Облікова картка дисертації

I. Загальні відомості

Державний обліковий номер: 0420U102468

Особливі позначки: відкрита

Дата реєстрації: 28-12-2020

Статус: Захищена

Реквізити наказу МОН / наказу закладу:

II. Відомості про здобувача

Власне Прізвище Ім'я По-батькові:

1. Грицак Анатолій Васильович
2. Hrytsak Anatoliy

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: 27-11-2020

Спеціальність за освітою: 124 Системний аналіз

Місце роботи здобувача: Вінницький державний педагогічний університет імені Михайла Коцюбинського

Код за ЄДРПОУ: 02125094

Місцезнаходження: вул. Острозького, 32, м. Вінниця, Вінницький р-н., Вінницька обл., 21100, 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 26.062.17

Повне найменування юридичної особи: Національний авіаційний університет

Код за ЄДРПОУ: 01132330

Місцезнаходження: проспект Любомира Гузара, 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: Вінницький національний технічний університет

Код за ЄДРПОУ: 02070693

Місцезнаходження: вул. Хмельницьке шосе, 95, м. Вінниця, Вінницький р-н., Вінницька обл., 21021, Україна

Форма власності:

Сфера управління: Міністерство освіти і науки України

Ідентифікатор ROR: Не застосовується

V. Відомості про дисертацію

Мова дисертації:

Коди тематичних рубрик: 20.53.37, 50.37.23

Тема дисертації:

1. Методи побудови ефективних криптографічних функцій гешування

2. Methods for effective cryptographic hash functions construction

Реферат/анотація:

1. Дисертаційна робота присвячена розв'язанню актуальної наукової задачі розробки та дослідження нових ефективних геш-функцій, які при достатньо високій швидкодії забезпечуватимуть необхідний рівень стійкості. Проведено аналіз сучасних методів і алгоритмів побудови та реалізації ефективних криптографічних функцій гешування, що дозволило виявити їх недоліки і формалізувати завдання наукового дослідження. Розроблено методи побудови функцій гешування, які дозволили підвищити стійкість і швидкість криптографічної обробки даних. Удосконалено метод побудови генераторів ПВП, що дозволило формувати статистично стійку гаму для криптографічних застосувань. Удосконалено метод криптографічного захисту інформації, що дало можливість забезпечити конфіденційність і цілісність даних. Розроблено спеціалізоване програмне забезпечення у вигляді консольних додатків на мові програмування C++ та методику, що дозволило провести експерименти і верифікувати запропоновані методи. результати дисертації використовуються у навчальному процесі Вінницького національного технічного університету,

науковому процесі Національного авіаційного університету та ННВК “Інформаційно-комунікаційні системи”.

2. The dissertation is devoted to solving the actual scientific problem of developing and researching new effective hash functions that will provide the necessary level of the security with a sufficiently high speed. The analysis of modern methods and algorithms for the construction and implementation of effective cryptographic hashing functions was carried out, which made it possible to identify their shortcomings and formalize the tasks of scientific research. A method of constructing hashing functions was developed, which made it possible to increase the speed of cryptographic data processing. A method of constructing hashing functions was developed, which made it possible to provide resistance to cryptanalytic attacks. The method of pseudorandom number generators construction has been improved, which allowed forming a statistically stable range for cryptographic applications. The method of cryptographic protection of information has been improved, which by means of fixing information on user ID, session ID, time of sending, length of message and its serial number, as well as use of the new procedure of formation of session key and encryption, made it possible to ensure confidentiality and integrity of data in the modern information and communication systems and technologies. Last chapter of the dissertation contains research study devoted to collision characteristics of proposed hash functions using so-called “baby versions” of hashing functions based on the existed experimental technique (relevant in cryptography). Specialized software was developed in the form of console applications in C ++ programming language (Microsoft Visual Studio 2013 (Release Version)) and a technique that allowed us to conduct experiments and verify the proposed methods. the results of the dissertation are used in the educational process of Vinnytsa National Technical University (to increase the efficiency of training of specialists in the specialty 125 “Cybersecurity”) as well as in scientific process of National Aviation University and Educational & Research Complex “Information and Communication Systems”. It was confirmed by the acts of implementation.

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. Яремчук Юрій Євгенович
2. Яремчук Юрій Євгенович

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. Василіу Євген Вікторович
2. Василіу Євген Вікторович

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. Охріменко Тетяна Олександрівна
2. Okhrimenko Tetiana

Кваліфікація: к. 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	Корченко Олександр Григорович
Власне Прізвище Ім'я По-батькові головуючого на засіданні	Корченко Олександр Григорович
Відповідальний за підготовку облікових документів	
Реєстратор	
Керівник відділу УкрІНТЕІ, що є відповідальним за реєстрацію наукової діяльності	Юрченко Т.А.