Використання блокчейн з точки зору інформаційної безпеки

УДК 681.3(043.2)

Антон Куліковський, Оксана Дуксенко, Марина Коломієць

Національний авіаційний університет, anton.kulikovskyi@gmail.com

Сьогодні в час все частішого використання централізованих інформаційно-телекомунікаційних систем для обробки і збереження даних стає складніше забезпечувати безпеку інформації.

Основною метою роботи є аналіз використання технології блокчейн для збереження та обробки даних з точки зору тріади сервісів інформаційної безпеки – цілісності, конфіденційності та доступності.

Мережа блокчейн добре справляється із забезпеченням збереження цілісності даних. За рахунок існування багатьох копій бази даних та внесення змін до неї лише після підтвердження правильності інформації іншими учасниками мережі, інформація залишається захищеною від навмисної, несанкціонованої або випадкової зміни, а також будь-яких змін в процесі зберігання обробки або передачі. Інформацію стає неможливо змінити через технічні збої в роботі вузла мережі або через людський фактор, оскільки підтвердження операцій відбувається завдяки складним математичним функціям. Як наслідок інформація залишається незмінною та коректною. Забезпечення цієї категорії інформаційної безпеки дає можливість стабільного проведення операцій, прийняття правильних рішень та можливість зберегти дані в тому вигляді, в якому вони були створені.

Відповідно до принципу доступності інформація має бути доступною авторизованим особам в потрібний момент часу. В мережі блокчейн кожен учасник вважається авторизованим та в будь-який момент може зчитати чи записати дані та приймати участь у верифікації даних, які додають інші учасники.

Конфіденційність інформації досягається наданням можливості доступу до неї з найменшими привілеями, тобто авторизована особа повинна мати доступ тільки до тих даних, які визначені для неї правами доступу. Кожен учасник мережі може отримати повну копію бази даних на свій пристрій, що в основі суперечить принципу конфіденційності даних. Зберігання даних в блокчейн в зашифрованому вигляді в основі не вирішить проблему конфіденційності, оскільки розшифрування отриманих даних стає питанням часу та залежить від обчислювальних потужностей зловмисника, який намагається отримати доступ до інформації.

В результаті проведеного аналізу можна зробити висновок, що за принципом своєї роботи блокчейн з високою надійністю можна використовувати у роботі з відкритими даними для забезпечення їх цілісності та доступності. Використовувати блокчейн в загальному вигляді для зберігання та обробки конфіденційних даних не є доцільним, оскільки будь-хто зможе отримати доступ до конфіденційних даних, які зберігаються у відкритій базі блокчейн.