Голові разової спеціалізованої вченої ради
Державного університету «Київський
авіаційний інститут»
доктору технічних наук, професору
Гнатюку Сергію Олександровичу

РЕЦЕНЗІЯ

кандидата технічних наук, доцента, завідувача кафедри кібербезпеки
«Державний університет «Київський авіаційний інститут»
Ільєнко Анни Вадимівни
на дисертацію Петляк Наталії Сергіївни
«Моделі та методи виявлення аномального трафіку в інформаційно-комунікаційних системах», представлену на здобуття наукового ступеня
доктора філософії за спеціальністю 125 – Кібербезпека
галузі знань 12 – Інформаційні технології

1. Актуальність теми дисертаційного дослідження

У сучасному цифровому середовищі, де інформаційно-комунікаційні системи є критично важливою складовою інфраструктури підприємств, установ і державних органів, проблема забезпечення кібербезпеки набуває особливої ваги. Зі зростанням обсягів передаваних та оброблюваних даних, а також із підвищенням складності атак, зокрема тих, що маскуються під звичайну мережеву активність, традиційні підходи до виявлення загроз втрачають свою ефективність. Значну небезпеку становлять атаки, які не мають явних ознак або є новими модифікаціями відомих шаблонів, що унеможливлює їхнє своєчасне виявлення засобами сигнатурного аналізу.

Одним із перспективних напрямів підвищення ефективності інформаційного захисту є виявлення аномального трафіку – підхід, що ґрунтується на виявленні відхилень від типової поведінки мережі. Такий

підхід дозволяє виявити приховані або розподілені в часі загрози, які не фіксуються класичними методами, та реагувати на них до настання негативних наслідків. Особливої актуальності це набуває в контексті аналізу вихідного трафіку, який традиційно залишається менш контрольованим, хоча може містити ознаки витоку даних або слугувати каналом для зловмисних дій, у тому числі DDoS-атак.

Зростання кількості кіберінцидентів, зокрема пов'язаних з розподіленими атаками на відмову в обслуговуванні, вимагає перегляду існуючих методів моніторингу та виявлення загроз. Статистика підтверджує стрімке зростання частоти та потужності таких атак, що веде до значних фінансових втрат для бізнесу, порушення безперервності бізнес-процесів і зниження довіри клієнтів.

Дисертаційне дослідження Петляк Наталії Сергіївни є своєчасним і актуальним у зв'язку з необхідністю розробки інтелектуальних моделей і методів виявлення аномального трафіку, орієнтованих на аналіз саме **вихідних мережевих потоків**. Результати дослідження сприятимуть побудові ефективних систем захисту, здатних виявляти як нові, так і приховані загрози, підвищити рівень безпеки інформаційно-комунікаційної інфраструктури, зменшити втрати від інцидентів безпеки та сформувати науково обґрунтовані рекомендації щодо оптимізації мережевого моніторингу в умовах постійно зростаючих кіберризиків.

2. Структура та зміст дисертаційного дослідження

Дисертація складається з анотації, переліку умовних позначень, вступу, 4 розділів, висновків, списку використаних джерел, 3 додатки. Загальний обсяг дисертації становить 153 сторінок, в тому числі 45 рисунків, 14 таблиць та 104 джерела використаної літератури. Основний текст роботи викладено на 122 сторінки. У вступі автором сформульовано актуальність, мету, задачі дослідження, об'єкт та предмет дослідження, наукову новизну та практичну цінність отриманих результатів, вказано особистий внесок здобувача, а також наведено результати впровадження рішення у ТОВ «X-CITY» (акт

впровадження від 10.04.2025р.) та у навчальному процесі кафедри кібербезпеки Хмельницького національного університету під час викладання дисциплін «Технології виявлення вразливостей та вторгнень», «Безпека безпроводових мереж та інтернет речей» та «Моніторинг та менеджмент інформаційної безпеки» (акт впровадження від 25.03.2025р.)

У першому розділі дисертаційної роботи автором здійснено комплексний аналіз сучасного стану інформаційної безпеки в контексті зростаючих загроз для інформаційно-комунікаційних систем. Особливу увагу приділено проблематиці виявлення аномалій у мережевому трафіку, що є ключовим елементом у запобіганні складним типам кібератак. Наведено огляд існуючих підходів до виявлення аномалій, таких як статистичні, кластеризаційні, поведінкові та моделі машинного навчання, а також висвітлено їх недоліки в умовах динамічного середовища. Окремо автором підкреслено важливість дослідження вихідного трафіку як джерела інформації про потенційно зловмисну активність. Обґрунтовано актуальність подальшого вдосконалення моделей і методів виявлення аномалій, що й стало підґрунтям для формулювання мети дослідження.

