Голові разової спеціалізованої вченої
ради Національного університету
«Львівська політехніка»
д.т.н., професору Василю ЛИТВИНУ

ВІДГУК ОФІЦІЙНОГО ОПОНЕНТА

на дисертаційну роботу Лукащука Юрія Андрійовича «Інформаційна технологія захисту даних у реальному часі для мобільних смарт-систем з використанням нейроподібних мереж», подану на здобуття наукового ступеня доктора філософії за спеціальністю 122 «Комп'ютерні науки» у галузі знань 12 «Інформаційні технології»

1. Актуальність теми дисертаційної роботи

На сучасному етапі розвитку інформаційних технологій, зосереджених на криптографічному захисті даних, спостерігається розширення сфер їх використання, зокрема у секторі мобільних смарт-систем. В таких системах критично важливим є забезпечення шифрування та дешифрування даних в режимі реального часу за допомогою апаратно-програмних комплексів, які відповідають встановленим критеріям енергоефективності, компактності, а також обмеженням за часом та вартістю розробки. Для створення ефективних апаратно-програмних засобів для криптографічного захисту інформаційних технологій необхідно використовувати широкий спектр сучасної компонентної бази, такої як програмовані логічні інтегральні схеми (ПЛІС) типу FPGA, мікроконтролери тощо, а також розробляти нові методи, алгоритми та структури для реалізації процесів криптографічного шифрування і дешифрування. Отже, надзвичайно актуальними стають завдання розробки нових та удосконалення існуючих методів і апаратно-програмних засобів криптографічного захисту для мобільних смарт-систем, які мають забезпечувати високі показники технічної ефективності та експлуатації.

Одним із методів створення таких апаратно-програмних засобів криптографічного захисту є використання автоасоціативних нейронних мереж прямого поширення, які навчаються за методом головних компонент. Особливістю цих нейронних мереж є можливість використання таблиць макрочасткових добутків, а також заздалегідь розрахованих вагових коефіцієнтів і використання базису елементарних арифметичних операцій для створення нейроподібних елементів. На основі цих нейроподібних елементів формується нейронна мережа, яка забезпечує шифрування та дешифрування даних. Високі технічні та експлуатаційні показники при реалізації нейроподібних засобів шифрування та дешифрування досягаються за допомогою проблемно-орієнтованого підходу, який передбачає синтез програмних і апаратних засобів. Цей процес взаємодії програмних (універсальних) і апаратних (спеціалізованих) компонентів сприяє високій ефективності використання обладнання та скороченню часу необхідного для їх розробки.

З вищевикладеного стає зрозумілим, що для створення інформаційних технологій нейроподібного лінійного захисту даних у реальному часі в мобільних смарт-системах найоптимальнішим є інтегрований підхід. Такий підхід включає в себе застосування засобів, методів та моделей для шифрування та дешифрування даних, використання сучасної елементної бази, методики паралелізації процесів, автоматизацію програмування та інструменти автоматизованого проектування.

2. Ступінь обґрунтованості наукових положень, висновків і рекомендацій

Наукові положення, висновки та рекомендації, представлені в дисертаційній роботі, є повністю обґрунтованими, оскільки вони логічно витікають з результатів, одержаних за допомогою точних математичних перетворень, що базуються на методах SVD та матричного обертання Якобі. Чіткість та послідовність етапів досліджень також підкреслюють конкретність викладених у роботі положень.

Достовірність отриманих результатів підкріплена виправданістю таких аспектів: розробка апаратно-програмних засобів для нейроподібного шифрування/дешифрування даних в реальному часі з високими техніко-експлуатаційними характеристиками; оптимізація часу обчислення скалярного добутку з плаваючою комою в нейроподібних елементах; зростання ефективності використання обладнання при реалізації нейроподібного елемента та мережі; вибір оптимальної елементної бази для створення засобів криптографічного захисту даних у реальному часі; скорочення часу налаштування нейроподібної мережі для шифрування та дешифрування даних, а також успішна апробація результатів дослідження на наукових конференціях. Наукова новизна та висновки роботи мають надійне наукове підґрунтя. Теоретична основа, логічність досліджень, експериментальні докази та результати комп'ютерної симуляції пропонованих методів забезпечують обґрунтованість та достовірність висновків.

3. Наукова новизна результатів досліджень

Дисертація Лукащука Ю. А. присвячена розробці нових та вдосконаленню існуючих методів, моделей та програмно-апаратних засобів для лінійного нейроподібного захисту даних у реальному часі з високими технічними та експлуатаційними характеристиками, призначених для мобільних смарт-систем. Оригінальність дослідження забезпечена через грамотне формулювання наукових завдань, використання адекватних методів їх рішення, застосування універсальних наукових методів дослідження, а також через інтеграцію досягнень вітчизняної та міжнародної наукової спільноти, відображених у науковій літературі.

