for the development of the improvement of settlements that would be suitable for all countries, in particular for Ukraine.

That is why the implementation of one or another model for the improvement of settlements will have negative consequences for the cities of Ukraine. Therefore, in our opinion, it is necessary to change the attitude and adapt the foreign to the public administration in the area of improvement of settlements. This would be a great incentive for Ukraine to take appropriate measures on the way to development and prosperity.

Валерія БАЛАЦЬКА
викладач кафедри управління
інформаційною безпекою
Львівського державного університету
безпеки життєдіяльності,
аспірант кафедри захисту інформації
Національного університету
«Львівська політехніка»
https://orcid.org/0000-0002-6262-6792

Василь ПОБЕРЕЖНИК
аспірант кафедри захисту інформації
Національного університету
«Львівська політехніка»,
(м. Львів, Україна)

ІНФОРМАЦІЙНА БЕЗПЕКА ДЕРЖАВНИХ РЕЄСТРІВ: ПОТЕНЦІАЛ БЛОКЧЕЙНУ ДЛЯ ЗАХИСТУ КРИТИЧНО ВАЖЛИВИХ ДАНИХ

Цифровізація державного управління потребує надійних механізмів забезпечення інформаційної безпеки, оскільки державні реєстри містять критично важливі дані, що впливають на функціонування суспільних інституцій. Традиційні централізовані моделі управління інформацією виявляють значні недоліки, пов'язані з їхньою вразливістю до зовнішніх атак, технічних збоїв та внутрішніх маніпуляцій. Відомі випадки кібератак на державні інформаційні системи вказують на те, що централізовані підходи до зберігання даних створюють ризики компрометації персональної інформації та порушення цілісності реєстраційних записів [1].

Проблема забезпечення захисту державних реєстрів ускладнюється відсутністю прозорих механізмів контролю внесення змін. Коригування записів часто залишається без належного аудиту, що унеможливлює відстеження несанкціонованих змін і підриває довіру до офіційних баз даних [2]. Також значним викликом є людський фактор: некоректне внесення інформації або навмисне зловживання доступом до реєстрів призводить до юридичних та економічних наслідків.

У такому контексті блокчейн-технологія постає як перспективний інструмент забезпечення достовірності даних у державних інформаційних системах [3]. Завдяки децентралізованій природі, механізму незмінності записів і прозорому алгоритму верифікації транзакцій, блокчейн може суттєво підвищити рівень інформаційної безпеки державних реєстрів та мінімізувати ризики маніпуляцій.

Постановка проблеми. Функціонування державних реєстрів передбачає систематичне внесення, оновлення та зберігання інформації, що має юридичну значущість. У традиційних централізованих системах дані зберігаються в єдиному інформаційному центрі, що робить їх уразливими до цілеспрямованих атак або технічних збоїв [4]. Будь-які зміни в централізованій базі можуть бути внесені без належної процедури аудиту, що підвищує ризики внутрішніх загроз.

Однією з ключових проблем є обмеженість механізмів верифікації коректності внесених записів. Процедури перевірки інформації часто залежать від людського фактору, що створює додаткові можливості для помилок або навмисного спотворення даних. Зокрема, уразливість реєстраційних систем до несанкціонованих змін може призвести до юридичних маніпуляцій, таких як незаконна перереєстрація власності чи підробка особистих даних громадян.

Відсутність надійного механізму контролю за змінами у державних реєстрах також сприяє корупційним схемам. У деяких випадках інформація може змінюватися без належного підтвердження автентичності змін, що підриває легітимність державних інформаційних систем [5].

У зв'язку з цим актуальним є пошук технологічного рішення, яке б забезпечило контрольованість внесення змін до державних реєстрів, прозорість операцій та підвищений рівень безпеки даних.

