ВПРОВАДЖЕННЯ ДЕЦЕНТРАЛІЗОВАНОЇ СИСТЕМИ ІДЕНТИФІКАЦІЇ

Власов А. В.
Харківський національний університет Повітряних Сил, Харків, Україна
Сєвєрінов О. В., Слиш О. В.
Харківський національний університет радіоелектроніки, Харків, Україна

Використання сучасних інформаційних технологій в повсякденному житті суспільства вимагає підвищення безпеки щодо персональних даних користувачів, в перше чергу щодо даних про фізичні характеристики (відбитки пальців, малюнок сітківки ока та інші) та їх цифрових аналогів (адреса електронної пошти, цифровий підпис тощо). Але існуючі в світі бази даних різних систем ідентифікації ніяк між собою не пов'язані і не синхронізовані. Таким чином, ми маємо ситуацію, коли однієї фізичної особи відповідає безліч умовних ідентифікаторів. Недоліками існуючих систем ідентифікації є: нераціональне використання ресурсів (користувач на кожному сервісі змушений витрачати час для реєстрації, використовувати ідентичні реєстраційні форми, логіни і паролі, підтверджувати реєстрацію за допомогою e-mail); недотримання політики обробки персональних даних (користувачі не мають уяви, що відбувається з їх персональними даними); постійно існує ризик розкрадання персональних даних користувача (при ідентифікації персональні дані передаються і обробляються в відкритому вигляді); недотримання політики безпеки (виникає необхідність в великій кількості ідентифікаторів і паролів).

Метою доповіді є аналіз сучасних систем цифрової ідентифікації та існуючих протоколів, які впроваджені для підвищення безпеки процедур цифрової ідентифікації. В доповіді розглянуті результати досліджень відомих сучасних протоколів OAuth, OpenID, OpenID Connect [1-3] з визначенням їх основних відмінностей, переваг та обмежень. Пропонується впровадити децентралізовані системи, які побудовано за технологією блокчейн, для створення розподіленої бази даних з мітками часу для кожної процедури ідентифікації з використанням користувачем свого власного ідентифікатору. Впровадження децентралізованої системи цифрової ідентифікації дозволить використовувати всі переваги багатофакторної автентифікації з обов'язковим етапом біометричної автентифікації користувачів (додаткова опція) та унеможливіть втручання в процедури ідентифікації (зміни їх історії).

Список літератури

1. Guide to Protecting the Confidentiality of Personally Identifiable Information (PII). NIST Special Publication 800-122.

2. OAuth 2.0 Authorization Framework. Internet Engineering Task Force (IETF). October 2012. - URL: https://tools.ietf.org/html/rfc6749

3. OpenID Authentication 2.0. - URL: https://openid.net/specs/openid-authentication-2_0.html.