Облікова картка дисертації

I. Загальні відомості

Державний обліковий номер: 0409U003850

Особливі позначки: відкрита

Дата реєстрації: 05-11-2009

Статус: Захищена

Реквізити наказу МОН / наказу закладу:

II. Відомості про здобувача

Власне Прізвище Ім'я По-батькові:

1. Московченко Ілларіон Валерійович
2. Moskovchenko Illarion Valerievych

Кваліфікація:

Ідентифікатор ORCID ID: Не застосовується

Вид дисертації: кандидат наук

Аспірантура/Докторантура: ні

Шифр наукової спеціальності: 01.05.02

Назва наукової спеціальності: Математичне моделювання та обчислювальні методи

Галузь / галузі знань: Не застосовується

Освітньо-наукова програма зі спеціальності: Не застосовується

Дата захисту: 14-10-2009

Спеціальність за освітою: 7.091401

Місце роботи здобувача: Військовий коледж сержантського складу Національного технічного університету"Харківський політехнічний інститут"

Код за ЄДРПОУ: 26605155

Місцезнаходження: 61034, Україна, м. Харків, вул. Полтавський шлях, 192

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 64.051.09

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 університет Повітряних Сил імені Івана Кожедуба

Код за ЄДРПОУ: 24980799

Місцезнаходження: 61023, Україна, Харків, вул. Сумська, 77/79

Форма власності:

Сфера управління: Міністерство оборони України

Ідентифікатор ROR: Не застосовується

V. Відомості про дисертацію

Мова дисертації:

Коди тематичних рубрик: 81.14.11.05

Тема дисертації:

1. Математичні моделі та обчислювальні методи імовірнісного формування нелінійних вузлів замін симетричних криптографічних засобів захисту інформації

2. Mathematical models and calculation methods of probabilistic forming the nonlinear substitution blocks for symmetric cryptographic means of information security

Реферат:

1. Об'єкт - процес імовірнісного формування нелінійних вузлів замін з поліпшеними властивостями для симетричних криптографічних засобів захисту інформації. Мета - ймовірнісне формування нелінійних вузлів замін з поліпшеними властивостями для симетричних криптографічних засобів захисту інформації. Методи дослідження: математичного моделювання й обчислювальної техніки, теорії захисту інформації, математичний апарат булевої алгебри, теорії чисел, комбінаторики, теорії складності, теорії ймовірності та математичної статистики. Результати, новизна: одержала подальший розвиток математична модель нелінійних вузлів замін симетричних криптографічних засобів захисту інформації; удосконалено обчислювальний метод градієнтного пошуку булевих функцій для нелінійних вузлів замін симетричних криптографічних засобів захисту інформації; вперше запропонована ймовірнісна модель синтезу нелінійних

вузлів замін блокових симетричних криптографічних засобів захисту інформації, що заснована на ймовірнісному відборі формованих булевих функцій, які задовольняють системі обмежень та дозволяють синтезувати нелінійні вузли замін з поліпшеними властивостями для симетричних криптографічних засобів захисту інформації. Результати впроваджені в навчальний процес, при проведенні науково-дослідних робіт та на виробництві. Сфера використання: освіта, науково-дослідні і дослідно-конструкторські роботи зі створення нових криптографічних засобів захисту інформації.

2. An object is a process of probabilistic forming of the non-linear substitution boxes with amended properties for symmetric cryptographic means of information security; a purpose is a probabilistic forming of the non-linear substitution boxes with amended properties for symmetric cryptographic means of information security; methods: mathematic modeling and calculating technique, information security theory, mathematic apparatus of Boolean algebra, numeric theory, combinatory, complexity theory, probability theory, mathematical statistic theory methods; novelty: the mathematic model of the non-linear substitution boxes of symmetric cryptographic means of information security obtained future development; the calculating method of gradient search of Boolean functions for non-linear substitution boxes of symmetric cryptographic means of information security has been amended; the probabilistic model of synthesis the non-linear substitution boxes of symmetric cryptographic means of information security which based on the probabilistic selection of formed Boolean functions satisfying the restriction system was first offered, which allows to synthesis the non-linear substitution boxes with amended properties for symmetric cryptographic means of information security; it is implemented in educational process, scientific and research development and production. Area of utilizing: education, research development pointed to construction of new cryptographic means of information security.

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. Кузнецов Олександр Олександрович
2. Kuznetsov Alexandr Alexandrovych

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. Корченко Олександр Григорович

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. ГоловашичСергій Олександрович
2. ГоловашичСергій Олександрович

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	Сорока Леонід Степанович
Власне Прізвище Ім'я По-батькові головуючого на засіданні	Сорока Леонід Степанович
Відповідальний за підготовку облікових документів	
Реєстратор	
Керівник відділу УкрІНТЕІ, що є відповідальним за реєстрацію наукової діяльності	 Юрченко Т.А.