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

ВІДГУК РЕЦЕНЗЕНТА

кандидата технічних наук, доцента Батюка Анатолія Євгеновича на дисертаційну роботу **Лукащука Юрія Андрійовича** «Інформаційна технологія захисту даних у реальному часі для мобільних смарт-систем з використанням нейроподібних мереж», подану до захисту на здобуття наукового ступеня **доктора філософії** з галузі знань 12 «Інформаційні технології» та спеціальності 122 «Комп'ютерні науки»

Актуальність теми дисертації. Сучасний етап розвитку інформаційних технологій криптографічного захисту даних характеризується розширенням галузей застосування, значна кількість з яких орієнтована на використання у мобільних смарт-системах. У таких смарт-системах вимагається шифрування та дешифрування даних у реальному часі на апаратно-програмних засобах, що задовольняють обмеженням щодо габаритів, енергоспоживання, вартості та часу розробки. Створення таких апаратно-програмних засобів інформаційних технологій криптографічного захисту вимагає широкого використання сучасної елементної бази (мікроконтролерів, програмованих логічних інтегральних схем (ПЛІС) типу FPGA) та розробки нових методів, алгоритмів і структур для реалізації алгоритмів криптографічного шифрування та дешифрування даних. У зв'язку з цим особливої актуальності набуває проблема розроблення нових і вдосконалення існуючих методів та апаратно-програмних засобів інформаційних технологій криптографічного захисту для мобільних смарт-систем, які забезпечать високі техніко-експлуатаційні показники.

Одним із шляхів розроблення таких апаратно-програмних засобів криптографічного захисту є використання автоасоціативної нейромережі прямого поширення, яка навчається на основі методу головних компонент. Особливістю таких нейромережах є можливість наперед обчислити вагові коефіцієнти, використати таблиці макрочасткових добутків і базис елементарних арифметичних операцій для реалізації нейроподібних елементів. На основі зазначених нейроподібних елементів синтезується нейроподібна мережа, яка забезпечує шифрування та дешифрування даних. 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.

З наведеного випливає, що розроблення інформаційної технології нейроподібного лінійного захисту даних у реальному часу в мобільних смарт-системах найдоцільніше створювати за інтегрованим підходом, який охоплює методи, моделі та засоби шифрування та дешифрування даних, методи розпаралелювання, сучасну елементну базу, засоби автоматизованого проектування та автоматизації процесу програмування.

Зв'язок роботи з науковими програмами, планами, темами. Дисертаційне дослідження проводилось згідно з планами науково-дослідних та навчальних робіт кафедри автоматизованих систем управління Національного університету «Львівська політехніка», у тому числі в межах держбюджетних науково-дослідницьких робіт: «Експериментальна система нейромережевого криптографічного захисту та передачі даних у реальному часі з використанням баркероподібних кодів» (номер держ. реєстр. 0121U109503), «Нейромережева технологія захисту та передачі даних у реальному часі з використанням

шумоподібних кодів» (номер держ. реєстр. 0119U002256) і «Експериментальна мобільна робототехнічна платформа з інтелектуальною системою управління та захистом передачі даних» (номер держ. реєстр. 0122U000891).

Наукова новизна роботи полягає в тому, що автором розв'язано актуальну наукову задачу – розроблення нових і вдосконалення існуючий методів, моделей та програмно-апаратних засобів інформаційної технології нейроподібного лінійного захисту даних у реальному часі з високими техніко-експлуатаційними характеристиками для мобільних смарт-систем. При цьому отримано такі нові результати:

