Облікова картка дисертації

I. Загальні відомості

Державний обліковий номер: 0412U002568

Особливі позначки: відкрита

Дата реєстрації: 28-05-2012

Статус: Захищена

Реквізити наказу МОН / наказу закладу:

II. Відомості про здобувача

Власне Прізвище Ім'я По-батькові:

1. Лєншина Юлія Михайлівна

2. Lyenshyna Iuliia Muhailivna

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: 25-04-2012

Спеціальність за освітою: 8.090702

Місце роботи здобувача: Харківський національний університет радіоелектроніки

Код за ЄДРПОУ: 02071197

Місцезнаходження: 61166, м. Харків, пр. Науки, 14

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 64.052.01

Повне найменування юридичної особи: Харківський національний університет радіоелектроніки

Код за ЄДРПОУ: 02071197

Місцезнаходження: проспект Науки, 14, м. Харків, Харківський р-н., Харківська обл., 61166, 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: Харківський національний університет радіоелектроніки

Код за ЄДРПОУ: 02071197

Місцезнаходження: 61166, м. Харків, пр. Науки, 14

Форма власності:

Сфера управління: Міністерство освіти і науки України

Ідентифікатор ROR: Не застосовується

V. Відомості про дисертацію

Мова дисертації:

Коди тематичних рубрик: 50.07.03

Тема дисертації:

1. Моделі та протоколи криптографічної підтримки послуг приватності з доказовим рівнем стійкості

2. Models and protocols of cryptographic support of privacy services with provable strength

Реферат:

1. Метою роботи є розробка нових та вдосконалення існуючих криптографічних моделей, протоколів та методів криптографічної підтримки послуг захисту від несанкціонованого доступу, що дозволяє забезпечити доказовий рівень стійкості послуг приватності у недовіреному середовищі. Об'єктом дослідження є процеси захисту інформації, що реалізують послуги приватності. Предметом досліджень є моделі, протоколи та методи криптографічної підтримки послуг приватності. Методи досліджень спираються на використання теорії груп, кілець та полів, теорії імовірності та математичної статистики, методів системного та структурного аналізу та методів програмного моделювання. Методи теорії груп, кілець та полів використовувалися під час дослідження методів хамелеон-гешування, групових підписів та хамелеон-підписів; методи теорії ймовірностей та математичної статистики застосовувалися при визначенні криптографічної стійкості перетворень типу електронного цифрового підпису; методи системного та структурного аналізу використовувалися під час розробки моделі політики безпеки послуг приватності з доказовим рівнем стійкості; методи програмного моделювання застосовувалися в процесі реалізації

криптографічних перетворень. Під час виконання дисертаційного дослідження було одержано такі нові наукові та практичні результати: 1. Вперше запропоновано модель політики безпеки послуг приватності у системах обслуговування замовлень, яка характеризується наданням формального доказу відсутності у таких системах ідентифікаційних даних суб'єктів за рахунок застосування механізму групового підпису, протоколу делегування повноважень з призначення псевдоніму та неінтерактивного алгоритму сповіщення користувачів, що дозволяє забезпечити доказовий рівень стійкості послуги приватності у недовіреному середовищі. 2. Вперше запропоновано метод хамелеон-гешування, який характеризується використанням криптографічних перетворень у групі точок еліптичної кривої, що дозволяє надавати криптографічну підтримку послуг приватності із експоненційним рівнем стійкості. 3. Удосконалено метод електронного цифрового підпису у групі точок еліптичної кривої, який на відміну від відомих використовує метод хамелеон-гешування та детермінований метод відображення бітового рядка у точку на еліптичній кривій, що дає можливість забезпечити криптографічну підтримку послуг приватності. Практичне значення отриманих результатів полягає у: отриманні практичних рекомендацій щодо впровадження розробленої моделі політики безпеки з доказово стійким рівнем забезпечення послуг приватності у системи обслуговування замовлень; розробці криптографічного протоколу на основі ДСТУ 4145-2002, що володіє властивостями прихованості повідомлення та непередаваності електронного цифрового підпису; формуванні пропозицій щодо створення нового формату сертифіката відкритого ключа з метою застосування вдосконаленого методу електронного цифрового підпису в існуючій національній системі електронного цифрового підпису; створенні тестового макета програмного комплексу інтернет-аукціону, що використовує запропонований метод електронного цифрового підпису у групі точок еліптичної кривої.

2. The aim is to develop new and improve existing models, protocols and methods for cryptographic support services privacy from unauthorized access, which allows for provable level of services stability of privacy in untrusted environments. The object of research are the processes of information security services that implement privacy. The subject of research is a model of cryptographic protocols and methods of support services privacy. Research methods use the theory of groups, rings and fields, the theory of probability and mathematical statistics, methods, systems and methods of structural analysis and simulation software. Methods of group theory, rings and fields used in the study of methods chameleon-hash of group signatures and chameleon-signatures, methods of probability theory and mathematical statistics used in determining the strength of cryptographic transformations such as digital signatures, methods of systemic and structural analysis were used to develop a model policy security services with a demonstrable level of confidentiality of resistance, methods of simulation software used in the implementation of cryptographic transformations. During the dissertation research were obtained by these new scientific and practical results: 1. For the first time a model of service privacy policy security systems service applications, which is characterized by providing a formal proof of the absence of such systems, the identity of the subject through the use of the mechanism of group signature, protocol, delegating authority to appoint an alias and non-interactive algorithms alert users that can provide provable level of persistence services privacy in untrusted environments. 2. For the first time a method is proposed chameleon hashing, which is characterized by the use of cryptographic transformations in the group of points of an elliptic curve, that allows to provide cryptographic services to support the level of privacy with the exponential stability. 3. Improved method of digital signature in the group of points of elliptic curve, which, unlike the existing uses hashing and chameleon-deterministic method of displaying a bit string to point to the elliptic curve, which makes it possible to provide cryptographic services to support privacy. The practical significance of these results is to provide practical guidance on implementation of the model of security policy demonstrably sustainable level of service provision in the privacy of service orders, designing a cryptographic protocol based on DSTU 4145-2002, has the properties of message hiding and non-transferability of digital signature; proposals for the formation of a new format of the certificate's public key to an improved method of digital signature in the existing national system of digital signature, creating a test layout software package online auction, which uses the proposed method signature in the group of points of elliptic curve.

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. Долгов Віктор Іванович
2. Dolgov Viktor Ivanovich

Кваліфікація: д.т.н., 20.00.16

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. Краснобеєв Віктор Анатолійович
2. Краснобеєв Віктор Анатолійович

Кваліфікація: д.т.н., 20.02.14

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. Єсін Віталій Іванович

2. Єсін Віталій Іванович

Кваліфікація: к.т.н., 20.02.12

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 Бондаренко Михайло Федорович

Власне Прізвище Ім'я По-батькові головуючого на засіданні Бондаренко Михайло Федорович

Відповідальний за підготовку облікових документів

Реєстратор

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