Облікова картка дисертації

I. Загальні відомості

Державний обліковий номер: 0418U002016

Особливі позначки: відкрита

Дата реєстрації: 12-01-2018

Статус: Захищена

Реквізити наказу МОН / наказу закладу:

II. Відомості про здобувача

Власне Прізвище Ім'я По-батькові:

1. Пономар Володимир Андрійович
2. Ponomar Volodymyr Andriiovych

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: 14-12-2017

Спеціальність за освітою: Безпека державних інформаційних ресурсів

Місце роботи здобувача: 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

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: 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

V. Відомості про дисертацію

Мова дисертації:

Коди тематичних рубрик: 20.51.35

Тема дисертації:

1. Моделі та методи управління і захисту для криптографічних засобів у пост квантовий період
2. Models and methods of management and protection for cryptographic means in the post-quantum period

Реферат:

1. Дисертаційна робота присвячена вирішенню важливої наукової задачі, яка полягає у розробці моделей та методів захисту засобів криптографічного захисту інформації (КЗІ) стосовно загроз с фізичним доступом і підтвердження походження, реалізація меха-нізмів безпечного управління засобами КЗІ в інформаційно-телкомунікаційних системах (ІТС), оцінка можливості застосування засобами КЗІ пост квантових алгоритмів. Об'єкт дослідження – процеси криптографічних перетворень, що виконуються засоба-ми КЗІ, для захисту критичних параметрів безпеки (КПБ), підтвердження походження і виконання послуг безпеки у пост кванто-вий період. Предмет дослідження – математичні моделі та методи захисту та безпечного управління засобами КЗІ в ІТС у пост квантовий період. У дисертаційній роботі вперше розроблено комплексну модель загроз відносно засобів КЗІ на всіх етапах їх розповсюдження та використання, яка дозволяє обґрунтувати вимоги та визначити умови забезпечення анонімності, безпечного управління, захисту від несанкціонованого доступу, втручання в процес функціонування, компрометації ключів, у тому числі у пост квантовий період, виконання цих вимог є необхідним для досягнення необхідного рівня захищеності. Удосконалено методи

безпечного управління та використання засобів КЗІ, на основі застосування спеціалізованої скриптової мови, що дозволяє реалі-зувати вимоги протидії інсайдерським атакам та виконанню команд управління, які несуть загрозу функціонуванню системи, що забезпечує підвищення захищеності до третього та четвертого рівнів в сфері захисту управління засобами КЗІ та їх параметрами. Удосконалено методи оцінювання пост квантових криптографічних примітивів, що відрізняється від існуючих тим, що в даних методах використовується декілька варіантів оцінки: метод аналізу ієрархій на основі попарних порівнянь та визначення вагових коефіцієнтів методом ранжування, в яких експертна оцінка застосовується лише для визначення вагових коефіцієнтів умовних критеріїв, а при самому оцінюванні використовуються лише об'єктивні характеристики і визначена шкала оцінювання. Вказане дозволило провести оцінку математичних моделей пост квантових криптографічних алгоритмів, що пропонуються, за критерія-ми стійкості, складності, оптимальності і визначити використання яких з них дозволить забезпечити необхідні рівні захисту. Отримали подальший розвиток моделі та механізми захисту інформації в умовах застосування методів та систем квантового криптоаналізу за рахунок використання пост квантової моделі загроз та аналізу вразливостей кандидатів на пост квантові крип-тографічні алгоритми, що було перевірено при отриманні результатів порівняльного аналізу кандидатів на пост квантові крипто-графічні алгоритми стосовно можливих сфер їх застосування. Це дозволило обґрунтувати вимоги до пост квантових механізмів направленого шифрування та електронного підпису, та запропонувати рекомендації щодо їх застосування в перехідний та пост квантовий періоди в умовах обмеження просторової та часової складності, з метою підвищення криптографічної стійкості засо-бів КЗІ.

2. The thesis is devoted to solving an important scientific problem, which consists in the development of security models and protection methods for cryptographic means in terms of threats with physical access and confirmation of origin, implementation of the safe manage-ment mechanisms for cryptographic means in information telecommunication system (ITS), assessment of the possibility of applying post-quantum algorithms in the cryptographic means. The object of the research – processes of cryptographic transformations. which are per-formed by cryptographic means, in order to perform of security services in the post-quantum period. Subject of research – mathematical models and methods of protection by cryptographic means in the information and telecommunication systems in the post-quantum period. In the thesis complex threat model for cryptographic means, which covers all stages of their distribution and exploitation was developed for the first time. Such model makes it possible to justify the requirements and determine the conditions for anonymity ensuring, safe man-agement, unauthorized access protection, meddling in the process of functioning, key compromising including in the post quantum period. The methods for cryptographic means safe management and using were improved due to specialized scripting language realization, which allows implementing the bucking requirements against insider attacks and executive instruction, which pose a threat to system operation. The evaluating methods of the post-quantum cryptographic primitives were improved. Introduced evaluating method differs from existent in that it uses several evaluating methods such as: hierarchy analysis method, based on pairwise comparison and weighting coefficient evaluation with rank order method, which uses peer review only for conditional tests weighting coefficient calculation, but for evaluation process itself objective characteristics and defined rating scale are used. That allowed to evaluate proposed post-quantum cryptographic al-gorithms mathematical models according to the criteria of security, complexity, and optimality. Security models and mechanisms of infor-mation protection in terms of using quantum crypto analysis methods and systems were developed. It was possible because of using the results of post quantum cryptographic algorithms candidates' comparative analysis concerning their scope. That allowed to ground the re-quirements for post-quantum mechanisms of encryption and electronic signature as well as propose recommendations on their using in transitional and post quantum periods subject to space and time complexity restriction.

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., 20.02.12

Ідентифікатор ORCID ID: Не застосовується

Додаткова інформація:

Повне найменування юридичної особи:

Код за ЄДРПОУ:

Місцезнаходження:

Форма власності:

Сфера управління:

Ідентифікатор ROR: Не застосовується

VII. Відомості про офіційних опонентів та рецензентів

Офіційні опоненти

Власне Прізвище Ім'я По-батькові:

1. Васіліу Євген Вікторович
2. Vasiliu Evhen Viktorovych

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. Ковальчук Людмила Василівна
2. Kovalchuk Liudmyla Vasulivna

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

Рецензенти

VIII. Заключні відомості

Власне Прізвище Ім'я По-батькові голови ради	Горбенко Іван Дмитрович
Власне Прізвище Ім'я По-батькові головуючого на засіданні	Краснобаєв Віктор Анатолійович
Відповідальний за підготовку облікових документів	
Реєстратор	

Керівник відділу УкрІНТЕІ, що є відповідальним за реєстрацію наукової діяльності

Юрченко Т.А.