Облікова картка дисертації

I. Загальні відомості

Державний обліковий номер: 0411U000505

Особливі позначки: відкрита

Дата реєстрації: 02-03-2011

Статус: Захищена

Реквізити наказу МОН / наказу закладу:

II. Відомості про здобувача

Власне Прізвище Ім'я По-батькові:

1. Мелащенко Андрій Олегович
2. Melashchenko Andrii Olegovich

Кваліфікація:

Ідентифікатор ORCID ID: Не застосовується

Вид дисертації: кандидат наук

Аспірантура/Докторантура: так

Шифр наукової спеціальності: 05.01.03

Назва наукової спеціальності: Технічна естетика

Галузь / галузі знань: Не застосовується

Освітньо-наукова програма зі спеціальності: Не застосовується

Дата захисту: 25-02-2011

Спеціальність за освітою:

Місце роботи здобувача: Інститут кібернетики ім. В.М.Глушкова НАН України

Код за ЄДРПОУ: 05417176

Місцезнаходження: 03680,МСП,м.Київ-187,пр.Академіка Глушкова, 40

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): 26.194.02

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 кібернетики ім. В.М.Глушкова НАН України

Код за ЄДРПОУ: 05417176

Місцезнаходження: 03680,МСП,м.Київ-187,пр.Академіка Глушкова, 40

Форма власності:

Сфера управління: Національна академія наук України

Ідентифікатор ROR: Не застосовується

V. Відомості про дисертацію

Мова дисертації:

Коди тематичних рубрик: 81.14.11.05

Тема дисертації:

1. Інструментарій та методи інтероперабельності Національної системи електронного цифрового підпису

2. Tools and methods for interoperability of national systems of digital signatures.

Реферат:

1. Дисертація на здобуття наукового ступеня кандидата фізико-математичних наук за спеціальністю 01.05.03 - Математичне та програмне забезпечення обчислювальних машин та систем. - Інститут кібернетики імені В.М. Глушкова НАН України, Київ, 2010. Ідентифіковано головні проблеми інтероперабельності НСЕЦП через співставлення її з еталонною моделлю кваліфікованої інфраструктури відкритих ключів QPKI. Запропоновано стандартне подання політики підписування, як базової складової бізнес-моделі ЕЦП згідно з Директивою 1999/93/ЄС. Запропоновано профілі безпеки комплекту підписів ГОСТ 34.311 + ДСТУ 4145 для інтероперабельних його імплементацій у криптомодулях. Реалізовано профілі безпеки комплекту підписів ГОСТ 34.311 + ДСТУ 4145 як бібліотеку "UPGCryptoProviderBasic" криптографічних перетворень згідно зі специфікацією Microsoft CryptoAPI. Розроблено формальну методику акредитації ЦСК, що ґрунтується на національних стандартах України, гармонізованих із європейськими. Розроблено і реалізовано специфікації тестового стенда для оцінювання ступеня інтероперабельності реалізацій еталонної моделі QPKI на основі формальної методики акредитації ЦСК. Запропоновано напрямки розвитку інфраструктури відкритих

ключів, виходячи з аналізу гомоморфного перетворення ASN.1-нотації у XSD-схему XML-документа.

2. Thesis for Ph.D. degree in physics and mathematics by specialty 01.05.03 - Mathematical and software of computers and systems. - VM Glushkov Institute of Cybernetics of the National Academy of Sciences of Ukraine, Kiev, 2010. Thesis for Ph.D. degree in physics and mathematics by specialty 01.05.03 - Mathematical and software of computers and systems. - VM Glushkov Institute of Cybernetics of the National Academy of Sciences of Ukraine, Kiev, 2010. Identified the main problems of interoperability of NSES through a comparison of it with a reference QPKI model. Proposed standard representation of the signing policy as a basic component of the business model of QPKI according to Directive 1999/93/EC. Proposed security profiles of signature suite GOST 34.311 + DSTU 4145 for interoperability of its implementation in cryptomodules. Implemented security profile for signature suite GOST 34.311 + DSTU 4145 as a crytomodule "UPGCryptoProviderBasic" which was implemented according to the Microsoft CryptoAPI specifications. Was proposed formal procedure of accreditation of CA, based on national standards of Ukraine, harmonized with the European. Developed and implemented the specification testbed for assessing the interoperability of implementations of the standard model QPKI on the basis of a formal accreditation procedure CA. Was proposed directions of development of public key infrastructure, based on the analysis of the homomorphic transform notation in the ASN.1-XSD-schema XML-document.

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. Перевозчикова Ольга Леонідівна

2. Perevozchikova Olga Leonidovna

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

VII. Відомості про офіційних опонентів та рецензентів

Офіційні опоненти

Власне Прізвище Ім'я По-батькові:

1. Анісімов Анатолій Васильович

2. Анісімов Анатолій Васильович

Кваліфікація: д.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

Власне Прізвище Ім'я По-батькові:

1. Глибовець Микола Миколайович

2. Глибовець Микола Миколайович

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

Рецензенти

VIII. Заключні відомості

Власне Прізвище Ім'я По-батькові голови ради	Сергієнко Іван Васильович
Власне Прізвище Ім'я По-батькові головуючого на засіданні	Сергієнко Іван Васильович
Відповідальний за підготовку облікових документів	
Реєстратор	
Керівник відділу УкрІНТЕІ, що є відповідальним за реєстрацію наукової діяльності	Юрченко Т.А.