Голові разової спеціалізованої вченої ради Державного некомерційного підприємства «Державний університет «Київський авіаційний інститут», доктору технічних наук, професору
Гнатюку Сергію Олександровичу

ВІДГУК
офіційного опонента,

доктора технічних наук, професора, професора кафедри систем та технологій Кібербезпеки Державного університету інформаційно-комунікаційних технологій Казмірчук Світлани Володимирівни на дисертаційну роботу 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 сучасних умовах стрімкого розвитку інформаційно-комунікаційних технологій дедалі більшої ваги набуває забезпечення надійного функціонування інформаційно-комунікаційних систем (ІКС), які стали критично важливою інфраструктурою у сферах державного управління, енергетики, транспорту, фінансів, охорони здоров'я, освіти тощо. Зі зростанням обсягу, складності та динамічності мережевого трафіку зростає і кількість та складність кіберзагроз, серед яких особливу небезпеку становлять атаки, що маскуються під нормальну активність – аномальний трафік. В цих умовах забезпечення своєчасного та надійного моніторингу мережевої активності набуває критичного значення, особливо щодо вихідного трафіку, який часто залишається поза фокусом систем захисту, хоча саме в ньому можуть приховуватись прояви шкідливої активності, витоку даних або спроби організації атак.

Наявні підходи до виявлення аномалій у мережевому трафіку здебільшого базуються на загальних принципах машинного навчання або статистичного аналізу, але не враховують особливості топології ІКС, її типового функціонування, динаміки поведінкових профілів користувачів і сервісів. Також потреба у дослідженні зумовлена недостатньою ефективністю традиційних сигнатурних підходів, що орієнтовані виключно на фіксацію вже відомих загроз. Такі системи не здатні враховувати складні сценарії, пов'язані з поведінковою мінливістю користувачів або новими типами атак, які не мають попередніх аналогів. Як свідчать аналітичні звіти останніх років, понад третину сучасних кіберінцидентів становлять нетипові атаки, що залишаються поза увагою класичних систем. Це вимагає переходу до адаптивних, інтелектуальних рішень, здатних аналізувати нетривіальні ознаки загроз у режимі реального часу.

Особливої актуальності тема набуває з огляду на посилення гібридних загроз, що поєднують технічні та соціальні методи впливу на інформаційну інфраструктуру, що характерно, зокрема, для кібербезпеки України в умовах збройної агресії. Формування національного кіберпростору, стійкого до

аномальної активності та кібератак, вимагає науково обґрунтованих підходів до моніторингу трафіку в реальному часі, автоматизованого виявлення нетипової поведінки та адаптивного реагування на інциденти.

Запропонована у дисертації тематика вирізняється високою актуальністю, адже зосереджена на створенні моделей і методів, що охоплюють не лише технічні характеристики трафіку, але й поведінкові шаблони взаємодії користувачів і потенційних атакуючих. Особливу цінність мають дослідження, в яких поєднано підходи на основі самоподібності, методи нечіткої логіки та ознакової класифікації в єдину гібридну систему виявлення аномалій. Така система має потенціал значно підвищити точність, адаптивність і стійкість до змін, що є надзвичайно важливим у контексті цифрової безпеки в умовах сучасних викликів.

2. Аналіз основного змісту, наукової новизни і практичної цінності, достовірності та обґрунтованості результатів.

Аналіз основного змісту, наукової новизни та практичної цінності

Дисертація складається із анотації, вступу, чотирьох розділів, загальних висновків, списку використаних джерел, додатків. Повний обсяг роботи становить 154 сторінки друкованого тексту, з них анотація – на 11 стор., зміст – на 2 стор., список публікацій за темою дисертації – на 3 стор. основний текст – на 110 стор., список із 104 використаних джерел – на 13 стор., додатки – на 14 стор. Дисертація містить 46 рисунків та 14 таблиць.

Зміст роботи відповідає темі роботи. Робота побудована логічно, її основний зміст вирішує сформульовані науково-прикладні задачі. Всі поставлені в роботі задачі виконано в повному обсязі, а мета досягнута.

У *вступі* чітко представлено актуальність дисертаційного дослідження, визначено мету, об’єкт та предмет дослідження, а також сформульовано проблему дослідження, описані задачі, які необхідно вирішити, надано інформацію про апробацію результатів дослідження, наведено інформацію про публікації та структуру роботи.

Перший розділ дисертації присвячено ґрунтовному аналізу сучасного стану досліджень у галузі виявлення аномального трафіку в ІКС. Здійснено глибокий огляд теоретичних основ та практичних реалізацій класичних і сучасних методів виявлення аномалій, зокрема — сигнатурного аналізу, поведінкового підходу, методів машинного навчання та самоподібності. Оцінюються переваги й недоліки кожного підходу в контексті їх застосування до високодинамічного мережевого середовища. На підставі виявлених обмежень обґрунтовано доцільність розроблення нових, більш адаптивних моделей виявлення загроз, з особливим акцентом на гібридизацію методів та застосування нечіткої логіки для підвищення чутливості системи до нетипових відхилень.

