Облікова картка дисертації

I. Загальні відомості

Державний обліковий номер: 0413U003836

Особливі позначки: відкрита

Дата реєстрації: 26-06-2013

Статус: Захищена

Реквізити наказу МОН / наказу закладу:

II. Відомості про здобувача

Власне Прізвище Ім'я По-батькові:

1. Євдіна Алла Камілівна

2. Ievdina Alla Kamilivna

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: 20-06-2013

Спеціальність за освітою: 7.080202

Місце роботи здобувача: Інститут проблем моделювання в енергетиці ім. Г.Є. Пухова НАН України

Код за ЄДРПОУ: 05516949

Місцезнаходження: 03164, Україна, Київ, вул. Генерала Наумова, 15

Форма власності:

Сфера управління: Національна академія наук України

Ідентифікатор ROR: Не застосовується

III. Відомості про організацію, де відбувся захист

Шифр спеціалізованої вченої ради (разової спеціалізованої вченої ради): Д 26.185.01

Повне найменування юридичної особи:

Код за ЄДРПОУ:

Місцезнаходження:

Форма власності:

Сфера управління:

Ідентифікатор ROR: Не застосовується

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

Повне найменування юридичної особи: Інститут проблем моделювання в енергетиці ім. Г.Є. Пухова НАН України

Код за ЄДРПОУ: 05516949

Місцезнаходження: 03164, Україна, Київ, вул. Генерала Наумова, 15

Форма власності:

Сфера управління: Національна академія наук України

Ідентифікатор ROR: Не застосовується

V. Відомості про дисертацію

Мова дисертації:

Коди тематичних рубрик: 50.37.23

Тема дисертації:

1. Побудова реконфігуровних апаратно-програмних засобів посилення захисту інформації на основі алгоритмів блокового симетричного шифрування

2. The construction of reconfigurable hardware-software tools of strengthening the protection of the information based on symmetric block encryption algorithms

Реферат/анотація:

1. Дисертація присвячена дослідженню та розробці принципів побудови реконфігуровних апаратно-програмних засобів, що реалізують способи посилення криптографічного захисту на основі алгоритмів блокового симетричного шифрування. На основі аналізу способів посилення захисту інформації та оцінки їх обчислювальної ресурсомісткості обґрунтовано доцільність використання для їх реалізації реконфігуровних обчислювачів на базі ПЛІС. На основі аналізу принципів побудови алгоритмів БСШ запропоновано узагальнену структуру реконфігуровного криптопроцесора, в якій виокремлено компоненти, що не залежать від конкретних алгоритмів, і тому можуть бути наперед розроблені, налагоджені та перевірені. Розроблено типові структурні схеми для реалізації усіх виявлених способів посилення захисту інформації. Розроблено метод синтезу реконфігуровних криптопроцесорів, що реалізують способи посилення криптографічного

захисту, який дозволяє погоджувати спосіб посилення з характеристиками наявних обчислювальних засобів, а також прискорює процес створення конфігурацій, що завантажуються в ПЛІС. Окремі засоби посилення на основі алгоритмів БСШ для деяких типів РУО реалізовано у вигляді експериментальної системи, компоненти якої можуть бути використані для практичної реалізації запропонованого методу.

2. Dissertation is dedicated to the research and development of construction principles of reconfigurable hardware-software tools for implementing the methods of strengthening cryptographic protection based on symmetric block encryption algorithms. The possible methods of strengthening information security based on block cipher algorithms are investigated in the paper. The appropriateness of reconfigurable coprocessor on FPGA for implementing those methods is substantiated. The generalized reconfigurable crypto processor structure on the basis of construction principles of block cipher algorithms is proposed. In this structure the components that independent from certain algorithms were singled out. Those components can be pre-designed, debugged and tested in advance. A typical block diagrams to implement all identified methods of strengthening information security were developed. The method of reconfigurable crypto processors synthesis, which implements tools of strengthening cryptographic protection, was developed. This method allows user to harmonize the strengthening method with characteristics of available computing facilities. The method is able to speed up the process of creating configurations to be loaded into the FPGA. Some strengthening tools based on block cipher algorithms for certain types of reconfigurable coprocessor were realized as an experimental system. Components of this system can be used for practical realization of the proposed method.

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. Гільгурт Сергій Якович
2. Hilhurt Sergii Yakovych

Кваліфікація: к.т.н., 05.13.13

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. Гамаюн Володимир Петрович
2. Гамаюн Володимир Петрович

Кваліфікація: д.т.н., 05.13.13

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. Кравець Петро Іванович
2. Кравець Петро Іванович

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	Євдокимов Віктор Федорович
Власне Прізвище Ім'я По-батькові головуючого на засіданні	Євдокимов Віктор Федорович
Відповідальний за підготовку облікових документів	
Реєстратор	
Керівник відділу УкрІНТЕІ, що є відповідальним за реєстрацію наукової діяльності	Юрченко Т.А.