Блокчейн є перспективною технологією для підвищення інформаційної безпеки державних реєстрів. Основні переваги цієї технології:

- Незмінність записів. Усі операції записуються у вигляді ланцюга блоків, що унеможливлює їхнє зворотне редагування без узгодження всієї мережі.
- Прозорість операцій. Всі зміни можна відстежити, що унеможливлює приховані маніпуляції.
- Криптографічний захист. Кожен запис має унікальний криптографічний хеш, а будь-яка спроба змінити хоча б один запис призводить до розбалансування всієї системи.

Запровадження блокчейн дозволяє мінімізувати ризики компрометації та створити механізм відкритого контролю над даними.

Методологія інтеграції блокчейн-технологій у державні реєстри. Запропонований метод інтеграції блокчейн-технологій у державні реєстри базується на принципах децентралізованого зберігання, криптографічного контролю достовірності даних та автоматизованого управління транзакціями за допомогою смарт-контрактів [6,7]. Основна ідея методу полягає у створенні розподіленої бази даних, в якій кожна зміна записується у вигляді незмінного блоку, що є частиною загального ланцюга.

Архітектура запропонованого підходу

Архітектурно система містить такі компоненти:

- Децентралізований реєстр, в якому зберігаються всі записи у вигляді зв'язаних блоків, що унеможливлює їх несанкціоновану модифікацію.
- Модуль валідації даних, який перевіряє автентичність та коректність усіх транзакцій перед внесенням їх у реєстр.
- Смарт-контракти, які регулюють правила змін у реєстрах, забезпечують автоматичне дотримання встановлених вимог та усувають людський фактор.
- Клієнтський інтерфейс для державних службовців та громадян, який дозволяє взаємодіяти з реєстром у межах передбачених прав доступу.

Взаємодія між компонентами здійснюється за допомогою механізму консенсусу, що забезпечує єдину узгоджену версію реєстру серед усіх вузлів мережі [8]. Кожна операція верифікується надійними криптографічними алгоритмами, що гарантує достовірність інформації [9].

Процес обробки даних у блокчейн-реєстрі

Функціонування запропонованої системи базується на таких етапах:

- Ініціація операції – користувач або державний службовець подає запит на внесення нової інформації або оновлення наявного запису в реєстрі.
- Валідація запиту – система перевіряє коректність наданих даних та їх відповідність встановленим стандартам.
- Формування транзакції – підтверджена операція записується у новий блок, що включає унікальний хеш попереднього запису, часову мітку та ідентифікатор користувача.
- Консенсусний механізм – усі учасники мережі підтверджують достовірність змін, після чого блок додається до загального ланцюга.
- Фіналізація запису – після завершення всіх перевірок оновлена інформація стає доступною для перегляду та аудиту.

Отже, забезпечується прозорий і захищений механізм управління державними реєстрами, що усуває ризики зловживань, втрати даних та кібератак.

На рис. 1 зображено блок-схему функціонування запропонованої системи, яка ілюструє процес обробки та внесення даних у блокчейн-реєстр.

