МОДЕЛЬ ЗАХИСТУ ДАНИХ У ДЕЦЕНТРАЛІЗОВАНІЙ ІНФРАСТРУКТУРІ ВІДКРИТИХ КЛЮЧІВ

Шафоростов М.О., Власов А.В.
Харківський національний університет радіоелектроніки, Харків, Україна

Як показує систематичний огляд літератури, присвяченої використанню технології блокчейн у кібербезпеці [1], криптографія з відкритим ключем – одна зі сфер, які добре підходять для нових застосовань блокчейна. Для забезпечення можливості надійно зв'язати відкритий ключ із його володільцем наразі здебільшого використовується ієрархічна інфраструктура відкритих ключів із довіреними центрами сертифікації (за стандартом X.509). Проте через централізовану архітектуру цій інфраструктурі властива проблема єдиної точки відмови, що зумовлює ризик припинення роботи всієї інфраструктури за компрометації кореневого центру сертифікації.

Мета доповіді – дослідження моделі захисту даних із використанням технології блокчейн, яка дозволяє реалізувати інфраструктуру відкритих ключів у децентралізований спосіб. У доповіді обґрунтовується одночасне використання двох розподілених баз даних (ланцюжка блоків і бібліотеки сертифікатів); розкриваються ролі учасників у системі, що застосовує досліджувану модель захисту даних; пояснюються особливості деяких модулів системи Bitcoin, які дають змогу забезпечити роботу інфраструктури відкритих ключів без центрів сертифікації. Також наводяться висновки щодо стійкості досліджуваної моделі захисту даних до хибних сертифікатних запитів, випереджальної реєстрації та шкідливої поведінки майнера [2].

Список літератури

1. Taylor P. J. A systematic literature review of blockchain cyber security. *Digital Comm. and Networks*. 2020. Т. 6, № 2. С. 147–156. DOI: https://doi.org/10.1016/j.dcan.2019.01.005.

2. B. Qin et al. Cecoin: A decentralized PKI mitigating MitM attacks. *Future Generation CS*. 2020. Т. 107. С. 805–815. DOI: https://doi.org/10.1016/j.future.2017.08.025.