У другому розділі дисертаційної роботи представлено розроблені моделі процесів, що описують типову поведінку користувачів і порушників у мережі, а також моделі класифікації мережевого трафіку. Визначено ключові сценарії взаємодії в мережі та побудовано відповідні поведінкові моделі. Описано модель сигнатури пакету як основу для класифікації трафіку, а також впроваджено концепцію нечіткої класифікації для врахування невизначеності вхідних даних. Формалізація моделей у цьому розділі створює основу для подальшого розроблення методів виявлення аномалій.

У третьому розділі дисертаційної роботи запропоновано та вдосконалено методи виявлення аномального трафіку, зокрема метод класифікації за ознаками, метод самоподібності та нечіткий метод на основі правил нечіткої логіки. На основі аналізу переваг окремих підходів побудовано гібридний метод виявлення аномалій, що дозволяє підвищити

точність, адаптивність та стійкість до нових типів атак. Проведено експериментальні дослідження, результати яких підтверджують ефективність запропонованого підходу.

У четвертому розділі дисертаційної роботи реалізовано структурну модель системи виявлення аномального трафіку на основі розробленого гібридного методу. Докладно описано реалізацію основних модулів системи, механізмів класифікації та логування результатів. Результати експериментального дослідження у тестовому середовищі демонструють високу точність виявлення аномалій, зменшення кількості хибнопозитивних спрацювань, а також стабільність роботи системи за умов змін навантаження. Таким чином, забезпечено повноцінну перевірку працездатності системи та підтверджено доцільність її впровадження для підвищення рівня кіберзахисту інформаційно-комунікаційних систем.

У висновках представлено основні наукові та практичні результати дисертаційного дослідження.

У додатках розміщено фрагменти вихідного коду та акт впровадження результатів дисертаційного дослідження.

Дисертаційна робота оформлена відповідно до вимог Наказу МОН України від 12 січня 2017 року № 40 «Про затвердження вимог до оформлення дисертації».

Наукова новизна дисертаційного дослідження

– *Вдосконалено* модель сигнатури пакету для пошуку аномального трафіку, що за рахунок виключення з параметрів сигнатури розміру заголовка, контрольної суми заголовку, корисного розміру пакета, мітки потоку, пріоритету пакету, контрольної суми пакету за принципом Парето, забезпечило зменшення часу аналізу трафіку.

– *Вдосконалено* модель процесу нечіткого виявлення аномального трафіку, в якій сформовано набір правил за рахунок експертного визначення кількості термів та їх значень для кожної лінгвістичної змінної, що дозволило розробити гібридний метод виявлення аномального трафіку в інформаційно-

комунікаційних системах.

– *Вперше* розроблено гібридний метод виявлення аномального трафіку в інформаційно-комунікаційних системах в якому за рахунок інтеграції методу класифікації трафіку за ознаками, методу самоподібності та нечіткого методу дозволило динамічно формувати множини сигнатур для методу класифікації трафіку за ознаками, що дозволило зменшити час аналізу трафіку.

– *Удосконалено* структурну модель системи виявлення аномального трафіку в інформаційно-комунікаційних системах, що за рахунок інтегрування розробленого гібридного методу виявлення аномального трафіку в інформаційно-комунікаційних системах, дозволило підвищити достовірність виявлення аномального трафіку та зменшити навантаження на процесор за рахунок зміни множини дозволених й заборонених з'єднань у режимі реального часу.

3. Практичне значення отриманих результатів

– розроблено алгоритмічне забезпечення системи виявлення аномального трафіку в інформаційно-комунікаційних системах, що реалізує гібридний метод, його складові метод класифікації трафіку за ознаками, метод самоподібності, нечіткий метод та моделі, що в низ використовуються;

– на основі алгоритму розроблено програмний застосунок, що дозволяє проводити аналіз трафіку в інформаційно-комунікаційних системах;

– можливість практичного використання розробленого програмного застосунку сумісно з маршрутизаторами в інформаційно-комунікаційній системі.

4. Апробація результатів дисертаційного дослідження

Результати дисертації доповідались та обговорювались на конференціях, серед яких: II студентська науково-технічна конференція «Інформаційна, функційна та кібербезпека» (СКІФіК-2022) (Харків, 2022), The International Workshop on Intelligent Information Technologies & Systems of Information Security (Хмельницький, 2022), VI Міжнародна науково-практична

конференція «Інформаційна безпека та комп'ютерні технології» (Кропивницький, 2023), XII Міжнародна науково-технічна конференція ITSec: Безпека інформаційних технологій (Ужгород, 2023), IX Міжнародна науково-практична конференція Захист інформації і безпека інформаційних систем (Львів, 2023), 13th International Conference on Dependable Systems, Services and Technologies (Athens, 2023), XIII Міжнародна науково-технічна конференція ITSec: Безпека інформаційних технологій (Львів, 2024), 4the International Workshop on Intelligent Information Technologies & Systems of Information Security (Хмельницький, 2024), 1st International Workshop on Advanced Applied Information Technologies (Khmelnytskyi, 2024), 1st International Workshop on Intelligent and CyberPhysical Systems (Khmelnytskyi, 2024), 2nd International Workshop on Computer Information Technologies in Industry 4.0 (Ternopil, 2024).

