Облікова картка дисертації

I. Загальні відомості

Державний обліковий номер: 0825U000603

Особливі позначки: відкрита

Дата реєстрації: 18-02-2025

Статус: Запланована

Реквізити наказу МОН / наказу закладу:

II. Відомості про здобувача

Власне Прізвище Ім'я По-батькові:

1. Рудницька Юлія Володимирівна
2. Yuliia V. Rudnytska

Кваліфікація: д.філософ, 126

Ідентифікатор ORCID ID: 0000-0001-6384-0523

Вид дисертації: доктор філософії

Аспірантура/Докторантура: ні

Шифр наукової спеціальності: 126

Назва наукової спеціальності: Інформаційні системи та технології

Галузь / галузі знань:

Освітньо-наукова програма зі спеціальності: Інформаційні системи та технології

Дата захисту: 25-04-2023

Спеціальність за освітою: Облік і аудит

Місце роботи здобувача: Черкаський державний технологічний університет

Код за ЄДРПОУ: 05390336

Місцезнаходження: бульвар Шевченка, буд. 460, Черкаси, Черкаський р-н., 18006, Україна

Форма власності: Державна

Сфера управління: Міністерство освіти і науки України

Ідентифікатор ROR:

III. Відомості про організацію, де відбувся захист

Шифр спеціалізованої вченої ради (разової спеціалізованої вченої ради): PhD 1061

Повне найменування юридичної особи: Черкаський державний технологічний університет

Код за ЄДРПОУ: 05390336

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

Код за ЄДРПОУ: 05390336

Місцезнаходження: бульвар Шевченка, буд. 460, Черкаси, Черкаський р-н., 18006, Україна

Форма власності: Державна

Сфера управління: Міністерство освіти і науки України

Ідентифікатор ROR:

V. Відомості про дисертацію

Мова дисертації: Українська

Коди тематичних рубрик: 20.56.02

Тема дисертації:

1. Інформаційна технологія моделювання симетричних операцій криптографічного кодування для захищених інформаційних систем критичної інфраструктури

2. The information technology for modeling symmetric operations of cryptographic encoding for protected information systems of critical infrastructure

Реферат:

1. Дисертаційна робота присвячена підвищенню продуктивності наукових досліджень процесів покращення захищеності інформаційних систем критичної інфраструктури шляхом створення нових методів моделювання та аналізу симетричних операцій криптографічного кодування. У першому розділі визначено, що одним із перспективних напрямів розвитку інформаційних систем і технологіїй є їх удосконалення для забезпечення можливості автоматизації проведення наукових досліджень направлених на підвищення захищеності інформаційних систем критичної інфраструктури. Проведено аналітичний огляду захищених інформаційних систем критичної інфраструктури який показав необхідність її постійного вдосконалення. Аналіз моделей і методів захисту інформації в інформаційних системах критичної інфраструктури показав, що вони як правило аналогічні методіам захисту інформації в інформаційних та телекомунікаційних системах, і не враховують особливості практичного застосування. Наведено результати сучасного стану

