Облікова картка дисертації

I. Загальні відомості

Державний обліковий номер: 0415U001837

Особливі позначки: відкрита

Дата реєстрації: 23-04-2015

Статус: Захищена

Реквізити наказу МОН / наказу закладу:

II. Відомості про здобувача

Власне Прізвище Ім'я По-батькові:

1. Літава Гжегож Владислав

2. Litawa Grzegorz Wladyslaw

Кваліфікація:

Ідентифікатор ORCID ID: Не застосовується

Вид дисертації: кандидат наук

Аспірантура/Докторантура: так

Шифр наукової спеціальності: 05.13.06

Назва наукової спеціальності: Інформаційні технології

Галузь / галузі знань: Не застосовується

Освітньо-наукова програма зі спеціальності: Не застосовується

Дата захисту: 31-03-2015

Спеціальність за освітою: 8.04020101

Місце роботи здобувача:

Код за ЄДРПОУ:

Місцезнаходження:

Форма власності:

Сфера управління:

Ідентифікатор ROR: Не застосовується

III. Відомості про організацію, де відбувся захист

Шифр спеціалізованої вченої ради (разової спеціалізованої вченої ради): К 58.052.06

Повне найменування юридичної особи: Тернопільський національний технічний університет імені Івана Пулюя

Код за ЄДРПОУ: 05408102

Місцезнаходження: вул. Руська, 56, м. Тернопіль, Тернопільський р-н., Тернопільська обл., 46001, 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: Тернопільський національний технічний університет імені Івана Пулюя

Код за ЄДРПОУ: 05408102

Місцезнаходження: м. Тернопіль, вул. Руська, 56

Форма власності:

Сфера управління: Міністерство освіти і науки України

Ідентифікатор ROR: Не застосовується

V. Відомості про дисертацію

Мова дисертації:

Коди тематичних рубрик: 28.21.19

Тема дисертації:

1. Моделі та засоби підвищення живучості інформаційно-управляючих систем на основі еліптичних кривих

2. Models and devices of improving survivability of the information control systems based on elliptic curves

Реферат:

1. Дисертація стосується удосконалення моделей та засобів підвищення живучості інформаційно-управляючих систем на основі еліптичних кривих (ІУСЕК) з врахуванням дефектів зовнішніх впливів за ознаками ймовірності та детермінованості. Розроблено моделі засобів та технології обчислень на еліптичних кривих (ЕК) із використанням теоретико-числових базисів Радемахера-Крестенсона для підвищення продуктивності обчислювальних методик здійснення основних операцій на ЕК у пристроях ІУСЕК. Створено апаратно-програмні засоби для виконання обчислень на ЕК і розв'язання дискретного логарифма вищої швидкодії із реалізацією паралельного ро-методу Полларда для живучих ІУСЕК.

2. The thesis focuses on the perfection of models and devices of improving survivability information control systems based on elliptic curves (ICSEC) considering the interaction faults based on probability and determinism.

Works on research and evaluation of survivability of ICSEC, based on the constructed models, which only increases the speed of basic calculations on elliptic curve (EC). Presents an analysis of evaluation models of survivability of ICSEC. Gives an overview of the main EC types in cryptography systems used in ICSEC. Shown the importance of the speed of solving the discrete logarithm for survivability of cryptographic systems.

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. Карпінський Микола Петрович
2. Karpinskyi Mykola Petrovych

Кваліфікація: д.т.н., 05.11.05

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. Алєксандер Марек Богуслав
2. Aleksander Marek Boguslav

Кваліфікація: к.т.н., 05.09.03

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. Козлюк Ірина Олексіївна

2. Козлюк Ірина Олексіївна

Кваліфікація: д.т.н., 05.13.06

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. Петров Олександр Степанович

2. Петров Олександр Степанович

Кваліфікація: д.т.н., 05.22.07

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. Рябий Мирослав Олександрович

2. Рябий Мирослав Олександрович

Кваліфікація: к.т.н., 05.13.06

Ідентифікатор ORCID ID: Не застосовується

Додаткова інформація:

Повне найменування юридичної особи:

Код за ЄДРПОУ:

Місцезнаходження:

Форма власності:

Сфера управління:

Ідентифікатор ROR: Не застосовується

Рецензенти

VIII. Заключні відомості

Власне Прізвище Ім'я По-батькові голови ради Приймак Микола Володимирович

Власне Прізвище Ім'я По-батькові головуючого на засіданні Приймак Микола Володимирович

Відповідальний за підготовку облікових документів

Реєстратор

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