Облікова картка дисертації

I. Загальні відомості

Державний обліковий номер: 0523U100076

Особливі позначки: відкрита

Дата реєстрації: 17-05-2023

Статус: Захищена

Реквізити наказу МОН / наказу закладу:

II. Відомості про здобувача

Власне Прізвище Ім'я По-батькові:

1. Соколов Артем Вікторович
2. Sokolov Artem Viktorovich

Кваліфікація: к. т. н., 05.13.21

Ідентифікатор ORCID ID: Не застосовується

Вид дисертації: доктор 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: 28-04-2023

Спеціальність за освітою: Системи технічного захисту інформації, автоматизація її обробки

Місце роботи здобувача: Національний університет "Одеська політехніка"

Код за ЄДРПОУ: 43861328

Місцезнаходження: пр. Шевченка, буд. 1, м. Одеса, Одеська обл., 65044, 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 35.052.18

Повне найменування юридичної особи: Національний університет "Львівська політехніка"

Код за ЄДРПОУ: 02071010

Місцезнаходження: вул. Степана Бандери, буд. 12, м. Львів, Львівська обл., 79013, 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: Національний університет "Одеська політехніка"

Код за ЄДРПОУ: 43861328

Місцезнаходження: пр. Шевченка, буд. 1, м. Одеса, Одеська обл., 65044, 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, 50.41.25

Тема дисертації:

1. Методологія розробки ефективної крипто-стеганографічної системи

2. Methodology for developing an effective crypto-steganographic system

Реферат/анотація:

1. В роботі вирішено важливу науково-практичну проблему, що полягає у забезпеченні ефективності роботи крипто-стеганографічних систем в режимі реального часу на ресурсообмежених платформах, шляхом розробки відповідної науково обґрунтованої методології, орієнтованої на управління вбудовуванням криптозахищеної додаткової інформації у просторовій області контейнера. Відсутність аналогічних рішень в Україні та за кордоном робить результати досліджень пріоритетними. Отримані наукові результати мають фундаментальне (теоретичне) та прикладне (практичне) значення для розвитку та вдосконалення крипто-стеганографічних систем. В роботі побудовано теоретичний базис для побудови крипто стеганографічних систем, який надає можливість формування необхідних властивостей стеганоповідомлення при вбудовуванні інформації у просторовій області за рахунок реалізації концепції кодового управління вбудовуванням інформації. В контексті підвищення крипостійкості крипто-стеганографічних систем в роботі представлено теоретичний базис оцінки та підвищення криптографічної якості шифрів на основі математичного апарату функцій багатозначної логіки, що є основою підвищення рівня імплементації

шифрами дифузії та конфузії, підвищення їх ефективності та криптостійкості, а також узгодженості криптографічної і стеганографічної компоненти крипто-стеганографічних систем. На основі побудованого теоретичного базису розроблено стеганографічні методи з кодовим управлінням вбудовуванням, а також спеціалізовані шифри для забезпечення узгодженості криптографічної та стеганографічної складової крипто стеганографічних систем. Встановлено простоту алгоритмічної реалізації представлених методів, доведено можливість роботи крипто-стеганографічної системи на основі розробленої методології у режимі реального часу на ресурсообмежених платформах.

2. An important scientific and practical problem of ensuring the effectiveness of crypto-steganographic systems in real time on resource-limited platforms has been solved by developing an appropriate scientifically based methodology, focused on code control of cryptographically protected additional information embedding in the spatial domain of the container. In the dissertation relationship between the transformants of the two dimensional, one-dimensional Walsh-Hadamard transform and the discrete cosine transform, as well as the components of the singular value decomposition of the container block, is established, based on which formal sufficient conditions for the given properties of the steganographic message are obtained, and the theoretical foundations for the formation of steganographic methods with code control are developed. The theoretical basis for the synthesis of effective codewords was formed, as well as indicators of energy and selectivity of the codeword were introduced and researched, which made it possible to synthesize multi-level codewords, which ensure the effectiveness of steganographic methods with code control developed on their basis. Two steganographic methods with code control of additional information embedding using binary and multi-level codewords have been created, which ensures their effectiveness, which exceeds modern analogs, in particular, in the conditions of a streaming container. Using the developed theoretical basis, Reed-Solomon codes, and the developed codes of spatial arrangements, two steganographic methods with multiple access are proposed, which allow, while preserving the advantages of code control, to support the registration in the system of up to several thousand users and the simultaneous operation of several tens of users. In the context of increasing the cryptographic strength of crypto-steganographic systems, the theoretical basis for ensuring the cryptographic quality of many-valued logic functions was built, which includes the following criteria: algebraic nonlinearity, distance nonlinearity, the avalanche effect criterion, the criterion of output independence from input variables, which made it possible to implement a justified choice of many-valued logic functions for the tasks of building specialized block symmetric ciphers for encrypting the states list sequence when using the steganographic method with code control of the additional information embedding. Based on the developed cryptographic quality criteria for many-valued logic functions, the sets of S-boxes of practically valuable lengths have been synthesized that have the maximum possible level of nonlinearity of both component Boolean functions and component many-valued logic functions, satisfy the error propagation criterion of the highest orders, and are also optimal in terms of the criterion of independence of the output of the component many-valued logic functions from their input variables, which makes it possible to increase the cryptographic quality of cipher constructions used in crypto-steganographic systems. Ready for practical implementation block symmetric cipher has been developed, the use of which allows to accelerate the destruction of the statistics of the plaintext, which made it possible to reduce the number of necessary iterations of the main step of cryptographic transformation, and, therefore, the computational costs for the operation of preliminary encryption of additional information in the preliminary coder of the crypto-steganographic system. The practical value of the manuscript consists in bringing the obtained scientific results to specific methods and algorithms that can be applied in practical information protection systems, including those that involve deployment on resource-limited platforms and require operation with streaming containers in real-time mode. Algorithmic implementations of steganographic methods with code control of information embedding are characterized by realization simplicity, as well as the flexibility of setting properties of steganographic message by certain codewords choosing.

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. Кобозєва Алла Анатоліївна
2. Kobozeva Alla A.

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. Кобозєва Алла Анатоліївна
2. Kobozeva Alla A.

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. Шелест Михайло Євгенович
2. Shelest Mykhailo Ye.

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. Хорошко Володимир Олексійович
2. Khoroshko Volodymyr Oleksiiovych

Кваліфікація: д.т.н., 05.13.13

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. Мілов Олександр Володимирович
2. Milov Oleksandr V

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 Дудикевич Валерій Богданович

Власне Прізвище Ім'я По-батькові головуючого на засіданні Дудикевич Валерій Богданович

Відповідальний за підготовку облікових документів

Реєстратор

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