РЕЦЕНЗІЯ

рецензента, к.т.н., доцента Мезенцева Миколи Вікторовича

на дисертаційну роботу **Хулапа Андрія Валерійовича**

«Моделі, методи та програмні компоненти засобів штучного інтелекту для захисту інформації систем Інтернету речей»

подану на здобуття наукового ступеня доктора філософії

за спеціальністю 123 – Комп'ютерна інженерія

Проведений аналіз дисертаційної роботи Хулапа Андрія Валерійовича «Моделі, методи та програмні компоненти засобів штучного інтелекту для захисту інформації систем Інтернету речей», поданої на здобуття ступеня доктора філософії у Національному технічному університеті «Харківський політехнічний інститут», дає підстави оцінити її як актуальне та завершене наукове дослідження, у якому обґрунтовано наукові положення, отримано достовірні результати, що мають наукову новизну, теоретичне та практичне значення.

1. Актуальність теми та зв'язок з науковими планами і програмами

У сучасних умовах активного розвитку технологій Інтернету речей та широкого впровадження IoT-пристроїв у різні сфери діяльності особливої важливості набувають питання забезпечення інформаційної безпеки таких систем. Обмежені обчислювальні ресурси, невисока продуктивність і енергетичні обмеження більшості IoT-пристроїв суттєво ускладнюють застосування традиційних засобів виявлення мережевих вторгнень.

У зв'язку з цим актуальним науково-технічним завданням є створення ефективних методів і програмних компонентів систем виявлення вторгнень, адаптованих до роботи на малоресурсних мікроконтролерних платформах. Перспективним напрямом розв'язання цієї задачі є використання

нейромережевих моделей та методів штучного інтелекту, однак їх практичне застосування потребує оптимізації обчислювальних алгоритмів і зменшення вимог до апаратних ресурсів.

Дисертаційна робота Хулапа Андрія Валерійовича присвячена вирішенню актуальної задачі підвищення ефективності нейромережевих методів виявлення мережевих вторгнень у системах Інтернету речей шляхом адаптації моделей та оптимізації обчислень для embedded- і мікроконтролерних платформ.

2. Зв'язок роботи з науковими програмами, планами, темами

Дисертаційна робота виконана в межах освітньо-наукової програми «Комп'ютерна інженерія» третього рівня вищої освіти на кафедрі «Комп'ютерна інженерія та програмування» Національного технічного університету «Харківський політехнічний інститут».

Тематика дослідження відповідає науковому напряму кафедри та пов'язана з виконанням науково-дослідної роботи НДР К6003 «Розробка пропозицій щодо оптимального розміщення даних та управління ресурсами в розподілених інформаційно-управляючих системах» (ДР №0124U001391), у якій здобувач брав участь як виконавець.

3. Наукова новизна одержаних результатів

До основних наукових результатів дисертаційної роботи, що визначають її наукову новизну, слід віднести:

– запропонований метод оптимізації нейромережевих обчислень для систем виявлення мережевих вторгнень у середовищі Інтернету речей, заснований на використанні fixed-point арифметики, що забезпечує можливість виконання нейромережевих алгоритмів на малоресурсних embedded-платформах;

– удосконалений підхід до реалізації нейромережевих моделей виявлення вторгнень для мікроконтролерних систем за рахунок оптимізації структури обчислень та використання апроксимації функцій активації;

– подальший розвиток методів побудови компактних нейромережевих моделей для IoT-систем шляхом адаптації архітектури мережі та скорочення набору інформативних ознак з урахуванням апаратних обмежень вбудованих пристроїв;

– удосконалений підхід до оцінювання ефективності систем виявлення мережевих вторгнень, який передбачає комплексний аналіз швидкодії, точності класифікації та використання апаратних ресурсів мікроконтролерних платформ.

Отримані результати мають наукове значення для розвитку методів застосування штучного інтелекту у системах захисту інформації Інтернету речей та становлять практичний інтерес для галузі комп'ютерної інженерії і embedded-систем.

4. Практична цінність одержаних результатів та рекомендації щодо їх подальшого використання

Практичне значення дисертаційної роботи полягає у можливості застосування запропонованих методів і програмних компонентів для побудови систем виявлення мережевих вторгнень у середовищі Інтернету речей на основі малоресурсних мікроконтролерних платформ. Розроблені підходи дозволяють зменшити обчислювальні витрати та вимоги до пам'яті при реалізації нейромережевих алгоритмів у вбудованих системах

Отримані результати можуть бути використані при створенні програмного забезпечення для IoT-пристроїв, embedded-систем та периферійних вузлів обробки мережевого трафіку, а також у подальших наукових дослідженнях у галузі штучного інтелекту, комп'ютерної інженерії та інформаційної безпеки.

