Бондарчук С.І., магістрант,
Науковий керівник – Сугоняк І.І., к.т.н., доц.,
Житомирський державний технологічний університет

АНАЛІЗ ЗАХИЩЕНОСТІ КОРИСТУВАЦЬКИХ ДАНИХ У ДЕЦЕНТРАЛІЗОВАНИХ КРИПТОВАЛЮТАХ

На сьогоднішній день надзвичайної популярності набули крипто валюти. Найуспішнішою крипто валютою являється Bitcoin з обсягом понад 15 мільйонів монет. Популярність принесла абсолютна відкритість і децентралізація системи. В основі лежить однорангова пірингова мережа, що складається з розподіленої множини рівноправних вузлів.

Надзвичайно важливим елементом для користувачів крипто валюти являється керування ключами. Адже втрата ключів призводить до негайних грошових втрат. Тому важливим є підтримання безпеки з клієнтської сторони. Однією з відмінностей крипто валюти є використання криптографії з відкритим ключем натомість звичних паролів або інформації про кредитну картку.

Гаманець користувачів слабо захищений від крадіжок, оскільки за замовчуванням він незашифрований. З цієї причини гаманець стає легкою здобиччю для шахраїв. Однак останні версії клієнтів Bitcoin вже містять шифри для захисту даних гаманця, але користувач повинен вручну підключити шифр, що вимагає від користувача додаткового рівня відповідальності.

Існує ряд моделей зберігання і управління ключами, але у кожної з них є ряд своїх недоліків. Найпростішою схемою зберігання ключів є зберігання у пам'яті девайсу. Така модель уразлива до шкідливого ПО, наприклад троянських програм. Вдосконаленням даної моделі є використання сценарію мультипідпису *k*-з-*n*. Це означає, що для аутентифікації повинні бути отримані *k* штук ключів із загальної кількості, що становить *n*. Ця схема схожа на двох фактору аутентифікпцію, коли на мобільний телефон приходить пароль з підтвердженням логіну в певній системі.

Клієнт Bitcoin може дозволити закодувати файл, що зберігає набір ключів за допомогою користувацького паролю. Це може збивати користувача з пантелику ніби пароль власне і являється ключем доступу до його гаманця на інших девайсах. Дані паролі мають уразливість до підбору паролю методом повного перебору.

Також небезпеку несе і процедура відновлення гаманця. Новий гаманець можна розкрити старим паролем через бекапи. Стару копію гаманця зі старим паролем часто можна легко відновити за допомогою створення програми відновлення: відновлення старого гаманця з паролем відновлює поточний гаманець і поточний пароль. Тому часта зміна пароля не є гарантією повної безпеки. Вирішити дану проблему можливо, наприклад, так, щоб зміна пароля гаманця автоматично створювала новий гаманець з новим паролем, і накопичені заощадження повинні автоматично переноситися на новий гаманець. При цьому при спробі відновлення копії старого гаманця і пароля будуть неробочими. З іншого боку, користувачі, які не розбираються в технічних тонкощах створення гаманців, не зможуть відновити дані своїх заощаджень криптовалюта і втратять біткоіни разом з гаманцем.

Певного поширення набули онлайн-сервіси, що пропонують звичні нам механізми управління ключами. Даний метод іде в розріз самої ідеї криптовалюти як децентралізованої грошової системи і вимагає високого рівня довіри клієнтів сервісу. Підтвердженням цього є реєстрація великої кількості випадків грошових втрат різного об'єму саме через подібні сервіси.

Також можливе встановлення адресних даних користувача, для цього може бути використано відстеження історії грошових переказів. Слід пам'ятати про те, що Bitcoin не є повністю анонімним засобом оплати.

Однією з проблем недалекого майбутнього може стати злам хеш-функцій. Алгоритми для обчислення хеш-функції стандартів SHA-256 і ECDSA вважаються такими, які неможливо зламати на поточних комп'ютерних потужностях. Проте поява нових високопродуктивних квантових комп'ютерів збільшить ризик злому даних функцій. В цьому випадку, хеш-функцію Bitcoin потрібно буде замінити на більш складну.

Криптовалюта увійшла в наше життя як альтернативна грошова система і уже користується немалим попитом. Різноманітні дослідження показують високий рівень безпеки даних систем, проте і крипт валюти мають ряд певних вразливостей. Тому важливим завданням є аналіз і розроблення методів зберігання і керування ключами, що поєднають у собі всі плюси існуючих підходів, заодно усунувши недоліки. Висока ж складність системи викликає нерозуміння у більшості людей і є одним з факторів, чому користувачі користуються сторонніми сервісами відходячи від основного принципу децентралізації валюти.