Відгук отриманий 25.08.2021 головою спеціалізованої вченої ради ДФ 64.051.021 Валентин ЛАЗУРИК

Голові спеціалізованої вченої ради
ДФ 64.051.021
Харківського національного
університету імені В. Н. Каразіна
61022, майдан Свободи, 4, м. Харків

ВІДГУК

опонента, завідувача кафедри безпеки інформаційних технологій факультету кібербезпеки, комп'ютерної та програмної інженерії Національного авіаційного університету, доктора технічних наук, професора Корченка Олександра Григоровича на дисертаційну роботу Ісірової Катерини Володимирівни «Моделі і методи побудови децентралізованих електронних довірчих послуг на основі технології blockchain та постквантової криптографії», що подана на здобуття ступеня доктора філософії з галузі знань 12 – Інформаційні технології за спеціальністю 122 – Комп'ютерні науки.

Актуальність теми представленої дисертаційної роботи обумовлюється тим, що сучасний стан розвитку цифрового суспільства, зокрема сфери надання електронних довірчих послуг, потребує використання нових методів для забезпечення стійкості вже розгорнутих та перспективних систем. Системи надання електронних довірчих послуг відносяться до переліку об'єктів критичних інформаційних інфраструктур держави. Проте на фоні швидкої еволюції квантових технологій, яка обумовлює зростання швидкості обчислень, традиційні методи, надійність яких ґрунтується на використанні стійких криптоалгоритмів, вважаються недостатніми для забезпечення надійного та безперебійного функціонування критичних систем. Іншою особливістю, на яку слід звернути увагу є розширення спектру електронних довірчих послуг та зростання кількості користувачів в системах. На сьогоднішній день переважна більшість функціонуючих систем побудована за ієрархічним принципом, що стає неефективним архітектурним рішенням зважаючи на сучасні умови функціонування. Метою роботи Ісірової К. В. є розробка методів забезпечення надійної і безпечної роботи систем електронних довірчих послуг за рахунок використання технології blockchain та постквантової криптографії. Виходячи із вище зазначеного, дослідження, які відображені у дисертації є актуальними.

Ступінь обґрунтованості наукових положень, висновків і рекомендацій, сформульованих у дисертації.

Дисертаційна робота складається із вступу, п'яти розділів, висновків, списку використаних джерел та п'яти додатків. Загальний обсяг роботи складає 165 сторінок.

У першому розділі наводяться результати аналізу міжнародних вимог до криптоалгоритмів у постквантовий період, зокрема обґрунтовуються моделі загроз для двох найпоширеніших алгоритмів типу шифрування та електронний підпис.

У другому розділі дисертації розкриті основні принципи децентралізованого підходу для побудови систем електронних довірчих послуг із використанням технології blockchain. Надані рекомендації щодо вибору децентралізованих протоколів консенсусу в залежності від вимог, які висуваються до системи.

Третій розділ присвячений розробці моделі децентралізованої інфраструктури відкритих ключів (ІВК). В ньому представлена відповідна модель із використанням технології blockchain та розкриті її переваги. Також наведені результати часових оцінок для формування blockchain-based ІВК.

На базі розробленої моделі децентралізованої ІВК, *у четвертому розділі* будується модель електронної системи голосування, яка представляє собою дворівневу архітектуру із двох неперетинаючихся мереж blockchain. У розділі, також, надані відповідні протоколи та алгоритми взаємодії між учасниками на чотирьох рівнях: нормативний, організаційний, рівень процесів, технологічний. Показано, що такий підхід дозволяє забезпечити інтероперабельність системи електронного голосування із розгорнутими в Україні системами електронної ідентифікації.

П'ятий розділ містить результати порівняльного аналізу алгоритмів електронних підписів (ЕП) на основі геш-функцій, які є перспективними у постквантовий період, експериментальні результати реалізації запропонованого алгоритму із національним стандартом гешування. Також у даному розділі наведений удосконалений постквантовий алгоритм одноразових ключів, який дозволяє суттєво зменшити розміри особистого та відкритого ключів.

