Облікова картка дисертації

I. Загальні відомості

Державний обліковий номер: 0821U102351

Особливі позначки: відкрита

Дата реєстрації: 29-09-2021

Статус: Захищена

Реквізити наказу МОН / наказу закладу:

II. Відомості про здобувача

Власне Прізвище Ім'я По-батькові:

1. Ісірова Катерина Володимирівна

2. Isirova Kateryna Volodymyrivna

Кваліфікація:

Ідентифікатор ORCID ID: Не застосовується

Вид дисертації: доктор філософії

Аспірантура/Докторантура: так

Шифр наукової спеціальності: 122

Назва наукової спеціальності: Комп'ютерні науки

Галузь / галузі знань:

Освітньо-наукова програма зі спеціальності: Не застосовується

Дата захисту: 10-09-2021

Спеціальність за освітою: Безпека інформаційних і комунікаційних систем

Місце роботи здобувача: Приватне акціонерне товариство "Інститут інформаційних технологій"

Код за ЄДРПОУ: 22723472

Місцезнаходження: вул. Бакуліна, буд. 12, м. Харків, Харківський р-н., Харківська обл., 61166, Україна

Форма власності:

Сфера управління: Держадміністрація

Ідентифікатор ROR: Не застосовується

III. Відомості про організацію, де відбувся захист

Шифр спеціалізованої вченої ради (разової спеціалізованої вченої ради): ДФ 64.051.021

Повне найменування юридичної особи: Харківський національний університет імені В. Н. Каразіна

Код за ЄДРПОУ: 02071205

Місцезнаходження: майдан Свободи, буд. 4, м. Харків, Харківський р-н., Харківська обл., 61022, Україна

Форма власності:

Сфера управління: Міністерство освіти і науки України

Ідентифікатор ROR: Не застосовується

IV. Відомості про підприємство, установу, організацію, в якій було виконано дисертацію

Повне найменування юридичної особи: Харківський національний університет імені В. Н. Каразіна

Код за ЄДРПОУ: 02071205

Місцезнаходження: майдан Свободи, буд. 4, м. Харків, Харківський р-н., Харківська обл., 61022, Україна

Форма власності:

Сфера управління: Міністерство освіти і науки України

Ідентифікатор ROR: Не застосовується

V. Відомості про дисертацію

Мова дисертації:

Коди тематичних рубрик: 50.41.25

Тема дисертації:

1. Моделі і методи побудови децентралізованих електронних довірчих послуг на основі технології blockchain та постквантової криптографії

2. Models and Methods of Development of Decentralized Electronic Trust Services Based on Blockchain Technology and Post-Quantum Cryptography

Реферат/анотація:

1. Дисертаційна робота присвячена розв'язанню актуальної задачі: розробка моделей і методів забезпечення стійкості та резильєнтності систем електронних довірчих послуг у постквантовий період. Метою дисертаційної роботи є розробка методів забезпечення надійної і безпечної роботи систем електронних довірчих за рахунок використання технології blockchain та постквантової криптографії. Обґрунтовані основні напрямки розробок нових квантово-захищених алгоритмів, показано, що децентралізовані системи здатні краще забезпечити функціонування електронних систем в умовах збільшення спектру електронних послуг та зростання кількості користувачів, удосконалена модель децентралізованої інфраструктури відкритих ключів із використанням технології blockchain, удосконалена модель системи електронного голосування, яка відрізняється від існуючих тим, що забезпечує формування деперсоналізованого списку виборців без використання сліпих підписів, удосконалений метод одноразових ключів Winternitz.

2. The dissertation is devoted to the actual problem solution: models and methods of ensuring the stability and resilience of electronic trust services in the post-quantum period development. The dissertation's purpose is to develop methods to ensure reliable and secure electronic trust systems operation through the use of blockchain technology and post-quantum cryptography. In the dissertation the main directions of new quantum-safe algorithms development are substantiated, it is shown that decentralized systems are able to better ensure the functioning of electronic systems in terms of increasing the range of electronic services and increasing the number of users, an improved model of decentralized Public Key Infrastructure is provided, an improved model of the electronic voting system, which differs from the existing ones in that it forms a depersonalized voter list without using blind signatures is presented, and an improved method of Winternitz one-time keys is developed.

Державний реєстраційний номер ДіР:

Пріоритетний напрям розвитку науки і техніки:

Стратегічний пріоритетний напрям інноваційної діяльності:

Підсумки дослідження:

Публікації:

Наукова (науково-технічна) продукція:

Соціально-економічна спрямованість:

Охоронні документи на ОПІВ:

Впровадження результатів дисертації:

Зв'язок з науковими темами:

VI. Відомості про наукового керівника/керівників (консультанта)

Власне Прізвище Ім'я По-батькові:

1. Потій Олександр Володимирович
2. Potii Oleksandr Volodymyrovych

Кваліфікація: д. т. н., 05.13.21

Ідентифікатор ORCID ID: Не застосовується

Додаткова інформація:

Повне найменування юридичної особи:

Код за ЄДРПОУ:

Місцезнаходження:

Форма власності:

Сфера управління:

Ідентифікатор ROR: Не застосовується

VII. Відомості про офіційних опонентів та рецензентів

Офіційні опоненти

Власне Прізвище Ім'я По-батькові:

1. Корченко Олександр Григорович

2. Korchenko Oleksandr Grigorovych

Кваліфікація: д. т. н., 05.13.21

Ідентифікатор ORCID ID: Не застосовується

Додаткова інформація:

Повне найменування юридичної особи:

Код за ЄДРПОУ:

Місцезнаходження:

Форма власності:

Сфера управління:

Ідентифікатор ROR: Не застосовується

Власне Прізвище Ім'я По-батькові:

1. Харченко Вячеслав Сергійович

2. Kharchenko Vyacheslav Serhiyovych

Кваліфікація: д. т. н., 20.02.14

Ідентифікатор ORCID ID: Не застосовується

Додаткова інформація:

Повне найменування юридичної особи:

Код за ЄДРПОУ:

Місцезнаходження:

Форма власності:

Сфера управління:

Ідентифікатор ROR: Не застосовується

Рецензенти

Власне Прізвище Ім'я По-батькові:

1. Олійников Роман Васильович Роман Васильович

2. Oliynykov Roman Vasylovych

Кваліфікація: д. т. н., 05.13.21

Ідентифікатор ORCID ID: Не застосовується

Додаткова інформація:

Повне найменування юридичної особи:

Код за ЄДРПОУ:

Місцезнаходження:

Форма власності:

Сфера управління:

Ідентифікатор ROR: Не застосовується

Власне Прізвище Ім'я По-батькові:

1. Нарєжній Олексій Павлович

2. Narezhniy Oleksiy Pavlovnch

Кваліфікація: к. т. н., 05.12.17

Ідентифікатор ORCID ID: Не застосовується

Додаткова інформація:

Повне найменування юридичної особи:

Код за ЄДРПОУ:

Місцезнаходження:

Форма власності:

Сфера управління:

Ідентифікатор ROR: Не застосовується

VIII. Заключні відомості

Власне Прізвище Ім'я По-батькові голови ради Лазурик Валентин Тимофійович

Власне Прізвище Ім'я По-батькові головуючого на засіданні Лазурик Валентин Тимофійович

Відповідальний за підготовку облікових документів

Реєстратор

Керівник відділу УкрІНТЕІ, що є відповідальним за реєстрацію наукової діяльності Юрченко Т.А.