Облікова картка дисертації

I. Загальні відомості

Державний обліковий номер: 0415U001796

Особливі позначки: відкрита

Дата реєстрації: 04-08-2015

Статус: Захищена

Реквізити наказу МОН / наказу закладу:

II. Відомості про здобувача

Власне Прізвище Ім'я По-батькові:

1. Макутоніна Лідія Вікторівна
2. Makutonina Lidiia Viktorivna

Кваліфікація:

Ідентифікатор ORCID ID: Не застосовується

Вид дисертації: кандидат наук

Аспірантура/Докторантура: так

Шифр наукової спеціальності: 05.13.21

Назва наукової спеціальності: Системи захисту інформації

Галузь / галузі знань: Не застосовується

Освітньо-наукова програма зі спеціальності: Не застосовується

Дата захисту: 24-03-2015

Спеціальність за освітою: 8.160101

Місце роботи здобувача: Харківський національний університет радіоелектроніки

Код за ЄДРПОУ: 02071197

Місцезнаходження: 61166, м. Харків, пр. Науки, 14

Форма власності:

Сфера управління: Міністерство освіти і науки України

Ідентифікатор ROR: Не застосовується

III. Відомості про організацію, де відбувся захист

Шифр спеціалізованої вченої ради (разової спеціалізованої вченої ради): К 64.052.05

Повне найменування юридичної особи: Харківський національний університет радіоелектроніки

Код за ЄДРПОУ: 02071197

Місцезнаходження: проспект Науки, 14, м. Харків, Харківський р-н., Харківська обл., 61166, 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 радіоелектроніки

Код за ЄДРПОУ: 02071197

Місцезнаходження: 61166, м. Харків, пр. Науки, 14

Форма власності:

Сфера управління: Міністерство освіти і науки України

Ідентифікатор ROR: Не застосовується

V. Відомості про дисертацію

Мова дисертації:

Коди тематичних рубрик: 50.37.23

Тема дисертації:

1. Методи та моделі криптографічних перетворень з доказовою стійкістю, які засновані на ідентифікаторах та алгебраїчних решітках

2. Methods and models of cryptographic transformations with proven resistance, which is based on an identity and algebraic lattices

Реферат/анотація:

1. У дисертації запропоновано та обґрунтовано методику оцінки гібридних методів направленого шифрування на ідентифікаторах за сукупністю умовних і безумовних критеріїв та показників оцінки, застосування якої дозволяє отримати оцінки стійкості як відносно окремих атак, так і за інтегральним критерієм. Запропоновано гібридний метод направленого шифрування на ідентифікаторах та алгебраїчних решітках та його програмну модель, для застосування в криптографічних механізмах і протоколах, який відрізняється від існуючих тим, що використання моделі на алгебраїчній решітці дозволило довести експоненціальну складність криптоаналізу методом повного розкриття, а також підвищити швидкодію криптографічного перетворення на 2-3 порядки. Отримані результати впроваджено до навчального процесу Харківського національного університету радіоелектроніки, а також в Акціонерному товаристві "Інститут інформаційних технологій".

2. In the thesis proposed and proved methods of assessment methods directional hybrid encryption identifier for a set of conditional and unconditional criteria and indicators for assessing the use of which allows you to assess the stability, both in terms of individual attacks, and by a combined criterion.The dissertation is devoted to solving important scientific and technical task - the development of the combined method Identity-Based Encryption from Lattices and its programming model, for use in cryptographic mechanisms and protocols, which differs from the current that models based on algebraic lattice can bring exponential complexity of cryptanalysis method of full-disclosure, and improve the performance of cryptographic conversion to 2-3 orders of magnitude. Results of dissertations were introduced in educational process of the Kharkiv National University of Radio Electronics and AT "Institute of Information technologies".

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. Горбенко Іван Дмитрович
2. Gorbenko Ivan Dmytrovych

Кваліфікація: д.т.н., 20.01.09

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. Толюпа Сергій Васильович

2. Толюпа Сергій Васильович

Кваліфікація: д.т.н., 05.12.02

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. Неласа Ганна Вікторівна

2. Неласа Ганна Вікторівна

Кваліфікація: к.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

Рецензенти

VIII. Заключні відомості

Власне Прізвище Ім'я По-батькові голови ради Горбенко Іван Дмитрович

Власне Прізвище Ім'я По-батькові головуючого на засіданні Горбенко Іван Дмитрович

Відповідальний за підготовку облікових документів

Реєстратор

Керівник відділу УкрІНТЕІ, що є відповідальним за реєстрацію наукової діяльності



Юрченко Т.А.