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

ВІДГУК РЕЦЕНЗЕНТА

доктора технічних наук, професора Ткаченка Романа Олексійовича 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»

1. Загальна характеристика роботи

Робота складається з анотації, вступу, чотирьох розділів, висновків, списку літератури. Загальний обсяг роботи становить 152 сторінки друкованого тексту, у тому числі 135 сторінок основного тексту та список із 152 найменувань використаних джерел.

До розгляду подано дисертацію на здобуття ступеня доктора філософії та копії усіх опублікованих автором робіт, які відображають результати та зміст дослідження.

2. Оцінка актуальності теми дисертації

Одним із шляхів розроблення апаратно-програмних засобів криптографічного захисту є використання автоасоціативної нейромережі прямого поширення, яка забезпечує формування сигналів головних компонентів даних на виходах нейронів прихованого шару. Як особливість таких нейромереж можна відзначити можливість використовувати таблиці макрочасткових добутків також наперед обчислювати вагові коефіцієнти та використовувати 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 захисту даних у реальному часу в мобільних смарт-системах найефективніше створювати саме за інтегрованим підходом, який охоплює засоби, методи та моделі шифрування та дешифрування даних, сучасну елементну базу, методи розпаралелювання, автоматизації процесу програмування й засоби автоматизованого проектування.

Тему дисертації актуальна, оскільки розроблення нових і вдосконалення існуючих методів, моделей та програмно-апаратних засобів інформаційної технології нейроподібного захисту даних у реальному часі з високими техніко-експлуатаційними характеристиками для мобільних смарт-систем є затребуваним напрямком розвитку інформаційних технологій.

Виконані у рамках цієї дисертаційної роботи дослідження, пропозиції та рекомендації стали складовою частиною держбюджетної науково-дослідної роботи Національного університету «Львівська політехніка» «Експериментальна система нейромережевого криптографічного захисту та передачі даних у реальному часі з використанням баркероподібних кодів» (номер держ. реєстр. 0121U109503) і «Експериментальна мобільна робототехнічна платформа з інтелектуальною системою управління та захистом передачі даних» (номер держ. реєстр. 0122U000891).

3. Оцінка наукових результатів дисертації

Вирішення поставлених завдань дисертаційної роботи виконане на основі нових наукових положень, які полягають у наступному:

- розроблення інформаційної технологію нейроподібного захисту даних у реальному часі із симетричними ключами (архітектура нейромережі, матриці вагових коефіцієнтів та коди маскування) для смарт-систем;
- розроблення моделі попередніх налаштувань для реалізації нейроподібного шифрування та дешифрування даних;
- розроблення методу таблично-алгоритмічного обчислення скалярного добутку з плаваючою комою в нейроподібних елементах;
- вдосконалення нейроподібної мережі прямого поширення автоасоціативного типу на основі парадигми «модель послідовних геометричних перетворень» і адаптація її до нейроподібного шифрування-дешифрування;
- вдосконалення методу вибору елементної бази для синтезу засобів криптографічного захисту даних у реальному часі;
- вдосконалення методу обчислення вагових коефіцієнтів.

4. Оцінка практичного значення результатів роботи

Практичне значення роботи полягає у тому, що на підставі проведених теоретичних і експериментальних досліджень вирішене важливе науковоприкладне завдання в галузі комп'ютерних наук – розроблення інформаційної технології нейроподібного захисту даних у реальному часі з симетричними ключами (архітектура нейромережі, матриці вагових коефіцієнтів та коди маскування) для смарт-систем.

Отримані автором результати можуть бути використані для: розроблення апаратно-програмних засобів нейроподібного шифрування/дешифрування даних у реальному часі із високими техніко-експлуатаційними характеристиками; зменшення часу обчислення скалярного добутку з пливучою комою в

нейроподібних елементах; підвищення ефективності використання обладнання при реалізації нейроподібного елемента та нероподібної мережі; вибору найефективнішої елементної бази для синтезу засобів криптографічного захисту даних у реальному часі; зменшення часу налаштування нейроподібної мережі для реалізації нейроподібного шифрування та дешифрування даних.

Результати проведених досліджень застосовуються у навчальному процесі Національного університету «Львівська політехніка» при викладанні навчальної дисципліни «Технологія захисту інформації».

Результати впровадження підтверджені відповідними актами.

5. Оцінка достовірності та обґрунтованості основних положень і висновків дисертації

Наукові положення, висновки та пропозиції у достатній мірі обґрунтовані теоретичним аналізом, експериментальними дослідженнями, тому їх можна вважати повністю достовірними.

У дисертаційній роботі використано: парадигму «модель послідовних геометричних перетворень»; метод головних компонент; таблично-алгоритмічний метод; теорію та методи розпаралелення алгоритмів, теорію автоматизованого проектування та автоматизації процесу програмування.

Використані в дисертації основні теоретичні положення та припущення є коректними і не містять суперечливостей. Обґрунтованість встановлених закономірностей підтверджувалась експериментальним шляхом. Висновки, які наведені в дисертаційній роботі, є достатньо обґрунтованими, їх достовірність підтверджена апробацією результатів.

Результати роботи достатньо висвітлено та апробовано на міжнародних науково-технічних конференціях. У повному обсязі ці результати доповідались на науковому семінарі кафедри «Автоматизованих систем управління» Національного університету «Львівська політехніка».

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 статей у наукових періодичних виданнях інших держав, що включені до наукометричних баз даних; 1 авторського твору та 5 тезах доповідей конференцій.

