Облікова картка дисертації

I. Загальні відомості

Державний обліковий номер: 0419U000548

Особливі позначки: відкрита

Дата реєстрації: 01-03-2019

Статус: Захищена

Реквізити наказу МОН / наказу закладу:

II. Відомості про здобувача

Власне Прізвище Ім'я По-батькові:

1. Косован Григорій Васильович
2. Kosovan Hryhorii V.

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: 08-02-2019

Спеціальність за освітою: Захист інформації з обмеженим доступом та автоматизація її обробки

Місце роботи здобувача: Чернівецький національний університет імені Юрія Федьковича

Код за ЄДРПОУ: 02071240

Місцезнаходження: вул. Коцюбинського, 2, м. Чернівці, Чернівецька обл., 58012, 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 41.816.02

Повне найменування юридичної особи: Одеська національна академія зв'язку ім. О.С. Попова

Код за ЄДРПОУ: 01180116

Місцезнаходження: Кузнечна вулиця, 1, м. Одеса, Одеська обл., 65029, 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: Чернівецький національний університет імені Юрія Федьковича

Код за ЄДРПОУ: 02071240

Місцезнаходження: вул. Коцюбинського, 2, м. Чернівці, Чернівецька обл., 58012, Україна

Форма власності:

Сфера управління: Міністерство освіти і науки України

Ідентифікатор ROR: Не застосовується

V. Відомості про дисертацію

Мова дисертації:

Коди тематичних рубрик: 20.56.02

Тема дисертації:

1. Синтез генераторів псевдовипадкових послідовностей із нелінійною динамікою для захисту інформації в телекомунікаційних системах

2. Synthesis of pseudo-random sequence generators with nonlinear dynamics for protection of information in telecommunication systems

Реферат/анотація:

1. Об'єкт дослідження - процес формування псевдовипадкових послідовностей на базі хаотичних систем, а також процеси криптографічного закриття інформації за допомогою синтезованих генераторів ПВП. Предмет дослідження - генератори псевдовипадкових послідовностей на основі одно- та багатовимірних хаотичних систем для захисту інформації в телекомунікаційних системах. Методи дослідження. Під час розв'язання поставлених завдань у роботі використовувалися методи чисельного інтегрування систем нелінійних диференційних рівнянь, математичне моделювання нелінійної динаміки (біфуркаційні діаграми, фазові портрети), методи теорії імовірності і випадкових процесів для дослідження статистичних характеристик псевдовипадкових генераторів та елементи криптоаналізу для оцінки стійкості методів шифрування. Теоретичні та практичні результати: Удосконалено генератор ПВП бітів, на основі двох

одновимірних хаотичних систем, формованих операцією сумування по модулю два відповідних елементів псевдовипадкових послідовностей генерованих одновимірними хаотичними генераторами; Вперше запропоновано генератор формування псевдовипадкових послідовностей на основі двох нелінійних хаотичних систем, значення хаотичних коливань, генерованих логістичним відображенням в якому слугують динамічним пороговим рівнем прийняття рішення щодо значення бітів у псевдовипадкових послідовностях, генерованих системою Лоренца; Удосконалено класичний метод М. Баптісти шифрування текстової інформації шляхом використання двох хаотичних систем, а саме система Ресслера та кубічне відображення; Удосконалено метод шифрування зображень на основі формованих логістичною, квадратною та кубічною функціями хаотичних відображень сіток пікселів.

2. The object of the study are process of forming of pseudorandom sequences based on chaotic systems, as well as processes of cryptographic close of information with the help of synthesized PRB generators. Subject of research - pseudorandom sequence generators based on single- and multidimensional chaotic systems for the protection of information in telecommunication systems. Research methods. In solving the set tasks in work methods of numerical integration of systems of nonlinear differential equations, mathematical modeling of nonlinear dynamics (bifurcation diagrams, phase portraits), methods of probability theory and random processes for studying the statistical characteristics of pseudorandom generators and elements of cryptanalysis for evaluation of the stability of encryption methods Theoretical and practical results: The generator of PVP bits is improved, based on two one-dimensional chaotic systems, formed by the operation of summing modulo two corresponding elements of pseudorandom sequences generated by one-dimensional chaotic generators; For the first time, the generator of the forming of pseudorandom sequences on the basis of two nonlinear chaotic systems was proposed, the values of chaotic oscillations generated by the logistic map serve as a dynamic threshold for decision making regarding the value of bits in pseudorandom sequences generated by the Lorentz system; The classical method of M. Baptista of the text information encryption improved by using two chaotic systems, namely the Ressler system and the cubic map; The method of encrypting images on the basis of formed logistic, square and cubic functions of chaotic map of pixel lattice is improved.

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. Кушнір Микола Ярославович

2. Kushnir Mykola Ya.

Кваліфікація: к. ф.-м. н., 01.04.10

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. Толюпа Сергій Васильович
2. Toliupa Serhii V.

Кваліфікація: д. т. н., 05.12.02

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. Корчинський Володимир Вікторович
2. Korchynskyi Volodymyr 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	Захарченко Микола Васильович
Власне Прізвище Ім'я По-батькові головуючого на засіданні	Захарченко Микола Васильович
Відповідальний за підготовку облікових документів	
Реєстратор	
Керівник відділу УкрІНТЕІ, що є відповідальним за реєстрацію наукової діяльності	Юрченко Т.А.

