Облікова картка дисертації

I. Загальні відомості

Державний обліковий номер: 0825U002040

Особливі позначки: відкрита

Дата реєстрації: 29-05-2025

Статус: Відмінена

Реквізити наказу МОН / наказу закладу:

II. Відомості про здобувача

Власне Прізвище Ім'я По-батькові:

1. Грищук Ольга Михайлівна
2. Olha M. Hryshchuk

Кваліфікація:

Ідентифікатор ORCID ID: 0000-0001-6957-4748

Вид дисертації: доктор філософії

Аспірантура/Докторантура: так

Шифр наукової спеціальності: 125

Назва наукової спеціальності: Кібербезпека та захист інформації

Галузь / галузі знань: інформаційні технології

Освітньо-наукова програма зі спеціальності: 36680 Кібербезпека (125 Кібербезпека)

Дата захисту:

Спеціальність за освітою: Системи управління і автоматики

Місце роботи здобувача: Національний університет оборони України

Код за ЄДРПОУ: 07834530

Місцезнаходження: проспект Повітряних Сил, буд. 28, Київ, 03049, Україна

Форма власності: Державна

Сфера управління: Міністерство оборони України

Ідентифікатор ROR:

III. Відомості про організацію, де відбувся захист

Шифр спеціалізованої вченої ради (разової спеціалізованої вченої ради): PhD 9303

Повне найменування юридичної особи: Державний університет інформаційно-комунікаційних технологій

Код за ЄДРПОУ: 38855349

Місцезнаходження: вул. Солом'янська, буд. 7, Київ, 03110, Україна

Форма власності: Державна

Сфера управління: Міністерство освіти і науки України

Ідентифікатор ROR:

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

Повне найменування юридичної особи: Державний університет інформаційно-комунікаційних технологій

Код за ЄДРПОУ: 38855349

Місцезнаходження: вул. Солом'янська, буд. 7, Київ, 03110, Україна

Форма власності: Державна

Сфера управління: Міністерство освіти і науки України

Ідентифікатор ROR:

V. Відомості про дисертацію

Мова дисертації: Українська

Коди тематичних рубрик: 20.56, 20.56.03

Тема дисертації:

1. Симетрична криптографічна система на диференціальних перетвореннях
2. Symmetric cryptographic system based on differential transformations

Реферат:

1. Грищук О. М. Симетрична криптографічна система на диференціальних перетвореннях. – Кваліфікаційна наукова праця на правах рукопису. Дисертація на здобуття наукового ступеня доктора філософії за спеціальністю “125–Кібербезпека”. – Державний університет “Київський авіаційний інститут”, Державний університет інформаційно-комунікаційних технологій, Київ, 2025. Дисертація присвячена вирішенню актуального наукового завдання, сутність якого полягає в розробленні та дослідженні симетричної криптографічної системи захисту інформації на диференціальних перетвореннях. Встановлено, що проблема кібербезпеки в наш час набуває особливої актуальності. Показано, що перш за все під загрозу зламу підпадають існуючі криптографічні системи захисту інформації. Доведено, що подальше загострення кібербезпекової ситуації в світі спонукає до розвитку новітніх вітчизняних криптографічних систем. Тому в дисертації за мету поставлено підвищення ефективності криптографічного захисту мовної інформації за

