Облікова картка дисертації

I. Загальні відомості

Державний обліковий номер: 0416U004815

Особливі позначки: відкрита

Дата реєстрації: 01-12-2016

Статус: Захищена

Реквізити наказу МОН / наказу закладу:

II. Відомості про здобувача

Власне Прізвище Ім'я По-батькові:

1. Аулов Іван Федорович

2. Aulov Ivan Fedorovych

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: 10-11-2016

Спеціальність за освітою: 8.17010101

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 64.051.29

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 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: 20.51.35

Тема дисертації:

1. Метод та засоби встановлення особистих ключів користувачів в хмарному середовищі

2. The method and means of the installation of personal user keys in the cloud

Реферат:

1. В дисертаційній роботі запропонована модель загроз ключовим даним користувачів хмарних сервісів, що враховує об'єкти хмарного середовища, для якого реалізується загроза, мету реалізації загрози та її ймовірність. Запропоновано механізм генерації та встановлення загальної ключової пари між N-апаратними засобами захисту в хмарі, що дозволяє встановлювати ключі без передавання особистих ключів через недовірений канал зв'язку. Запропонована модель системи масового обслуговування для механізму управління ключовими даними в середовищі хмари, дозволяє оцінити ефективність реалізації механізму та провести його оптимізацію за такими показниками, як середній час відповіді, середній час очікування обробки запиту, середня довжина черги запитів та середня кількість запитів в системі. Розроблена практична реалізація кросплатформеної криптографічної бібліотеки для надання послуг з захисту інформації кінцевим користувачам в браузері з використанням мови програмування JavaScript. Ключові слова: хмарні обчислення, механізми управління ключами, модель загроз, апаратні модулі захисту, системи масового обслуговування.

2. In the thesis proposed the user's key data threat model for cloud services considering objects of the cloud environment for which threat, the purpose of realization of threat and its probability is realized is offered. The improved cloud computing threats model allows evaluating the effectiveness of remedies and minimizing losses due to the use of risk assessment and methods for assessing effectiveness. The proposed model differs from the NIST SP 500-299 that threats are considered, using profile of attacker, goal that achieved in the implementation of the threat and the potential threat. The mechanism of generation and installation the general key pair between N hardware secure modules in the cloud is proposed. It allows to establish keys without transfer private keys through not entrusted communication channel by using a modified Diffie-Hellman algorithm. For the mechanism of key management in the cloud environment in the thesis proposed the model of mass service system. It allows to estimate efficiency of realization of the mechanism and to perform its optimization on such indicators as average time of the answer, average time of expectation of processing of inquiry, average length of turn of inquiries and average amount of inquiries in system. Keywords: cloud computing, key management mechanisms, the threat model, hardware secure modules, queuing theory

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. Толюпа Сергій Васильович

2. Толюпа Сергій Васильович

Кваліфікація: д.т.н., 05.12.02

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. Горбенко Анатолій Вікторович

2. Горбенко Анатолій Вікторович

Кваліфікація: д.т.н., 05.13.06

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.