Облікова картка дисертації

I. Загальні відомості

Державний обліковий номер: 0418U002871

Особливі позначки: відкрита

Дата реєстрації: 11-07-2018

Статус: Захищена

Реквізити наказу МОН / наказу закладу:

II. Відомості про здобувача

Власне Прізвище Ім'я По-батькові:

1. Пригара Михайло Петрович
2. Prygara Mykhailo

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: 27-06-2018

Спеціальність за освітою: Інформаційні управляючі системи та технології

Місце роботи здобувача: Державний вищий навчальний заклад "Ужгородський національний університет"

Код за ЄДРПОУ: 02070832

Місцезнаходження: вул. Підгірна, 46, м. Ужгород, Ужгородський р-н., Закарпатська обл., 88000, 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 26.062.17

Повне найменування юридичної особи: Національний авіаційний університет

Код за ЄДРПОУ: 01132330

Місцезнаходження: пр. Космонавта Комарова 1, м. Київ, Київ, 03058, 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: Державний вищий навчальний заклад "Ужгородський національний університет"

Код за ЄДРПОУ: 02070832

Місцезнаходження: вул. Підгірна, 46, м. Ужгород, Ужгородський р-н., Закарпатська обл., 88000, 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

Тема дисертації:

1. Захищена система технічної підтримки процесів дистанційного волевиявлення

2. Secure system of technical support of processes of remote expression of will

Реферат/анотація:

1. Дисертаційна робота присвячена технічному захисту інформації (ТЗІ) у рамках системи дистанційного волевиявлення (СДВ), що гарантує збереження таємниці голосів та забезпечує свободу волевиявлення в умовах адміністративного тиску. Виявлено «слабкі місця» у захисті існуючих СДВ, зокрема специфічні загрози для інформації, відсутність протидії котрим підриває довіру громадян до її «чесної» роботи. Визначено можливості та шляхи нейтралізації цих «слабких місць». Побудовано модель СДВ, у якій завдяки введенню необмеженої кількості користувачів з правами доступу на ознайомлення з усіма файлами і процесами на сервері, але без права на будь-яку модифікацію, забезпечена можливість виявлення всіх порушень політики безпеки щодо цілісності результатів волевиявлення та конфіденційності голосів в умовах недовіри до всіх без винятку осіб, що беруть участь у розробці, створенні та обслуговуванні СДВ. Запропоновано удосконалений метод захищеного обміну даними через Інтернет, який завдяки використанню випадкових бітових послідовностей та сумісного застосування шифру Вернама і алгоритму

Диффі-Геллмана з параметрами, що гарантують стійкий захист даних, і завдяки збереженню відстані єдиності згідно з К. Шенноном, забезпечують формально обґрунтовану неможливість порушення конфіденційності даних в каналі зв'язку.

2. The dissertation is devoted to the technical protection of information within the remote voting system (RVS), which guarantees secrecy of votes and ensures freedom of expression of will in conditions of administrative pressure. "Weaknesses" are identified in the protection of existing RVS, including specific threats to information, the lack of counteraction which undermines the trust of citizens in its "honest" work. The possibilities and ways of neutralizing these "weaknesses" are determined. The model of the RVS was constructed, which, by introducing an unlimited number of users with access rights to reviewing all files and processes on the server, but without the right of any modification, was able to detect all violations of the security policy regarding the integrity of the results of the expression of will and the confidentiality of votes in conditions of distrust to all, without exception, persons involved in the development, creation and servicing of the RVS. An improved method of secure data exchange over the Internet is proposed, which, due to the use of random bit sequences and the coherent application of the Vername cipher and the Diffie-Hellman algorithm with parameters that guarantee the stable data protection, and, due to the preservation of the distance of unity according to K. Shannon, provide a formally grounded impossibility of violation confidentiality of data in the communication channel.

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. Вишняков Володимир Михайлович

2. Vyshnyakov Volodymyr

Кваліфікація: к. т. н., 05.13.00

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. Цуркан Василь Васильович

2. Tsurkan Vasyl

Кваліфікація: к. т. н., 21.05.01

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. Шелест Михайло Євгенович

2. Shelest Mykhailo

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	Корченко Олександр Григорович
Власне Прізвище Ім'я По-батькові головуючого на засіданні	Корченко Олександр Григорович
Відповідальний за підготовку облікових документів	
Реєстратор	
Керівник відділу УкрІНТЕІ, що є відповідальним за реєстрацію наукової діяльності	Юрченко Т.А.