Практична цінність результатів підтверджується їх впровадженням у навчальний процес кафедри «Комп'ютерна інженерія та програмування» НТУ «ХПІ» при викладанні дисципліни «Проєктування програмного забезпечення мікроконтролерних пристроїв».

5. Повнота викладення матеріалів дисертації в наукових працях, які опубліковані автором.

Результати дисертаційного дослідження достатньо повно відображені у 11 наукових публікаціях автора, з яких 3 статті опубліковано у фахових наукових виданнях України, 1 стаття – у міжнародному науковому виданні, що індексується у базі даних Scopus, а також 7 публікацій представлено у матеріалах міжнародних наукових конференцій.

Опубліковані праці охоплюють основні положення дисертації, висвітлюють наукову новизну отриманих результатів та їх практичне значення. Результати дослідження пройшли апробацію на наукових конференціях і відповідають тематиці дисертаційної роботи.

Це дає підстави вважати дисертаційну роботу самостійним завершеним науковим дослідженням, результати якого мають значення для розвитку методів застосування штучного інтелекту та нейромережевих технологій у системах захисту інформації Інтернету речей.

6. Аналіз змісту дисертації. Ступінь обгрунтованост наукових положень, висновків і рекомендацій, сформульованих в дисертації

Дисертаційна робота Хулапа А.В. є завершеним науковим дослідженням і складається з анотації українською та англійською мовами, вступу, чотирьох розділів, висновків, списку використаних джерел і додатків.

Дисертацію присвячено розв'язанню актуальної науково-технічної задачі підвищення ефективності систем виявлення мережевих вторгнень у середовищі Інтернету речей на основі методів штучного інтелекту. Основну увагу в роботі приділено оптимізації нейромережевих алгоритмів для їх виконання на малоресурсних мікроконтролерних платформах та embedded-пристроях.

Об'єктом дослідження є процес виявлення мережевих вторгнень у системах Інтернету речей, а предметом дослідження – моделі, методи та програмні компоненти систем виявлення вторгнень з урахуванням обмежень апаратних ресурсів IoT-пристроїв.

У першому розділі наведено аналіз сучасного стану досліджень у сфері виявлення мережевих вторгнень та застосування нейромережевих методів у системах Інтернету речей. Розглянуто основні проблеми реалізації алгоритмів штучного інтелекту на embedded-платформах та сформульовано задачі дисертаційного дослідження.

У другому розділі досліджено методи машинного та глибокого навчання для задач аналізу мережевого трафіку, обґрунтовано вибір архітектури компактної нейромережевої моделі та набору інформативних ознак. Також наведено характеристику наборів даних, використаних під час експериментальних досліджень.

У третьому розділі розроблено методи та програмні компоненти оптимізації нейромережевих обчислень для мікроконтролерних платформ. Запропоновано підхід на основі fixed-point представлення параметрів нейронної мережі, використання табличної апроксимації функцій активації та оптимізації структури зберігання вагових коефіцієнтів. Проведено оцінювання ефективності запропонованих рішень за показниками швидкодії та використання пам'яті.

У четвертому розділі наведено результати експериментальної перевірки запропонованих методів на мікроконтролерній платформі STM32L476. Проведено порівняльний аналіз fixed-point та floating-point реалізацій нейромережевих алгоритмів, досліджено вплив оптимізації на швидкість виконання обчислень, використання пам'яті та точність класифікації мережевого трафіку.

Висновки до розділів і загальні висновки дисертаційної роботи є логічними, обґрунтованими та відповідають поставленим завданням дослідження. Список використаних джерел охоплює сучасні наукові праці у сфері штучного інтелекту, систем виявлення вторгнень, Інтернету речей та embedded-систем.

Обґрунтованість наукових положень, висновків і рекомендацій підтверджується використанням сучасних методів аналізу, математичного та програмного моделювання, а також результатами експериментальних

досліджень, виконаних із використанням наборів даних NSL-KDD та UNSW-NB15 на реальній мікроконтролерній платформі.

7. Достовірність отриманих результатів та висновків

Достовірність результатів, отриманих у дисертаційній роботі, забезпечується коректною постановкою задач дослідження, використанням сучасних методів математичного аналізу, програмного та комп'ютерного моделювання, а також комплексним підходом до дослідження нейромережевих методів виявлення мережевих вторгнень у системах Інтернету речей.

