ШИФРУВАННЯ ДАНИХ У ДЕЦЕНТРАЛІЗОВАНИХ СИСТЕМАХ

Новік Т.О., В'юхін Д.О., Фроленко В.О.
Харківський Національний університет радіоелектроніки, Харків, Україна

Сучасний світ характеризується зростаючою залежністю від цифрових технологій, що робить питання захисту даних у централізованих системах надзвичайно актуальним.

Метою доповіді є проведення порівняльного аналізу методів шифрування в централізованих системах.

Централізовані системи зберігають великі обсяги конфіденційної інформації, що робить їх привабливою ціллю для зловмисників. У зв'язку з цим, дослідження та впровадження ефективних методів шифрування є критично важливим завданням.

У першій половині 2024 року в блокчейні зафіксовано 185 значних інцидентів безпеки, які призвели до збитків у розмірі до 920 мільйонів доларів. Однак порівняно з першим півріччям 2022 року, коли збитки сягнули близько 2 мільярдів доларів, цей показник знизився на 54% [1]. Інцидент зі зломом DMM Bitcoin підкреслює фундаментальну важливість захисту даних у децентралізованих системах шляхом використання передових методів шифрування [2].

Вразливість, що виникла внаслідок соціальної інженерії, дозволила хакерам отримати доступ до приватних ключів і контролювати транзакції в блокчейні.

Втрата доступу до приватного ключа в децентралізованій мережі фактично означає втрату активів, адже криптовалюта в таких системах зберігається не фізично, а через криптографічний захист записів у ланцюзі блоків.

У цьому контексті шифрування виконує такі ключові функції.

1. Захист приватних ключів: використання апаратних криптогаманців із мультипідписами або шифрування ключів у корпоративних сховищах може запобігти подібним атакам.

2. Мультифакторна автентифікація (MFA): складне шифрування даних автентифікації та додатковий рівень безпеки у вигляді біометрії чи динамічних ключів унеможливили б доступ до системи лише на основі викрадених облікових даних.

3. Децентралізовані ідентифікаційні системи (DID): це ще один перспективний напрямок, де криптографічні ключі забезпечують безпеку автентифікації в децентралізованих мережах і блокують доступ для шахраїв, що діють через соціальну інженерію.

Одним з перспективних напрямків у сфері захисту даних є використання децентралізованих технологій, таких як блокчейн, Internet Computer Protocol (ICP) та смарт-протоколи. Ці технології пропонують ряд переваг щодо безпеки даних.

Серед основних переваг блокчейну виділяють децентралізацію, яка мінімізує ризик атак на центральний сервер; незмінність інформації, що ускладнює її підробку чи видалення без згоди більшості учасників мережі; прозорість транзакцій, які доступні для публічної перевірки; та підвищену стійкість до атак завдяки розподіленому зберіганню даних [3]. Водночас блокчейн має і певні обмеження: високу потребу в обчислювальних ресурсах, недостатню масштабованість для систем із високим навантаженням та значні витрати на впровадження [4].

У доповіді представлений порівняльний аналіз методів шифрування децентралізованих систем.

Основні методи шифрування в децентралізованих системах:

- асиметричне шифрування (Public-key crypto) (RSA, ECC (Elliptic Curve Cryptography), ElGamal);
- симетричне шифрування (AES, ChaCha20);
- гомоморфне шифрування (Homomorphic Encryption) [5];
- атрибутивне шифрування (Attribute-Based Encryption, ABE);
- порогове шифрування / секретне діління (Shamir's Secret Sharing);
- Zero-Knowledge Proofs (ZKP).

З огляду на все складніші схеми кібератак, подібні методи шифрування та розподіленої автентифікації мають стати стандартом у криптовалютному секторі та інших децентралізованих системах.

Комбінування методів шифрування є основною стратегією шифрування у децентралізованих системах. Перспективними напрямами залишаються: гомоморфне шифрування та ZKP, попри їхню складність.

Використання технологій блокчейну, ICP та смарт-протоколів забезпечує значне підвищення рівня безпеки та зменшує ризик зловживань.

Попри виклики, пов’язані з їх впровадженням, ці технології мають значний потенціал для розвитку та вдосконалення систем кібербезпеки у майбутньому.

Список літератури

1. Марія Огнівчук. Прогноз проблем безпеки для технологій блокчейн у 2024 році [електронний документ] URL: https://www.h-x.technology/ua/blog-ua/top-blockchain-security-threats-in-2024-ua.
2. Slowmist. Blockchain Security and AML Annual Report. 2024.
3. Зражевець, К. П. Дослідження рішень щодо збереження безпеки ключів у блокчейн-технологіях. Харків, 2023 URL: https://openarchive.nure.ua/handle/document/24113
4. Терещенко, Г. Ю. Дослідження та оцінка ефективності алгоритмів шифрування, що використовуються в технології Блокчей Харків, 2020, URL:http://openarchive.nure.ua/handle/document/14878.
5. Khalimov, Gennady, et al. "Encryption Based on the Group of the Hermitian Function Field and Homomorphic Encryption." 2021 IEEE 8th International Conference on Problems of Infocommunications, Science and Technology (PIC S&T). IEEE, 2021.