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 комп'ютерних систем, мереж і кібербезпеки факультету радіоелектроніки, комп'ютерних систем та інфокомунікацій Національного аерокосмічного університету імені М. Є. Жуковського «Харківський авіаційний інститут», доктора технічних наук, професора Харченко Вячеслава Сергійовича 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.

1. Актуальність обраної теми. Забезпечення надійного та безпечного функціонування систем надання електронних довірчих послуг, зокрема, системи електронної ідентифікації та інфраструктури відкритих ключів, є невід'ємною умовою побудови і виконання успішних транзакцій в online-середовищі.

Традиційно канал зв'язку для взаємодії розглядався як надійний за умови використання стійких криптоалгоритмів. Проте внаслідок зростання швидкості обчислень, обумовленого динамічним розвитком квантових технологій, таке припущення збільшує ризики неточного оцінювання і виконання вимог до безпеки. Отже необхідні системні рішення з використанням модерних методів, які б толерували ці виклики.

Це обумовлює актуальність теми досліджень, мета якої сформульована авторкою як розробка методів забезпечення надійної і безпечної роботи систем електронних довірчих послуг за рахунок використання технології blockchain та постквантової криптографії.

2. Ступінь обґрунтованості наукових положень, висновків і рекомендацій, сформульованих у дисертації. Дисертація Ісірової К. В. містить вступ, п'ять розділів, висновки, список використаних джерел та п'ять додатків. Загальний обсяг роботи складає 165 сторінок.

У першому розділі дисертації проведений аналіз національних і міжнародних вимог до криптоалгоритмів постквантового періоду. На основі його результатів обґрунтована необхідність пошуку нових шляхів забезпечення безпеки систем надання електронних довірчих послуг, які за певних умов можуть бути віднесені до критичних. Визначено, що їх безпека може забезпечуватися не лише за рахунок криптостійкості примітивів, але і з

використанням організаційно-технічних методів. Показано, що за умови забезпечення безпеки інформації, яка обробляється в системі лише за рахунок підвищення параметрів стійкості, можуть виникати ситуації значного ускладнення протоколів взаємодії між користувачами або внесення надмірності в розгорнуту систему захисту. Обґрунтовано необхідність задіяння поняття резильєнтності систем, що охоплює додаткові властивості, пов'язані із можливістю системи продовжувати функціонування навіть в умовах кібератак.

Зауваження: на наш погляд, поняття резильєнтності визначено недостатньо чітко. Визначення надається суто через шляхи її забезпечення («…здатність системи бути надійною не лише за рахунок використання надійних (стійких) криптопримітивів, а також за рахунок розгорнутих архітектурних рішень та впроваджених нових технологій», стор. 29). Здається, доцільно було б зробити в цій частині аналізу посилання на відповідні стандарти NIST (наприклад, https://www.nist.gov/news-events/news/2019/09/cyber-resiliency-engineering-final-public-draft-nist-sp-800-160-volume-2).

У другому розділі дисертації досліджено, яким чином децентралізований підхід, зокрема, технологія blockchain, може бути використана для забезпечення резильєнтності систем електронних довірчих послуг у постквантовий період, а також надано рекомендації щодо використання децентралізованих протоколів консенсусу в залежності від призначення та функціональних особливостей цільової системи.

Зауваження: при проведенні порівняльного аналізу децентралізованих протоколів консенсусу не взяті до уваги гібридні протоколи консенсусу, які можуть поєднувати властивості різних груп.

У третьому розділі удосконалено модель децентралізованої інфраструктури відкритих ключів (ІВК) на основі технології blockchain. Обґрунтовано її відмінності, показано, що вона дозволяє надійно реалізувати модель довіри, сконцентровану навколо користувача, і використовувати її для побудови системи електронного голосування. Наведено результати експериментальних оцінок часу формування децентралізованої ІВК для різних топологій мереж. Доведено також, що застосування технології blockchain дозволить полегшити перехід на постквантові алгоритми підписів завдяки раціональному управлінню сертифікатами відкритих ключів.

Зауваження: при проведені часових оцінок децентралізованої ІВК досліджено обмежений клас топологій мереж, які частково відображають спектр реальних систем. Внаслідок цього результати експериментів не можуть бути легко апроксимовані на довільну топологію.

Четвертий розділ присвячений розробці дворівневої архітектури системи електронного голосування, яка є сумісною із запропонованою вище децентралізованою ІВК. Обґрунтовано, що система електронного голосування охоплює процеси на чотирьох рівнях:

нормативному, організаційному, процесному, технологічному. Розроблено відповідні алгоритми та протоколи, що дозволяє зробити висновок про створення системи електронного голосування, яка забезпечує формування деперсоналізованого списку виборців без використання сліпих підписів.

Зауваження: результати практичної реалізації та їх впровадження слід було б подати більш системно з визначенням кількісних показників.

У п'ятому розділі досліджено методи криптографічних перетворень типу електронний підпис, на основі геш-функцій, що можуть бути застосованими у постквантовий період, отримано експериментальні результати використання національного стандарту гешування ДСТУ 7564:2014 «Інформаційні технології. Криптографічний захист інформації. Функція гешування» в алгоритмі XMSS. Обґрунтовано складові методу одноразових ключів Winternitz для постквантового періоду на основі геш-функцій. Він відрізняється модифікованими функціями зашифрування та перевірки, що дозволяє зменшити розміри особистого та відкритого ключів у 100 разів.

