УДК 004.56
Назар Шевченко, Константин Швирло, Григорій Шимчук, старший викладач
Тернопільський державний технічний університет імені Івана Пулюя

ОГЛЯД ПОТЕНЦІЙНИХ КІБЕРАТАК НА ДЕЦЕНТРАЛІЗОВАНІ МЕРЕЖІ

Nazar Shevchenko, Konstantin Shvyrlo, Grigorii Shymchuk, Senior lecturer

OVERVIEW OF POTENTIAL CYBER ATTACKS ON DECENTRALIZED NETWORKS

Децентралізовані мережі, такі як блокчейн та інші децентралізовані системи, не є імунними до потенційних кібератак, але вони мають свої унікальні особливості та методи захисту.

Ось деякі з потенційних кіберзагроз для децентралізованих мереж:

– 51% атака – це тип атаки на блокчейн, коли атакуюча сторона отримує контроль над більшістю обчислювальної потужності мережі, що дозволяє їй змінювати дані в блоках або навіть подвоювати транзакції.

– DDoS-атаки – це атаки на доступність, коли зловмисники перенавантажують мережу трафіком, що призводить до перерв у роботі мережі та відмови у обслуговуванні.

– Соціальна інженерія, наприклад, шахраї можуть намагатися отримати доступ до особистих ключів або фінансових даних користувачів шляхом маніпулювання ними.

– Вразливості смарт-контрактів, якщо смарт-контракти не перевірені на вразливості, це може призвести до втрати коштів або можливості виконання небажаних операцій.

– Фішинг – це атаки, спрямовані на отримання особистих даних, паролів або ключів шляхом підступних методів.

Для захисту від цих загроз можуть використовуватися різноманітні підходи:

– криптографічні методи;
– мультипідписи та багаторівнева автентифікація;
– аудит смарт-контрактів;
– мережеві обмеження;
– постійне вдосконалення.

Криптографічні методи грають ключову роль у забезпеченні безпеки децентралізованих мереж, розглянемо деякі з них.

Шифрування використовується для захисту конфіденційності даних. Сучасні алгоритми шифрування, такі як AES (Advanced Encryption Standard) або RSA (Rivest-Shamir-Adleman), застосовуються для захисту інформації від несанкціонованого доступу.

Хеш-функції перетворюють вхідні дані в унікальний хеш-код фіксованої довжини. Це використовується для перевірки цілісності даних. SHA-256 — один з найбільш відомих хеш-алгоритмів, який застосовується в багатьох криптовалютних протоколах, наприклад, у біткойні.

Цифрові підписи дозволяють підтверджувати автентичність повідомлень або транзакцій у децентралізованих мережах. Наприклад, електронні підписи за допомогою алгоритмів RSA, ECDSA (Elliptic Curve Digital Signature Algorithm).

Протоколи обміну ключами, такі як, протоколи Diffie-Hellman чи Elliptic-curve Diffie-Hellman, використовуються для безпечного обміну ключами у відкритій мережі.

Криптографічні протоколи, зокрема TLS/SSL для захисту комунікації в мережі, які шифрують трафік між сервером і клієнтом.

Zero-knowledge proofs, ці методи дозволяють доводити факт знання певної інформації, не розкриваючи саму інформацію. Вони застосовуються у приватних блокчейн-мережах для підтвердження операцій без розголошення конфіденційної інформації.

Мультипідписи та багаторівнева автентифікація – це методи, що використовуються для збільшення рівня безпеки, вимагаючи додаткових перевірок для підтвердження особи чи транзакції. Зокрема мультипідписи (Multisig) – це метод, при

якому для здійснення транзакції необхідно декілька приватних ключів замість одного. Наприклад, у схемі 2-of-3 мультипідпису треба два з трьох можливих ключів для підтвердження транзакції. Це підвищує безпеку, оскільки потрібно мати доступ до декількох ключів для проведення операції. А багаторівнева автентифікація (MFA) – це процес, при якому користувач для входу або підтвердження операції повинен пройти кілька етапів перевірки. Це може включати пароль, код, отриманий на мобільний телефон, відбиток пальця або інші методи. Комбінування кількох факторів автентифікації зменшує ризик несанкціонованого доступу.

Аудит смарт-контрактів – це процес перевірки коду смарт-контракту з метою виявлення потенційних вразливостей, помилок або проблем безпеки перед його розгортанням у блокчейні чи децентралізованій мережі.

Основні кроки аудиту смарт-контрактів включають:

- перевірка на відповідність специфікаціям;
- пошук вразливостей безпеки;
- тестування безпеки;
- надання рекомендацій та вдосконалень.

Аудит смарт-контрактів є критично важливим етапом у розгортанні будь-якої блокчейн-додаткової програми чи додатка, оскільки він допомагає уникнути багатьох потенційних проблем безпеки та забезпечити відповідність контракту вимогам його функціонування.

Мережеві обмеження (Network Limitations) – це заходи безпеки, спрямовані на обмеження та контроль трафіку, який входить чи покидає децентралізовану мережу. Це може бути застосовано для захисту від DDoS-атак, перешкоджаючи надмірному трафіку чи іншим шкідливим діям, які можуть призвести до перебоїв у роботі мережі.

Основні методи мережевих обмежень включають:

- фільтрація пакетів;
- Rate limiting (обмеження швидкості);
- трафікові коридори (Traffic Shaping);
- Blacklisting та Whitelisting;
- тунелювання (Tunneling).

Ці методи допомагають забезпечити стійкість та безпеку децентралізованих мереж, мінімізуючи можливість негативного впливу шкідливого трафіку чи атак на їхню працездатність та доступність.

Постійне вдосконалення (Continuous Improvement) в сфері кібербезпеки та технологій включає в себе низку практик та процесів, які спрямовані на постійне підвищення рівня безпеки, ефективності та реагування на нові загрози чи виклики. Ось деякі аспекти цього:

- моніторинг та аналіз;
- вдосконалення заходів безпеки;
- оновлення програмного забезпечення;
- навчання та розвиток персоналу;
- тестування на проникнення;
- аудит безпеки.

Цей процес не є статичним, він вимагає постійного оновлення, адаптації та вдосконалення залежно від нових загроз та технологічних змін. Важливо пам'ятати, що кібербезпека – це постійний процес, а не одноразова подія.

Література

1.Vitalik Buterin .On stake // Ethereum Blog.2014 [Електроний ресурс] — Режим доступу: https://blog.ethereum.org/2014/07/05/stake.

2. Шимчук Г. Основні проблеми та загрози хмарної безпеки / Г. Шимчук, О. Голотенко, Роман Захарійович Золотий // Матеріали X науково-технічної конференції „Інформаційні моделі, системи та технології“, 7–8 грудня 2022 року. – Т. : ТНТУ, 2022. — С. 59–60. – (Інформаційні системи та технології, кібербезпека).