УДК 004.056

# ЗАХИСТ КОНФІДЕНЦІЙНИХ ДАНИХ У ВЕБСЕРВІСАХ ЧЕРЕЗ БЛОКЧЕЙН ІЗ ВИКОРИСТАННЯМ ZERO-KNOWLEDGE PROOFS

А. В. Шматко[1,a], В. Ю. Зубок[1]

[1] Навчально-науковий Фізико-технічний інститут

## Анотація

У роботі розглянуто питання захисту конфіденційних даних у вебсервісах із використанням блокчейну та доказів з нульовим розголошенням. Проаналізовано базові методи захисту інформації, їхні обмеження та переваги технології блокчейн для забезпечення цілісності даних. Описано концепцію Zero-Knowledge Proofs (ZKP) і можливості її застосування для аутентифікації і приватних транзакцій без розкриття самого змісту даних. Запропоновані підходи демонструють, що поєднання блокчейну та ZKP дозволяє істотно підвищити конфіденційність у розподілених веб-системах, хоча потребує додаткових обчислювальних ресурсів.

**Ключові слова**: конфіденційність, вебсервіси, блокчейн, доказ з нульовим розголошенням

## Вступ

За останні роки спостерігається стрімке зростання кількості випадків компрометації конфіденційних даних у вебсервісах. За оцінками, у 2023 році інциденти витоку інформації вплинули на понад 1,35 млрд осіб [1]. Це зумовлює актуальність проблеми захисту приватності користувацьких даних. Існуючі підходи до забезпечення конфіденційності базуються на шифруванні та політиках доступу, проте вони вимагають довіри до самого сервісу та не гарантують захисту даних у випадку компрометації сервера.

Новітні технології пропонують принципово нові рішення для підвищення рівня безпеки даних. Одним із перспективних напрямів є застосування блокчейн-технології та криптографічних доказів з нульовим розголошенням (ZKP) для мінімізації залежності від довіри до сервісу [2]. Поєднання блокчейну та ZKP дозволяє перевіряти певні факти або повноваження користувача без прямого доступу до його конфіденційних даних. У цій роботі запропоновано підхід, що реалізує такий принцип, і спрямований на нейтралізацію основних загроз приватності у вебсервісах.

## 1. Постановка задачі

Метою роботи є розробка підходу до забезпечення конфіденційності даних у вебсервісах з використанням технологій блокчейну та ZKP. Для досягнення поставленої мети необхідно вирішити такі завдання: проаналізувати основні загрози для конфіденційності даних у середовищі вебсервісів; здійснити огляд технологій блокчейну та ZKP і існуючих методів захисту даних; розробити алгоритм, що поєднує блокчейн та ZKP для захисту конфіденційних даних; визначити основні метрики для оцінки запропонованого рішення та проаналізувати його ефективність.

## 2. Загрози

Уразливість конфіденційних даних у вебсервісах спричинена різними факторами. Основні загрози включають:

- **Зловмисні атаки.** Хакери можуть отримати несанкціонований доступ до конфіденційних даних, викравши облікові дані користувачів або експлуатуючи вразливості системи.
- **Внутрішні загрози.** Недобросовісні адміністратори чи інші співробітники з доступом до системи здатні навмисно або випадково розкрити або викрасти чутливі дані.
- **Витоки даних.** Конфіденційні відомості можуть бути оприлюднені через помилки конфігурації, уразливості програмного забезпечення або небезпечні інтеграції зі сторонніми сервісами.
- **Перехоплення інформації.** Дані, що передаються між клієнтом і сервісом, можуть бути перехоплені (атака типу «людина посередині»), якщо канали зв'язку недостатньо захищені, що призводить до компрометації інформації.

Зазначені загрози підкреслюють необхідність впровадження рішень, які забезпечують захист даних навіть у випадку, якщо традиційні механізми безпеки було обійдено.

## 3. Огляд технологій

Для протидії вказаним загрозам доцільно використати дві ключові технології: блокчейн та докази з нульовим розголошенням. Блокчейн забезпечує децентралізоване та незмінне зберігання даних, а ZKP

[a] andshma-ipt25@lll.kpi.ua

надають можливість криптографічно підтверджувати властивості даних без їх розкриття.