Зауваження: результати цього розділу є ключовими, але б доцільно було б запропонувати інтегровану послідовність використання і взаємозв'язку всіх запропонованих моделей і методів.

В цілому основні положення і висновки обґрунтовані. Достовірність отриманих наукових результатів підтверджується коректністю використання сучасних методів досліджень (методи системного аналізу та прийняття рішень, методи теорії чисел, теорії груп, полів, кілець, методи структурного та математичного моделювання), а також практичним впровадженням результатів. Крім того, отримано експериментальні результати використання національного стандарту гешування ДСТУ 7564:2014 «Інформаційні технології. Криптографічний захист інформації. Функція гешування» в алгоритмі XMSS.

3. Наукова новизна результатів досліджень полягає у наступному:

- удосконалено модель децентралізованої інфраструктури відкритих ключів на основі технології blockchain, яка відрізняється від відомих тим, що реалізує модель довіри, сконцентрованої навколо користувача, що надає змогу використовувати її для побудови системи електронного голосування;
- удосконалено модель системи електронного голосування, яка відрізняється від відомих тим, що забезпечує формування деперсоналізованого списку виборців без використання сліпих підписів, що спрощує алгоритми взаємодії між сторонами;
- удосконалено метод одноразових ключів Winternitz для постквантового періоду на основі геш-функцій, який відрізняється від існуючого модифікованими функціями зашифрування та перевірки і зменшує розміри особистого та відкритого ключів на один-два порядки.

Формулювання наукової новизни в цілому співпадає з авторською за виключенням деяких стилістичних та мовних відмінностей і коректівів.

4. Повнота викладу результатів у наукових публікаціях, що відповідають темі дисертації. Нові наукові результати достатньо повно викладено у 7 статтях, із яких 6 статей у фахових наукових журналах, які входять до переліку МОН України, та 1 стаття в науковому закордонному виданні, включеному до наукометричної бази Scopus. Загальна кількість публікацій – 22, серед яких 6 індексовано Scopus.

5. Практичне значення результатів полягає у тому, що розроблено програмне забезпечення для проведення симуляції і визначення часу формування децентралізованої інфраструктури відкритих ключів для різних мережних топологій. Крім того, розроблені алгоритми та протоколи для децентралізованої системи електронного голосування, впроваджені у комплексі для проведення досліджень криптографічних властивостей технології blockchain.

Результати дисертаційних досліджень впровадженні у ПАТ «Інститут інформаційних технологій», м. Харків (акт від 11.09.2020 р.) і навчальному процесі (акт від 10.09.2020 р.).

6. Оцінка академічної доброчесності. Після вивчення тексту дисертації та ознайомлення із науковими працями можна зробити висновок, що робота виконана самостійно та не містить ознак порушення академічної доброчесності.

7. Зауваження та недоліки. Частину зауважень надано в розділі 2. Крім того, слід зазначити наступне:

1) структурування дисертації та розподіл матеріалу по розділах не є бездоганним. Перший розділ мав би більш чітко визначити методику проведення досліджень. Розділи 2 і 3 мають питому частину матеріалів оглядового характеру, які тяжіють до розділу 1;

2) є вади оформлення, якості графічних матеріалів. Пояснення до деяких рисунків надано дуже стисло, без детальних пояснень. Це стосується, зокрема, рис. 1.3. З іншого боку, частина рисунків має ілюстративний характер і могла б не використовуватися взагалі;

3) кращою могла б бути критеріальна частина дисертації. Йдеться про резильєнтність, але відповідні показники чітко не визначені, обмеження не сформульовані і кількісні оцінки системно не надані. Є певна неузгодженість в термінології та співвідношенні понять (надійність, безпечність і резільєнтність);

Наведені зауваження не знижують наукової цінності роботи і не впливають на позитивний висновок.

8. Висновки. Дисертаційна робота Ісірової К.В. «Моделі і методи побудови децентралізованих електронних довірчих послуг на основі технології blockchain та постквантової криптографії» є завершеним науковим дослідженням, виконаним за актуальною тематикою, та має наукову і практичну значимість. Тема і зміст роботи

відповідають 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) дотримано. Дисертація оформлена у відповідності із наказом Міністерства освіти і науки України від 12.01.2017 р. № 40 «Про затвердження вимог до оформлення дисертацій».

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

27.08.2021 р.

Опонент
завідувач кафедри комп'ютерних систем, мереж і кібербезпеки факультету радіоелектроніки, комп'ютерних систем та інфокомунікацій Національного аерокосмічного університету ім. М. Є. Жуковського «Харківський авіаційний інститут»
Лауреат Державної премії України у галузі науки і техніки,
заслужений винахідник України,
доктор технічних наук, професор — Вячеслав ХАРЧЕНКО

Підпис професора Харченка Вячеслава Сергійовича засвідчую
Вчений секретар Вченої ради Національного аерокосмічного університету ім. М. Є. Жуковського «Харківський авіаційний інститут»
кандидат філософських наук, доцент — С. Є. Чмихун

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ * НАЦІОНАЛЬНИЙ АЕРОКОСМІЧНИЙ УНІВЕРСИТЕТ ІМ. М. Є. ЖУКОВСЬКОГО "ХАРКІВСЬКИЙ АВІАЦІЙНИЙ ІНСТИТУТ" * №02066769 *