наукових досліджень пов'язаних із синтезом та аналізом операцій криптографічного кодування. Дані результати показали можливість адаптації систем захисту інформації до особливостей представлення інформації, яка використовується в інформаційних систем управління об'єктами критичної інфраструктури. Встановлено що симетричні двохоперандні операції використовуються при побудові практично всіх криптоалгоритмів, проте процесам автоматизації їх моделювання та дослідження не приділялося достатньої уваги. Формулюється мета і задачі наукового дослідження. Другий розділ присвячений побудові методу синтезу моделей симетричних двохоперандних операцій криптографічного кодування на основі кортежів симетричних одноопераднихоперацій. Для цього досліджено можливість синтезу моделей симетричних двохоперандних операцій криптографічного кодування на основі об'єднання за модулем моделей симетричних одноопераднихоперацій. Досліджено можливість синтезу симетричних двохоперандних операцій криптографічного кодування на основі дублювання та об'єднання за модулем моделей симетричних одноопераднихоперацій. Досліджено можливість синтезу моделей симетричних двохрозрядних двохоперандних операцій криптографічного кодування на основі кортежів симетричних одноопераднихоперацій перетворення інформації. Під час проведення досліджень було встановлено якісні і кількісні характеристики різних підходів до синтезу симетричних двохоперандних операцій. На основі отриманих результатів побудовано методу синтезу моделей симетричних двохоперандних операцій криптографічного кодування на основі кортежів симетричних одноопераднихоперацій та розроблено алгоритм його реалізації. Третій розділ присвячений розробленню методу синтезу груп моделей симетричних двохоперандних операцій криптографічного кодування для блокового шифрування на основі заданої симетричної двохоперандної операції. Для цього на основі узагальнення відомих методів аналізу результатів синтезу груп симетричних модифікованих запропоновано концепцію синтезу, яка дозволяє об'єднати методи синтезу груп симетричних двохрозрядних двохоперандних операцій, які досліджувалься. На основі запропонованої концепції синтезовано дві нові групи симетричних двохоперандних операцій. Побудовані групи операцій підтвердили коректність запропонованої концепції синтезу модифікованих двохоперандних операцій. На основі запропонованої концепции синтезу та аналізу синтезованих груп симетричних двохоперандних операцій розроблено метод синтезу моделей симетричних двохоперандних операцій криптографічного кодування, та алгоритм його реалізації. Четвертий розділ присвячено удосконаленню методів побудови інформаційних систем і інформаційних технологій моделювання і дослідження операцій криптографічного кодування. Для цього досліджено особливості реалізації методу синтезу моделей симетричних двохоперандних операцій криптографічного кодування на основі кортежів симетричних одноопераднихоперацій для систем блокового шифрування. На основі отриманих практичних результатів запропоновано алгоритм пошуку симетричних комутативних двохоперандних операцій. Досліджено особливості реалізації методу синтезу груп симетричних двохоперандних операцій криптографічного кодування на основі вибраної симетричної комутативної операції. На основі отриманих результатів удосконаленно методи побудови інформаційних систем і інформаційних технологій моделювання і дослідження операцій криптографічного кодування. Розроблено структуру інформаційної системи яка забезпечує реалізацію ієрархічної інформаційної технології моделювання симетричних двохоперандних операцій криптографічного кодування. Наведено алгоритми функціонування інформаційної технології на різних рівнях ієрархії. Вертикальні і горизонтальні зв'язки в даній технології реалізовано за допомогою бази даних та бази знань. Побудована інформаційна технологія порівняно з іншими дозволила автоматизувати процес синтезу та дослідження моделей симетричних двохоперандних операцій криптографічного кодування.

2. The thesis is devoted to increasing the scientific research productivity of the security improving processes in the information systems of critical infrastructure by creating new methods of symmetric cryptographic coding operations' modeling and analysis. In the first section, it is determined that one of the promising directions of information systems and technologies development is their improvement to ensure the possibility of automating the scientific research conduction aimed at increasing the security of information systems of critical infrastructure. An analytical review of protected information systems of critical infrastructure was conducted,

which showed the need for its constant improvement. As a result of analysizing the models and methods of information protection in information systems of critical infrastructure it was found that they are generally similar to the information protection methods in information and telecommunication systems, and do not take into account the peculiarities of practical application. The results of the current state of scientific research related to the synthesis and analysis of cryptographic coding operations are presented. The results have shown the possibility of information protection systems adaptation to the features of information representation, which is used in information systems of critical infrastructure objects management. It has been established that symmetric two-operand operations are used in the construction of almost all cryptographic algorithms, but not enough attention was paid to the automating processes of their modeling and research. The aim and objectives of the study are formulated. The second section is devoted to constructing a method for synthesizing the models of symmetric two-operand operations of cryptographic encoding based on tuples of symmetric one-operand operations. For this purpose, the possibility of synthesizing the models of symmetric two-operand operations of cryptographic encoding based on modulo union of symmetric one-operand operations models was investigated. The possibility of synthesizing symmetric two-operand operations of cryptographic encoding based on modulo duplication and modulo union of symmetric one-operand operations models has been studied. The possibility of synthesizing the models of symmetric two-bit two-operand operations of cryptographic encoding based on the tuples of symmetric one-operand operations of information transformation has been investigated. At the research, the qualitative and quantitative characteristics of various approaches to synthyzing symmetric two-operand operations were established. Basing on the obtained results, a method for synthesizing the models of symmetric two-operand operations of cryptographic encoding through the tuples of symmetric one-operand operations was proposed and an algorithm for its implementation was developed. The third section is devoted to developing a method of synthesizing the models' groups of symmetric two-operand operations of cryptographic encoding for block cypher based on a given symmetric two-operand operation. For this purpose, based on the generalization of the known methods of analyzing the results of the groups of symmetric modified operations synthesis, it was proposed a concept of synthesis, which allows combining the methods of synthesizing the groups of symmetric two-bit two-operand operations that were studied. Based on the proposed concept, two new groups of symmetric two-operand operations are synthesized. The constructed groups of operations confirmed the correctness of the proposed concept of modified two-operand operations synthesis. On the basis of the proposed concept of the synthesized groups of symmetric two-operand operations synthesis and analysis, a method of synthesizing models of symmetric two-operand operations of cryptographic encoding was constructed and an algorithm for its implementation has been developed. The fourth section is devoted to the improvement of the methods for building information systems and information technologies of cryptographic encoding operations modeling and research. For this purpose, the implementation features of the method for synthesizing the models of symmetric two-operand operations of cryptographic encoding based on tuples of symmetric one-operand operations for the block cipher systems were investigated. Based on the obtained practical results, a search algorithm of symmetric commutative two-operand operations is proposed. The implementation peculiarities of the method for synthesizing the groups of symmetric two-operand operations of cryptographic encoding on the basis of the selected symmetric commutative operation are studied. Basing on the obtained results, the methods for building information systems and information technologies of cryptographic encoding operations modeling and research have been improved. It has been developed the structure of the information system, which ensures the impl