***вперше розроблено*:**

- інформаційну технологію нейроподібного захисту даних у реальному часі з симетричними ключами (коди маскування, архітектура нейромережі та матриці вагових коефіцієнтів) для смарт-систем, яка за рахунок використання моделі попередніх налаштувань, вдосконаленого методу обчислення та вагових коефіцієнтів, методу таблично-алгоритмічного обчислення скалярного добутку забезпечує високу криптографічну стійкість і апаратно-програмну реалізацію з високими техніко-експлуатаційними характеристиками;
- модель попередніх налаштувань для реалізації нейроподібного шифрування/дешифрування даних основними компонентами якої є формувач архітектури нейроподібної мережі, обчислювач матриць вагових коефіцієнтів і обчислювач таблиць макрочасткових добутків, реалізація якої забезпечує зменшення часу налаштування;
- метод таблично-алгоритмічного обчислення скалярного добутку з плаваючою комою в нейроподібних елементах, який за рахунок приведення до найбільшого спільного порядку вхідних даних, вагових коефіцієнтів і використання таблиць макрочасткових добутків мантис забезпечує зменшення часу обчислення скалярного добутку та підвищення ефективності використання обладнання;

вдосконалено:

- нейроподібну мережу прямого поширення автоасоціативного типу на основі парадигми «модель послідовних геометричних перетворень» і адаптовано її до нейроподібного шифрування-дешифрування даних шляхом попереднього обчислення вагових коефіцієнтів, що забезпечило повторюваність результатів і орієнтацію на апаратну реалізацію;
- метод вибору елементної бази для синтезу засобів криптографічного захисту даних у реальному часі, який за рахунок використання наповненої сучасною елементною базою бази даних і врахування вимог технічного завдання забезпечує автоматизацію процесу вибору найефективнішої елементної бази;
- метод обчислення вагових коефіцієнтів, який за рахунок використання сингулярного розкладу матриць, з використанням алгоритму Якобі для знаходження власних значень та власних векторів, забезпечує швидке налаштування та обчислення матриць вагових коефіцієнтів для різних архітектур нейроподібних мереж.

Ступінь обгрунтованості наукових положень і висновків дисертації та їх достовірність. При вирішенні поставлених у дисертації задач, створені наукових положень, висновків та рекомендацій автором застосовані дані, які одержані з літературних джерел, з результатів аналізу сучасного стану та перспектив розвитку методів і алгоритмів підвищення надійності нейроподібного захисту даних у реальному часі. Тому наведені в дисертації результати слід вважати достатньо обгрунтованими, що підтверджується даними моделювань, експериментальних досліджень та практичними результатами, що підтверджуєтьсяся актами впроваджень.

Наукове значення виконаного дослідження.

Отримані автором наукові положення та практичні результати можуть бути використані при розробці систем різних архітектур нейроподібних мереж для

синтезу засобів криптографічного захисту даних у реальному часі. Результати є значущими для галузі 12 «Інформаційні технології» та спеціальності 122 «Комп'ютерні науки».

Практичне значення одержаних результатів полягає в тому, що розроблена інформаційна технологія нейроподібного лінійного захисту даних у реальному часі з симетричними ключами (коди маскування, архітектура нейромережі та матриці вагових коефіцієнтів) для смарт-систем дає змогу розробляти апаратно-програмні засоби нейроподібного шифрування та дешифрування даних у реальному часі з високими техніко-експлуатаційними характеристиками, а також вибрати найефективнішу елементну базу для синтезу засобів криптографічного захисту даних у реальному часі і зменшити час налаштування нейроподібної мережі для реалізації нейроподібного шифрування та дешифрування даних.

Повнота оприлюднення результатів дисертаційної роботи. Результати дисертаційної роботи Лукащука Ю. А. доповідалися і обговорювалися на міжнародних науково-практичних та науково-технічних конференціях та викладено у 14 наукових публікаціях повністю відображені основні результати дисертації, з них отримано вагомий науковий доробок аспіранта у вигляді опублікованих 6 статей у наукових фахових виданнях України; 2 статей у наукових періодичних виданнях інших держав, що включені до наукометричних баз даних; 1 авторського твору та 5 тезах доповідей конференцій.

Короткий аналіз структури та змісту дисертаційної роботи. Дисертаційна робота викладена на 152 сторінках та складається з анотації, змісту, переліку скорочень, вступу, чотирьох основних розділів, в яких міститься 21 рисунків та 9 таблиць, списку використаних джерел з 152 найменувань. За структурою, мовою та стилем викладення дисертація відповідає вимогам МОН України. Робота написана грамотною українською мовою з використанням сучасної наукової термінології, а стиль викладення матеріалу є послідовним та логічним.