### 3.1. Блокчейн

Блокчейн — це розподілений реєстр, що складається з послідовно пов'язаних блоків транзакцій [3]. Кожен блок містить хеш попереднього блоку, що гарантує незмінність ланцюга: будь-яка спроба змінити дані в одному з блоків порушить цілісність усього ланцюжка. Децентралізація блокчейн-мережі означає відсутність єдиного центру керування — дійсність транзакцій підтверджується консенсусом між багатьма вузлами. Ці властивості забезпечують високий рівень цілісності даних та стійкості до несанкціонованих змін.

Водночас у публічних блокчейнах всі дані у реєстрі зазвичай доступні учасникам мережі, тому для зберігання конфіденційної інформації необхідно застосовувати додаткові методи захисту (шифрування, хешування тощо). Існують також приватні (корпоративні) блокчейни з обмеженим доступом, що підвищує контроль над тим, хто може переглядати дані, але зменшує рівень децентралізації.

### 3.2. Докази з нульовим розголошенням

Доказ з нульовим розголошенням — це криптографічний протокол, у якому одна сторона (провідник) може переконати іншу сторону (верифікатора) в істинності певного твердження, не розкриваючи жодної додаткової інформації про нього [4]. Класичний приклад — доведення знання пароля без його розголошення: провідник демонструє, що знає секретне значення, не повідомляючи самого значення.

Існують інтерактивні та неінтерактивні реалізації ZKP. Сучасні схеми, такі як zk-SNARK (Zero-Knowledge Succinct Non-interactive Argument of Knowledge) [5], дозволяють генерувати та перевіряти криптографічні докази ефективно, що відкрило можливості для використання ZKP у блокчейн-системах. Зокрема, у криптовалютних протоколах (наприклад, Zcash) ZKP застосовуються для приховування сум транзакцій та адрес від сторонніх спостерігачів, зберігаючи при цьому можливість верифікації їх дійсності [5].

У контексті вебсервісів докази з нульовим розголошенням можуть використовуватися для автентифікації користувачів або перевірки виконання певних умов (наприклад, досягнення користувачем необхідного віку чи наявності відповідних прав) без розкриття самих персональних даних. Комбінація блокчейну та ZKP дозволяє створити систему, у якій конфіденційні дані не покидають межі користувача, а сервіс отримує лише криптографічне підтвердження їх відповідності заданим вимогам [2].

## 4. Алгоритм

Запропонований алгоритм функціонування системи захисту конфіденційних даних за допомогою блокчейну та ZKP складається з наступних кроків [6]:

1) Користувач генерує та зберігає на блокчейні криптографічний об'єкт, пов'язаний зі своїми конфіденційними даними. Це може бути хеш від даних або цифровий сертифікат, виданий довіреним органом, який підтверджує певні властивості (атрибути) користувача.
2) При зверненні до вебсервісу користувач формує Zero-Knowledge доказ, що підтверджує виконання необхідної умови на основі його конфіденційних даних. Наприклад, доказ того, що вік користувача перевищує встановлений поріг, або що він володіє дійсним сертифікатом, зареєстрованим у блокчейні, — без розкриття самого віку чи сертифікату.
3) Користувач надсилає сформований криптографічний доказ (та, за потреби, ідентифікатор відповідного запису в блокчейні) вебсервісу для перевірки.
4) Вебсервіс виконує перевірку достовірності отриманого доказу. Верифікація може здійснюватися або засобами самого вебсервісу (шляхом звернення до блокчейну для отримання публічних даних, потрібних для перевірки), або через смарт-контракт у блокчейні, який автоматично підтверджує валідність доказу.
5) У разі успішної верифікації вебсервіс отримує підтвердження того, що користувач відповідає необхідним критеріям (пройшов автентифікацію, має відповідні права доступу тощо), не отримуючи при цьому конфіденційну інформацію. Після цього користувачу надається доступ до запитуваного ресурсу або послуги.
6) (Опційно) Факт успішної перевірки доказу та відповідна транзакція можуть бути зафіксовані в блокчейні. Такий запис не розкриває приватних даних, проте забезпечує прозорий журнал подій для можливості аудиту у майбутньому.

