Облікова картка дисертації

I. Загальні відомості

Державний обліковий номер: 0418U001265

Особливі позначки: відкрита

Дата реєстрації: 26-03-2018

Статус: Захищена

Реквізити наказу МОН / наказу закладу:

II. Відомості про здобувача

Власне Прізвище Ім'я По-батькові:

1. Лада Наталія Володимирівна

2. Lada Nataliia

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: 25-01-2018

Спеціальність за освітою: Управління проектами

Місце роботи здобувача: Черкаський державний технологічний університет

Код за ЄДРПОУ: 05390336

Місцезнаходження: бульвар Шевченка, 460, м. Черкаси, Черкаський р-н., Черкаська обл., 18006, Україна

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, Київ, 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: Черкаський державний технологічний університет

Код за ЄДРПОУ: 05390336

Місцезнаходження: бульвар Шевченка, 460, м. Черкаси, Черкаський р-н., Черкаська обл., 18006, Україна

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. Метод синтезу операцій потокового шифрування з точністю до перестановки

2. Methods and tools for synthesizing streaming encryption operations to within a permutation

Реферат:

1. Дисертаційна робота присвячена підвищенню якості систем потокового шифрування конфіденційної інформації за рахунок підвищення стійкості та надійності перетворення на основі використання модифікованих операцій додавання за модулем два з точністю до перестановки. Для цього розроблено метод синтезу модифікованих операцій додавання за модулем два з точністю до перестановки на основі експериментальних досліджень шляхом поєднання матричних криптоалгоритмів з перестановками операндів і результатів виконання операцій. Синтезовано симетричні та несиметричні модифікації операцій криптографічного додавання за модулем два. Синтезовано та досліджено повну групу модифікованих операцій криптографічного додавання по модулю два з точністю до перестановки на основі операцій додавання за модулем два з точністю до перестановки операндів, шляхом поєднання матричних криптоалгоритмів з перестановками результатів виконання операцій. Розроблено метод підвищення стійкості та надійності потокового шифрування на основі застосування групи модифікованих операцій додавання за модулем два з точністю до перестановки шляхом використання додаткової гамуючої

послідовності для вибору операцій на кожному етапі шифрування

2. The dissertation is devoted to the improvement of the quality of the systems of streaming encryption of confidential information at the expense of increasing the stability and reliability of the transformation based on the use of modified addition operations by the module two to within a permutation. For this purpose, symmetric and asymmetric modifications of cryptographic addition operations by the module two have been synthesized on the basis of experimental studies by combining matrix cryptographic algorithms with permutations of operands in operations. The complete group of modified operations of cryptographic addition by the module two to within a permutation on the basis of addition operations by the module two to within a permutation of operands, by combining matrix cryptographic algorithms with permutations of results of operations execution, has been synthesized and investigated. A method for increasing the stability and reliability of streaming encryption based on the application of the group of modified addition operations by the module two to within the permutation by the use of additional subdued sequence for the selection of operations at each stage of encryption has been developed.

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. Бабенко Віра Григорівна

2. Babenko Vira

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. Білецький Анатолій Якович

2. Biletskiy Anatoliy

Кваліфікація: д. т. н., 05.12.04

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. Халімов Геннадій Зайдулович

2. Khalimov Gennadiy

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

Рецензенти

VIII. Заключні відомості

Власне Прізвище Ім'я По-батькові голови ради Корченко Олександр Григорович

Власне Прізвище Ім'я По-батькові головуючого на засіданні Павленко Петро Миколайович

Відповідальний за підготовку облікових документів

Реєстратор

Керівник відділу УкрІНТЕІ, що є відповідальним за реєстрацію наукової діяльності

Юрченко Т.А.