рахунок збільшення кількості операцій та часу криптоаналізу, а також зменшення ймовірності підбору ключа шифрування. Основні наукові та практичні результати. Проаналізовано чинники, що негативно впливають на кібероборону держави. Зроблено висновок про необхідність подальшого розвитку національних криптографічних систем. З'ясовано, що відомі криптосистеми є потенційно нестійкими до квантового криптоаналізу. Обґрунтовано вид інформації, яка підлягатиме захисту в розроблюваній криптосистемі. Отримала подальший розвиток математична модель симетричної криптографічної системи захисту інформації, яка за рахунок застосування для шифрування мовної інформації інтегрального рівняння Фредгольма першого роду та диференціальних перетворень, а для розшифрування – методу регуляризації, диференціальних перетворень та некоректності вирішення оберненої задачі криптоаналізу, дозволяє забезпечити гарантовану теоретичну та практичну криптостійкість. У результаті в реальному масштабі часу здійснюється шифрування та розшифрування мовної інформації, яка подається математичними моделями гармонічних сигналів. Розроблена криптографічна система з ключем шифрування у 8 дискрет забезпечує: збільшення з 256 до 16 777 216 кількості операцій з підбору ключа шифрування порівняно з відомою системою з довжиною ключа шифрування у 8 біт; збільшення часу криптоаналізу з 0,003 діб до 194 діб; зменшення ймовірності підбору ключа шифрування. Вперше розроблено метод генерування ключів шифрування в симетричній криптографічній системі захисту мовної інформації в якому за рахунок визначених вимог до ключів шифрування, які є ядрами інтегральних рівнянь Фредгольма першого роду в режимі реального часу генерується необхідна кількість ключів у вигляді множини дискрет диференціальних спектрів елементарних функцій, що дозволяє забезпечити високу якість та одночасно надійність передачі захищеної мовної інформації. На основі розробленого методу згенеровано базу даних ключів шифрування.Набув подальшого розвитку метод криптографічного захисту мовної інформації, який за рахунок використання диференціальних перетворень, які забезпечують теоретичну криптостійкість на рівні кількості дискрет диференціального спектра, визначених за цілочислового аргументу та практичну криптостійкість, забезпечувану чутливістю параметра регуляризації до задачі криптоаналізу на всьому діапазоні його існування, дозволяє в режимі реального часу шифрувати та розшифровувати мовну інформацію, подану моделями гармонічних сигналів. Розроблений метод з точністю до параметра регуляризації забезпечує точне розшифрування мовної інформації, яка описується оберненою некоректною задачею у вигляді інтегрального рівняння Фредгольма першого роду.Доведено, що гарантована теоретична криптостійкість визначається кількістю дискрет диференціального спектра, а практична криптостійкість забезпечується нерозв'язуваністю оберненої некоректної задачі. Достовірність результатів підтверджено їх збіжністю з результатами відомих досліджень, відповідністю отриманих теоретичних результатів з результатами обчислювальних експериментів. Впровадження результатів: ГШ ЗС України; ЖВІ імені С. П. Корольова; ТОВ "Сайфер". Наукове значення дисертації полягає в подальшому розвитку вітчизняних симетричних криптографічних систем захисту інформації. Практичне значення дисертації полягає у можливості розроблення нових апаратних, програмно-апаратних та програмних криптографічних засобів захисту мовної інформації.

2. Hryshchuk O. M. Symmetric cryptographic system based on differential transformations. – Qualification scientific work in the form of a manuscript. Dissertation for the degree of Doctor of Philosophy in the specialty "125–Cybersecurity". – State University "Kyiv Aviation Institute", State University of Information and Communication Technologies, Kyiv, 2025. The dissertation is devoted to the solution of an actual scientific problem, the essence of which is the development and research of a symmetric cryptographic system of information protection based on differential transformations. It has been established that the problem of cyber security is gaining special relevance nowadays. It is shown that, first of all, existing cryptographic information protection systems are at risk of being hacked. It is proved that the further aggravation of the cybersecurity situation in the world encourages the development of new domestic cryptographic systems. Therefore, the dissertation aims to increase the efficiency of cryptographic protection of speech information by increasing the number of operations and cryptanalysis time, as well as reducing the probability of a brute force encryption key selection.Main scientific and practical results.Factors that negatively affect the state's cyber defense are analyzed.

