ВІДГУК

офіційного опонента

доктора технічних наук, професора Корченка Олександра Григоровича

на дисертаційну роботу Рудницької Юлії Володимирівни

«Інформаційна технологія моделювання симетричних операцій криптографічного кодування для захищених інформаційних систем криптографічної інфраструктури»

подану на здобуття наукового ступеня доктора філософії

за спеціальністю 126 – Інформаційні системи та технології,

галузь знань 12 – Інформаційні технології

Актуальність теми дослідження

Створення та впровадження захищених інформаційних систем, особливо для управління об'єктами критичної інфраструктури є одним з пріоритетних напрямків розвитку інформаційних технологій. Слід відмітити, що процеси вирішення задач вдосконалення систем захисту інформації, в тому числі і криптографічного захисту, відносяться до наукоємних і потребують використання висококваліфікованих наукових кадрів. Одним з шляхів підвищення продуктивності наукових досліджень може стати використання інформаційних систем і технологій для моделювання і дослідження процесів захисту інформації. Дана дисертаційна робота присвячена створенню інформаційної технології моделювання і дослідження симетричних операцій криптографічного кодування.

Дисертаційна робота виконувалась відповідно до Постанови Президії НАНУ від 30.01.19 № 30 «Основні наукові напрями та найважливіші проблеми фундаментальних досліджень у галузі природничих, технічних і гуманітарних наук Національної академії наук України на 2019–2023 рр.», і НДР Черкаського державного технологічного університету: «Дослідження шляхів розвитку потокового шифрування на основі криптографічного кодування» (ДР № 0121U114389).

Виходячи з цього, тему дисертації Рудницької Ю.В. «Інформаційна технологія моделювання симетричних операцій криптографічного кодування для захищених інформаційних систем критичної інфраструктури» безумовно слід визнати важливою і актуальною.

Наукова новизна одержаних результатів

Наукова новизна результатів дисертаційного дослідження полягає в наступному:

- вперше побудовано метод синтезу моделей симетричних двохоперандних операцій криптографічного кодування на основі кортежів симетричних одноопераднних операцій шляхом встановлення взаємозв'язків та моделювання коефіцієнтів наявності розрядів першого операнда в елементарних функціях операції;
- вперше розроблено метод синтезу груп моделей симетричних двохоперандних операцій криптографічного кодування для блокового шифрування на основі заданої симетричної двохоперандної операції шляхом виконання над нею одноопераднних операцій криптографічного перетворення за умови однакової розрядності;
- удосконалено методи побудови інформаційних систем та інформаційних технологій моделювання і дослідження операцій криптографічного кодування на основі розроблених методів синтезу моделей та математичних груп моделей симетричних двохоперандних операцій криптографічного кодування шляхом їх використання як надбудови над методами побудови одноопераднних операцій.

Теоретичне та практичне значення одержаних результатів

Отримані теоретичні результати забезпечили вирішення важливої науково-технічної задачі, яка полягає в підвищенні продуктивності наукових досліджень процесів покращення захищеності інформаційних систем критичної інфраструктури. Підвищення продуктивності наукових досліджень забезпечується удосконаленням інформаційної системи та інформаційних технологій моделювання і дослідження операцій криптографічного кодування,

шляхом створення нових методів моделювання та аналізу симетричних операцій криптографічного кодування.

Практична цінність дисертаційного дослідження полягає доведенні отриманих теоретичних результатів до інженерних методик які забезпечили можливість вдосконалення інформаційної технології для моделювання і дослідження симетричних операцій криптографічного кодування та оцінки варіантів їх застосування. Практична цінність отриманих результатів підтверджена актами впровадження в виробничу діяльність ПАТ «Черкасиавтотранс» та навчальний процес Черкаського державного технологічного університету.

Структура роботи, оцінка змісту дисертації та її завершеність

Дисертаційна робота включає вступ, чотири розділи, висновки, список використаних джерел, додатків. Загальний обсяг дисертації – 162 сторінок із яких 155 сторінок основного тексту.

У вступі сформульовано актуальність теми роботи, мету і задачі дослідження, наукову новизну і практичне значення отриманих результатів, наведено відомості про публікації по темі дисертації, апробацію і реалізацію результатів дослідження.

У першому розділі дисертації обґрунтовується тема дисертаційного дослідження, проводиться аналіз сучасного стану та перспектив розвитку захищених інформаційних систем критичної інфраструктури. Наводяться результати моделювання процесів перетворення інформації на основі операцій криптографічного кодування. Формулюється мета і задачі наукового дослідження.

Другий розділ присвячений вирішенню першої наукової задачі яка полягає в розробці методу синтезу моделей симетричних двохоперандних операцій криптографічного кодування на основі кортежів симетричних одноопераднних операцій.