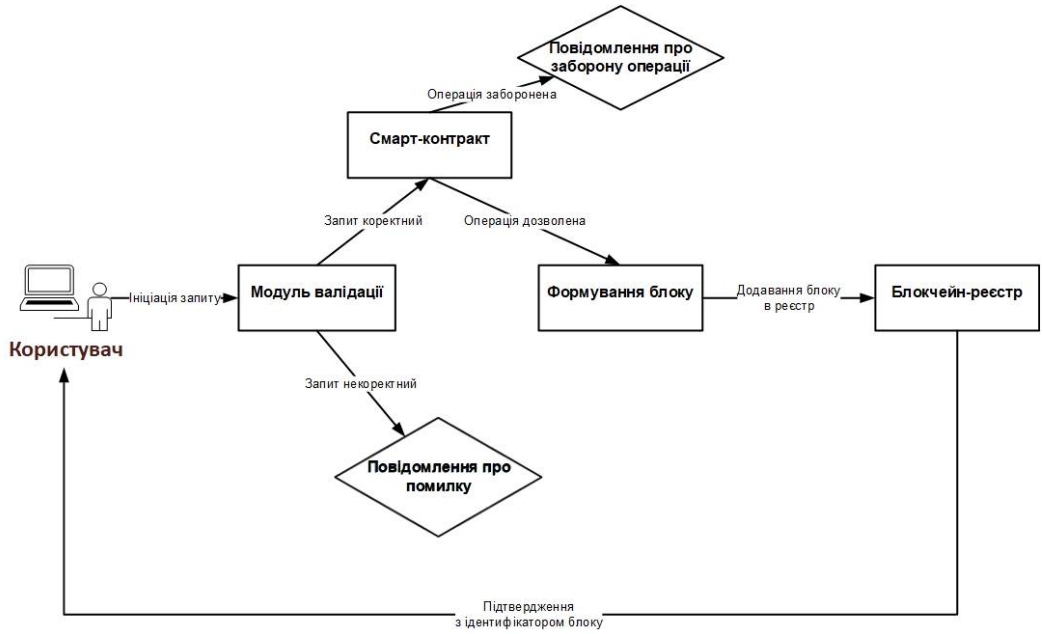

Рис. 1. Блок-схема процесу обробки даних у блокчейн-реєстрі

Як показано на рис. 1, процес внесення змін у реєстр містить декілька послідовних етапів, кожен з яких перевіряється децентралізованою мережею.

Запропонований механізм інтеграції блокчейн-технологій у державні реєстри ґрунтується на автоматизованому контролі внесення змін і забезпеченні достовірності даних завдяки децентралізованій структурі [10]. Основними функціональними компонентами системи є:

1. Користувач та ініціація запиту. Процес починається з того, що користувач надсилає запит на додавання або оновлення інформації в реєстрі. Це може бути державний службовець або авторизований представник, який має відповідний рівень доступу.

2. Модуль валідації. Отриманий запит проходить перевірку на відповідність встановленим вимогам. Якщо дані некоректні або порушують встановлені правила внесення інформації, система автоматично відхиляє запит, надсилаючи користувачеві повідомлення про помилку.

3. Смарт-контракт. У разі успішної перевірки модуль валідації передає запит до смарт-контракту, який визначає, чи дозволена ця операція відповідно до заздалегідь визначених умов. Смарт-контракт функціонує як автоматизований регулятор, який виконує лише ті операції, що відповідають протоколу.

4. Формування нового блоку. Якщо смарт-контракт схвалює транзакцію, система формує новий блок із унікальним хешем, який зв'язується з попереднім блоком у ланцюгу. Це гарантує незмінність записів і неможливість їхньої подальшої корекції без погодження всієї мережі.

5. Додавання блоку в блокчейн-реєстр. Після успішного формування новий блок включається в децентралізований реєстр. Всі учасники мережі отримують оновлення, що виключає можливість прихованих змін або несанкціонованого редагування.

6. Підтвердження користувачу. Завершальним етапом є повідомлення користувача про успішне внесення змін із зазначенням унікального ідентифікатора нового блоку. Це забезпечує прозорість усіх операцій і дозволяє перевіряти достовірність даних у будь-який момент.

Отже, інтеграція блокчейн у державні реєстри забезпечує високу безпеку та незмінність інформації [11]. Відсутність централізованої точки управління знижує ризики атак, а автоматизовані механізми контролю унеможливлюють несанкціоновані зміни або втручання.

Висновки. Аналіз наявних загроз для державних реєстрів демонструє критичну необхідність модернізації їхньої архітектури з метою підвищення рівня безпеки, прозорості та достовірності інформації. Традиційні централізовані системи виявляються вразливими до атак та маніпуляцій, що підриває довіру громадян до державних інформаційних ресурсів.

Запропонована методологія використання блокчейн-технологій дозволяє усунути основні недоліки централізованих підходів завдяки розподіленому характеру зберігання даних, незмінності записів та автоматизованим механізмам валідації змін. Розроблена архітектура передбачає використання смарт-контрактів для контролю над операціями, що забезпечує мінімізацію впливу людського фактору та підвищення рівня надійності реєстраційних процесів.

