**Новак Б.В., гр. КІСП-21**
*Науковий керівник – Рак Т.Є.*

## Метод захисту каналів обміну інформацією з використанням блокчейн-технологій

**Стан проблеми.** Захист каналів обміну інформацією стає критично важливим через зростання кіберзагроз, таких як перехоплення та модифікація даних. Традиційні методи, як-от шифрування й аутентифікація, часто обмежені централізованою природою, що робить їх вразливими до атак на єдину точку відмови [1]. Блокчейн-технології забезпечують децентралізацію, підвищуючи стійкість до атак і прозорість змін даних. У цьому контексті блокчейн-технології набувають дедалі більшої популярності завдяки своїм унікальним властивостям децентралізації, прозорості та стійкості до змін даних [2]

**Розв'язання задачі.** Для вирішення проблеми захисту каналів обміну інформацією з використанням блокчейн-технологій, спочатку необхідно провести аналіз вимог та проектування системи. Це передбачає визначення специфікацій, включаючи вимоги до безпеки, швидкості передачі даних та масштабованості. На цьому етапі розробляється архітектура системи, яка включає блокчейн, вузли, протоколи зв’язку та методи шифрування

Однією з ключових частин розробки є механізм шифрування, який потрібно реалізувати для захисту даних під час їх передачі. Застосування шифрування даних забезпечує конфіденційність переданих відомостей. Навіть якщо зловмисник отримає доступ до мережі, шифровані дані будуть важкими для розшифрування. Криптографічні методи, такі як асиметричне шифрування, можуть бути використані для забезпечення безпеки транзакцій, що ще більше підвищує захищеність.

Важливо вибрати відповідну технологію блокчейн, яка найбільше підходить для реалізації запропонованого методу. Платформи, такі як Cosmos чи Near Protocol [3], забезпечують необхідні функції, зокрема підтримку смарт-контрактів, конфіденційність та швидкість обробки транзакцій.

Наступним етапом є інтеграція блокчейн-технологій у мережеві протоколи. Це передбачає розробку нових або адаптацію існуючих протоколів для забезпечення безперебійного обміну інформацією між учасниками системи. Механізми консенсусу відіграють ключову роль у забезпеченні безпеки та швидкості транзакцій у блокчейні. Серед них, найбільш відомими є алгоритми *Proof of Stake* (PoS) і *Proof of Work* (PoW). Вище згадані платформи

працюють на механізмі консенсусу PoS, оскільки він має високу пропускну здатність. Даний механізм меншує ризики атак на мережу, а також і знижує енергетичні витрати в порівнянні з PoW [4].

У структурній схемі (рис. 1) ключові елементи організовані так, що відображають основні аспекти процесу передачі та захисту інформації.

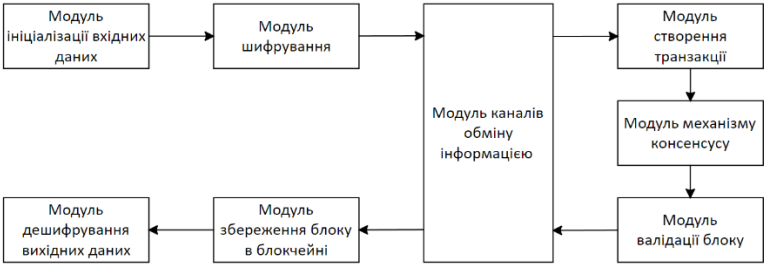


Рисунок. 1. Структурна схема програмної системи захисту каналів обміну інформацією з використанням блокчейн-технологій,

**Висновки.** У цій роботі розглянуто метод захисту каналів обміну інформацією за допомогою блокчейн-технологій. Запропоновано підхід до створення програмної системи, яка забезпечує захист даних під час їх передачі в мережі. Розроблена структурна схема системи відображає основні модулі, що включають управління блокчейном, шифрування інформації, а також верифікацію транзакцій.

**Література**


1. Nakamoto, S. (2008). Bitcoin: A Peer-to-Peer Electronic Cash System. Опис основної концепції блокчейна, яка стала основою для більшості сучасних блокчейн-інфраструктур.
2. Zheng, Z., Xie, S., Dai, H., Chen, X., & Wang, H. (2017). An overview of blockchain technology: Architecture, consensus, and future trends. IEEE International Congress on Big Data.
3. Iqra Sadia Rao, M. L. Mat Kiah, M. Muzaffar Hameed, Zain Anwer Memon (2024), Scalability of blockchain: a comprehensive review and future research direction
4. Snehlata, Pallavi Shukla, Ashutosh Kumar Singh, Saloni Tiwari, Rishabh & Vijay Kumar Dwivedi (2023). An Intelligent Blockchain-Oriented Digital Voting System Using NEAR Protocol