Облікова картка дисертації

I. Загальні відомості

Державний обліковий номер: 0412U002602

Особливі позначки: відкрита

Дата реєстрації: 29-05-2012

Статус: Захищена

Реквізити наказу МОН / наказу закладу:

II. Відомості про здобувача

Власне Прізвище Ім'я По-батькові:

1. Дмитришин Олександр Васильович
2. Dmytryshyn Oleksandr Vasilevich

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: 18-05-2012

Спеціальність за освітою: 8.160105

Місце роботи здобувача: Вінницький національний технічний університет

Код за ЄДРПОУ: 02070693

Місцезнаходження: 21021 м. Вінниця, вул. Хмельницьке шосе, 95

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 05.052.01

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

IV. Відомості про підприємство, установу, організацію, в якій було виконано дисертацію

Повне найменування юридичної особи: Вінницький національний технічний університет

Код за ЄДРПОУ: 02070693

Місцезнаходження: 21021 м. Вінниця, вул. Хмельницьке шосе, 95

Форма власності:

Сфера управління: Міністерство освіти і науки України

Ідентифікатор ROR: Не застосовується

V. Відомості про дисертацію

Мова дисертації:

Коди тематичних рубрик: 50.33.14

Тема дисертації:

1. Методи і засоби блокового шифрування підвищеної стійкості на основі арифметичних операцій за модулем.

2. Methods and means of the block ciphers for increased security based on the arithmetic operations after the modulo.

Реферат/анотація:

1. Об'єкт дослідження - процес криптографічного захисту інформації в комп'ютерних системах; метою роботи є підвищення рівня захищеності інформації в комп'ютерних системах шляхом розробки методів та засобів блокового шифрування підвищеної криптографічної стійкості на основі арифметичних операцій за модулем; використані методи теорії чисел, криптології, математичної статистики і методи теорії цифрових автоматів; теоретичні результати - методи симетричного блокового шифрування на основі арифметичних операцій за модулем, які передбачають використання комбінованого розгортання ключів та псевдовипадкове зав'язуванням блоків даних, що забезпечує підвищення рівня стійкості блокового шифрування до відомих криптографічних атак за рахунок ускладнення аналізу в 2^p та 2^N раз, відповідно. Структури спеціалізованих процесорів для блокового шифрування, які забезпечують підвищення швидкості

шифрування порівняно з реалізацією на основі універсальних мікропроцесорів у L разів. Метод симетричного блокового шифрування на основі арифметичних операцій за модулем, що використовує модуль як одну з складових секретного ключа; практичні результати - програмні засоби та структури спеціалізованих процесорів, які реалізують методи симетричного блокового шифрування на основі арифметичних операцій за модулем; це дає можливість підвищення рівня захищеності інформації в комп'ютерних системах; ступінь впровадження - результати роботи впроваджено у ТОВ "ВІАТЕЛ", ПП "ВІНБУДІЗОЛ" та в навчальний процес ВНТУ. Сфера(галузь) використання - виробництво програмних засобів та засобів комп'ютерної техніки.

2. A research object is the process of cryptographic security of information in computer systems; the aim of work is to improve information security in computer systems by developing methods and tools for block cipher cryptographic strength increased on the basis of arithmetic operations after the modulo; used methods of number theory, methods of cryptology, the methods of mathematical statistics,methods of automata theory; theoretical results - the method of symmetric block cipher based on the arithmetic operations after the modulo, which involves the use of the combined deployment of keys and pseudorandom tying blocks of data, which increases level of stability to the block cipher known cryptographic attacks by complicating the analysis in 2^p and 2^N times, respectively. The structure of specialized processors for the block cipher are proposed and provide a speed boost over encryption implementation based on the universal chip in L times. The method for the symmetric block cipher based on arithmetic modulo by using one of the components of the secret key as a module are improved; practical results - software tools and structures of specialized processors that implement the methods of a symmetric block cipher based on arithmetic modulo are proposed; It gives an opportunity to improve the security of information in computer systems; the degree of implementation - the results have been implemented in PLC "VIATEL", firm "VINBUDIZOL" and in the scientific process of VNTU. Scope of - the production of software and hardware.

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. Лужецький Володимир Андрійович

2. Luzhetsky Volodymyr Andreevich

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. Борисенко Олексій Андрійович
2. Борисенко Олексій Андрійович

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. Рудницький Володимир Миколайович
2. Рудницький Володимир Миколайович

Кваліфікація: д.т.н., 05.13.06

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 Квєтний Роман Наумович

Власне Прізвище Ім'я По-батькові головуючого на засіданні Квєтний Роман Наумович

Відповідальний за підготовку облікових документів

Реєстратор

Керівник відділу УкрІНТЕІ, що є відповідальним за реєстрацію наукової діяльності



Юрченко Т.А.