Практичне впровадження блокчейн-рішень у державні реєстри може забезпечити не лише підвищений рівень безпеки, але й сприяти цифровій трансформації адміністративних послуг, створюючи нову модель взаємодії між державою та громадянами. Подальші дослідження у цій сфері можуть бути спрямовані на розробку алгоритмів масштабування блокчейн-систем, адаптацію до нормативно-правових вимог та оптимізацію швидкості транзакцій для забезпечення високої продуктивності державних інформаційних систем.

1. Балацька В. С., Опірський І. Р. Забезпечення конфіденційності персональних даних і підтримки кібербезпеки за допомогою блокчейну. *Кібербезпека: освіта, наука, техніка*. 2023. № 4 (20). С. 6–19. DOI: https://doi.org/10.28925/2663-4023.2023.20.619

2. Балацька В., Побережник В., Опірський І. Використання Non-Fungible Tokens та блокчейн для розмежування доступу до державних реєстрів. *Кібербезпека: освіта, наука, техніка*. 2024. № 4 (24). С. 99–114. DOI: https://doi.org/10.28925/2663-4023.2024.24.99114

3. Балацька В., Побережник В. Концепція застосування блокчейн-технологій для підвищення захищеності персональних даних платформи «Дія»: відповідність вимогам GDPR та українському законодавству. *Кібербезпека: освіта, наука, техніка*. 2024. № 2 (26). С. 268–290. DOI: https://doi.org/10.28925/2663-4023.2024.26.681

4. Застосування блокчейну у державному секторі. *KLONA*. URL: https://klona.ua/uk/blog/blog-uk/zastosuvannya-blokchejnu-u-derzhavnomu-sektori

5. Навіщо впроваджувати блокчейн в державний устрій і як це зробити. *AIN.ua*. URL: https://ain.ua/2022/12/29/bornjakov-pro-blockchain/

6. Opirskyy I., Balatska V., Poberezhnyk V. Modern possibilities of use blockchain technology in the education system. *Ukrainian Scientific Journal of Information Security*. 2023. Vol. 29. Is. 3. S. 138–146. DOI: https://doi.org/10.18372/2225-5036.29.18073

7. Balatska V., Opirskyy I. Blockchain as a tool for transparency and protection of government registries. Ukrainian Scientific Journal of Information Security. 2024. Vol. 30. Is. 2. S. 221–230. DOI: https://doi.org/10.18372/2225-5036.30.19211

8. Balatska V., Opirskyy I., Slobodian N. Blockchain for enhancing transparency and trust in government registries. *CEUR Workshop Proceedings*. 2024. Vol. 3826: Cybersecurity Providing in Information and Telecommunication Systems II 2024. S. 50–59. URL: https://ceur-ws.org/Vol-3826/

9. Balatska V., Poberezhnyk V., Opirskyy I. Utilizing blockchain technologies for ensuring the confidentiality and security of personal data in compliance with GDPR. *CEUR Workshop Proceedings*. 2024. Vol. 3800: Cyber Security and Data Protection 2024. S. 70–80. URL: https://ceur-ws.org/Vol-3800/

10. Poberezhnyk V., Balatska V., Opirskyy I. Development of the learning management system concept based on blockchain technology. *CEUR Workshop Proceedings*. 2023. Vol. 3550: Cybersecurity Providing in Information and Telecommunication Systems II 2023. S. 143–156. URL: https://ceur-ws.org/Vol-3550/

11. Balatska V., Poberezhnyk V., Petriv P., Opirskyy I. Blockchain Application Concept in SSO Technology Context. *CEUR Workshop Proceedings*. 2024. Vol. 3654: Cybersecurity Providing in Information and Telecommunication Systems 2024. S. 38–49. URL: https://ceur-ws.org/Vol-3654/