У *другому розділі* представлено методологічну основу дисертаційного дослідження, що включає розроблення формалізованих моделей поведінки легітимного користувача та потенційного зловмисника в умовах функціонування сучасної ІКС. Здійснено математичну формалізацію моделей класифікації трафіку. Вдосконалено сигнатурну модель шляхом застосування принципу Парето для виключення малозначущих параметрів, що дозволяє зменшити обчислювальне навантаження без втрати інформативності. Уведення нечітких

змінних у систему класифікації дозволяє враховувати невизначеність та варіативність у поведінці трафіку.

У *третьому розділі* розглянуто практичну реалізацію запропонованих теоретичних підходів. Розроблено гібридний метод виявлення аномального трафіку, який поєднує ознакову класифікацію, аналіз самоподібності та механізм нечіткого виведення. Такий підхід забезпечує значне підвищення точності виявлення загроз, зменшення рівня хибнопозитивних спрацювань та підвищення адаптивності системи до змін у структурі трафіку. Надані результати експериментального моделювання засвідчують ефективність розробленої методики в умовах реального мережевого середовища.

У *четвертому розділі* дисертації подано архітектурну реалізацію системи виявлення аномального трафіку, створену на основі запропонованого гібридного методу. Детально описано структуру програмного забезпечення, взаємодію між його модулями, принципи обробки та класифікації мережевого трафіку в реальному часі. Проведено тестування системи у тестовому середовищі з реалістичними навантаженнями, здійснено аналіз її продуктивності, масштабованості та стійкості до змін у мережевій інфраструктурі. Представлені результати свідчать про можливість практичного впровадження розробленої системи у корпоративних і державних структурах.

Висновки дисертаційної роботи логічно завершують дослідження, систематизуючи основні теоретичні та прикладні здобутки. Продемонстровано досягнення поставлених цілей, підтверджує наукову новизну результатів, обґрунтовує їх практичну цінність, що дозволяє розглядати роботу як завершене наукове дослідження, що відповідає вимогам до дисертацій на здобуття ступеня доктора філософії.

Новизна одержаних результатів. Усі наукові положення, які описані в дисертаційній роботі та виносяться на захист отримані Петляк Н.С. особисто:

1) *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.

2) *вдосконалено* модель процесу нечіткого виявлення аномального трафіку, в якій за рахунок використання експертного підходу сформована множина правил та набір відповідних лінгвістичних змінних, що дозволило розробити нові підходи до виявлення аномального трафіку в інформаційно-комунікаційних системах.

3) *вперше* розроблено гібридний метод виявлення аномального трафіку в інформаційно-комунікаційних системах в якому за рахунок інтеграції методу класифікації трафіку за ознаками, методу самоподібності та розробленої моделі процесу нечіткого виявлення дозволило динамічно формувати множини сигнатур при класифікації трафіку за ознаками та підвищити показники виявлення аномального трафіку.

4) *вдосконалено* структурну модель системи виявлення аномального трафіку в інформаційно-комунікаційних системах, що за рахунок інтегрування розробленого гібридного методу виявлення аномального трафіку в

інформаційно-комунікаційних системах та динамічного варіювання множиною дозволених та заборонених з'єднань у режимі реального часу дозволило зменшити навантаження на процесор.

Практичне значення одержаних автором наукових результатів.

1. Одержані в дисертаційній роботі результати стали підґрунтям для забезпечення зменшення обсягів аномального трафіку в інформаційно-комунікаційні системі.
2. 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 них використовуються.
3. На основі алгоритму розроблено програмний застосунок, що дозволяє проводити аналіз трафіку в інформаційно-комунікаційних системах.
4. Можливість практичного використання розробленого програмного застосунку сумісно з маршрутизаторами в інформаційно-комунікаційній системі.
5. Результати дисертаційної роботи апробовано і використано у ТОВ «X-CITY» (акт впровадження від 10.04.2025р) та у навчальному процесі кафедри кібербезпеки Хмельницького національного університету (акт впровадження від 25.03.2025р.).

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).

Ступінь достовірності й обґрунтованості наукових положень, висновків і рекомендацій, сформульованих у дисертації.

Наукові положення, висновки та практичні рекомендації, викладені у дисертації Петляк Наталії Сергіївни, відзначаються належним рівнем обґрунтованості, що досягається завдяки системному підходу до постановки і розв'язання дослідницьких завдань. Теоретичні положення, покладені в основу розроблених моделей і методів виявлення аномального трафіку, логічно випливають із сучасного наукового уявлення про функціонування ІКС та базуються на міждисциплінарному поєднанні підходів з кібербезпеки, теорії

нечітких множин, поведінкового аналізу, класифікації даних та системного моделювання.