До ключових і новаторських результатів дисертаційного дослідження можна віднести:

1. Вперше розроблено інформаційну технологію нейроподібного захисту даних у реальному часі із симетричними ключами (архітектура нейромережі, матриці вагових коефіцієнтів та коди маскування) для смарт-систем.
2. Вперше розроблено модель попередніх налаштувань для реалізації нейроподібного шифрування та дешифрування даних.
3. Вперше розроблено метод таблично-алгоритмічного обчислення скалярного добутку з плаваючою комою в нейроподібних елементах.
4. Вдосконалено нейроподібну мережу прямого поширення автоасоціативного типу на основі парадигми «модель послідовних геометричних перетворень» і адаптовано її до нейроподібного шифрування-дешифрування.
5. Вдосконалено метод вибору елементної бази для синтезу засобів криптографічного захисту даних у реальному часі.
6. Вдосконалено метод обчислення вагових коефіцієнтів.

4. Зміст дисертації та відповідність встановленим вимогам

Дисертаційне дослідження представляє собою повністю сформовану наукову роботу. Дисертація складена з вступу, чотирьох основних розділів, висновків, а також списку використаних джерел, який включає 152 позиції. Загальна кількість сторінок дисертації становить 152, з яких 135 сторінок – це основний текст. Зміст дисертації та її логічна послідовність відповідають цілям та завданням поставленого дослідження. Рукопис дисертації відрізняється цілісністю у вирішенні визначеної мети. Проте, варто відмітити, що в деяких розділах висновки мають дещо декларативний характер.

Розділ 1 «Аналіз методів, алгоритмів і засобів нейромережевого захисту даних у мобільних смарт-системах» описує проведений аналіз архітектур нейронних мереж. Проведено аналіз методів та алгоритмів навчання у результаті чого орієнтовано задачі нейромережевого шифрування-дешифрування даних нейроподібної мережі прямого поширення автоасоціативного типу на основі парадигми «модель послідовних геометричних перетворень» шляхом неітеративного обчислення вагових коефіцієнтів, що забезпечило повторюваність результатів і орієнтацію на апаратну реалізацію.

Розділ 2 «Адаптація автоасоціативної нейронної мережі до задач криптографічного захисту даних і розроблення імітаційної моделі обчислення вагових коефіцієнтів» описує вдосконалену і орієнтовану на задачі нейромережевого шифрування-дешифрування даних нейроподібну мережу прямого поширення автоасоціативного типу на основі парадигми «модель послідовних геометричних перетворень». Вибрано для синтезу СЗПД у реальному часі такі принципи: конвеєризації та просторового паралелізму; модульності;

програмованості архітектури блоків кодування-декодування і шифрування-дешифрування даних за допомогою використання програмованих логічних інтегральних мікросхем; змінності складу обладнання; спеціалізації та адаптації апаратно-програмних засобів до структури алгоритмів нейроподібного шифрування та дешифрування даних; відкритості програмного забезпечення.

Розділ 3 «Розроблення інформаційної технології нейроподібного криптографічного захисту даних» описує розроблену інформаційну технологію нейроподібного криптографічного захисту даних у реальному часі із симетричними ключами: (матриці вагових коефіцієнтів, архітектура нейроподібної мережі та коди маскування).

Запропоновано розроблення інформаційної технології нейроподібного криптографічного захисту даних у реальному часі здійснювати на базі інтегрованого підходу, який охоплює: дослідження та розроблення теоретичних основ нейроподібного криптографічного захисту даних; дослідження та розроблення нових алгоритмів та структур нейроподібного шифрування та дешифрування даних, орієнтованих на сучасну елементну базу.

Розділ 4 «Розроблення засобів нейроподібного криптографічного шифрування та дешифрування даних у реальному часі» описує розроблення імітаційної моделі вибору елементної бази даних. Розроблено імітаційну модель знаходження вагових коефіцієнтів для заданої архітектури нейромережі. Удосконалено метод сингулярного розкладу матриці для знаходження матриці вагових коефіцієнтів.

Реалізація нейроподібних засобів шифрування та дешифрування даних з високими техніко-експлуатаційними показниками досягається шляхом використання проблемно-орієнтованого підходу, який передбачає поєднання програмних і апаратних засобів. Процес взаємопроникнення програмного (універсального) і апаратного (спеціалізованого) забезпечує високу ефективність використання обладнання та зменшує час їх розробки.

