УДК 004.75

С. В. Сідак
Я. А. Кулик

РОЗРОБКА ЗАХИЩЕНОГО СХОВИЩА ДАНИХ ІЗ ВИКОРИСТАННЯМ ТЕХНОЛОГІЙ БЛОКЧЕЙН

[1] Вінницький національний технічний університет;

Анотація
У цьому дослідження було розглянуто розробку захищеного сховища даних із використанням технологій блокчейн, розроблено алгоритм шифрування який використовує каскадне шифрування та технологію блокчейн для забезпечення захисту даних.
Ключові слова: сховище даних, шифрування, блокчейн, захист даних.

Abstract
This study developed the design of a secure data storage using blockchain technology, developed an encryption algorithm that uses cascaded encryption and blockchain technology to ensure data security.
Keywords: data storage, encryption, blockchain, data protection.

Вступ

Стрімкий технологічний розвиток призвів до переходу багатьох систем, а в результаті даних, якими оперують ці системи у цифровий формат. Це Різноманітні таблиці із даними, текстові дані, фото та відео. Процес контролю доступу до цих даних потребує особливої уваги не тільки у контексті підприємства, яке може втратити важливі дані, які є їх інтелектуальною власністю, державних установ, які працюють із конфіденційними даними, а також простих людей, які в епоху інтернет втрачають своє право на конфіденційність[1] та приватне життя.

Метою роботи є зменшення ймовірності компрометації файлів та втрати приватних даних.

Результати дослідження

Для забезпечення безпеки конфіденційної інформації, було вирішено використати комбінацію каскадного шифрування[2] – для захисту даних від крадіжки або неправомірного доступу та технології блокчейн для захисту від підміни даних у файлі.

Принцип каскадного шифрування може бути ілюстрований наступним чином:

Етап 1: шифрування Алгоритмом 1 з Ключем 1. Перші дані шифруються за допомогою першого алгоритму з використанням ключа 1.

Етап 2: шифрування Алгоритмом 2 з Ключем 2. Зашифровані дані з етапу 1 подаються на вхід другого алгоритму, який використовує другий ключ для шифрування і так далі.

Процес може продовжуватися каскадно, використовуючи більше етапів шифрування.

Для забезпечення захисту від підміни даних у файлі було використано наступний алгоритм.

Збереження Хешу Файлу. Спочатку користувач завантажує файл на систему. Після завантаження система автоматично обчислює хеш-суму цього файлу за допомогою криптографічних хеш-функцій, таких як SHA-256. Отриманий хеш-код потім записується в блокчейн. Блокчейн використовується для забезпечення недоступності зміни хешу, що дозволяє користувачу перевірити цілісність файлу у будь-який момент. Блоки з хешами об'єднуються у ланцюг, забезпечуючи безпеку та надій-

ність збереження інформації. Блок схему алгоритму шифрування файлів із використанням технології блокчейн та каскадного шифрування зображено на рисунку1.

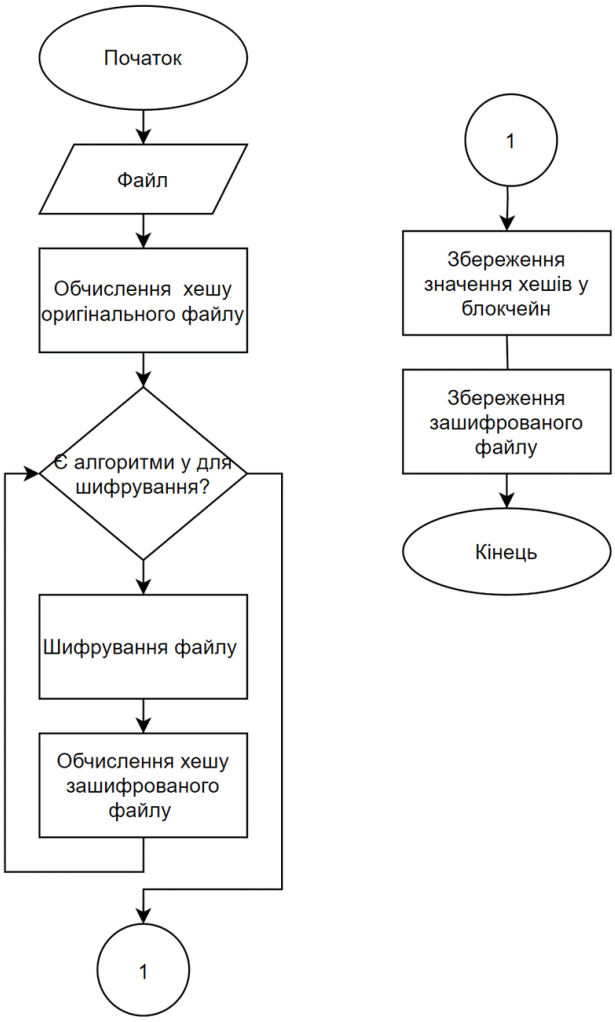

Рис. 1. Алгоритм шифрування файлів із використанням технології блокчейн та каскадного шифрування

Завдяки цьому двоетапному алгоритму захищеного збереження даних, користувачі можуть бути впевнені в безпеці та конфіденційності своєї інформації. Кожна взаємодія із файлами буде зафіксована в блокчейні, а шифрування гарантує, що навіть при потенційному порушенні безпеки, важлива інформація залишається недоступною для зловмисників.

Висновки

Запропонований підхід забезпечує безпеку конфіденційної інформації. Використаний алгоритм шифрування використовує каскадне шифрування з метою захисту від крадіжки або несанкціонованого доступу, а також технологію блокчейн для запобігання підміні даних у файлі.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Конфіденційна інформація [Електронний ресурс]: https://wiki.legalaid.gov.ua – Режим доступу: https://wiki.legalaid.gov.ua/index.php/Конфіденційна_інформація

2. David Wong. Real-World Cryptography, Manning (October 19, 2021), 399 p. ISBN 9781617296710

Сідак Степан Васильович — студент групи 1ІСТ-22м, кафедра автоматизації та інтелектуальних інформаційних технологій, Факультет інтелектуальних інформаційних технологій та автоматизації, Вінницький національний технічний університет, м.Вінниця, e-mail: 01-22-322.stud@vntu.vn.ua

Кулик Ярослав Анатолійович – доцент кафедри автоматизації та інтелектуальних інформаційних технологій, Факультет інтелектуальних інформаційних технологій та автоматизації, Вінницький національний технічний університет, м.Вінниця, e-mail: kulyk.y.a@vntu.edu.ua

Sidak Stepan V. – student of 1IST-22m group, Department of Automatization and Intelligent Information Technologies, Faculty of Intellectual Information Technologies and Automation, Vinnytsia National Technical University, Vinnytsia, E-mail: 01-22-322.stud@vntu. .vn.ua

Kulik Yaroslav A. – Associate Professor of the Department of Automation and Intellectual Information Technology, Faculty of Intellectual Information Technologies and Automation, Vinnytsia National Technical University, Vinnytsia, E-mail: kulyk.y.a@vntu.edu.ua