Облікова картка дисертації

I. Загальні відомості

Державний обліковий номер: 0409U005163

Особливі позначки: відкрита

Дата реєстрації: 24-11-2009

Статус: Захищена

Реквізити наказу МОН / наказу закладу:

II. Відомості про здобувача

Власне Прізвище Ім'я По-батькові:

1. Бабенко Віра Григорівна
2. Babenko Vera Grigorivna

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: 29-10-2009

Спеціальність за освітою: 7.091503

Місце роботи здобувача: Черкаський державний технологічний університет

Код за ЄДРПОУ: 05390336

Місцезнаходження: 18006, м. Черкаси, бульвар Шевченка, 460

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 26.062.01

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: Черкаський державний технологічний університет

Код за ЄДРПОУ: 05390336

Місцезнаходження: 18006, м. Черкаси, бульвар Шевченка, 460

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 підвищення швидкодії систем захисту інформації на основі використання спеціалізованих логічних функцій

2. The method of increase of fast-acting of the protection systems of information on the basis of the use of the specialized boolean functions

Реферат/анотація:

1. Основна мета полягає у вирішенні важливої науково-технічної задачі підвищення швидкодії систем захисту інформації на основі використання спеціалізованих логічних функцій криптографічного перетворення. Об'єкт дослідження - процес захисту інформації, яка зберігається, обробляється і передається в комп'ютерних системах і мережах. У процесі синтезу спеціалізованих логічних функцій використовується математичний апарат теорії інформації, систем числення, методів дискретної математики, теорії логіки, криптографії та комп'ютерного моделювання. Вперше розроблено метод підвищення швидкодії криптографічного перетворення інформації на основі спеціалізованих логічних функцій, реалізація якого за наведеними розрахунками покращує оперативність обробки інформації від 1,57 до 2,92 разів залежно від часу отримання ключової послідовності та розрядності перетворення; вперше одержано формалізовану модель уніфікованого пристрою криптографічного перетворення інформації, що реалізує розроблений метод

підвищення швидкодії систем захисту інформації на основі застосування наборів спеціалізованих логічних функцій; удосконалено методи синтезу та аналізу спеціалізованих логічних функцій для криптографії, що дало змогу розширити множину функцій та обґрунтувати ефективність їх застосування в криптосистемах. Практична цінність роботи полягає в доведенні здобувачем отриманих наукових результатів до конкретних інженерних методик, алгоритмів, моделей та варіантів функціональних схем спеціалізованих дискретних пристроїв криптографічного перетворення для систем захисту інформації. Сферою застосування предмета дослідження є спеціалізовані дискретні пристрої криптографічного перетворення і спеціалізоване програмне забезпечення комп'ютерних систем для захисту інформації в реальному часі.

2. A primary purpose consists in the decision of important scientific and technical task of increase of fast-acting of the protection systems of information on the basis of the use of the specialized boolean functions of cryptographic transformation. A research object is a process of defence of information, which is saved, processed and passed in the computer systems and networks. In the process of synthesis of the specialized boolean functions the mathematical vehicle of information, scales of notation, methods of discrete mathematics theory, theory of logic, cryptography and computer design is used. The method of increase of fast-acting of cryptographic transformation of information is first developed on the basis of the specialized boolean functions, realization of which upon resulted settlements improves operativeness of treatment of information from 1,57 to 2,92 times depending on time of receipt of key sequence and bit of transformation; the formalized model of compatible device of cryptographic transformation of information which will realize the developed method of increase of fast-acting of the protection systems of information on the basis of application of sets of the specialized boolean functions is first got; the methods of synthesis and analysis of the specialized boolean functions is improved for cryptography, that enabled to extend the plural of functions and ground efficiency of their application in cryptosystems. The practical value of work consists in taking of the got scientific results a competitor to the concrete engineerings methods, algorithms, models and variants of functional diagrams of the specialized discrete devices of cryptographic transformation for the protection systems of information. A purview of the object of research are the specialized discrete devices of cryptographic transformation and specialized software of the computer systems for defence of information in the real time.

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. Rudnitskiy Volodymyr Mykoloyovich

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. Лужецький Володимир Андрійович
2. Лужецький Володимир Андрійович

Кваліфікація: д.т.н., 01.05.02, 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 Філоненко Сергій Федорович

Власне Прізвище Ім'я По-батькові головуючого на засіданні Філоненко Сергій Федорович

Відповідальний за підготовку облікових документів

Реєстратор

Керівник відділу УкрІНТЕІ, що є відповідальним за реєстрацію наукової діяльності Юрченко Т.А.