У третьому розділі вирішена друга наукова задача сутність якої полягала в розробці методу синтезу груп моделей симетричних двохоперандних операцій

криптографічного кодування для блокового шифрування на основі заданих симетричних двохоперандних операцій.

Четвертий розділ присвячено удосконаленню методів побудови інформаційних технологій моделювання і дослідження операцій криптографічного кодування на основі застосування розроблених методів синтезу моделей симетричних двохоперандних операцій криптографічного кодування.

У висновках наведені основні результати дисертаційного дослідження.

У додатках подано акти про впровадження результатів дисертаційної роботи, списки публікацій з основними результатами дисертаційного дослідження, та публікацій які засвідчують апробацію дисертації.

Дисертація є завершеною самостійною роботою виконаною на достатньому науковому рівні. Отримані результати підтверджують досягнення поставленої мети. Здобувач володіє методологією наукових досліджень і успішно використовує її на практиці.

Відсутність (наявність) порушень принципів академічної доброчесності

Дисертаційна робота є оригінальною авторською науковою працею, в якій відсутні порушення принципів академічної доброчесності.

Повнота викладення дисертації в опублікованих роботах

Основні результати дисертаційної роботи викладено в 12 друкованих працях, у тому числі: 5 статей, опубліковані у фахових виданнях України категорії Б; 2 статті у збірнику матеріалів конференції «CPITS-II 2021», проіндексовані в Scopus; 4 тезах доповідей на міжнародних науково-технічних конференціях.

Зауваження по дисертації.

1. На мою думку аналітичний огляд систем легкої криптографії необхідно було деталізувати і розширити. Констатація напрямів її з переліками відповідних наукових публікацій не дозволила повною мірою показати

існуючий взаємозв'язок між легкою криптографією і криптографічним кодуванням.

2. Направленість наукового дослідження на забезпечення захищеності інформації в інформаційних системах критичної інфраструктури приводить до зменшення області застосування отриманих наукових і практичних результатів.

3. В різних наукових публікаціях існують різні трактування симетричних і несиметричних криптосистем, криптоалгоритмів та операцій криптографічного перетворення. Було б доцільно автору навести дані визначення, а не обмежитися посиланнями на літературні джерела (ст. 32, 37). На мою думку, було б доцільно звернути увагу та дослідити комутативні і не комутативні властивості симетричних операцій криптографічного кодування.

4. На ст. 50 і 51 присутні технічні описки в індексах, які не вплинули на результати виведення моделей двохоперандних операцій криптографічного кодування $O^*_{3,1}$, та $O^*_{3,4}$.

5. Відсутність детального опису реалізації взаємозв'язків між різними рівнями ієрархії в інформаційній технології, а також особливостей представлення методів синтезу операцій в базі знань, зменшують практичну цінність дисертаційної роботи.

Зазначені зауваження не впливають на загальну оцінку роботи як позитивного внеску в науку, і можуть розглядатися як план подальших наукових досліджень, та впровадження отриманих результатів в практику побудови легких криптографічних систем.

Висновок щодо відповідності дисертації вимогам, які висуваються до наукового ступеня доктора філософії

Дисертаційна робота Рудницької Ю.В. на тему «Інформаційна технологія моделювання симетричних операцій криптографічного кодування для захищених інформаційних систем критичної інфраструктури», є завершеною науковою працею, в якій отримані нові науково обґрунтовані результати, що в сукупності вирішують важливу науково-технічну задачу підвищення продуктивності наукових досліджень процесів покращення захищеності інформаційних систем критичної інфраструктури шляхом створення нових

методів моделювання та аналізу симетричних операцій криптографічного кодування. Дана дисертація відповідає вимогам до дисертаційного дослідження на здобуття наукового ступеня доктора філософії, наведеним у Постанові Кабінету Міністрів України № 44 від 12.01.2022 «Про затвердження Порядку присудження ступеня доктора філософії та скасування рішення разової спеціалізованої вченої ради закладу вищої освіти, наукової установи про присудження ступеня доктора філософії».

Дисертаційна робота може бути представлена для офіційного захисту у разовій спеціалізованій вченій раді, а її автор, Рудницька Юлія Володимирівна, заслуговує на присудження наукового ступеня доктора філософії за спеціальністю 126 – Інформаційні системи та технології, галузь знань 12 – Інформаційні технології.

Рецензент:
Заслужений діяч науки і техніки України,
лауреат Державної премії України в галузі науки і техніки,
доктор технічних наук, професор,
завідувач кафедри безпеки інформаційних технологій
Національного авіаційного університету

Олександр КОРЧЕНКО

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ * НАЦІОНАЛЬНИЙ АВІАЦІЙНИЙ УНІВЕРСИТЕТ * 01132330 * МІСТО КИЇВ *

засвідчую
Вчений секретар
Національного авіаційного університету
М. Лемешкін