A conclusion is made about the need for further development of national cryptographic systems. It is found that known cryptosystems are potentially susceptible to quantum cryptanalysis. The type of information that will be protected in the developed cryptosystem is substantiated.The mathematical model of a symmetric cryptographic information protection system has been further developed, which, due to the use of the Fredholm integral equation of the first kind and differential transformations for encryption of speech information, and the regularization method, differential transformations, and the incorrectness of solving the inverse cryptanalysis problem for decryption, allows ensuring guaranteed theoretical and practical cryptoresistance. As a result, encryption and decryption of speech information, which is provided by mathematical models of harmonic signals, are carried out in real time. The developed cryptographic system with an encryption key of 8 discretes provides: an increase from 256 to 16,777,216 in the number of operations for selecting the encryption key compared to the known system with an encryption key length of 8 bits; an increase in cryptanalysis time from 0.003 days to 194 days; a decrease in the probability of brute force encryption key selection.For the first time, a method for generating encryption keys in a symmetric cryptographic system for protecting speech information has been developed, in which, due to the specified requirements for encryption keys, which are the kernels of Fredholm integral equations of the first kind, the required number of keys is generated in real time in the form of a set of discrete differential spectra of elementary functions, which allows ensuring high quality and at the same time reliability of the transmission of protected speech information. Based on the developed method, a database of encryption keys has been generated.The method of cryptographic protection of speech information has been further developed, which, due to the use of differential transformations, which provide theoretical cryptoresistance at the level of the number of discrete differential spectrums defined by the integer argument and practical cryptoresistance, provided by the sensitivity of the regularization parameter to the cryptanalysis problem over the entire range of its existence, allows real-time encryption and decryption of speech information provided by harmonic signal models. The developed method, with accuracy up to the regularization parameter, provides accurate decryption of speech information, which is described by an inverse ill-posed problem in the form of an integral Fredholm equation of the first kind.It is proven that guaranteed theoretical cryptoresistance is determined by the number of discretes of the differential spectrum, and practical cryptoresistance is ensured by the unsolvability of the inverse ill-posed problem. The reliability of the results is confirmed by their convergence with the results of known studies, the correspondence of the obtained theoretical results with the results of computational experiments. Implementation of results: General Staff of the Armed Forces of Ukraine; S. P. Korolev Zhytomyr Military Institute; “Cypher” LLC. The scientific significance of the dissertation lies in the further development of domestic symmetric cryptographic information protection systems. The practical significance of the dissertation lies in the possibility of developing new hardware, software-hardware and software cryptographic means of speech information protection.

Державний реєстраційний номер ДіР: 0121U000114д

Пріоритетний напрям розвитку науки і техніки: Інформаційні та комунікаційні технології

Стратегічний пріоритетний напрям інноваційної діяльності: Розвиток сучасних інформаційних, комунікаційних технологій, робототехніки

Підсумки дослідження: Нове вирішення актуального наукового завдання

Публікації:

- Корченко О. Г., Грищук О. М. Порівняльний аналіз математичних моделей мовної інформації // Безпека інформації. 2022. Т. 28 (Вип. 2). С. 48–56. https://doi.org/10.18372/2225-5036.28.16949
- Грищук О. М. Диференціальний спектр мовної інформації // Захист інформації. 2022. Т. 24, № 3. С. 120–128. https://doi.org/10.18372/2410-7840.24.17189
- Математична модель розрахунку цінності інформації установи / О. С. Бойченко, Д. С. Костерев, І. Ю. Маковський, О. М. Грищук // Проблеми створення, випробування, застосування та експлуатації

складних інформаційних систем : зб. наук. праць. Житомир : ЖВІ, 2022. Вип. 22. С. 30–40. https://doi.org/10.46972/2076-1546.2022.22.03

- Грищук О. М. Формалізована постановка наукового завдання з розроблення симетричної криптографічної системи захисту мовної інформації // Безпека інформації. 2024. Т. 30 (Вип. 2). С. 297–302. https://doi.org/10.18372/2225-5036.30.19242
- Hryshchuk O. Mathematical Model of a Symmetrical Cryptographic System for the Protection of Speech Information Based on Differential Transformations // Кібербезпека: освіта, наука, техніка. 2024. № 1 (25). С. 401–409. https://doi.org/10.28925/2663-4023.2024.25.401409
- Грищук О. М. Алгоритм генерування ключів шифрування в симетричній криптографічній системі захисту мовної інформації на основі диференціальних перетворень // Сучасний захист інформації. 2024. № 4 (60). С. 6–15. https://doi.org/10.31673/2409-7292.2024.040001
- Корченко О. Г., Грищук О. М. Метод криптографічного захисту мовної інформації на основі диференціальних перетворень // Проблеми створення, випробування, застосування та експлуатації складних інформаційних систем : зб. наук. праць. Житомир : ЖВІ, 2024. Вип. 27 (I). С. 4–19. https://doi.org/10.46972/2076-1546.2024.27.01
- Грищук Р. В., Грищук О. М. Узагальнена модель криптосистеми Фредгольма // Кібербезпека: освіта, наука, техніка. 2019. № 4. С. 14–23. https://doi.org/10.28925/2663-4023.2019.4.1423

