Облікова картка дисертації

I. Загальні відомості

Державний обліковий номер: 0412U003988

Особливі позначки: відкрита

Дата реєстрації: 10-07-2012

Статус: Захищена

Реквізити наказу МОН / наказу закладу:

II. Відомості про здобувача

Власне Прізвище Ім'я По-батькові:

1. Кравченко Павло Олександрович
2. Kravchenko Pavlo Oleksandrovich

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: 06-06-2012

Спеціальність за освітою: 8.160101

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: 81.14.11.05

Тема дисертації:

1. Модель та методи забезпечення послуг безпеки у комбінованих інфраструктурах відкритих ключів

2. Model and methods of ensuring security in combined public key infrastructures

Реферат:

1. Об'єкт дослідження - процеси криптографічних перетворень у інфраструктурі відкритих ключів при реалізації узгодження загальносистемних параметрів, генерації ключів та направленого шифрування. Мета дослідження - розробка моделі та методів забезпечення послуг безпеки у комбінованій інфраструктурі відкритих ключів за рахунок використання унікальних загальносистемних параметрів та політик безпеки для множин користувачів, що дозволяє реалізувати модель взаємної недовіри та взаємного захисту. Методи дослідження: методи теорії чисел - під час розробки моделі та методів комбінованої ІВК, аналіз і синтез комбінованої ІВК, методи теорії ймовірностей при визначенні криптографічної стійкості перетворень типу направленого шифрування та показників доступності розподіленого уповноваженого на генерацію ключів, методи практичної криптографії та системного аналізу при порівнянні існуючих комбінованих ІВК, методи програмного моделювання при реалізації процесів криптографічних перетворень тощо. Наукова новизна: 1) вперше отримано модель комбінованої ІВК, яка характеризується використанням унікальних загальносистемних параметрів та політик безпеки ІВК на базі ідентифікаторів для різних множин

користувачів, забезпеченням цілісності ідентифікаторів і загальносистемних параметрів, що дозволяє реалізувати модель взаємної недовіри і взаємного захисту; 2) удосконалено метод направленого шифрування у комбінованій ІВК, який відрізняється від існуючих протоколами отримання і перевірки загальносистемних параметрів та ідентифікатора отримувача і дозволяє взаємодіяти користувачам, які не володіють погодженими загальносистемними параметрами, що дозволяє скоротити кількість необхідних операцій шифрування у 3 рази порівняно з прототипом; 3) удосконалено метод генерації особистого ключа для комбінованої ІВК, який відрізняється паралельними запитами користувача до розподіленого уповноваженого на генерацію ключів та формуванням особистого ключа користувачем, що дозволяє збільшити показники доступності для розподіленого уповноваженого на генерацію ключів; 4) удосконалено метод аналізу безпеки криптопротоколів, який відрізняється від існуючого пошуком збігів термів у попередніх сеансах протоколу та сеансах протоколу з іншими учасниками, що дозволяє знайти протоколи, які не є криптоживучими. Ступінь упровадження - результати дослідження впроваджено у ЗАТ "ІІТ" (акт від 12.10.2011 р.); у Харківському національному університеті радіоелектроніки в навчальному процесі у дисциплінах "Прикладна криптологія" та "Криптографічні системи та протоколи" (акт від 14.10.2011 р.). Сфера використання - в організаціях, що займаються проблемами розробки, дослідження, впровадження та експлуатації комплексних систем захисту інформації; у навчальному процесі під час підготовки фахівців у галузі захисту інформації.

2. Research object - the processes of cryptographic transformations in public key infrastructure for the agreement of system parameters, key generation and encryption. Research target is to develop the model and methods of ensuring security in combined public key infrastructures by using the unique system parameters and security policies for sets of users, which allows to implement a model of mutual distrust and mutual protection. Methods of research: methods of the numbers' theory - during the development of models and methods for combined PKI, analysis and synthesis of combined PKI, methods of probability theory to determine the security of cryptographic transformations such as encryption and availability of distributed private key generator, methods of practical cryptography and system analysis when comparing existing combined PKI, methods of modeling software processes in the implementation of cryptographic transformations and so on. Scientific novelty: 1) a new model of the combined public key infrastructure, which is characterized by using a unique system parameters and security policies for identity-based PKIs, ensuring the integrity of identifiers and system parameters, which allows to implement a model of mutual distrust and mutual protection; 2) improved encryption method for the combined PKI, which differs mechanisms for check system parameters and receiver identifier, and allows users, which don't have agreed system parameters, to interact and reduces the number of operations required for 3 times compared with the prototype; 3) improved key-issuing method for the combined PKI, which differs from existing in parallel requests to the distributed private key generator and calculation of private key on user side and allows to increase rate of availability of distributed private key generator; 4) improved method for security analysis of cryptoprotocols, which differs from the existing in matching terms in previous sessions of the protocol and protocol sessions with other participants, that allows to find protolols that are not forward secure. Degree of implementation - the research results are used in the LLC "IIT" (act of 12.10.2011) scientific statements, conclusions, and recommendations contained in the thesis are used in courses "Applied Cryptology" and "Cryptographic systems and protocols" which are taught to students of Kharkiv National University of Radio Electronics (act of 06.09.2010). The scope of use - in organizations that deal with development, research, implementation and operation of complex systems of protect information; in the education process for preparing specialists in the area of information security.

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. Бондаренко Михайло Федорович
2. Bondarenko Michael Fedorovych

Кваліфікація: д.т.н., 05.13.04

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. Краснобаєв Віктор Анатолійович
2. Краснобаєв 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.