Облікова картка дисертації

I. Загальні відомості

Державний обліковий номер: 0413U001641

Особливі позначки: відкрита

Дата реєстрації: 26-03-2013

Статус: Захищена

Реквізити наказу МОН / наказу закладу:

II. Відомості про здобувача

Власне Прізвище Ім'я По-батькові:

1. Веретельник Віталій Васильович

2. Veretelnyk Vitaly Vasilevych

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: 28-02-2013

Спеціальність за освітою: 7.091.501

Місце роботи здобувача: ТОВ Лакофарбовий завод "АВРОРА"

Код за ЄДРПОУ: 32741978

Місцезнаходження: 18030, м. Черкаси, вул. Будіндустрії 3

Форма власності:

Сфера управління:

Ідентифікатор ROR: Не застосовується

III. Відомості про організацію, де відбувся захист

Шифр спеціалізованої вченої ради (разової спеціалізованої вченої ради): К 73.052.01

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: 18006, м. Черкаси, бульвар Шевченка, 460

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 підвищення швидкості та достовірності доступу до конфіденційних інформаційних ресурсів

2. Methods for improving the speed and reliability of access to confidential information resources

Реферат/анотація:

1. Об'єкт дослідження - процеси захисту інформації, які зберігаються, оброблюються і передаються в комп'ютерних системах та мережах. Мета дослідження - підвищення швидкості та достовірності доступу до конфіденційних інформаційних ресурсів на основі введення інформаційної та апаратної надлишковості. Розширена науково-технічна база проектування систем захисту інформації на основі суміщення процесів завадостійкого і криптографічного кодування. Побудовані алгоритми функціонування та математичні моделі пристроїв криптографічного кодування, декодування і перекодування, на основі спеціалізованих логічних функцій і двійково-четвіркової систем числення з постійною кількістю одиниць. Побудований генератор конґруентних чисел, що забезпечує вирішення багатьох практичних завдань, в тому числі формування команд криптографічного перетворення інформації. Розроблені функціональні і структурні схеми, що реалізують запропонований метод і в сукупності забезпечують підвищення швидкості та достовірності доступу до конфіденційних інформаційних ресурсів на 25%. Розроблено метод криптографічного

(кодування, декодування та перекодування) з введенням інформаційної надлишковості на основі двохрозрядних логічних функцій і двійково-четвіркової систем числення з постійною кількістю одиниць, що дозволило зменшити час доступу до інформації за рахунок суміщення процесів завадостійкого і криптографічного кодування, а також спростити функціональні схеми пристроїв. Запропоновано модель процесу підвищення швидкості та достовірності доступу до конфіденційних інформаційних ресурсів, що дозволило обґрунтувати задачі дисертаційного дослідження. удосконалено метод підвищення швидкості та достовірності доступу до конфіденційних інформаційних ресурсів на основі використання стохастичних генераторів псевдовипадкових чисел із заданими вимогами та суміщення процесів криптографічного кодування з введенням інформаційної надлишковості, що забезпечило можливість створення і розробки програмно-апаратних засобів практичного застосування. Набув подальшого розвитку метод побудови генераторів псевдовипадкових чисел для генерації рівномірно розподіленої некорельованої послідовності чисел із заданими вимогами на основі об'єднання генератора конґруентних чисел і стохастичного кінцевого автомата, що забезпечило формування псевдовипадкових послідовностей із заданими вимогами. Одержані в дисертації теоретичні й практичні результати використані та впроваджені, на державному підприємстві "Науково-виробничий комплекс "ФОТОПРИЛАД" (м. Черкаси). У Черкаському державному технологічному університеті на кафедрі комп'ютерних систем в циклі лабораторних робіт. У товаристві з обмеженою відповідальністю Лакофарбовий завод"АВРОРА" (м. Черкаси).

2. The object of study - the processes of information security, which are stored, processed and transmitted to the computer systems and networks. The purpose of research - improving the speed and reliability of access to confidential information resources through the introduction of information and hardware redundancy. Advancing scientific and technical basis of design security systems, based on the combined processes of error-correcting coding and cryptography. Algorithms and mathematical models of the functioning of cryptographic devices encoding, decoding, and transcoding, based on specific logical functions and chetvirkovoi binary number system with a fixed number of units. Built generator congruent numbers, which provides a solution to many practical problems, including the formation of teams of cryptographic transformation of data. Develop functional and structural schemes that implement the proposed method and together provide increased speed and reliability of access to confidential information resources by 25%. Developed a method of encryption (encoding, decoding, and transcoding) with the introduction of information redundancy based dvohrozryadnih logic functions and binary-quaternary number system with a fixed number of units, thus reducing the time to access information by combining the processes of error-correcting coding and cryptography, as well as to simplify the functional circuit devices. A model of the process of improving the speed and reliability of access to confidential information resources that will inform the task of the research. An improved method for increasing the speed and reliability of access to confidential information resources through the use of stochastic generators of pseudorandom numbers with specified requirements and aligning processes with the introduction of cryptographic encryption of information redundancy, which enabled the design and development of software and hardware of practical application. Was further developed a method for constructing pseudo-random number generators to generate uniformly distributed uncorrelated sequence of numbers with the specified requirements by combining the generator congruent numbers and stochastic finite state machine, ensuring the formation of pseudo-random sequences with specified requirements. Obtained in the thesis theoretical and practical results are used and implemented at the state enterprise "Scientific and Production Complex" photodevice "(Cherkassy). In Cherkassy State Technological University in the department of computer systems in a series of laboratory work. As a limited liability paint factory" AURORA "(Cherkassy)

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. Рудницький Володимир Миколайович
2. Rudnitsky Vladimir Nikolaevich

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

VII. Відомості про офіційних опонентів та рецензентів

Офіційні опоненти

Власне Прізвище Ім'я По-батькові:

1. Кулик Анатолій Ярославович
2. Кулик Анатолій Ярославович

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. Бараннік Володимир Вікторович

2. Бараннік Володимир Вікторович

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

Рецензенти

VIII. Заключні відомості

Власне Прізвище Ім'я По-батькові голови ради Лега Юрій Григорович

Власне Прізвище Ім'я По-батькові головуючого на засіданні Лега Юрій Григорович

Відповідальний за підготовку облікових документів

Реєстратор

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