## 5. Метрики

Для оцінювання запропонованого рішення визначено ряд ключових метрик:

- **Конфіденційність даних:** обсяг інформації, що розкривається під час верифікації. Ідеальна ситуація досягається, коли доказ є нульового розголошення і сервіс не отримує жодних даних про користувача, окрім підтвердження заданого факту [4].
- **Час та ресурси на перевірку:** витрати часу та обчислювальних ресурсів на формування і перевірку ZKP-доказів. Ця метрика визначає продуктивність системи та впливає на масштабованість рішення [7].
- **Розмір доказів та даних:** обсяг додаткових даних, які необхідно передати і зберігати (наприклад, розмір криптографічного доказу, дані транзакції у блокчейні). Менший розмір доказу знижує навантаження на мережу і покращує швидкодію.
- **Масштабованість:** здатність системи ефективно працювати зі збільшенням кількості користу-

вачів та транзакцій. Вимірюється пропускною здатністю (кількість транзакцій або перевірок на секунду) та затримками при високому навантаженні [8].

- **Криптографічна стійкість:** надійність використаних алгоритмів шифрування і доказів проти сучасних атак. Ця якісна метрика відображає безпековий запас системи (використання перевірених алгоритмів, достатні розміри ключів тощо) [9].
- **Прозорість для аудиту:** можливість зберігати факти верифікації у блокчейні без розкриття персональних даних, що забезпечує перевірку історії доступів та дій користувачів.
- **Гнучкість:** адаптованість алгоритму до різних типів запитів і умов верифікації, включно з динамічними правилами доступу.
- **Стійкість до людського фактора:** зниження залежності від правильних дій користувачів і адміністраторів за рахунок криптографічних гарантій.

Як узагальнення, табл. 1 демонструє основні переваги та потенційні недоліки запропонованого підходу в порівнянні з традиційною моделлю роботи вебсервісів.

Таблиця 1. Переваги та недоліки підходу на основі блокчейну та ZKP [10]

| **Переваги** | **Недоліки** |
|---|---|
| Децентралізація (відсутність єдиного центру) | Високі вимоги до обчислювальних ресурсів |
| Конфіденційність даних (мінімальне розголошення) | Складність впровадження та налаштування |
| Цілісність та незмінність даних у реєстрі | Затримки у виконанні через генерацію доказів |
| Не потребує довіри до сервісу | Обмежена масштабованість при значному навантаженні |

## 6. Приклад використання

Розглянемо типовий приклад застосування запропонованого підходу — верифікація віку користувача для доступу до ресурсу з віковим обмеженням (наприклад, онлайн-магазину з обмеженим контентом).

Користувач бажає підтвердити, що йому більше 18 років, не розкриваючи точну дату народження. Для цього:

- Користувач має електронний сертифікат, виданий державним або приватним органом, який містить його дату народження.
- На основі сертифіката користувач локально генерує Zero-Knowledge доказ того, що його вік перевищує заданий поріг (наприклад, 18 років).
- Вебсервіс отримує лише доказ, без доступу до самого сертифіката або дати народження.
- За допомогою криптографічного алгоритму сервіс перевіряє валідність доказу (без потреби в централізованій базі даних чи посереднику).

Після успішної перевірки користувач отримує доступ до ресурсу, а система фіксує факт верифікації у блокчейні, зберігаючи анонімність користувача.

Цей підхід може бути також адаптований для інших сценаріїв: підтвердження наявності прав доступу до документа, верифікація членства в організації, участь у голосуванні тощо. У всіх випадках основна перевага полягає у можливості підтвердити істинність певного факту без розкриття конфіденційної інформації.

Таким чином, запропонована модель не тільки відповідає вимогам приватності, а й дозволяє гнучко інтегрувати її в існуючі вебсервіси без необхідності кардинальної зміни архітектури.

## Висновки

У роботі розглянуто питання захисту конфіденційних даних у вебсервісах шляхом поєднання блокчейн-технології та доказів з нульовим розголошенням (Zero-Knowledge Proofs). На основі аналізу існуючих загроз конфіденційності (розділ 3) і сучасних технологій захисту (розділ 4) було запропоновано власний підхід, який детально представлено у розділі 5 («Алгоритм»). Запропонований алгоритм передбачає локальну генерацію користувачем криптографічного доказу, що підтверджує виконання умов доступу без розкриття конфіденційних даних. Даний доказ верифікується вебсервісом чи блокчейн-мережею, при цьому самі дані залишаються прихованими.

