ВІДГУК

офіційного опонента
Пєвнєва Володимира Яковлевича
на дисертаційну роботу Бондаренка Микити Олеговича
« Моделі та методи інформаційної технології створення
криптосистем на основі функцій дійсних змінних»,
представлену на здобуття наукового ступеня доктора філософії
в галузі знань 12 Інформаційні технології
за спеціальністю 122 – Комп'ютерні науки

Актуальність теми. Актуальність роботи зумовлена подальшим розвитком штучного інтелекту та квантових комп'ютерів. Розвиток цих напрямків дозволяє досить швидко вирішувати переборні завдання, до яких можливо віднести і криптологічні. В сфері криптографії з'являються нові направлення, розвиток яких буде визначати шлях цих систем в майбутньому. Вказані особливості предметної області дослідження визначають актуальність теми роботи Бондаренка М. О.

У дисертаційній роботі розв'язано науково-практичне завдання розробки моделей та методів криптографічних систем на основі функцій дійсної змінної, яке має важливе значення в процесі розвитку інформаційних технологій.

Тема відповідає пріоритетним напрямкам наукових досліджень Сумського державного університету. Дослідження виконано відповідно до плану науково-дослідних робіт за держбюджетною темою «Методи, математичні моделі та інформаційні технології аналізу і синтезу інфокомунікаційних систем» (ДР № 0118U006971, 2018-2023). Роль автора в роботі полягала в розробці моделей та методів шифрування і дешифрування даних для застосування в інфокомунікаційних системах.

Обгрунтованість і достовірність наукових положень, висновків і рекомендацій. На основі аналізу змісту розділів дисертаційної роботи можна зробити висновок про належну обгрунтованість наукових положень дисертаційної роботи. Достовірність результатів теоретичних досліджень грунтується на основі функцій дійсної змінної та теорії інтегральної непропорційності та підтверджується результатами відповідних

експериментальних досліджень. Наукові тези та висновки, викладені в дисертації, мають тверде теоретичне обгрунтування. . Автор успішно вирішив науково-прикладну задачу розробки моделей, методів, алгоритмів і програмних засобів створення криптосистем на основі функцій дійсних змінних. Це дозволило отримати низку нових і суттєвих наукових результатів. Отримані наукові результати застосовані під час експлуатації програмного забезпечення, що реалізує запропоновані методи.

До основних наукових результатів слід віднести наступне:

– удосконалено моделі та методи створення криптосистем на основі функцій дійсної змінної;

– уперше впроваджено метод дешифрування шляхом використання інтегральних функцій непропорційності, що дозволяє визначати невідомі коефіцієнтів в сумі функцій дійсної змінної;

– уперше розроблено комбіновану криптосистему, яка поєднує шифрування за допомогою суми функцій дійсної змінної та шифрування за допомогою інтегральної функції непропорційності;

– удосконалено метод шифрування даних шляхом впровадження додаткового елементу перестановки функцій-ключів;

– уперше розроблено криптосистему для захисту зображень на основі функцій дійсної змінної шляхом використання функцій інтегральної непропорційності, де інше довільне зображення використовується в якості криптографічного ключа.

Практична значення отриманих результатів. Отримані результати дозволяють практичну реалізацію запропонованих криптосистем. Усі теоретичні розробки дисертації автором доведено до інженерних методик, алгоритмів, з використанням запропонованої інформаційної технології шифрування та дешифрування даних за допомогою функцій дійсних змінних. Запропонована криптосистема для захисту зображень з використанням довільного зображення як ключа може бути застосована для експериментального захисту візуальної інформації в різних сферах. Створене

програмне забезпечення для реалізації розроблених криптографічних алгоритмів може бути використане для проведення подальших досліджень та експериментів в області криптографії на основі функцій дійсної змінної. Результати експериментальних досліджень крипостійкості розроблених методів можуть бути використані для порівняльного аналізу різних підходів до шифрування.

Повнота викладу результатів роботи в опублікованих працях. За темою дисертаційної роботи опубліковано 10 наукових праць, з них: 4 статті у наукових фахових виданнях України, з яких 2 включені до міжнародних наукометричних баз (у тому числі, одна стаття у виданні, що індексується міжнародною наукометричною базою Scopus), 4 публікації за матеріалами конференцій, 2 патенти на корисну модель.

Участь здобувача у роботах, що опубліковані у співавторстві, зазначена у дисертаційній роботі. Опубліковані матеріали повністю відображають зміст дисертації та відповідають вимогам пункту 8 «Порядку присудження ступеня доктора філософії та скасування рішення разової спеціалізованої вченої ради закладу вищої освіти, наукової установи про присудження ступеня доктора філософії», затвердженого Постановою КМУ від 12.01.2022 р. №44 зі змінами від 03.05 2024 р. (Постанова КМУ від №507).

Оцінка змісту дисертації. Дисертація складається зі анотації, вступу, чотирьох розділів, висновків, списку використаних джерел і одного додатку. Загальний обсяг дисертації складає 170 сторінок, з яких анотація на 5 сторінках, основна частина на 182 сторінках, список використаних джерел із 182 найменувань на 20 сторінках і додаток на 3 сторінках. За структурою, мовою та стилем викладення дисертаційна робота відповідає вимогам МОН України.

У вступі обгрунтовано актуальність теми дослідження, сформульовано мету та завдання роботи, визначено об'єкт, предмет та методи дослідження, розкрито наукову новизну та практичне значення отриманих результатів.