Державний реєстраційний номер ДіР:

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:

- Лада Н. В., Козловська С. Г., Рудницька Ю. В. Дослідження і синтез групи симетричних модифікованих операцій додавання за модулем чотири. Центральноукраїнський науковий вісник. Технічні науки: зб. наук. пр. Кропивницький: КНТУ, 2019. Вип. 2 (33). С. 181–189. DOI: https://doi.org/ 10.32515/2664-262X.2019.2(33).181-189
- Лада Н. В., Рудницький С. В., Зажома В. М., Рудницька Ю. В. Дослідження і синтез групи симетричних модифікованих операцій правостороннього додавання за модулем чотири. Системи управління, навігації та зв'язку: зб. наук. пр. Полтава: ПНТУ, 2020. № 1 (59). С. 93–96. DOI: https://doi.org/10.26906/SUNZ.2020.1.093
- Прокопенко Т. О., Можаєв М. О., Рудницький С. В., Рудницька Ю. В. Програмування режиму ненавантаженого резервування у комп'ютерних системах критичного застосування. Вісник Черкаського державного технологічного університету. Черкаси: ЧДТУ, 2020. № 4. С. 77–83. DOI: https://doi.org/10.24025/2306-4412.4.2020.221845
- Рудницький В. М., Лада Н. В., Рудницька Ю. В., Короткий Т. К. Моделювання симетричних двохоперандних операцій криптографічного кодування на основі об'єднання одноопераднних операцій. Сучасна спеціальна техніка. 2021. № 4. С. 32–38.
- Lada N., Rudnytska Yu. Implementation of a method for synthesizing groups of symmetric double-operand operations of cryptographic information coding for block encryption systems. Innovative Technologies and Scientific Solutions for Industries / Information Technology. 2022. No. 2 (20). DOI: https://doi.org/10.30837/ ITSSI.2022.20.035
- Rudnytskyi V., Babenko V., Lada N., Tarasenko Ya., Rudnytska Yu. Constructing symmetric operations of cryptographic information encoding. Workshop on Cybersecurity Providing in Information and Telecommunication Systems (CPITS II 2021), Oct. 26, 2021. Kyiv, Ukraine: CEUR Workshop Proceedings, 2022. P. 182–194. ISSN 1613-0073 (Scopus)
- Prokopenko T., Tarasenko Ya., Lavdanska O., Rudnytskyi S., Rudnytska Yu. Developing the comprehensive technology for alternative management of complex organizational and technological objects in the conditions of cyber threats. Workshop on Cybersecurity Providing in Information and Telecommunication Systems (CPITS II 2021), Oct. 26, 2021. Kyiv, Ukraine: CEUR Workshop Proceedings, 2022. P. 170–181. ISSN 1613-0073 (Scopus)
- Лада Н. В., Рудницька Ю. В. Класифікація груп несиметричних двохоперандних операцій криптоперетворення інформації на основі перестановочних схем їх синтезу. Проблеми інформатизації: матеріали Шостої міжнар. наук.-техн. конф.: тези доп., Черкаси – Баку – Бельсько-Бяла – Харків, 14–16 листоп. 2018 р. Черкаси: ЧДТУ; Баку: ВА ЗС АР, Бельсько-Бяла: УТіГН, Харків: НТУ «ХПІ», 2018. С. 11.
- Лада Н. В., Бреус Р. В., Рудницька Ю. В., Висоцький С. В. Аналіз групи двохоперандних симетричних операцій криптоперетворення. Проблеми інформатизації: матеріали Сьомої міжнар. наук.-техн. конф.: тези доп., Черкаси – Харків – Баку – Бельсько-Бяла, 13–15 листоп. 2019 р. Черкаси: ЧДТУ; Баку: ВА ЗС АР, Бельсько-Бяла: УТіГН, Харків: НТУ «ХПІ», 2019. Т. 1. С. 85.
- Прокопенко Т. О, Рудницька Ю. В. Автоматизація проектування криптопримітивів. Проблеми інформатизації: матеріали Дев'ятої міжнар. наук.-техн. конф.: тези доп., Черкаси – Харків – Баку – Бельсько-Бяла, 16– 18 листоп. 2021 р. Черкаси: ЧДТУ; Баку: ВА ЗС АР, Бельсько-Бяла: УТіГН, Харків: НТУ «ХПІ», 2021. Т. 1. С. 85.
- Рудницька Ю. В. Короткий Т. К. Інформаційна технологія моделювання та дослідження симетричних сет-операцій. Проблеми інформатизації : Десята міжнар. наук.-техн. конф.: тези доп. Черкаси – Баку – Бельсько-Бяла – Харків, 24 – 25 листоп. 2022 р. Черкаси: ЧДТУ; Баку: ВА ЗС АР, Бельсько-Бяла: УТіГН, Харків: НТУ «ХПІ», 2022. Т. 1. С. 40.
- Рудницька Ю. В. Рудницький С. В. Моделювання симетричних операцій криптографічного кодування. Проблеми інформатизації : Десята міжнар. наук.-техн. конф.: тези доп. Черкаси – Баку – Бельсько-Бяла

