Облікова картка дисертації

I. Загальні відомості

Державний обліковий номер: 0418U002716

Особливі позначки: відкрита

Дата реєстрації: 25-06-2018

Статус: Захищена

Реквізити наказу МОН / наказу закладу:

II. Відомості про здобувача

Власне Прізвище Ім'я По-батькові:

1. Титарчук Євгеній Олександрович
2. Tytarchuk Yevhenii Oleksandrovych

Кваліфікація: 05.13.05

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: 22-06-2018

Спеціальність за освітою: Комп’ютеризовані системи управління та автоматика

Місце роботи здобувача: ФОП Титарчук Є.О.

Код за ЄДРПОУ: 3386304319

Місцезнаходження: вул. Стахурського, 2а,, м. Вінниця, Вінницький р-н., Вінницька обл., 21000, Україна

Форма власності:

Сфера управління:

Ідентифікатор ROR: Не застосовується

III. Відомості про організацію, де відбувся захист

Шифр спеціалізованої вченої ради (разової спеціалізованої вченої ради): Д 05.052.01

Повне найменування юридичної особи: Вінницький національний технічний університет

Код за ЄДРПОУ: 02070693

Місцезнаходження: вул. Хмельницьке шосе, 95, м. Вінниця, Вінницький р-н., Вінницька обл., 21021, 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: Вінницький національний технічний університет

Код за ЄДРПОУ: 02070693

Місцезнаходження: вул. Хмельницьке шосе, 95, м. Вінниця, Вінницький р-н., Вінницька обл., 21021, Україна

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, 50.01

Тема дисертації:

1. Захист персональної інформації користувачів комп'ютерних систем при використанні публічних хмарних сервісів

2. Protection of personal information of users of computer systems which use public cloud services

Реферат:

1. У дисертаційній роботі поставлена та вирішена задача підвищення ефективності захисту інформації в комп`ютерних системах, що використовують у своєму складі публічні хмарні сервіси, на основі розробки та впровадження нових методів і засобів шифрування. Розроблено метод захисту інформації користувачів у комп'ютерній системі, яка містить у своєму складі публічні хмарні сервіси комп'ютерних обчислень, на основі частково гомоморфного алгоритму шифрування, що дозволив виконувати обчислення у публічному хмарному сервісі без розкриття приватної інформації користувачів. Визначено критерій ефективності алгоритму частково гомоморфного шифрування. Розроблено теоретично обґрунтовану модифікацію методу шифрування на основі еліптичних кривих з метою надання їй гомоморфних властивостей відносно операції додавання. Розроблено математичну модель комп'ютерної системи з обмеженням доступу до інформації, що

в ній обробляється, зі сторони провайдеру хмарного сервісу з використанням частково гомоморфного алгоритму шифрування на основі еліптичних кривих. Розроблено метод декодування чисел, закодованих точками еліптичної кривої. Розроблено методику створення систем, що орієнтовані на захист приватної інформації користувачів, шляхом перетворення моделі обчислень з метою використання алгоритмів частково або повністю гомоморфного шифрування. Реалізовано програмне забезпечення, що використовує обчислювальні процедури частково гомоморфного шифрування на основі еліптичних кривих з використанням обчислювальних потужностей технічних засобів.

2. In the dissertation work was set and solved the urgent task of increasing the efficiency of information security in computer systems, using in its structure public cloud services, is based on the development and implementation of new methods and means of encryption. The method of protecting the information of users in a computer system containing the public cloud computing services, based on a partially homomorphic encryption algorithm, that's allowed to perform calculations in public cloud service without disclosing private user information is developed. The criterion of efficiency of the partially homomorphic encryption algorithm is determined. A theoretically substantiated modification of the encryption method on the basis of elliptic curves was developed in order to provide to it homomorphic properties with respect to the addition operation. A mathematical model of a computer system with limited access to the information processed in it from the side of the provider of cloud service with the use of partially homomorphic encryption algorithm on the basis of elliptic curves is developed. A method for decoding numbers encoded by points of an elliptic curve is developed. The method of creation of systems aimed at protecting private information of users by the transformation of the computing model with the purpose of using algorithms of partial or fully homomorphic encryption is developed. Software was implemented that uses computational procedures for partially homomorphic encryption based on elliptic curves using computing power of technical means.

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. Квєтний Роман Наумович

2. Kvetny Roman

Кваліфікація: д. т. н., 01.05.02

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. Вишнівський Віктор Вікторович
2. Vyshnivskyi Viktor Viktorovych

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

Власне Прізвище Ім'я По-батькові:

1. Семенов Сергій Геннадійович
2. Semenov Serhii Hennadiiovych

Кваліфікація: д. т. н., 05.13.05

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 Квєтний Роман Наумович

Власне Прізвище Ім'я По-батькові головуючого на засіданні Дубовой Володимир Михайлович

Відповідальний за підготовку облікових документів

Реєстратор

Керівник відділу УкрІНТЕІ, що є відповідальним за реєстрацію наукової діяльності Юрченко Т.А.