Облікова картка дисертації

I. Загальні відомості

Державний обліковий номер: 0418U003751

Особливі позначки: відкрита

Дата реєстрації: 19-11-2018

Статус: Захищена

Реквізити наказу МОН / наказу закладу:

II. Відомості про здобувача

Власне Прізвище Ім'я По-батькові:

1. Розломій Інна Олександрівна

2. Rozlomii Inna

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: 15-11-2018

Спеціальність за освітою: Спеціалізовані комп'ютерні системи

Місце роботи здобувача: Черкаський національний університет імені Богдана Хмельницького

Код за ЄДРПОУ: 02125622

Місцезнаходження: бульв. Шевченка, 81, м. Черкаси, Черкаський р-н., Черкаська обл., 18031, 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 національний університет імені Богдана Хмельницького

Код за ЄДРПОУ: 02125622

Місцезнаходження: бульв. Шевченка, 81, м. Черкаси, Черкаський р-н., Черкаська обл., 18031, 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 та засоби протидії фальсифікації електронних документів
2. Methods and tools of counteracting falsifications of electronic documents

Реферат/анотація:

1. Дисертаційна робота присвячена розробці методів виявлення фальсифікацій у електронних документах для підвищення достовірності інформації. Для досягнення поставленої мети було розроблено методи обчислення хеш-функції електронного документа шляхом використання операцій матричного криптографічного перетворення. На основі запропонованих методів обчислення хеш-функції було побудовано метод перехресного хешування, який дає змогу виявити фальсифікований фрагмент інформації. Наступний метод надлишкового хешування на основі використання методів обчислення хеш-функції електронного документу, шляхом введення контрольних блоків інформації, який забезпечує гарантоване виявлення заданої кількості фальсифікованих фрагментів електронного документу. Для додаткового рівня захисту електронних документів запропоновано метод комплексного використання електронного цифрового підпису та цифрового водяного знаку. Розроблений метод формування умовного цифрового водяного знаку на основі операцій матричного криптографічного перетворення значень з заданого

проміжку, які визначають правила накладання цифрового водяного знаку.

2. The dissertation is devoted to actual issues of developing new and improving existing methods and tools of counteracting falsifications of electronic documents. The cryptographic and steganographic tools of electronic documents protection such as electronic digital signature and digital watermark were consider in dissertation research. The research showed that electronic digital signature is one of the main mechanisms for ensuring the integrity and reliability of electronic documents. Thus, methods for calculating hash functions of electronic documents were construct. The research reveals solving the problem of ensuring the authenticity of electronic documents by developing methods for detecting falsifications. Methods of calculating hash functions were use to develop methods for finding false fragments in electronic documents. The method of complex use of electronic digital signature and digital watermark for an additional level of protection of electronic documents was proposed. The methods of calculating the hash functions of an electronic document based on using operations of matrix cryptographic transformation has been developed. The functional schemes of the methods of keyless calculation of the hash function of the electronic document were construct. Hash algorithms for each of the proposed schemes were develop. The algorithms with successive and parallel execution of operations of calculating the hash function were show. Modifications of algorithms for calculating hash functions were propose, which are improved by addition of operations of matrix cryptographic transformation. The methods of key hashing were develop, the result of which is the matrix, which is changed on the basis of analysis of the information of the electronic document. The method for detecting a false fragment of an electronic document by a method of cross-hashing has been developed. The method of cross-hashing is calculating hash functions in the vertical and horizontal blocks of the electronic document. This will allow to detect a false fragment of information on the intersection of blocks. The method of redundant hashing, which is based on Hamming's coding principle, has been further developed. This method ensures the guaranteed detection of several false fragments in electronic document based on the excessive hashing of the control block of information. The method for forming a conditional digital watermark based on operations of a matrix cryptographic transformation of values from a given interval, which determine the rules for the imposition of a digital watermark, was develop. The method of complex use of electronic digital signature and digital watermark in order to provide an additional level of protection of electronic documents was propose. The developed algorithms and functional schemes of the proposed methods will allow implementation of methods for their practical application.

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. Косенюк Григорій Володимирович

2. Koseniuk Hryhorii

Кваліфікація: к. т. н., 20.02.14

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. Семенов Сергій Геннадійович

2. Semenov Serhii Hennadiiovych

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 Анна Олександрівна

2. Korchenko Anna

Кваліфікація: к. 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 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.