Облікова картка дисертації

I. Загальні відомості

Державний обліковий номер: 0409U005799

Особливі позначки: відкрита

Дата реєстрації: 23-12-2009

Статус: Захищена

Реквізити наказу МОН / наказу закладу:

II. Відомості про здобувача

Власне Прізвище Ім'я По-батькові:

1. Іванов Інокентій Юрійович
2. Ivanov Inokentiy Yuriyovych

Кваліфікація:

Ідентифікатор ORCID ID: Не застосовується

Вид дисертації: кандидат наук

Аспірантура/Докторантура: так

Шифр наукової спеціальності: 01.05.03

Назва наукової спеціальності: Математичне та програмне забезпечення обчислювальних машин і систем

Галузь / галузі знань: Не застосовується

Освітньо-наукова програма зі спеціальності: Не застосовується

Дата захисту: 17-12-2009

Спеціальність за освітою: 01.01

Місце роботи здобувача: ТОВ "Софтпанорама плюс плюс"

Код за ЄДРПОУ: 32849350

Місцезнаходження: пр-т Алішера Навої, 76, м. Київ, Україна, 02125

Форма власності:

Сфера управління:

Ідентифікатор ROR: Не застосовується

III. Відомості про організацію, де відбувся захист

Шифр спеціалізованої вченої ради (разової спеціалізованої вченої ради): Д 26.001.09

Повне найменування юридичної особи: Київський національний університет імені Тараса Шевченка

Код за ЄДРПОУ: 02070944

Місцезнаходження: вул. Володимирська, 60, м. Київ, Київська обл., 01033, 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: Київський національний університет імені Тараса Шевченка

Код за ЄДРПОУ: 02070944

Місцезнаходження: 01033, м. Київ, вул. Володимирська, 64

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. Дослідження методів захисту інформації в динамічних рівноправних групових середовищах

2. The research on information protection methods in dynamic peer group environments

Реферат:

1. Дисертація присвячена питанню побудови прототипу програмної системи, задачею якої є забезпечення захисту інформації, що зберігається і передається в умовах динамічних рівноправних групових середовищ. Формалізовано представлення довірчих зв'язків в групових середовищах; представлено груповий тип інфраструктури цифрових підписів та адаптацію схеми порогового підпису Лі-Ченга для використання в умовах інфраструктур такого типу. Розроблено модифікації алгоритмів створення цифрового підпису та перевірки пари великих чисел на простоту відповідно до схеми RSA, що передбачають можливість перенесення обчислювально складних операцій на обслуговуючий пристрій без розкриття таємних параметрів закритого ключа. Запропоновано набір алгоритмів делегування процедури узгодження ключа в неоднорідних та великих за розміром середовищах з використанням структури даних "дерево внесків". Запропоновано метод прогнозування продуктивності розподілених криптографічних алгоритмів в

динамічних середовищах, моделюючи їх роботу системами масового обслуговування. Ключові слова: групове середовище, захист інформації, делегування, продуктивність алгоритмів, інфраструктура цифрових підписів, узгодження ключа, рівноправність.

2. The thesis is devoted to the problem of construction of the prototype of software system, whose main purpose is providing the capabilities of protection of the information kept and transferred within dynamic peer group environments. The paper formalizes trust relations in group environments; the group type of digital signatures infrastructures and the Lee-Chang threshold signature algorithm adaptation to be used within such infrastructures are proposed. The developed modifications of digital signing and big numbers primality checking algorithms according to the RSA scheme provide the ability of delegation of computationally costly operations to the serving device without revealing secret parameters of the private key. A set of key agreement delegation algorithms based on the "contributions tree" data structure for heterogeneous and large environments is proposed. A distributed cryptographic algorithms productivity prediction method for dynamic groups that considers the environment as a queuing system is defined. Key words: group environment, information protection, delegation, algorithms productivity, digital signature infrastructure, key agreement, peer group.

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. Анісімов Анатолій Васильович
2. Anisimov Anatoliy Vasylyovych

Кваліфікація: д.ф.-м.н., 01.05.01

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. Лавріщева Катерина Михайлівна

2. Лавріщева Катерина Михайлівна

Кваліфікація: д.ф.-м.н., 01.05.03

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. Бублік Володимир Васильович

2. Бублік Володимир Васильович

Кваліфікація: к.ф.-м.н., 01.01.09

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 Редько Володимир Никифорович

Власне Прізвище Ім'я По-батькові головуючого на засіданні

Редько Володимир Никифорович

Відповідальний за підготовку облікових документів

Реєстратор

Керівник відділу УкрІНТЕІ, що є відповідальним за реєстрацію наукової діяльності

Юрченко Т.А.