Облікова картка дисертації

I. Загальні відомості

Державний обліковий номер: 0518U000743

Особливі позначки: відкрита

Дата реєстрації: 01-10-2018

Статус: Захищена

Реквізити наказу МОН / наказу закладу:

II. Відомості про здобувача

Власне Прізвище Ім'я По-батькові:

1. Фауре Еміль Віталійович

2. Faure Emil

Кваліфікація: д. т. н., 05.13.21

Ідентифікатор ORCID ID: Не застосовується

Вид дисертації: доктор 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: 27-09-2018

Спеціальність за освітою: Комп'ютерні системи та мережі

Місце роботи здобувача: Черкаський державний технологічний університет

Код за ЄДРПОУ: 05390336

Місцезнаходження: бульвар Шевченка, 460, м. Черкаси, Черкаський р-н., Черкаська обл., 18006, 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: Черкаський державний технологічний університет

Код за ЄДРПОУ: 05390336

Місцезнаходження: бульвар Шевченка, 460, м. Черкаси, Черкаський р-н., Черкаська обл., 18006, 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. Методологія захисту інформації на основі факторіального кодування даних

2. Methodology of information security based on factorial data coding

Реферат/анотація:

1. Дисертаційна робота спрямована на вирішення актуальної науково-технічної проблеми створення методології захисту інформації на основі факторіального кодування даних з необхідними ансамблевими, статистичними, структурними властивостями кодових послідовностей для побудови систем захисту інформації від помилок каналу зв'язку, несанкціонованої модифікації та/або несанкціонованого доступу. У роботі вдосконалено метод формування випадкової послідовності перестановок, який дозволив уникнути порушення рівномірності їх розподілу, зменшити розрядність додаткового ГПВЧ та підвищити швидкість роботи генератора. Розроблено методи роздільного факторіального кодування інформації, які дозволяють забезпечити її захист від модифікації внаслідок випадкових і умисних деструктивних дій, забезпечити властивість самосинхронізації та підвищити показники достовірності в умовах обмежень пропускної здатності каналів зв'язку. Розроблено методи нероздільного факторіального кодування інформації, які дозволяють забезпечити її захист від несанкціонованого читання та помилок каналу зв'язку, забезпечити властивість самосинхронізації та підвищити показники достовірності в умовах обмежень пропускної

здатності каналів зв'язку. Розроблено математичну модель процесу декодування факторіальних кодів, яка дозволяє оцінити їх показники достовірності. Розроблено модель узагальненого графа станів лінійного конгруентного генератора, яка дозволяє виконати класифікацію типів компонент зв'язності графа і дослідити вплив параметрів на його топологію. Удосконалено метод формування ПВП на основі лінійного конгруентного методу, який дозволяє формувати ПВП рівномірно розподілених чисел незалежно від топології графа станів генератора, мінімізувати часові витрати на вибір параметрів ЛКГ та збільшити розмір простору їх допустимих значень для досягнення максимального періоду. Удосконалено метод симетричного криптографічного захисту інформації, який дозволяє виключити можливість винесення гами та підвищити стійкість до статистичного криптоаналізу. Теоретично обґрунтовано принципи побудови комбінаційного генератора на основі підсумовування за модулем, що дозволило сформулювати загальні вимоги до параметрів генератора. Розроблено метод, критерії та методики оцінювання послідовностей випадкових чисел. Розроблено методологію захисту інформації на основі факторіального кодування даних, яка дає можливість використовувати розроблені методи та моделі в єдиній стратегії досліджень в галузі інтегрованого захисту інформації в телекомунікаційних системах і мережах та ефективно будувати відповідні системи захисту з заданими властивостями.

2. The thesis is devoted to the actual scientific and technical problem of creating the methodology of information security in telecommunication systems and networks based on factorial data coding with necessary ensemble, statistical, and structural properties of code sequences for building systems of information security against communication channels errors, unauthorized modifications and/or unauthorized access. It is shown that to date, the developed methods of integrating channel coding and encryption exist only for broadband telecommunication systems. However, these methods do not allow controlling data integrity. The solution of the problem of providing a complex information security provides related problems associated with the improvement of existing and development of new methods of cryptographic transformation and methods of generating and estimating sequences of random and pseudorandom numbers. The methodology of information security based on factorial data coding has been developed. It allows supporting the processes of creation of information security systems that implement the joint data protection from communication channel errors, unauthorized modifications and/or unauthorized access. Application of the methodology makes it possible to use the developed methods and models in a united research strategy in the field of integrated information security in telecommunication systems and networks and to effectively build appropriate security systems with given properties.

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. Рудницький Володимир Миколайович

2. Rudnytskyi Volodymyr

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

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

VII. Відомості про офіційних опонентів та рецензентів

Офіційні опоненти

Власне Прізвище Ім'я По-батькові:

1. Казмірчук Світлана Володимирівна

2. Kazmirchuk Svitlana

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. Василіу Євген Вікторович

2. Vasiliu Yevhen Viktorovich

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. Халімов Геннадій Зайдулович

2. Khalimov Gennadiy

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	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.