Сформульовані у роботі наукові положення та висновки підтверджуються результатами експериментальних досліджень, проведених із використанням наборів даних NSL-KDD та UNSW-NB15, а також результатами практичної реалізації запропонованих методів на мікроконтролерній платформі STM32L476.

Отримані результати експериментів узгоджуються з теоретичними положеннями дисертаційної роботи та підтверджують ефективність запропонованих підходів до оптимізації нейромережевих обчислень для embedded- та IoT-пристроїв з обмеженими апаратними ресурсами.

8. Оформлення дисертації, дотримання вимог академічної доброчесності та повнота викладення наукових положень та результатів в опублікованих працях

Дисертаційна робота оформлена відповідно до чинних вимог до дисертаційних досліджень. У роботі дотримано принципів академічної доброчесності, а всі використані наукові джерела належним чином процитовані та відображені у списку використаної літератури.

Подані у дисертації наукові положення, результати досліджень і висновки є самостійними напрацюваннями автора та достатньою мірою висвітлені у наукових публікаціях. За темою дисертації опубліковано 11 наукових праць, з яких 3 статті – у фахових наукових виданнях України, 1

стаття – у міжнародному науковому виданні, що індексується у базі даних Scopus, а також 7 публікацій у матеріалах міжнародних наукових конференцій, де здійснювалася апробація результатів дослідження..

9. Недоліки та зауваження до дисертаційної роботи

1. У дисертаційній роботі недостатньо детально розглянуто можливі обмеження запропонованого підходу при збільшенні кількості вхідних параметрів або ускладненні нейромережевої моделі.

2. У роботі основну увагу приділено оптимізації нейромережевих обчислень, тоді як питання інтеграції запропонованих рішень у комплексні системи моніторингу мережевого трафіку IoT-середовища розглянуто обмежено.

3. У дисертації лише частково проаналізовано вплив особливостей архітектури мікроконтролерних платформ на ефективність реалізації fixed-point обчислень, що могло б бути перспективним напрямом подальших досліджень.

4. Окремі результати експериментальних досліджень доцільно було б супроводити більш детальним порівнянням із результатами інших сучасних реалізацій систем виявлення вторгнень для embedded-платформ.

5. У п. 4.3.1 описано метод: перемикання світлодіода до і після обробки всього набору з 8000 записів. Це дає період меандра, де половина періоду – час обробки. Але не враховано час на перемикання GPIO та накладні витрати циклу. Для точності варто було б виконати багаторазові вимірювання та відняти час холостого циклу. Втім, для порівняльного аналізу це не є критичним.

6. У тексті дисертаційної роботи трапляються окремі неточності стилістичного та технічного характеру, зокрема незначні відмінності в оформленні окремих елементів тексту та допоміжних матеріалів, що не впливає на загальну позитивну оцінку роботи.

10. Висновки

Дисертаційна робота Хулапа Андрія Валерійовича є завершеним науковим дослідженням, у якому отримано нові науково обґрунтовані результати, що мають теоретичне та практичне значення для розвитку галузі комп'ютерної інженерії. У дисертації розв'язано актуальну науково-технічну задачу підвищення ефективності систем виявлення мережевих вторгнень у середовищі Інтернету речей шляхом оптимізації нейромережевих обчислень та адаптації моделей штучного інтелекту до виконання на малоресурсних embedded- і мікроконтролерних платформах.

З огляду на актуальність теми дослідження, належний рівень обґрунтованості та достовірності отриманих результатів, їх наукову новизну і практичну цінність, вважаю, що дисертаційна робота Хулапа Андрія Валерійовича «Моделі, методи та програмні компоненти засобів штучного інтелекту для захисту інформації систем Інтернету речей» відповідає вимогам пунктів 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», затвердженого Постановою Кабінету Міністрів України від 12.01.2022 р. № 44, а її автор заслуговує на присудження ступеня доктора філософії за спеціальністю 123 «Комп'ютерна інженерія».

Рецензент – кандидат технічних наук,
доцент кафедри комп'ютерної інженерії
та програмування Національного
технічного університету «Харківський
політехнічний інститут» Микола МЕЗЕНЦЕВ
01.06.2026

Підпис
ЗАСВІДЧУЮ:
ВЧЕНИЙ СЕКРЕТАР
НАЦІОНАЛЬНОГО ТЕХНІЧНОГО УНІВЕРСИТЕТУ
"ХАРКІВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ"
"___" _____ 20____ р.

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ * Національний технічний університет "Харківський політехнічний інститут" * код 02070180 *