6. Оцінка змісту й оформлення дисертації

У дисертаційній роботі на основі отриманих нових науково обґрунтованих результатів вирішено актуальне в галузі знань 12 «Інформаційні технології» наукове та прикладне завдання розроблення нових і 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. Наукова та прикладна проблема, розв'язанню якої присвячена дисертація, поставлена коректно.

У роботі послідовно розглянуто окремі складові проблеми та розроблено засоби для їх вирішення.

У **першому розділі** «Аналіз методів, алгоритмів і засобів нейромережевого захисту даних у мобільних смарт-системах» 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** «Адаптація автоасоціативної нейронної мережі до задач криптографічного захисту даних і розроблення імітаційної моделі обчислення вагових коефіцієнтів» вдосконалено і орієнтовано на задачі нейромережевого шифрування-дешифрування даних нейроподібну мережу прямого поширення

автоасоціативного типу на основі парадигми «модель послідовних геометричних перетворень».

Розроблено модель попередніх налаштувань для реалізації нейроподібного шифрування/дешифрування даних, основними компонентами якої є: блок обчислення таблиць макрочасткових добутків, блок формування архітектури нейроподіної мережі, а також блок обчислення матриць вагових коефіцієнтів. Разом реалізації цих блоків забезпечує зменшення часу для налаштувань.

У **третьому розділі** «Розроблення інформаційної технології нейроподібного криптографічного захисту даних» розроблено інформаційну технологію нейроподібного криптографічного захисту даних у реальному часі із симетричними ключами.

Вдосконалено метод вибору елементної бази для синтезу засобів криптографічного захисту даних у реальному часі, який за рахунок обчислення інтегрованої оцінки ефективності елементної бази та врахування вимог конкретного застосування забезпечує вибір найефективнішої елементної бази із множини елементних баз, які відповідають вимогам технічного завдання.

У **четвертому розділі** «Розроблення засобів нейроподібного криптографічного шифрування та дешифрування даних у реальному часі» розроблено імітаційну модель вибору елементної бази даних. Розроблено імітаційну модель знаходження вагових коефіцієнтів для заданої архітектури нейромережі. Удосконалено метод сингулярного розкладу матриці для знаходження матриці вагових коефіцієнтів.

Наведені в дисертаційній роботі висновки і рекомендації є достатніми і належним чином обґрунтованими. Для їх висвітлення автором проведені необхідні теоретичні дослідження та здійснена апробація результатів, розроблені відповідні методики. Отже, на основі розгляду матеріалів дисертації можна зробити позитивний висновок про повноту розв'язання поставленої науково-прикладної задачі.

Дисертація оформлена відповідно до вимог щодо оформлення дисертації, добре ілюстрована. Стиль, логічна послідовність та мова викладення матеріалу відповідають необхідним вимогам до написання наукових робіт.

7. Зауваження до дисертаційної роботи

Оцінюючи дисертаційну роботу загалом позитивно, можна відзначити наступні зауваження.

1. У першому розділі занадто велику увагу приділено опису базових операцій мереж БШП, РБФ, GRNN, які не використовуються для криптографічного захисту в реальному часі.
2. Крім переваг симетричних криптосистем на мережах МПГП варто було би вказати на недоліки такої системи шифрування – зокрема перехід від цілочисельної системи подання на входах і виходах до дробової в прихованому шарі, що ускладнює створення апаратних рішень.
3. Не зовсім зрозуміло використання алгоритму SVD при наявності швидкого алгоритму МПГП, який вже існує; було би доречним отримати порівняльні оцінки їх застосування.
4. Висновки до розділів дисертації найчастіше подаються у вигляді переліку отриманих результатів, а не в плані їх аналізу.
5. Недостатня увага зверталася опису переваг реалізованих апаратних рішень в порівнянні з програмними реалізаціями.
6. У тексті дисертаційної роботи є певні неточності редакційного характеру, неузгодження відмінків слів в деяких реченнях.

8. Загальна оцінка дисертаційної роботи

Дисертаційна робота Лукащука Юрія Андрійовича «Інформаційна технологія захисту даних у реальному часі для мобільних смарт-систем з використанням нейроподібних мереж» є завершеною науковою працею і має важливе значення в галузі комп'ютерних наук на сучасному етапі її розвитку. Вирішено актуальну проблему розроблення нових і вдосконалення існуючих методів, моделей та програмно-апаратних засобів інформаційної технології

нейроподібного захисту даних у реальному часі з високими техніко-експлуатаційними характеристиками для мобільних смарт-систем .

Одержані нові розв'язки науково-прикладної проблеми. Актуальність, практичне значення, новизна та завершеність дослідження, обґрунтування висновків заслуговують позитивної оцінки.

Зміст дисертаційної роботи, отримані основні наукові положення та висновки відповідають паспорту спеціальності 122 «Комп'ютерні науки».

Вказані у пункті 7 цього відгуку зауваження щодо представленого досліджння не знижують вагомості отриманих у роботі наукових та практичних результатів і не змінюють її позитивної оцінки.

Робота відповідає вимогам «Порядку присудження ступеня доктора філософії», затвердженого постановою Кабінету Міністрів України від 12 січня 2022р. № 44, а її автор Лукащук Юрій Андрійович заслуговує на присудження наукового ступеня доктора філософії за спеціальністю 122 «Комп'ютерні науки»

Рецензент – доктор технічних наук, професор,
Професор кафедри інформаційних технологій
Видавничої справи
Національного Університету «Львівська політехніка»
Роман ТКАЧЕНКО

«Підпис Ткаченка Р.О. засвідчую»:
Вчений секретар
Національного університету «Львівська політехніка»,
к.т.н., доц. Роман БРИЛИНСЬКИЙ