Облікова картка дисертації

I. Загальні відомості

Державний обліковий номер: 0417U002808

Особливі позначки: відкрита

Дата реєстрації: 27-07-2017

Статус: Захищена

Реквізити наказу МОН / наказу закладу:

II. Відомості про здобувача

Власне Прізвище Ім'я По-батькові:

1. Єсіна Марина Віталіївна

2. Yesina Maryna Vitaliivna

Кваліфікація:

Ідентифікатор ORCID ID: Не застосовується

Вид дисертації: кандидат наук

Аспірантура/Докторантура: так

Шифр наукової спеціальності: 05.13.21

Назва наукової спеціальності: Системи захисту інформації

Галузь / галузі знань: Не застосовується

Освітньо-наукова програма зі спеціальності: Не застосовується

Дата захисту: 03-07-2017

Спеціальність за освітою: 8.17010101

Місце роботи здобувача: Харківський національний університет імені В.Н. Каразіна

Код за ЄДРПОУ: 02071205

Місцезнаходження: Україна, 61022, м. Харків, майдан Свободи,4

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 64.051.29

Повне найменування юридичної особи: Харківський національний університет імені В.Н. Каразіна

Код за ЄДРПОУ: 02071205

Місцезнаходження: майдан Свободи, 4, м. Харків, Харківський р-н., Харківська обл., 61022, 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 імені В.Н. Каразіна

Код за ЄДРПОУ: 02071205

Місцезнаходження: Україна, 61022, м. Харків, майдан Свободи,4

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. Моделі та методи порівняльного аналізу властивостей електронних підписів, визначення та обґрунтування умов їх застосування

2. Models and methods of the electronic signatures properties comparative analysis, identification and substantiation of their use conditions

Реферат:

1. Дисертаційна робота присвячена вирішенню важливої наукової задачі, яка полягає у розробці моделей, методів та засобів оцінки криптографічної стійкості електронних підписів з додатком та протидії щодо атак на основі створення колізій та зв'язування ключів, удосконалення методики їх оцінювання та порівняльного аналізу. Об'єктом дослідження є процеси криптографічних перетворень типу електронний підпис (ЕП) з додатком, що використовуються в електронних довірчих послугах, та які базуються на операціях в групі точок еліптичної кривої (ЕК) та в групі точок ЕК зі спарюванням точок ЕК. У роботі вперше запропоновано математичні моделі реалізації атаки "повне розкриття" на механізми ЕП, що базуються на математичному апараті спарювання точок ЕК, які мають поліноміальну складність, а також викладено пропозиції із можливих варіантів їх захисту. Дістали подальший розвиток: методи оцінювання захищеності механізмів ЕП на основі ідентифікаційних даних та анонімних підписів від потенційних атак; методи оцінювання та

порівняння криптографічних примітивів на основі методу аналізу ієрархій та варіацій методу визначення вагових коефіцієнтів, що дозволяє отримати більш достовірні дані оцінювання. Удосконалено метод анонімного ЕП на ЕК за рахунок того, що дії підписувача та перевірника такі самі, як описано у відповідних стандартах для звичайного підпису та перевірки в групі точок ЕК, що дозволяє виконувати впровадження функціоналу анонімного підпису в існуючі інформаційно-телекомунікаційні системи таким, що не потребує додаткових зусиль, а також можна напряму посилатися на існуючі стандарти і не вступати з ними в протиріччя.

2. The thesis is devoted to the solution of important scientific problem, which is the development of models, methods and estimation means of the electronic signatures with appendix cryptographic stability and counteracting to attacks basic on collisions creating and key binding, the technique of their estimation and comparative analysis improving. The research object is processes of cryptographic transformations such as electronic signature (ES) with the appendix, that are used in electronic trust services, and that are based on the group of elliptic curve (EC) points operations and on the group of elliptic curve (EC) points with pairing EC points. In the thesis first the mathematical models of attack "full disclosure" realization on ES mechanisms are proposed, which are based on mathematical apparatus pairing EC points, that have polynomial complexity, and set out the proposals for possible options for their protection. Get further development: methods for estimating the security of ES mechanisms based on the identification data and anonymous signatures from potential attacks; evaluation and comparison methods of cryptographic primitives based on hierarchy analysis method and variations of the determining weight indices method, that allows to receive more accurate estimation data. The anonymous ES method on EC was improved due to the fact, that the subscriber and validator actions are the same as described in the relevant standards for the usual signature and verification in the EC points group, that allows to carry out the implementation an anonymous signature functionality into existing information and telecommunications systems so, that it does not require additional efforts, and you can also directly refer to the existing standards and not to enter into conflict with them.

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. Горбенко Іван Дмитрович
2. Gorbenko Ivan Dmytrovych

Кваліфікація: д.т.н., 20.01.09

Ідентифікатор ORCID ID: Не застосовується

Додаткова інформація:

Повне найменування юридичної особи:

Код за ЄДРПОУ:

Місцезнаходження:

Форма власності:

Сфера управління:

Ідентифікатор ROR: Не застосовується

VII. Відомості про офіційних опонентів та рецензентів

Офіційні опоненти

Власне Прізвище Ім'я По-батькові:

1. Василіу Євген Вікторович
2. Василіу Євген Вікторович

Кваліфікація: д.т.н., 05.13.21

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. Чевардін Владислав Євгенійович
2. Чевардін Владислав Євгенійович

Кваліфікація: к.т.н., 05.13.21

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 Горбенко Іван Дмитрович

Власне Прізвище Ім'я По-батькові головуючого на засіданні Горбенко Іван Дмитрович

Відповідальний за підготовку облікових документів

Реєстратор

Керівник відділу УкрІНТЕІ, що є відповідальним за реєстрацію наукової діяльності

Юрченко Т.А.