У **вступі** обґрунтовано актуальність теми дисертаційного дослідження , сформульовано мету дослідження та науково-прикладні завданнянеобхідні для її досягнення, показано зв'язок дослідження з науковими програмами та темами, наведено наукову новизну отриманих результатів, їх практичну цінність та особистий внесок здобувача.

У **першому розділі** дисертаційного дослідження проведено аналіз архітектур нейронних мереж, а також проаналізовано методи та алгоритми 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.

У **другому розділі** вдосконалено і орієнтовано на задачі нейромережевого шифрування-дешифрування даних нейроподібну мережу прямого поширення автоасоціативного типу на основі парадигми «модель послідовних геометричних перетворень».

Запропоновано синтез системи захисту та передавання даних у реальному часі з високими техніко-економічними характеристиками із використанням інтегрованого підходу.

У **третьому розділі** розроблено інформаційну технологію нейроподібного криптографічного захисту даних у реальному часі з симетричними ключами (коди маскування, архітектура нейроподібної мережі та матриці вагових коефіцієнтів), яка за рахунок попереднього обчислення матриць вагових коефіцієнтів і динамічної зміни архітектури нейроподібної мережі забезпечує високу криптографічну стійкість і апаратно-програмну реалізацію з високими техніко-економічними характеристиками.

У **четвертому розділі** дисертаційної роботи на основі вдосконаленого методу вибору елементної бази розроблено імітаційну модель, яка за рахунок використання наповненої сучасною елементною базою бази даних і врахування

вимог технічного завдання забезпечує автоматизацію процесу вибору найефективнішої елементної бази для синтезу засобів криптографічного захисту даних у реальному часі.

У загальних висновках дисертаційної роботи сформульовано основні результати дисертаційної роботи, які узгоджуються з метою та завданнями дослідженнями.

Зауваження та дискусійні положення щодо змісту дисертації.

1. Недостатньо обгрунтовано вибір SVD методу для обрахунку вагових коефіцієнтів. Було б добре, якщо б автор чіткіше розписав переваги цього методу.
2. У першому розділі не в повній мірі висвітлено вклад авторів, на яких йде посилання, у розвиток інформаційних технологій нейроподібного захисту даних.
3. У висновках до розділів 2 і 3 доцільно навести конкретні чисельні значення та переваги розроблених методів у порівнянні з існуючими.
4. У четвертому розділі, для кращого розуміння роботи автору варто обгрунтувати детальніше вибір тестових даних для імітаційних моделей.
5. У тексті дисертаційної роботи зустрічається ряд стилістичних та орфографічних неточностей.

Слід відмітити, що зазначені зауваження не знижують загальної позитивної оцінки дисертаційної роботи.

Висновок

Не зважаючи на виявлені недоліки дисертаційна робота Лукащука Юрія Андрійовича на тему «Інформаційна технологія захисту даних у реальному часі для мобільних смарт-систем з використанням нейроподібних мереж» є завершеною науковою працею, яка представлена на здобуття наукового ступення доктора філософії за спеціальністю 122 «Комп'ютерні науки» (галузь знань 12

«Інформаційні технології»), яка за своїм змістом, структурою, обсягом, науковою новизною та практичним значенням відповідає паспорту спеціальності 122 «Комп'ютерні науки», вимогам «Порядку присудження ступення доктора філософії та скасування рішення разової спеціалізованої ради закладу вищої освіти, наукової установи про присудження доктора філософії», затвердженого постановою Кабінету Міністрів України від 12 січня 2022 року №44 зі змінами згідно з Постановою КМ №9341 від 21.03.2022, а її автор, Лукащук Юрій Андрійович, заслуговує присудження йому наукового ступення доктора філософії за спеціальністю 122 «Комп'ютерні науки».

Рецензент, кандидат технічних наук,
доцент, доцент кафедри автоматизованих систем
Національного університету
«Львівська політехніка» Анатолій БАТЮК

«Підпис Батюка А.Є. засвідчую»:
Вчений секретар
Національного університету
«Львівська політехніка» Роман БРИЛИНСЬКИЙ