Облікова картка дисертації

I. Загальні відомості

Державний обліковий номер: 0419U003277

Особливі позначки: відкрита

Дата реєстрації: 04-07-2019

Статус: Захищена

Реквізити наказу МОН / наказу закладу:

II. Відомості про здобувача

Власне Прізвище Ім'я По-батькові:

1. Нестеренко Оксана Борисівна
2. Nesterenko Oksana B.

Кваліфікація:

Ідентифікатор ORCID ID: Не застосовується

Вид дисертації: кандидат наук

Аспірантура/Докторантура: так

Шифр наукової спеціальності: 05.13.05

Назва наукової спеціальності: Комп'ютерні системи та компоненти

Галузь / галузі знань: Не застосовується

Освітньо-наукова програма зі спеціальності: Не застосовується

Дата захисту: 27-06-2019

Спеціальність за освітою: Пожежна безпека

Місце роботи здобувача: Черкаський інститут пожежної безпеки імені Героїв Чорнобиля Національного університету цивільного захисту України

Код за ЄДРПОУ: 39117736

Місцезнаходження: вул. Онопрієнка, 8, м. Черкаси, Черкаський р-н., Черкаська обл., 18034, Україна

Форма власності:

Сфера управління: Державна служба України з надзвичайниїх ситуацій

Ідентифікатор ROR: Не застосовується

III. Відомості про організацію, де відбувся захист

Шифр спеціалізованої вченої ради (разової спеціалізованої вченої ради): К 73.052.04

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

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: 19.45, 28.01

Тема дисертації:

1. Методи та засоби синтезу операцій потокового шифрування за критерієм строгого стійкого кодування
2. The methods and means of synthesizing the stream ciphering operations on the criterion of strict stable coding

Реферат:

1. Дисертаційна робота присвячена підвищенню невизначеності результатів потокового шифрування за рахунок використання нових операцій криптоперетворення й синтезованих за критерієм строгого стійкого кодування. Для цього вперше розроблено метод синтезу операцій за критерієм строгого стійкого кодування шляхом використання таблиць мінімальних відстаней за Хеммінгом, які забезпечують максимальну невизначеність результатів перетворення та збільшення варіативності криптоалгоритмів; розроблено метод синтезу операцій за критерієм строгого стійкого кодування мінімальної складності, на основі використання операцій перестановки і гамування, шляхом встановлених обмежень та залежностей між операціями перетворення і таблицями мінімальних відстаней за Хеммінгом, які забезпечують максимальну невизначеність результатів перетворення при мінімальній складність схемо технічної та програмної реалізації. Набули подальшого розвитку методи синтезу програмних і апаратних криптографічних засобів комп'ютерної техніки на основі використання нової групи операцій, побудованих за критерієм строгого стійкого кодування, шляхом застосування методів синтезу моделей операцій із новими властивостями, які

забезпечили спрощення синтезу, а синтез моделей операцій за критерієм строгого стійкого кодування мінімальної складності реалізовано без побудови таблиць істинності їх мінімізації.

2. The thesis is devoted to increasing the uncertainty of the stream ciphering results due to the use of new cryptographic transformations' operations synthesized by the criterion of strict stable coding. For this purpose, a method for synthesizing the operations by the criterion of strict stable coding has been developed for the first time, using the Hamming minimum distances tables, which provide the maximum uncertainty of the transformation's results and increase the variability of cryptographic algorithms. The method for synthesizing operations by the criterion of strict stable coding of minimal complexity is developed, based on the use of permutation and subdued operations, by the established limitations and relationships between transformation operations and the tables of Hamming minimum distances, which provide the maximum uncertainty of the transformation results with the minimal complexity of the circuit-technical and program implementation. Further development methods for the synthesis of software and hardware cryptographic means of computer technology is done on the basis of the use of a new group of operations built on the criterion of strictly stable coding, by applying the methods of synthesis of models of operations with new properties, which provided simplification of synthesis. The synthesis of operations models according to the criterion of strictly stable encoding of minimal complexity is realized without the construction of tables of truth and their minimization

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. Рудницький Володимир Миколайович

2. Rudnytskyi Volodymyr M.

Кваліфікація: д. т. н., 05.13.06

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. Кулик Анатолій Ярославович
2. Kulyk Anatolii Ya.

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. Пархуць Любомир Теодорович
2. Parhuts Liubomyr T.

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	Рудницький Володимир Миколайович
Власне Прізвище Ім'я По-батькові головуючого на засіданні	Первунінський Станіслав Михайлович
Відповідальний за підготовку облікових документів	
Реєстратор	
Керівник відділу УкрІНТЕІ, що є відповідальним за реєстрацію наукової діяльності	Юрченко Т.А.