Перший розділ присвячено аналізу сучасного стану та перспектив розвитку криптологічних систем. Автором проведено грунтовний огляд

існуючих підходів до побудови криптосистем, методів реалізації, виявлено їх недоліки та окреслено напрямки подальших досліджень.

У другому розділі запропонована математична модель повідомлення, зашифрованого за допомогою суми функцій дійсної змінної. Ці функції представлені у вигляді одновимірних масивів. Збільшення криптостійкості досягається завдяки використанню генераторів псевдовипадкових чисел. Запропонований метод дешифрування шляхом використання функцій інтегральної непропорційності дозволяє обчислити невідомі коефіцієнти при відомих функціях в їх сумі.

У третьому розділі досліджено криптосистему на основі функцій дійсної змінної. Досліджено метод розшифрування повідомлення, зашифрованого сумою функцій дійсної змінної, для якого використовуються властивості функцій інтегральної непропорційності до розпізнавання невідомих коефіцієнтів. Визначені і надані обмеження, які накладаються на ключові функції. Запропоновані модифікації наведених алгоритмів для подальшого посилення криптостійкості.

У четвертому розділі досліджено можливості створення спеціалізованих криптосистем для захисту зображень, використовуючи інше зображення в якості ключа. Для цього спроектована криптосистема на основі дійсних чисел, розроблені алгоритми шифрування та дешифрування, які використовують властивості інтегральної непропорційності. Експериментально перевірено робота запропонованого алгоритму. Виявлена чутливість алгоритму до змін ключа, складність зламу системи методом брутфорсу, та здатність до декореляції шифротексту.

Дисертаційна робота оформлена відповідно до вимог наказу МОН України від 12 січня 2017 р. № 40 «Про затвердження вимог до оформлення дисертації».

Таким чином, у дисертаційній роботі наукове завдання було виконано в повному обсязі, і здобувач глибоко осягнув методологію наукових досліджень.

Академічна доброчесність. Порушень академічної доброчесності в дисертації та наукових публікаціях, у яких висвітлені основні наукові результати роботи, не виявлено. Наукові результати, які винесено здобувачем на захист, отримано самостійно і висвітлено в опублікованих роботах. У роботах, опублікованих у співавторстві, використано тільки ті ідеї, положення та розрахунки, які є результатом особистих наукових пошуків.

Зауваження до змісту дисертаційної роботи

1. При аналізі криптоалгоритмів не було використано Національного стандарту шифрування ДСТУ 7624:2014 («Калина»).

2. При шифруванні тексту велику роль грають коефіцієнти *k*, які виробляються випадковим чином. Вимоги до генераторів у роботі не розглядалися. Залежно від використовуваних генераторів ПВЧ змінюватимемося і довжина зашифрованої послідовності, яка може у багато разів перевищувати розмітку елемента, що шифрується (8 біт). Це призводить до порушення однієї з вимог до сучасних криптосистем про не перевищення розміру шифрованої інформації.

3. На мій погляд було надмірним включення до тексту дисертаційної роботи параграфів, які показували роботу запропонованих алгоритмів для відновлення випадкового періодичного сигналу.

4. У роботі немає оцінки ефективності пропонованих алгоритмів для шифрування/розшифрування текстової інформації (розмір інформації, що передається, час шифрування/розшифрування) та їх порівняння з існуючими.

5. У роботі мають місце описки та неточності. Наприклад, стор. 20. «Більшість сучасних криптографічних систем, таких як AES та RSA, базуються на операціях з цілими числами»; стор. 99 «Отриманий шифротекст представляється у вигляді T одновимірних масивів y(j,i) …». У тексті роботи багаторазово використовується коефіцієнт *k*, з різним смисловим наповненням.

6. Оформлення тексту дисертації не відповідає вимогам ДСТУ 3008:2015 (оформлення списків, таблиць).

Висновки. Дисертаційна робота Бондаренка Микити Олеговича. є завершеною науково-дослідною роботою, яка містить науково-обгрунтовані результати, має наукову новизну та дає перспективи подальших досліджень. Тематика проведених дослідження за змістом відповідає галузі знань 12 Інформаційні технології та спеціальності 122 Комп'ютерні науки.

Враховуючи актуальність теми, отримані результати та практичну значущість вважаю, що дисертаційна робота Бондаренка Микити Олеговича «Моделі та методи інформаційної технології створення криптосистем на основі функцій дійсних змінних» відповідає вимогам чинного законодавства України, що передбачені в п.6, 7, 8, 9 «Порядку присудження ступеня доктора філософії та скасування рішення разової спеціалізованої вченої ради закладу вищої освіти, наукової установи про присудження ступеня доктора філософії», від 12 січня 2022 р. № 44 зі змінами від 03.05 2024 р. (Постанова КМУ від №507) та вимогам до оформлення дисертації МОН України від 12.01.2017 № 40, сам автор, Бондаренко Микита Олегович, заслуговує присудження йому наукового ступеня доктора філософії зі спеціальності 122 Комп'ютерні науки.

Офіційний опонент:
професор кафедри комп'ютерних мереж,
систем і кібербезпеки
Національного аерокосмічного університету
ім. М.Є. Жуковського «ХАІ»
доктор технічних наук, доцент Володимир ПЄВНЄВ
«08» жовтня 2024 року

Підпис Пєвнєва Володимира Яковлевича **засвідчую**:
Учений секретар Національного аерокосмічного
університету ім. М.Є. Жуковського «ХАІ»

Тетяна БОНДАРЄВА