Наукова новизна отриманих результатів полягає у наступному:

1. *Удосконалена* модель децентралізованої інфраструктури відкритих ключів на основі технології blockchain, яка дозволяє надійно реалізувати модель довіри, сконцентрованої навколо користувача, та дозволяє використовувати її для побудови системи електронного голосування.
2. *Удосконалена* модель системи електронного голосування, яка забезпечує формування деперсоналізованого списку виборців без використання сліпих підписів, та дозволяє спростити алгоритми взаємодії між сторонами.
3. *Удосконалений* метод одноразових ключів Winternitz для постквантового періоду на основі геш-функцій, який за рахунок модифікованих функцій зашифрування та перевірки, дозволяє зменшити розміри особистого та відкритого ключів у 100 разів.

Практичне значення отриманих результатів полягає у наступному:

- розроблене програмне забезпечення для проведення симуляцій для визначення часу формування децентралізованої інфраструктури відкритих ключів для різних топологій мереж;
- розроблені алгоритми та протоколи для децентралізованої системи електронного голосування, що впроваджені у комплексі проведення досліджень криптографічних властивостей технології blockchain;
- отримані експериментальні результати використання національного стандарту гешування ДСТУ 7564:2014 «Інформаційні технології. Криптографічний захист інформації. Функція гешування» в алгоритмі XMSS.

Наукові результати отримані за допомогою коректного використання обраних методів дослідження, а саме: методів теорії чисел, теорії груп, полів, кілець, методів системного аналізу і прийняття рішень та методів структурного і математичного моделювання, що підтверджує їхню достовірність.

Повнота викладу в наукових публікаціях, що відповідають темі дисертації

Дослідження були представленні у 22 наукових працях, серед яких 6 статей у наукових фахових виданнях України, 1 стаття у періодичному науковому виданні країни Організації економічного співробітництва та розвитку, включеному до наукометричної бази Scopus і **12** праць, які засвідчують апробацію матеріалів дисертації.

Наведені в дисертації результати є новими, робота не містить запозичених висновків інших авторів без наведення належних посилань на їх дослідження, що **відповідає вимогам академічної доброчесності**.

Загалом можна оцінити високу значимість отриманих у дисертації результатів, які можуть бути використані, як при розгортанні нових систем надання електронних довірчих послуг, так і при модернізації вже існуючих. Проте необхідно звернути увагу на певні **дискусійні положення та зауваження:**

1) в першому та другому пункті наукової новизни не зазначено за рахунок чого досягається визначений ефект;
2) при описі дворівневої архітектури системи електронного голосування не роз'яснено яким чином представники нижньої мережі blockchan передають Агенству до верхньої мережі дані про списки легітимних виборців;
3) у першому розділі дисертації зазначено, що виділяється п'ять сімейств крипто примітивів, які можуть розглядатися як перспективні у постквантовий період, проте в п'ятому експериментальному розділі не наведено пояснень, чому саме були обрані примітиви на основі геш-функцій.

Наведені зауваження не є критичними та не можуть впливати на загальний позитивний висновок про роботу.

Загальний висновок. Дисертаційна робота Ісірової К. В. «Моделі і методи побудови децентралізованих електронних довірчих послуг на основі технології blockchain та постквантової криптографії» **є завершеним, самостійним науковим дослідженням, яке є актуальним та має наукову і практичну значимість**. Структура та обсяг дисертації відповідають встановленим нормам, а зміст – поставленій меті. Тема роботи відповідає спеціальності 122 – Комп'ютерні науки. Вимоги «Тимчасового порядку присудження ступеня доктора філософії», затвердженого постановою Кабінету міністрів України від 06.03.2019 р. №167 (зі змінами), наказу Міністерства освіти і науки України від 12.01.2017 р. № 40 «Про затвердження вимог до оформлення дисертацій» **дотримано.**

Вважаю, що Ісірова Катерина Володимирівна заслуговує на присудження ступеня доктора філософії з галузі знань 12 – Інформаційні технології за спеціальністю 122 – Комп'ютерні науки.

25.08.2021 р.

Опонент:

завідувач кафедри безпеки
інформаційних технологій
факультету кібербезпеки,
комп'ютерної та програмної
інженерії Національного
авіаційного університету, лауреат
Державної премії України в галузі
науки і техніки,
доктор технічних наук,
професор

Олександр КОРЧЕНКО

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ * НАЦІОНАЛЬНИЙ АВІАЦІЙНИЙ УНІВЕРСИТЕТ * 01132330 * МІСТО КИЇВ

Підпис гр. Корченка О.
засвідчую
Вчений секретар
Національного авіаційного університету
М. Мелешкін