У процесі дослідження обґрунтовано використано широкий спектр формальних методів: методи нечіткого логічного висновку, алгоритми класифікації трафіку за ознаками, аналіз самоподібності, а також методи гібридного поєднання механізмів розпізнавання та адаптації. До формулювання моделей було залучено також елементи експертного оцінювання, апроксимації нечітких залежностей та статистичного аналізу результатів.

Достовірність отриманих наукових результатів підтверджено багатократною перевіркою в експериментальному середовищі, що наближене до реальних умов функціонування сучасних ІКС. Здобуті емпіричні дані узгоджуються з аналітичними висновками та демонструють стабільність поведінки запропонованих моделей в умовах змінних параметрів мережевого трафіку, що засвідчує їхню адаптивність і потенціал практичного використання. Усі розрахунки та висновки представлені у логічній послідовності та підтверджуються чисельними прикладами.

Таким чином, положення дисертації мають високий ступінь наукової виваженості, методологічної прозорості та практичної релевантності, що дозволяє розглядати їх як достовірну наукову базу для подальших розробок у сфері систем виявлення аномального трафіку.

Повнота викладу наукових результатів дисертації в публікаціях. 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.

Зауваження та недоліки до тексту дисертації

1) В предметі дослідження здобувач зазначає тільки методи та моделі виявлення аномального трафіку в інформаційно-комунікаційних системах, але в першому розділі п. 1.1 ще додатково проводить аналіз загроз безпеки інформації в сучасних ІКС та мережах.

2) В дисертаційній роботі немає формального обґрунтування вибору показника Херста для визначення самоподібності трафіку.

3) В розділі 1 на відміну від інших розділів чітко не структуровані відповідні висновки.

4) В формулі 2.1 на стор. 66 кількість компонентів в кортежі вказано k, однак далі не зазначається, що в кортежі 9 компонентів, і далі не зрозуміло чи може k приймати відмінні від 9 значення.

5) Оскільки, в формулі 2.17 лічильник m змінюється від 1 до k, то запис в такому вигляді: $\sum_{m=1}^{k} d_i^j$ втрачає смисл, оскільки його можна записати як kd_i^j.

6) В роботі містяться незначні орфографічні помилки, наприклад, на сторінках 37 та 79 помилка зроблена в словах в режимі (в режимії) та оскільки (Оскіцльки), в кінці речення після формул 2.4, 2.9, 2.10, 2.12, 4.5 немає крапки, а після формули 2.8 немає коми тощо.

Проте, незважаючи на вище зазначені недоліки, не знижується значущість отриманих наукових та практичних результатів і не впливають на загальну

позитивну оцінку дисертаційного дослідження.

3. Загальний висновок по роботі.

Дисертаційна робота Петляк Наталії Сергіївни становить собою завершене самостійне наукове дослідження, присвячене вирішенню актуальної проблеми забезпечення кібербезпеки шляхом виявлення аномального трафіку в ІКС. У межах дисертації реалізовано комплексний підхід до аналізу сучасних загроз у мережевому середовищі та розроблено інноваційні методи детектування відхилень у поведінці трафіку, що мають як теоретичне, так і прикладне значення.

Запропоновано гібридний метод виявлення аномалій, який базується на інтеграції кількох підходів. Така комбінація забезпечила підвищену точність і адаптивність системи до змін у структурі трафіку, що підтверджено результатами експериментального моделювання в тестовому середовищі. Значущим результатом роботи є також розробка структурної моделі системи виявлення загроз, адаптованої до реального часу функціонування, та створення відповідного програмного забезпечення, яке продемонструвало свою ефективність під час апробації.

Представлена робота є вагомим внеском у розвиток методологічних основ кіберзахисту й може бути використана в галузях, пов'язаних із моніторингом мережевої безпеки, проектуванням інтелектуальних систем виявлення загроз і навчальними програмами з інформаційної безпеки.

Вважаю, що дана дисертаційна робота відповідає вимогам до дисертаційних досліджень на здобуття ступеня доктора філософії, визначеним Постановою Кабінету Міністрів України №44 від 12.01.2022 «Про затвердження Порядку присудження ступеня доктора філософії та скасування рішення разової спеціалізованої вченої ради закладу освіти, наукової установи про присудження ступеня доктора філософії».

Дисертаційна робота може бути представлена до офіційного захисту у разовій спеціалізованій вченій раді, а її автор, Петляк Наталія Сергіївна, заслуговує на присудження ступеня доктора філософії за спеціальністю 125 – Кібербезпека, галузі знань 12 – Інформаційні технології.

ОФІЦІЙНИЙ ОПОНЕНТ:
доктор технічних наук, професор
професор кафедри систем
та технологій кібербезпеки
Державного університету інформаційно-
комунікаційних технологій Світлана КАЗМІРЧУК
«16» 07 2025 року

Підпис професора Казмірчук С.В. з а с в і д ч у ю:

Т.в.о. ректора
Державного університету
інформаційно-комунікаційних технологій Олександр КОРЧЕНКО
«16» 07 2025 р.