Висновки

У даній роботі було проведено аналіз стану щодо інформаційної безпеки БД, основних її загроз та вразливостей. Визначено базові методи захисту БД, їх недоліки. Запропоновано усунути дані недоліки шляхом удосконалення системи захисту БД від несанкціонованої модифікації на основі технології блокчейн та алгоритму консенсусу PoW. Застосування блокчейну забезпечило підвищення рівня захищеності БД за рахунок створення децентралізованого реєстру взаємодій з БД, інформація якого зберігається як на сервері, так і на вузлах мережі блокчейну. Дані вузли використовують спеціальний протокол консенсусу Proof-of- work для узгодження вмісту реєстру, а також криптографічні алгоритми хешування та електронно-цифрові підписи для забезпечення цілісності транзакції передавання параметрів.

Для забезпечення захисту БД розроблено програмний засіб у вигляді модулю, інтеграція якого включає попередньо визначені інструменти та методи для взаємодії з існуючими середовищами додатків. Крім того, модуль захисту БД взаємодіє з будь-якими змінами в БД та своєчасно передає вхідні дані.

Використовуючи бібліотеки для автоматичного тестування unittest та концепції test case, було проведено тестування обраних функцій модулю захисту та отримано позитивні результати. Також було здійснено порівняльний аналіз розробленої підсистеми захисту з існуючими аналогами та продемонстровано її переваги.

Література

1. Касянчук Н. В., Ткачук Л. М. Захист інформації в базах даних. URL: https://conferences.vntu.edu.ua/index.php/all-fm/all-fm-2019/paper/download/ 7001/5715. 2019

2. Вілігура В. В. Систематизація загроз і вразливостей характерних для баз даних і СУБД. Праці 7-ї Міжнародної конференції «Комп'ютерне моделювання в наукоємних технологіях» (КМНТ-2021), 21-23 квітня 2021 р. Харків: Харк. нац. ун-т імені В. Н. Каразіна, 2021. С. 83-86.

3. Пєвнєв В. Я. Безпека баз даних: загрози та превентивні заходи. Сучасні інформаційні системи, Т. 2, № 1, с. 69-72, 2018, doi: https://doi.org/10.20998/2522-9052.2018.1.13

4. Paul P., Aithal P. S. Database Security: An Overview and Analysis of Current Trend. International Journal of Management, Technology, and Social Sciences (IJMTS), Vol. 4, no. 2, pp. 53-58, 2019, doi: https://dx.doi.org/10.2139/ssrn.3497728

5. Mousa A., Karabatak M., Mustafa T. Database Security Threats and Challenges. in Proc. 8th International Symposium on Digital Forensics and Security (ISDFS), Remote. Online, 2020, pp. 1-5, doi: https://doi.org/10.1109/ISDFS49300.2020.9116436

6. Teimoor R. A. A Review of Database Security Concepts, Risks, and Problems. UHD Journal of Science and Technology, Vol. 5, no. 2, pp. 38-46, 2021, doi: https://doi.org/10. 21928/uhdjst, 2021. pp. 38-46.

7. Swati J., Dimple Ch. A Relative Study on Different Database Security Threats and their Security Techniques. International Journal of Innovative Science and Research Technology, Vol. 5, no. 1, pp. 794-799, 2020, doi: http://dx.doi.org/10.13140/RG.2.2.11657.60000

8. Acra – єдине рішення для захисту життєвого циклу даних. URL: https://kz.iitd.com.ua/wp-content/uploads/2020/03/acra-feature-presentation-q3-ua-iitd.pdf

9. Imperva SecureSphere Data Security. URL: https://www.imperva.com/resources/datasheets/DS_SecureSphere_Data-Security.pdf

10. McAfee Vulnerability Manager for Databases. URL: https://www.mcafee.com/enterprise/ru-ru/assets/data-sheets/ds-vulnerability-manager-for-databases.pdf

11. Unit testing framework System. URL: https://docs.python.org/3/library/unittest.html

References

1. Kasianchuk N. V., Tkachuk L. M. Zakhyst informatsii v bazakh danykh. URL: https://conferences.vntu.edu.ua/index.php/all-fm/all-fm-2019/paper/download/ 7001/5715. 2019

2. Vilihura V. V. Systematyzatsiia zahroz i vrazlyvostei kharakternykh dlia baz danykh i SUBD. Pratsi 7-yi Mizhnarodnoi konferentsii «Kompiuterne modeliuvannia v naukoiemnykh tekhnolohiiakh» (KMNT-2021), 21-23 kvitnia 2021 r. Kharkiv: Khark. nats. un-t imeni V. N. Karazina, 2021. S. 83-86.

3. Pievniev V. Ya. Bezpeka baz danykh: zahrozy ta preventyvni zakhody. Suchasni informatsiini systemy, T. 2, № 1, c. 69-72, 2018, doi: https://doi.org/10.20998/2522-9052.2018.1.13

4. Paul P., Aithal P. S. Database Security: An Overview and Analysis of Current Trend. International Journal of Management, Technology, and Social Sciences (IJMTS), Vol. 4, no. 2, rr. 53-58, 2019, doi: https://dx.doi.org/10.2139/ssrn.3497728

5. Mousa A., Karabatak M., Mustafa T. Database Security Threats and Challenges. in Proc. 8th International Symposium on Digital Forensics and Security (ISDFS), Remote. Online, 2020, pp. 1-5, doi: https://doi.org/10.1109/ISDFS49300.2020.9116436

6. Teimoor R. A. A Review of Database Security Concepts, Risks, and Problems. UHD Journal of Science and Technology, Vol. 5, no. 2, pp. 38-46, 2021, doi: https://doi.org/10. 21928/uhdjst, 2021. pp. 38-46.

7. Swati J., Dimple Ch. A Relative Study on Different Database Security Threats and their Security Techniques. International Journal of Innovative Science and Research Technology, Vol. 5, no. 1, pp. 794-799, 2020, doi: http://dx.doi.org/10.13140/RG.2.2.11657.60000

8. Acra – yedyne rishennia dlia zakhystu zhyttievoho tsyklu danykh. URL: https://kz.iitd.com.ua/wp-content/uploads/2020/03/acra-feature-presentation-q3-ua-iitd.pdf

9. Imperva SecureSphere Data Security. URL: https://www.imperva.com/resources/datasheets/DS_SecureSphere_Data-Security.pdf

10. McAfee Vulnerability Manager for Databases. URL: https://www.mcafee.com/enterprise/ru-ru/assets/data-sheets/ds-vulnerability-manager-for-databases.pdf

11. Unit testing framework System. URL: https://docs.python.org/3/library/unittest.html