– Харків, 24 – 25 листоп. 2022 р. Черкаси: ЧДТУ; Баку: ВА ЗС АР, Бельсько-Бяла: УТіГН, Харків: НТУ «ХПІ», 2022. Т. 2. С. 10.

Наукова (науково-технічна) продукція:

Соціально-економічна спрямованість:

Охоронні документи на ОПІВ:

Впровадження результатів дисертації: Впроваджено

Зв'язок з науковими темами:

VI. Відомості про наукового керівника/керівників (консультанта)

Власне Прізвище Ім'я По-батькові:

1. Прокопенко Тетяна Олександрівна
2. Prokopenko Tatiana Oleksandrivna

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

Ідентифікатор ORCID ID: Не застосовується

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

VII. Відомості про офіційних опонентів та рецензентів

Офіційні опоненти

Власне Прізвище Ім'я По-батькові:

1. Корченко Олександр Григорович
2. Oleksandr Korchenko

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

Ідентифікатор ORCID ID: Не застосовується

Додаткова інформація:

Повне найменування юридичної особи: Національний авіаційний університет

Код за ЄДРПОУ: 01132330

Місцезнаходження: проспект Любомира Гузара, буд. 1, Київ, 03058, Україна

Форма власності: Державна

Сфера управління: Міністерство освіти і науки України

Ідентифікатор ROR:

Власне Прізвище Ім'я По-батькові:

1. Кучук Георгій Анатолійович
2. Heorhii Kuchuk

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

Ідентифікатор ORCID ID: 0000-0002-2862-438X

Додаткова інформація: https://www.scopus.com/authid/detail.uri?authorId=57057781300; https://www.webofscience.com/wos/author/record/2485726; https://scholar.google.com.ua/citations?user=gHejYRUAAAAJ

Повне найменування юридичної особи: Національний технічний університет "Харківський політехнічний інститут"

Код за ЄДРПОУ: 02071180

Місцезнаходження: вул. Кирпичова, буд. 2, Харків, Харківський р-н., 61002, Україна

Форма власності: Державна

Сфера управління: Міністерство освіти і науки України

Ідентифікатор ROR:

Рецензенти

Власне Прізвище Ім'я По-батькові:

1. Голуб Сергій Васильович
2. Serhii V. Holub

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

Ідентифікатор ORCID ID: Не застосовується

Додаткова інформація:

Повне найменування юридичної особи: Черкаський державний технологічний університет

Код за ЄДРПОУ: 05390336

Місцезнаходження: бульвар Шевченка, буд. 460, Черкаси, Черкаський р-н., 18006, Україна

Форма власності: Державна

Сфера управління: Міністерство освіти і науки України

Ідентифікатор ROR:

Власне Прізвище Ім'я По-батькові:

1. Миронець Ірина Валеріївна

2. Irina Myronets

Кваліфікація: к. т. н., доц., 05.13.05

Ідентифікатор ORCID ID: Не застосовується

Додаткова інформація:

Повне найменування юридичної особи: Черкаський державний технологічний університет

Код за ЄДРПОУ: 05390336

Місцезнаходження: бульвар Шевченка, буд. 460, Черкаси, Черкаський р-н., 18006, Україна

Форма власності: Державна

Сфера управління: Міністерство освіти і науки України

Ідентифікатор ROR:

VIII. Заключні відомості

Власне Прізвище Ім'я По-батькові голови ради	Палагін Володимир Васильович
Власне Прізвище Ім'я По-батькові головуючого на засіданні	Палагін Володимир Васильович
Відповідальний за підготовку облікових документів	Зубко Ігор Анатолійович
Реєстратор	УкрІНТЕІ
Керівник відділу УкрІНТЕІ, що є відповідальним за реєстрацію наукової діяльності	Юрченко Тетяна Анатоліївна