Облікова картка дисертації

I. Загальні відомості

Державний обліковий номер: 0421U100646

Особливі позначки: відкрита

Дата реєстрації: 29-03-2021

Статус: Захищена

Реквізити наказу МОН / наказу закладу:

II. Відомості про здобувача

Власне Прізвище Ім'я По-батькові:

1. Складанний Павло Миколайович

2. Skladannyi Pavlo Mykolaiovych

Кваліфікація:

Ідентифікатор ORCID ID: Не застосовується

Вид дисертації: кандидат наук

Аспірантура/Докторантура: так

Шифр наукової спеціальності: 05.13.06

Назва наукової спеціальності: Інформаційні технології

Галузь / галузі знань: Не застосовується

Освітньо-наукова програма зі спеціальності: Не застосовується

Дата захисту: 25-03-2021

Спеціальність за освітою: Безпека інформаційних і комунікаційних систем

Місце роботи здобувача: Київський університет імені Бориса Грінченка

Код за ЄДРПОУ: 02136554

Місцезнаходження: вул. Бульварно-Кудрявська 18/2, м. Київ, 04053, 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 26.255.01

Повне найменування юридичної особи: Інститут телекомунікацій і глобального інформаційного простору Національної академії наук України

Код за ЄДРПОУ: 26022051

Місцезнаходження: Чоколівський бульвар, буд. 13, м. Київ, Київська обл., 03186, Україна

Форма власності:

Сфера управління: Національна академія наук України

Ідентифікатор ROR: Не застосовується

IV. Відомості про підприємство, установу, організацію, в якій було виконано дисертацію

Повне найменування юридичної особи: Київський університет імені Бориса Грінченка

Код за ЄДРПОУ: 02136554

Місцезнаходження: вул. Бульварно-Кудрявська 18/2, м. Київ, 04053, 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. Моделі і методи забезпечення імітостійкості та конфіденційності в системах обробки інформації

2. Models and Methods of Ensuring Imitation Resistance and Confidentiality in Information Processing Systems

Реферат:

1. Об’єкт дослідження - процеси створення та використання нових моделей та методів забезпечення імітостійкості та конфіденційності КЗІ в СОІ. Предмет дослідження - моделі та методи для забезпечення імітостійкості та конфіденційності даних в СОІ в умовах зростання потужності кібератак та ймовірності цільового ураження систем. При вирішенні поставлених задач в дисертаційній роботі було використано методи теорії ймовірностей та математичної статистики, математичного моделювання, синтезу та аналізу криптосистем. Новими результатами, отриманими в дисертаційній роботі є: вперше розроблений метод виявлення атак на програмні реалізації засобів криптографічного захисту інформації в СОІ; вперше розроблена модель функціонування (криптосхема) шифратора БАЗ (модулю криптографічного захисту інформації) в СОІ; вперше розроблений метод генерації потоку підстановок шифру багатоалфавітної заміни для забезпечення в СОІ конфіденційності та цілісності інформації; удосконалений метод оцінки ефективності застосування криптосистем, на базі врахування співвідношення середнього значення

максимальних втрат власника СОІ у випадку успішних кібератак на систему захисту до мінімальної вартості реалізації таких атак. Результати роботи впроваджені в Інституті проблем математичних машин і систем НАН України під час виконання НДР «Базис-Наука», в Національному центрі управління та випробувань космічних засобів під час виконання НДР «Розробка науково-технічних пропозицій з організації віддаленого управління станціями оптико-електронних спостережень типу 1 та типу 2», в Київському університеті імені Бориса Грінченка в рамках навчальних дисциплін «Методи побудови та аналізу криптосистем», «Математичні методи криптографії» та впроваджені в програмно-апаратне забезпечення «Центру технологій захисту інформаційних активів» при розгортанні Лабораторії криптографічного та технічного захисту інформації. Сфера використання – системи обробки інформації.

2. The dissertation is devoted to the decision of the actual scientific problem in development of theoretical and applied bases of construction and maintenance by methods of cryptographic processing of the information of imitation stability and confidentiality of the data in SOI taking into account set of cyberthreats and potential consequences of their realization. The paper proposes models and methods that form the basis for a new model of operation (cryptoscheme) of a multi-alphabetic substitution encoder (module of cryptographic protection of information) in data processing systems. In the time scale close to the real one, simulation experiments were carried out to study this cryptoschema. The obtained results showed its effectiveness in ensuring the imitation stability and confidentiality of information circulating in the SOI, as well as in providing under the influence of cyberattacks the actual functional security and survivability of the system itself. The use of a new model of multi-alphabetic replacement encoder allowed: determine the boundaries for the relative effectiveness of the information security system in SOI in cyber attacks; reduce the likelihood of forgery of the management team to an acceptable value for practical use, estimated at 10-6; reduce attack detection time by approximately 20%; reduce the cost of the system for detecting attacks on software implementations of CCI by about 25%; to ensure the possibility of automatic transition of the UAV to the mode of autonomous execution of tasks in case of detection of threats to the security of the protection system of its radio control channel and data transmission.

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. Гулак Геннадій Миколайович

2. Hulak Hennadii Mykolaiovych

Кваліфікація: к. т. н., 21.07.02

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. Зибін Сергій Вікторович
2. Zybin Serhii 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. Рудницький Володимир Миколайович
2. Rudnytskyi Volodymyr Mykolaiovych

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

Власне Прізвище Ім'я По-батькові:

1. Копійка Олег Валентинович
2. Kopiika Oleh Valentynovych

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

VIII. Заключні відомості

Власне Прізвище Ім'я По-батькові голови ради Довгий Станіслав Олексійович

Власне Прізвище Ім'я По-батькові головуючого на засіданні Довгий Станіслав Олексійович

Відповідальний за підготовку облікових документів

Реєстратор

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