Облікова картка дисертації

I. Загальні відомості

Державний обліковий номер: 0418U003301

Особливі позначки: відкрита

Дата реєстрації: 18-10-2018

Статус: Захищена

Реквізити наказу МОН / наказу закладу:

II. Відомості про здобувача

Власне Прізвище Ім'я По-батькові:

1. Сисоєнко Світлана Володимирівна
2. Sysoienko Svitlana Volodymyrivna

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: 11-10-2018

Спеціальність за освітою: Технологія машинобудування

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): 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: 50.37.23

Тема дисертації:

1. Методи і моделі підвищення швидкості та стійкості матричного криптографічного перетворення інформації

2. Methods and models for increasing the speed and stability of matrix cryptographic transformation of information

Реферат/анотація:

1. Дисертаційна робота присвячена питанням підвищення швидкості та стійкості матричного криптографічного перетворення інформації шляхом впровадження ієрархічної структури групового перетворення та встановлення нових взаємозв'язків між прямими й оберненими операціями. Для досягнення мети в роботі було розроблено метод підвищення стійкості псевдовипадкових послідовностей, побудованих на основі застосування операцій матричного криптографічного перетворення, шляхом їх паралельної реалізації з наступним додавання за модулем. Удосконалено моделі побудови криптоперетворення на основі використання двохоперандних операцій шляхом впровадження ієрархічної структури групового перетворення та встановлення нових взаємозв'язків між прямими та оберненими операціями. На основі запропонованої узагальненої математичної моделі групового матричного криптографічного перетворення було розроблено метод підвищення швидкості реалізації групового матричного криптографічного

перетворення, що відзначається зменшенням складності побудови та реалізації оберненого криптоперетворення інформації.

2. The thesis is devoted to questions of increasing the speed and stability of matrix cryptographic transformation of information by introducing the hierarchical structure of group transformation and establishing new relationships between direct and reverse operations. The first section substantiates the need of improving computer security systems in global computer networks and Internet. It was determined that one of the ways to ensure confidentiality and integrity of information for solving the problems of increasing the stability, speed and reliability of transformations, it is necessary to use matrix operations based on Boolean functions. The second section is devoted to the development of a method for increasing the resistance of pseudo-random sequences constructed on the basis of the operations of matrix cryptographic transformation, by adding them by module, which increased the probability of degenerate transformation results. As a result of the research, it was determined that the improvement of the quality of pseudo-random sequences is achieved by adding several primary sequences by module as a result of which certain generalized transformations become degenerate. The third section is devoted to the synthesis of a nondegenerate cryptographic transformation based on the group use of two-operand data transformation operations. It was proposed to adapt the method of increasing the resistance of pseudo-random sequences to increase the resistance of the results of encryption based on the replacement of the addition module operation by the operation, which will provide the possibility of decryption. The algorithm of a two-operand hierarchical group transformation was introduced, which ensures the synthesis of non-degenerate group operations. The given algorithm was investigated with the purpose of finding both the inverse operation and the inverse algorithm for information reproduction based on the construction of two inverse intermediate transformations and the inverse resultant transformation. A model of direct and inverse two-operand group cryptographic transformation was proposed, which makes it easier to find the reverse cryptographic transformation. The fourth section is devoted to the development of a method for increasing the speed of implementation of group matrix cryptographic transformation based on the proposed generalized mathematical model of group matrix cryptographic transformation, by reducing the complexity of constructing and implementing the inverse transformation, which reduced the mathematical complexity and increased the speed of cryptographic transformation. Based on the mathematical apparatus of block matrices, the correctness of the mathematical model of constructing an inverse group matrix cryptographic transformation was checked. The following practical results were obtained: improved models and developed encryption methods are brought to the structural and functional schemes of devices, encryption algorithms, which provide increased resistance and speed of crypto-conversion. The results of modeling and practical implementation determined that the reduction in the complexity of the implementation of the mathematical model of the group matrix cryptographic transformation was from 8 to 33 times, depending on the matrix size, and also increased the implementation rate by 6-8 % based on the results of practical implementation. The results of the work were implemented at the enterprises and organizations of the Ministry of Education and Science of Ukraine.

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. Ланських Євген Володимирович
2. Lanskykh Yevhen Volodymyrovych

Кваліфікація: к. 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. Куц Юрій Васильович
2. Kuts Yurii

Кваліфікація: д. т. н., 05.11.16

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. Можаєв Олександр Олександрович

2. Mozhaiev Oleksandr Oleksandrovych

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. Корченко Олександр Григорович
2. Korchenko Oleksandr Grygorovych

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 Рудницький Володимир Миколайович

Відповідальний за підготовку облікових документів

Реєстратор

Керівник відділу УкрІНТЕІ, що є відповідальним за реєстрацію наукової діяльності



Юрченко Т.А.