Такий підхід дозволяє ефективно протидіяти основним загрозам безпеки, оскільки не потребує довіри до центральних серверів, мінімізує ризик витоку конфіденційної інформації та забезпечує децентралізовану перевірку. Оцінка запропонованого рішення базується на чітко визначених метриках конфіденційності, масштабованості, продуктивності та криптографічної стійкості (розділ 6).

Таким чином, запропоноване в роботі поєднання блокчейну та доказів з нульовим розголошенням створює ефективну основу для посилення приватності в сучасних вебсервісах. Подальші дослідження можуть бути спрямовані на оптимізацію продуктивності алгоритмів ZKP та впровадження запропонованого підходу в реальні системи.

Крім того, важливо відзначити, що використані в роботі метрики дозволяють комплексно оцінити як ефективність, так і практичну доцільність запропонованого рішення. Метрика конфіденційності дозволяє оцінити, наскільки добре система захищає приватні дані користувача, а продуктивність і масштабованість безпосередньо впливають на її здатність працювати у високонавантажених середовищах.

На тлі традиційних підходів, які покладаються на централізовані сервери та бази даних, запропонована модель має важливу перевагу — мінімізацію ризику компрометації внаслідок зловживання правами доступу або технічних вразливостей. Однак слід враховувати, що реалізація ZKP вимагає значних обчислювальних ресурсів, що на сьогоднішній день

може бути стримувальним фактором для повномасштабного впровадження в комерційні вебплатформи.

Описаний підхід має потенціал до широкого застосування — від фінансових сервісів до охорони здоров'я, де конфіденційність особливо критична. Зокрема, використання блокчейну як засобу ведення прозорих і незмінних журналів подій дозволяє не тільки забезпечити аудит, а й зменшити ризик фальсифікацій.

У подальшому розвиток технологій, зокрема поява легших і швидших реалізацій ZKP, сприятиме зниженню бар'єрів впровадження та відкриє нові сценарії використання для захисту приватних даних у цифровому середовищі.

## Перелік використаних джерел


1. *Statista*. Number of data breaches and individuals affected worldwide in 2023. — 2024. — Online: https://statista.com.
2. Leveraging zero-knowledge proofs for blockchain-based identity sharing: A survey of advancements, challenges and opportunities / L. Zhou, A. Diro, A. Saini, S. Kaisar, P. C. Hiep // Journal of Information Security and Applications. — 2024.
3. *Nakamoto S.* Bitcoin: A Peer-to-Peer Electronic Cash System. — 2008. — Whitepaper.
4. *Goldwasser S.*, *Micali S.*, *Rackoff C.* The knowledge complexity of interactive proof systems // SIAM Journal on Computing. — 1989. — Т. 18, № 1. — С. 186—208.
5. Zerocash: Decentralized Anonymous Payments from Bitcoin / E. Ben-Sasson [та ін.] // IEEE Symposium on Security and Privacy. — 2014. — С. 459—474.
6. Enhancing Digital Privacy: The Application of Zero-Knowledge Proofs in Authentication Systems / S. Bhattacharya, D. Seth, S. Panyam, P. Gangrade // International Journal of Computer Theory and Technology. — 2024. — Т. 72, № 4. — С. 34—41.
7. *El-Hajj M.*, *Oude Roelink B.* Evaluating the Efficiency of zk-SNARK, zk-STARK, and Bulletproof in Real-World Scenarios: A Benchmark Study // Information. — 2024. — Т. 15, № 8. — С. 463. — DOI: 10.3390/info15080463.
8. A Survey on the Applications of Zero-Knowledge Proofs / R. Lavin, X. Liu, H. Mohanty, L. Norman, G. Zaarour, B. Krishnamachari // arXiv preprint arXiv:2408.00243. — 2024.
9. if-ZKP: Intel FPGA-Based Acceleration of Zero Knowledge Proofs / S. A. Butt, B. Reynolds, V. Ramamurthy, X. Xiao, P. Chu, S. Sharifian, S. Gribok, B. Pasca // arXiv preprint arXiv:2412.12481. — 2024.
10. Blockchain Technology: Benefits, Challenges, Applications, and Integration of Blockchain Technology with Cloud Computing / G. Habib, S. Sharma, S. Ibrahim, I. Ahmad, S. Qureshi, M. Ishfaq // Future Internet. — 2022. — Т. 14, № 11. — С. 341. — DOI: 10.3390/fi14110341.