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

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, які задовольняють обмеження щодо енергоспоживання та габаритів, а також часу й вартості необхідних для розробки. Для того щоб створити такі апаратно-програмні засоби інформаційних технологій криптографічного захисту необхідне широке використання сучасної елементної бази (програмованих логічних інтегральних схем (ПЛІС) типу FPGA, мікроконтролерів тощо) та розробки нових методів, алгоритмів і структур для реалізації алгоритмів криптографічного шифрування та дешифрування даних.

Через це особливої актуальності набуває проблематика розробки нових і вдосконалення існуючих методів та апаратно-програмних засобів інформаційних технологій криптографічного захисту для мобільних смарт-систем, які забезпечать високі техніко-експлуатаційні показники.

## 2. Ступінь обґрунтованості наукових положень, висновків і рекомендацій

Висвітлені в дисертаційній роботі наукові положення, висновки та запропоновані рекомендації науково і теоретично обґрунтовані, достовірні та апробовані. При проведенні наукового дослідження, висвітленні результатів, формулюванні пропозицій та практичних рекомендацій здобувачем використано ряд загальних та суто специфічних для даної тематики апробованих методів дослідження та прийомів аналізу. Отримані автором результати достатньо обґрунтовані, ступінь їх достовірності не викликає запитань та зауважень.

У першому розділі «Аналіз методів, алгоритмів і засобів нейромережевого захисту даних у мобільних смарт-системах» проведено 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. Також проведено аналіз едементної бази для реалізації нейронних мереж реального часу.

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». 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.

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

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. Одним із шляхів розроблення апаратно-програмних засобів криптографічного захисту є використання автоасоціативної нейромережі прямого поширення, що навчається на основі методу головних компонентів. Як особливість таких нейромереж можна відзначити можливість використовувати таблиці макрочасткових добутків також наперед обчислювати вагові коефіцієнти та використовувати базис елементарних

арифмеичних 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.

Структура дисертаційної роботи Лукащука Ю. А. логічна та сприяє в достатній мірі сприйняттю викладеного автором матеріалу. Робота добре проілюстрована, а оформлення підкреслює логіку та функціональність розділення на складові частини. Структура та наповнення розділів характеризує логічну стрункість процесу дослідження протягом усієї дисертаційної роботи.

### 3. Наукова новизна результатів досліджень

Наукові положення, висновки та рекомендації, викладені у дисертаційній роботі, містять наукову новизну та є обґрунтованими. Новизна результатів дисертації забезпечується коректною постановкою наукових завдань і адекватністю методів їхнього розв'язання, застосуванням загальнонаукових та спеціальних методів дослідження, використанням досягнень вітчизняної та зарубіжної літератури в галузі комп'ютерних наук.

Новизна наукових результатів дисертаційної роботи, яка відображає особистий внесок дисертанта, полягає в наступному:

Вперше розроблено:

- інформаційну технологію нейроподібного захисту даних у реальному часі із симетричними ключами (архітектура нейромережі, матриці вагових коефіцієнтів та коди маскування) для смарт-систем;
- модель попередніх налаштувань для реалізації нейроподібного шифрування та дешифрування даних;
- метод таблично-алгоритмічного обчислення скалярного добутку з плаваючою комою в нейроподібних елементах;

Вдосконалено:

- нейроподібну мережу прямого поширення автоасоціативного типу на основі парадигми «модель послідовних геометричних перетворень» і адаптовано її до нейроподібного шифрування-дешифрування;
- метод вибору елементної бази для синтезу засобів криптографічного захисту даних у реальному часі;
- метод обчислення вагових коефіцієнтів.

**4. Значення результатів дослідження для науки і практики**

Значення отриманих результатів у даній дисертаційній роботі полягає у тому, що на підставі проведених теоретичних і експериментальних досліджень вирішено наукове завдання в галузі комп'ютерних наук, а саме розроблення інформаційної технології нейроподібного захисту даних у реальному часі з симетричними ключами (архітектура нейромережі, матриці вагових коефіцієнтів та коди маскування) для смарт-систем. Ця система має прикладне застосування, а саме: розроблення апаратно-програмні засоби нейроподібного шифрування/дешифрування даних у реальному часі із високими техніко-експлуатаційними характеристиками; зменшення часу обчислення скалярного добутку з плаваючою 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. Актуальність також обґрунтовується окремими розділами, які ввійшли у науково-дослідницькі теми: «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).

Результати впровадження підтверджені відповідними актами.

**5. 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.

**6. Мова та стиль дисертаційної роботи**

Дисертаційна робота написана доступно, на високому науковому та технічному рівні. Виклад лаконічний, без непотрібних та зайвих деталізацій, з використанням сучасної професійної термінології. Тема, зміст та отримані наукові результати роботи відповідають спеціальності 122 «Компютерні науки», галузі знань 12 «Інформаційні технології».

**7. Дискусійні положення та зауваження до дисертаційної роботи**

Як зауваження до роботи можна зазначити наступні пункти:

1. Автору роботи варто було детальніше розписати здобутки інших авторів у вибраній галузі за останні декілька років.
2. Недосконало обгрунтовано критерії вибору елементної бази для синтезу мобільних апаратних засобів нейроподібного криптографічного шифрування та дешифрування даних.
3. Автору треба детальніше розписати можливості застосування моделі попередніх налаштувань. Оскільки імітаційна модель не розкриває повноту застосування даної розробки.
4. Не проведено оцінювання складності алгоритмів нейроподібного криптографічного шифрування та дешифрування даних.
5. У дисертаційному дослідженні присутні описки, дрібні недоліки редакційно-стильового оформлення, що взагальному знижують позитивне враження від роботи

Зазначені зауваження та неділоки не впливають на науковий рівень, новизну та практичне значення отриманих автором результатів.

**8. Загальний висновок**

Дисертаційна робота ЛУКАЩУКА Юрія Андрійовича «Інформаційна технологія захисту даних у реальному часі для мобільних смарт-систем з використанням нейроподібних мереж» є завершеним науковим дослідженням, що стосується вирішенню актуальної проблеми 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 .

Беручи до уваги актуальність дисертаційного дослідження «Інформаційна технологія захисту даних у реальному часі для мобільних смарт-систем з використанням нейроподібних мереж», обгрунтованість наукових положень, висновків, новизну, практичну цінність, апробацію представлених до захисту результатів у наукових статтях, матеріалах конференції, а також наявність авторського твору, відповідність нормам академічної доброчесності, вважаю, що дисертація 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».

Офіційний опонент:
професора кафедри кібербезпеки
Львівського Національного університету
імені Івана Франка
д.т.н., професор Дмитро ПЕЛЕШКО

Підпис
ПІДТВЕРДЖУЮ
Нач. ВК ЛНУ ім. І. Франка

ВІДДІЛ КАДРІВ
ЗКПО 02070987