Облікова картка дисертації

I. Загальні відомості

Державний обліковий номер: 0417U001488

Особливі позначки: відкрита

Дата реєстрації: 29-03-2017

Статус: Захищена

Реквізити наказу МОН / наказу закладу:

II. Відомості про здобувача

Власне Прізвище Ім'я По-батькові:

1. Сторожук Артем Юрійович
2. Storozhuk Artem

Кваліфікація:

Ідентифікатор ORCID ID: Не застосовується

Вид дисертації: кандидат наук

Аспірантура/Докторантура: так

Шифр наукової спеціальності: 21.05.01

Назва наукової спеціальності: Інформаційна безпека держави

Галузь / галузі знань: Не застосовується

Освітньо-наукова програма зі спеціальності: Не застосовується

Дата захисту: 16-03-2017

Спеціальність за освітою: 7.17010102

Місце роботи здобувача: Інститут спеціального зв'язку та захисту інформації Національного технічного університету України "Київський політехнічний інститут імені Ігоря Сікорського"

Код за ЄДРПОУ: 34979237

Місцезнаходження: 03056, м. Київ, вул Верхньоключова, 4

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): Д 26.062.17

Повне найменування юридичної особи: Національний авіаційний університет

Код за ЄДРПОУ: 01132330

Місцезнаходження: пр. Космонавта Комарова 1, м. Київ, Київська обл., 03058, 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: Інститут спеціального зв'язку та захисту інформації Національного технічного університету України "Київський політехнічний інститут імені Ігоря Сікорського"

Код за ЄДРПОУ: 34979237

Місцезнаходження: 03056, м. Київ, вул Верхньоключова, 4

Форма власності:

Сфера управління: Міністерство освіти і науки України

Ідентифікатор ROR: Не застосовується

V. Відомості про дисертацію

Мова дисертації:

Коди тематичних рубрик: 27.43.15

Тема дисертації:

1. Методи оцінювання та обґрунтування стійкості потокових шифрів відносно статистичних атак на основі алгебраїчно вироджених наближень булевих функцій

2. Evaluation and provability methods of stream ciphers' security against statistical attacks based on algebraic degenerate approximations of Boolean functions

Реферат:

1. Дисертаційна робота присвячена вирішенню актуального наукового завдання обґрунтування практичної стійкості потокових шифрів відносно розроблених статистичних атак, які узагальнюють та уніфікують раніше відомі атаки. Теоретичною основою досліджень є теорія ймовірностей та математичний апарат булевих функцій. В роботі запропоновано ряд методів, які дозволяють, за достатньо загальних умов, обґрунтовувати стійкість сучасних потокових шифрів відносно найбільш потужних статистичних атак на основі підібраних векторів ініціалізації. Запропоновані методи доцільно використовувати при проведені експертних досліджень алгоритмів потокового шифрування, призначених для захисту державних інформаційних ресурсів України.

2. The dissertation is dedicated to solving of an actual scientific task of stream ciphers' security evaluation against designed statistical attacks that summarize and unify already known attacks. Theoretical basis of the research is Probability theory and Boolean functions' theory. The proposed methods allow to prove modern stream ciphers' security against most powerful choosen-IV statistical attacks. The proposed methods can be expedienlty used for expert research of stream ciphers, intended for protection of Ukrainian national informational resources.

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. Конюшок Сергій Миколайович
2. Konushok Sergey

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. Олійников Роман Васильович

2. Олійников Роман Васильович

Кваліфікація: д.т.н., 05.13.05

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. Кінзерявий Василь Миколайович

2. Кінзерявий Василь Миколайович

Кваліфікація: к.т.н., 21.05.01

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 Корченко Олександр Григорович

Власне Прізвище Ім'я По-батькові головуючого на засіданні Корченко Олександр Григорович

Відповідальний за підготовку облікових документів

Реєстратор

Керівник відділу УкрІНТЕІ, що є відповідальним за реєстрацію наукової діяльності

Юрченко Т.А.