Облікова картка дисертації

I. Загальні відомості

Державний обліковий номер: 0411U001005

Особливі позначки: відкрита

Дата реєстрації: 06-01-2011

Статус: Захищена

Реквізити наказу МОН / наказу закладу:

II. Відомості про здобувача

Власне Прізвище Ім'я По-батькові:

1. Широков Олексій Вікторович
2. Alexey Shyrokov

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: 09-12-2010

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:

Код за ЄДРПОУ:

Місцезнаходження:

Форма власності:

Сфера управління:

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: 81.14.11.05

Тема дисертації:

1. Методи формування S-блокових конструкцій випадкового типу з покращеними показниками стійкості для блокових симетричних шифрів

2. Methods of forming S-block structures of a random type with improved security indiators for block symmetric ciphers

Реферат:

1. Об'єкт - процеси криптографічних перетворень з використанням блокових симетричних шифрів; мета полягає в розробці методів формування S-блоків випадкового типу з покращеними показниками стійкості для БСШ; методи теорії ймовірностей, математичної статистики, комбінаторики; новизна - вперше розроблені нові методи формування S-блоків, що враховують крипт. показники стійкості проти атак дифф. та лін. криптоаналізу; результати - запропоновані методи відбору підстановок, що дозволяють покращити показники шифрів; впроваджено в діяльність ЗАТ "ІІТ" та навчальний процес ХНУРЕ; галузь - системи захисту інформації.

2. The object is processes of cryptographic information transformation using block symmetric ciphers; aims - to develop methods of forming random type S-boxes with improved security properties; methods of probability theory, mathematic statistics, combinatorics; news - first time were developed new methods of forming S-boxes

considering cryptographic properties of strenght against differencial and linear cryptoanalysis; the results - new methods of substitution selection were proposed, that allow to improve security properties of ciphers; all ties thesis has been used in activity of "IIT" and education process of KHNURE; the field - Information Security 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. Долгов В.І.
2. Dolgov V.I.

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. Лисицька І.В.
2. Lysytska I.V.

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

VII. Відомості про офіційних опонентів та рецензентів

Офіційні опоненти

Власне Прізвище Ім'я По-батькові:

1. Олексійчук А.М.
2. Олексійчук А.М.

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. Сорока Л.С.
2. Сорока Л.С.

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. Потій О.В.

2. Потій О.В.

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

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.