Наукова (науково-технічна) продукція: методи, теорії, гіпотези

Соціально-економічна спрямованість: підвищення ефективності криптографічного захисту мовної інформації

Охоронні документи на ОПІВ:

Впровадження результатів дисертації: Впроваджено

Зв'язок з науковими темами: 0121U000114д

VI. Відомості про наукового керівника/керівників (консультанта)

Власне Прізвище Ім'я По-батькові:

1. Корченко Олександр Григорович
2. Oleksandr Korchenko

Кваліфікація: д.т.н., професор, 05.13.21

Ідентифікатор ORCID ID: 0000-0003-3376-0631

Додаткова інформація:

Повне найменування юридичної особи: Державний університет інформаційно-комунікаційних технологій

Код за ЄДРПОУ: 38855349

Місцезнаходження: вул. Солом'янська, буд. 7, Київ, 03110, Україна

Форма власності: Державна

Сфера управління: Міністерство освіти і науки України

Ідентифікатор ROR:

VII. Відомості про офіційних опонентів та рецензентів

Офіційні опоненти

Власне Прізвище Ім'я По-батькові:

1. Смірнов Олексій Анатолійович
2. Oleksii Smirnov

Кваліфікація: д. т. н., професор, 21.05.01

Ідентифікатор ORCID ID: 0000-0001-9543-874X

Додаткова інформація:

Повне найменування юридичної особи: Центральноукраїнський національний технічний університет

Код за ЄДРПОУ: 02070950

Місцезнаходження: просп. Університетський, буд. 8, Кропивницький, Кропівницький р-н., 25006, Україна

Форма власності:

Сфера управління: Міністерство освіти і науки України

Ідентифікатор ROR: Не застосовується

Власне Прізвище Ім'я По-батькові:

1. Лаптєв Олександр Анатолійович
2. Oleksandr A. Laptiev

Кваліфікація: д. т. н., старший науковий співробітник, 05.13.21

Ідентифікатор ORCID ID: 0000-0002-4194-402X

Додаткова інформація:

Повне найменування юридичної особи: Київський національний університет імені Тараса Шевченка

Код за ЄДРПОУ: 02070944

Місцезнаходження: вул. Володимирська, буд. 60, Київ, 01033, Україна

Форма власності:

Сфера управління: Міністерство освіти і науки України

Ідентифікатор ROR: Не застосовується

Рецензенти

Власне Прізвище Ім'я По-батькові:

1. Гайдур Галина Іванівна
2. Halyna I. Haidur

Кваліфікація: д. т. н., професор, 05.13.06

Ідентифікатор ORCID ID: 0000-0003-0591-3290

Додаткова інформація:

Повне найменування юридичної особи: Державний університет інформаційно-комунікаційних технологій

Код за ЄДРПОУ: 38855349

Місцезнаходження: вул. Солом'янська, буд. 7, Київ, 03110, Україна

Форма власності: Державна

Сфера управління: Міністерство освіти і науки України

Ідентифікатор ROR:

Власне Прізвище Ім'я По-батькові:

1. Рабчун Дмитро Ігорович
2. Dmytro I. Rabchun

Кваліфікація: к. т. н., 21.05.01

Ідентифікатор ORCID ID: 0000-0002-5555-0910

Додаткова інформація:

Повне найменування юридичної особи: Державний університет інформаційно-комунікаційних технологій

Код за ЄДРПОУ: 38855349

Місцезнаходження: вул. Солом'янська, буд. 7, Київ, 03110, Україна

Форма власності: Державна

Сфера управління: Міністерство освіти і науки України

Ідентифікатор ROR:

VIII. Заключні відомості

Власне Прізвище Ім'я По-батькові голови ради	Іванченко Євгенія Вікторівна
Власне Прізвище Ім'я По-батькові головуючого на засіданні	Іванченко Євгенія Вікторівна
Відповідальний за підготовку облікових документів	Лазоренко Л.М.
Реєстратор	УкрІНТЕІ

Керівник відділу УкрІНТЕІ, що є відповідальним за реєстрацію наукової діяльності

Юрченко Тетяна Анатоліївна