Облікова картка дисертації

I. Загальні відомості

Державний обліковий номер: 0418U003188

Особливі позначки: відкрита

Дата реєстрації: 05-10-2018

Статус: Захищена

Реквізити наказу МОН / наказу закладу:

II. Відомості про здобувача

Власне Прізвище Ім'я По-батькові:

1. Гришаков Сергій Володимирович
2. Gryshakov Sergiy

Кваліфікація:

Ідентифікатор ORCID ID: Не застосовується

Вид дисертації: кандидат наук

Аспірантура/Докторантура: ні

Шифр наукової спеціальності: 21.05.01

Назва наукової спеціальності: Інформаційна безпека держави

Галузь / галузі знань: Не застосовується

Освітньо-наукова програма зі спеціальності: Не застосовується

Дата захисту: 27-09-2018

Спеціальність за освітою: Безпека інформації в спеціальних інформаційних системах

Місце роботи здобувача: Служба зовнішньої розвідки України; військова частина К1410

Код за ЄДРПОУ: 33240845

Місцезнаходження: вул. Володимирська, 33, м. Київ, Київ, 01034, Україна

Форма власності:

Сфера управління: Служба безпеки 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: Інститут спеціального зв'язку та захисту інформації Національного технічного університету України "Київський політехнічний інститут"

Код за ЄДРПОУ: 34979237

Місцезнаходження: вул Московська, 45/1, м. Київ, Київ, 01011, 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. Метод побудови рандомізованих потокових шифросистем з нелінійним випадковим кодуванням
2. Method for designing randomized stream ciphers with non-linear random coding

Реферат:

1. У дисертації розв’язано актуальну наукову задачу розробки методу побу-дови рандомізованих потокових шифросистем (РПШ) з нелінійним випадко-вим кодуванням для забезпечення безпеки державних інформаційних ресурсів. Вперше отримано аналітичні оцінки параметрів, що визначають стійкість РПШ Міхалевича-Імаї відносно атак на основі відомих шифрованих повідомлень, а також підібраних векторів ініціалізації. Вперше доведено, що клас РПШ Міхалевича-Імаї володіє суттєвою слабкістю, яка полягає в змен-шенні кількості інформації, що необхідна для відновлення за реальний час символів відкритого тексту. Вперше отримано аналітичні межі для швидкос-ті передачі інформації в РПШ Міхалевича-Імаї при заданих обмеженнях що-до ймовірності правильного прийому повідомлень законним користувачем та стійкості шифрування. Отримав подальший розвиток метод побудови РПШ, який, на відміну від раніше відомих, базується на застосуванні для випадко-вого кодування нелінійних відображень або безключових геш-функцій. Отримані нові наукові результати надають розробникові більше можливос-тей для побудови

обчислювально стійких РПШ за рахунок розширення класу перетворень, що використовуються в конструкції рандомізатора. Головним практичним результатом роботи є можливість на практиці будувати обґрун-товано стійкі РПШ без внесення змін в алгоритми шифрування для забезпе-чення безпеки державних інформаційних ресурсів.

2. This thesis is devoted to solving actual scientific problem of development the method for designing randomized stream ciphers (RSC) with nonlinear random coding to provide the security of state information resources. Analytical estimates of the parameters that determine the security of the Mihalević-Imai RSC against known ciphertext attacks and chosen initialization vectors attacks are obtained in the thesis for the first time. It was proved for the first time that a class of the Mihalević-Imai RSC has a significant weakness which consists in reducing the amount of information which is necessary for real-time recovery of the plaintext. Analytical bounds of the transmission rate for the Mihalević-Imai RSC given the limitations on the encryption security and the probability of the correct reception of messages by the legitimate receiver are obtained for the first time. The tech-nique for designing RSC was further developed. In contrast to before known ap-proaches, the proposed method is based on the employment of the nonlinear transformations or keyless hash functions for random coding. Obtained new scien-tific results give the developer more capabilities for designing computationally se-cure RSC by enlarging the class of transformations used in the construction of a randomizer. Main practical result of the thesis is a possibility to design provably se-cure RSC without changing the encryption algorithms to ensure the security of state information resources.

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. Олексійчук Антон Миколайович
2. Oleksiychuk Anton

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

VII. Відомості про офіційних опонентів та рецензентів

Офіційні опоненти

Власне Прізвище Ім'я По-батькові:

1. Кузнецов Олександр Олександрович
2. Kuznetsov Oleksandr

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. Кінзерявий Василь Миколайович
2. Kinzeryavyy 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

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.