АНОТАЦІЯ

Ісірова К. В. Моделі і методи побудови децентралізованих електронних довірчих послуг на основі технології blockchain та постквантової криптографії. — Кваліфікаційна наукова праця на правах рукопису

Дисертація на здобуття ступеня доктора філософії за спеціальністю 122 — Комп'ютерні науки (Галузь знань 12 — Інформаційні технології). – Харківський національний університет імені В. Н. Каразіна Міністерства освіти і науки України, Харків, 2021.

В сучасних умовах стрімкого розвитку електронних технологій, а також різкого збільшення користувачів відповідних систем, побудова довіри в online-середовищі виступає одним із ключових питань для забезпечення соціального та економічного розвитку суспільства. Основною метою України є не тільки впровадження повного спектру електронних довірчих послуг, а також забезпечення їхньої інтероперабельності та транскордоності з міжнародними системами. З іншого боку, прогрес у сфері квантових обчислень обумовлює значне зростання швидкості, що формує нові виклики для сучасних систем безпеки інформації.

Дисертаційна робота присвячена розв'язанню актуальної задачі: розробка моделей і методів забезпечення стійкості та резильєнтності систем електронних довірчих послуг у постквантовий період.

Мета і завдання дослідження. Метою дисертаційної роботи є розробка методів забезпечення надійної і безпечної роботи систем електронних довірчих за рахунок використання технології blockchain та постквантової криптографії.

Для досягнення поставленої мети були розв'язані наступні задачі.

1. Аналіз міжнародних вимог до криптоалгоритмів постквантового періоду.

2. Аналіз можливості використання децентралізованих технологій, зокрема технології blockchain, для забезпечення резильєнтності систем у постквантовий період.

3. Розробка моделі децентралізованої інфраструктури відкритих ключів на основі технології blockchain для використання у постквантовий період.

4. Розробка моделі децентралізованої системи електронного голосування на основі технології blockchain для використання у постквантовий період.

5. Аналіз методів криптографічних перетворень типу електронний підпис, на основі геш-функцій, що можуть бути застосованими у постквантовий період.

6. Розробка методу одноразових ключів на основі схеми Winternitz для постквантового періоду.

У першому розділі дисертації (E*лектроні довірчі послуги у сучасному світі*) на основі проведеного аналізу показано, що успіхи в галузі квантових обчислень формують нові виклики для сучасної криптографії та обумовлюють необхідність пошуку нових шляхів забезпечення безпеки інформації. Обґрунтовані основні напрямки розробок нових квантово-захищених алгоритмів. Показано, що на сьогоднішній день визначені основні напрямки розробок нових квантово-захищених алгоритмів: криптографічні перетворення на основі завадостійких кодів (CB-криптографія), перетворення на основі геш-функцій (HB-криптографія), криптографічні перетворення на решітках (LB-криптографія), мультіваріативно-квадратичні криптографічні перетворення (MQ-перетворення), а також використання ізогеніїв еліптичних кривих. Розкрито, що безпека систем може забезпечуватися не лише за рахунок криптостійкості примітивів, які покладені в її основу, а також шляхом впровадження відповідних організаційних, організаційно-технічних рішень та методів. Сформульоване поняття резильєнтності систем, а також показано як вона пов’язана із можливістю системи продовжувати функціонування навіть в умовах кібератак. Розкрита сутність моделей загроз для постквантового періоду, таких як IND-CCA2 (Indistinguishability under Adaptive Chosen Ciphertext Attack для алгоритмів шифрування та EUF-CMA (Existentially

unforgeable under adaptive chosen message attacks для алгоритмів електронного підпису.

У другому розділі дисертації *(Принципи використання розподілених технологій для забезпечення надійного надання електронних довірчих послуг)* показано, що децентралізовані системи здатні краще забезпечити функціонування електронних систем в умовах збільшення спектру електронних послуг та зростання кількості користувачів. Обґрунтовано, що для надійного функціонування децентралізованих систем, в тому числі у критичних інфраструктурах, можливе використання технології blockchain із децентралізованими протоколами консенсусу. Сформульовані рекомендації щодо використання децентралізованих протоколів консенсусу в залежності від типу та призначення цільової системи.

У третьому розділі дисертації *(Принципи побудови децентралізованої інфраструктури відкритих ключів)* розкриті основні недоліки існуючих інфраструктур відкритих ключів (ІВК), переважна більшість яких побудована за ієрархічним принципом із реалізацією відповідного ланцюга уповноважених органів (центрів сертифікації ключів). Базуючись на основі проведеного аналізу у розділі 2, у даному розділі наведена *удосконалена* модель децентралізованої інфраструктури відкритих ключів із використанням технології blockchain, яка відрізняється від існуючих тим, що дозволяє надійно реалізувати модель довіри, сконцентрованої навколо користувача, що дозволяє використовувати її для побудови системи електронного голосування. Описані переваги запропонованої децентралізованої системи, розроблені алгоритми для її функціонування, а саме: алгоритм первинної ідентифікації за умови генерації ключової пари в межах контрольованої зони довіреного вузла, алгоритм первинної ідентифікації за умови самостійної генерації ключової пари користувачем, алгоритм перевірки підпису, алгоритм оновлення статусу сертифіката та алгоритм оновлення сертифікату. Наведені результати часових оцінок для формування децентралізованої ІВК для двох топологій мереж.

В четвертому розділі дисертації *(Електронна система таємного голосування з використанням принципів розвитку децентралізованих*

технологій) проаналізовані основні та додаткові вимоги до електронних систем голосування, а також висвітлені загрози для систем такого типу. Обгрунтовано, що система електронного голосування охоплює процеси на чотирьох рівнях: правовий, організаційний, рівень процесів та технологічний. Наведена *удосконалена* модель системи електронного голосування, яка відрізняється від існуючих тим, що забезпечує формування деперсоналізованого списку виборців без використання сліпих підписів, що дозволяє спростити алгоритми взаємодії між сторонами. Запропонована дворівнева архітектура системи електронного голосування, яка дозволяє забезпечити процеси електронної ідентифікації за допомогою вже існуючих засобів, таких як BankID, MobileID, електронний підпис. Показано, що такий підхід дозволяє забезпечити інтероперабельність системи електронного голосування із розгорнутими в Україні системами електронної ідентифікації. Розроблені алгоритми та протоколи для децентралізованої системи електронного голосування, які впроваджені у комплексі для проведення досліджень криптографічних властивостей технології blockchain.

У п’ятому розділі дисертації *(Методи та механізми електронного підпису на геш-функціях для постквантового періоду)* наведені результати порівняльного аналізу алгоритмів квантово-захищенних електронних підписів (ЕП) на основі геш-функцій. Отримані експериментальні результати використання національного стандарту гешування ДСТУ 7564:2014 «Інформаційні технології. Криптографічний захист інформації. Функція гешування» в алгоритмі XMSS. Розкриті особливості одноразового механізму ЕП Lamport, особливості одноразового механізму ЕП Lamport-Diffie, а також ЕП Вінтерніц. Наведений удосконалений метод одноразових ключів Winternitz для постквантового періоду на основі геш-функцій, який відрізняється від існуючого модифікованими функціями зашифрування та перевірки, що дозволяє зменшити розміри особистого та відкритого ключів у 100 разів.

Ключові слова: постквантовий період, електронний підпис, децентралізована інфраструктура відкритих ключів, децентралізована система електронного голосування, технологія blockchain