Висновки відображають отримані результати, сформульовані коректно з використанням кількісних оцінок досягнутих результатів.

5. Значення результатів дослідження для науки і практики

Важливість результатів, отриманих автором, для наукового співтовариства полягає в створенні фундаменту для розробки та вдосконалення нових методів, моделей та програмно-апаратних засобів для лінійного нейроподібного захисту даних у реальному часі з високими техніко-експлуатаційними параметрами для мобільних смарт-систем. Це досягнуто завдяки сукупності теоретичних положень, практичних висновків та розробок, представлених у дисертації. Теоретична та практична значущість цих робіт підтверджена актами їх впровадження, як у процесі науково-дослідних робіт, так і для практичного використання. Актуальність дисертації також підкріплена включенням окремих її розділів у державнобюджетні проекти, такі як "Експериментальна система нейромережевого криптографічного захисту та передачі даних у реальному часі з використанням баркероподібних

кодів" (державний реєстраційний номер 0121U109503) та "Експериментальна мобільна робототехнічна платформа з інтелектуальною системою управління та захистом передачі даних" (державний реєстраційний номер 0122U000891).

6. Повнота відображення наукових положень, висновків і рекомендацій в опублікованих автором дисертації працях

У 14 наукових публікаціях повністю відображені основні результати дисертаційного дослідження, з цих робіт отримано вагомий науковий доробок аспіранта у вигляді опублікованих 6 статей у наукових фахових виданнях України; 2 статтей у наукових періодичних виданнях інших держав, що включені до наукометричних баз даних; 1 авторського твору та 5 тезах доповідей конференцій.

7. Відомості про дотримання академічної доброчесності

У дисертації та наукових публікаціях Лукащука Ю. А. порушень академічної доброчесності не виявлено.

8. Дискусійні положення та зауваження до дисертаційної роботи

1. У першому розділі дисертації потрібно чіткіше окреслити внесок інших дослідників у цю галузь. Також бажано додати більш детальний опис того, що мається на увазі під терміном "мобільні смарт-системи".
2. Було б корисно глибше проаналізувати узагальнену модель нейроподібного шифрування управлінських команд із застосуванням таблично-алгоритмічного методу.
3. Необхідно приділити більше уваги питанню імплементації засобів нейроподібного криптографічного шифрування (дешифрування) з використанням універсального процесорного ядра, доповненого спеціалізованими апаратно-програмними ресурсами.
4. Важливим є проведення оцінки ефективності зменшення часу криптографічного шифрування (дешифрування) даних за допомогою спеціалізованих апаратно-програмних засобів.
5. У дисертації містяться редакційні і стилістичні неточності, а також використовуються англіцизми, які слід замінити на відповідні українські терміни.

Вказані вище зауваження та дискусійні аспекти, хоча й важливі для деталізації та уточнення дослідження, не є критичними чи принциповими. Вони не впливають на загальне позитивне сприйняття та оцінку дисертаційної роботи.

Загальний висновок

Дисертаційна робота Лукащука Юрія Андрійовича на тему «Інформаційна технологія захисту даних у реальному часі для мобільних смарт-систем з використанням нейроподібних мереж», подана на здобуття ступеня доктора філософії за спеціальністю 122 «Комп'ютерні науки», є завершеним науковим дослідженням, що стосується вирішення важливого наукового завдання - розробка нових та вдосконалення існуючих методів, моделей та програмно-апаратних засобів інформаційної технології нейроподібного лінійного захисту даних у реальному часі з високими техніко-експлуатаційними характеристиками для мобільних смарт-систем.

Вважаю, що за актуальністю, новизною, практичним значенням та обсягом дисертаційна робота відповідає вимогам наказу МОН України №40 від 12.01.2017 р. «Про затвердження Вимог до оформлення дисертації» (з наступними змінами) та «Порядку присудження ступеня доктора філософії та скасування рішення разової спеціалізованої вченої ради закладу вищої освіти, наукової установи про присудження ступеня доктора філософії», затвердженого Постановою Кабінету Міністрів України №44 від 12 січня 2022, а її автор Лукащук Юрій Андрійович заслуговує на присудження йому наукового ступеня доктора філософії за спеціальністю 122 «Комп'ютерні науки».

Офіційний опонент:
завідувача кафедри інформатики та комп'ютерних наук
Херсонського національного технічного університету

д.т.н., професор Володимир ЛИТВИНЕНКО

Підпис Литвиненка В.І. завіряю:

Начальник відділу кадрів ХНТУ Л.С. Іонова

ВІДДІЛ КАДРІВ