5. Публікації дисертаційного дослідження

За матеріалами дисертаційних досліджень опубліковано 17 наукових робіт, у тому числі: 6 наукових статей – у наукових фахових виданнях України; 11 тез і матеріалів доповідей на міжнародних і науково-практичних конференціях, з них 5 – у рецензованому виданні, що входить до бази даних Scopus, 1 – у рецензованому виданні, що входить до бази даних IEEE.

6. Оцінка змісту дисертації, її завершеність та дотримання принципів академічної доброчесності

За змістом дисертаційна робота Петляк Наталії Сергіївни повністю відповідає Стандарту вищої освіти зі спеціальності 125 «Кібербезпека».

Дисертаційна робота є завершеною науковою працею та містить особистий внесок здобувача у обраному напрямку. За результатами поглибленого аналізу дисертаційної роботи можна зробити висновок, що робота Петляк Н.С. є результатом власних досліджень і не містить елементів фальсифікації, плагіату чи запозичень.

7. Зауваження та недоліки до дисертаційного дослідження

1) У другому розділі дисертаційної роботи автором представлено одразу кілька моделей (поведінки користувача, порушника, сигнатури пакету тощо), однак їх формалізація є надто фрагментованою та перевантажена повторюваними поясненнями. Це ускладнює сприйняття логіки переходу між моделями. Доцільним було б представити загальну логіку переходів та інтеграцію моделей через єдину схему або опис, що дозволило б уникнути дублювань і покращити сприйняття матеріалу.

2) У третьому розділі методи виявлення аномалій подані окремими підрозділами (ознаковий, самоподібності, нечіткий, гібридний), проте не зовсім зрозуміло, які саме етапи реалізації повторюються в кожному з них, а які є унікальними. У зв'язку з цим виникає потреба у більш чіткій систематизації алгоритмів (наприклад, у вигляді табличного порівняння), що підвищить читабельність і забезпечить краще розуміння відмінностей між методами.

3) Автор стверджує про вперше розроблений гібридний метод виявлення аномального трафіку, однак більшість його складових (класифікація за ознаками, нечіткий аналіз, самоподібність) вже використовувались у відомих підходах. Інноваційність рішення полягає у їх інтеграції, однак це варто чіткіше підкреслити, оскільки наразі виникає враження, що частина тверджень щодо новизни потребує додаткового обґрунтування через зіставлення з існуючими рішеннями.

4) У таблицях із результатами експериментів (зокрема в розділі 4) відсутні вказівки на кількість запусків експериментів, довірчі інтервали або відхилення. Це унеможливлює оцінку статистичної достовірності отриманих результатів. Для підвищення об'єктивності необхідно було б додати кількісні метрики валідації, особливо при порівнянні ефективності різних методів.

5) У процесі реалізації програмного модуля та тестування системи аномального трафіку автор наводить опис компонентів системи, однак відсутній аналіз продуктивності (наприклад, час реакції системи в реальному часі, навантаження на апаратне забезпечення, масштабованість). Це

ускладнює розуміння практичної придатності системи до впровадження в умовах великого обсягу трафіку або реальної інформаційно-комунікаційної системи.

Незважаючи на всі вище згадані зауваження та недоліки, вони не є принциповими та не зменшують загальну наукову новизну та значимість одержаних результатів дослідження. Висловлені зауваження не впливають на позитивне оцінювання дисертаційного дослідження здобувача.

8. Висновок

Вважаю, що дисертаційна робота здобувача Петляк Наталії Сергіївни на тему «Моделі та методи виявлення аномального трафіку в інформаційно-комунікаційних системах» є завершеною кваліфікаційною роботою та виконана на високому рівні, що не порушує принципів академічної доброчесності та є цілісною, і має вагоме значення для галузі знань 12 «Інформаційні технології».

Таким чином, дисертаційна робота відповідає вимогам п. 6-9 Постанові Кабінету Міністрів України №44 від 12.01.2022 «Про затвердження Порядку присудження ступеня доктора філософії та скасування рішення разової спеціалізованої вченої ради закладу вищої освіти, наукової установи про присудження ступеня доктора філософії», а її автор, Петляк Наталія Сергіївна, заслуговує на присудження ступеня доктора філософії за спеціальністю 125 «Кібербезпека», галузі знань 12 «Інформаційні технології».

РЕЦЕНЗЕНТ
кандидат технічних наук, доцент,
завідувач кафедри кібербезпеки
Державного некомерційного
підприємства «Державний університет
«Київський авіаційний інститут» Анна ІЛЬЄНКО
«11» 07 2025 року

Підпис Ільєнко А.В.
засвідчую
Сергій ГНАТЮК, проректор з наукових досліджень та трансферу технологій ДУКІ