

Голові разової спеціалізованої вченої ради
Державного університету інформаційно-комунікаційних технологій
професору кафедри систем та технологій кібербезпеки
Навчально-наукового інституту кібербезпеки та захисту інформації
КАЗМІРЧУК Світлані Володимирівні

ВІДГУК

офіційного опонента

ДЕЛЕМБОВСЬКОГО Максима Михайловича

кандидата технічних наук, доцента,

завідувача кафедри кібербезпеки та комп'ютерної інженерії

Київського національного університету будівництва та архітектури

на дисертаційну роботу Гамзи Дмитра Євгенійовича на тему:

**«МЕТОДИ ВИЯВЛЕННЯ ШКІДЛИВОЇ АКТИВНОСТІ В
ІНФОРМАЦІЙНІЙ СИСТЕМІ ОРГАНІЗАЦІЇ НА ОСНОВІ ГІБРИДНОЇ
КЛАСИФІКАЦІЇ»**

подану на здобуття наукового ступеня доктора філософії
за спеціальністю 125 – «Кібербезпека», галузь знань 12 – «Інформаційні
технології».

1. Актуальність теми

Питання виявлення шкідливої активності в інформаційних системах організацій набуває дедалі більшої гостроти в умовах стрімкого зростання кількості кіберінцидентів. За даними аналітичних звітів ENISA Threat Landscape 2024 та IBM Cost of a Data Breach Report 2024, кількість верифікованих кіберінцидентів у ЄС сягає майже 4 900 на рік, а середній час виявлення витoku даних становить 241 день. Ці факти переконливо свідчать про недостатню ефективність традиційних сигнатурних методів захисту та моно-класифікаторів на основі машинного навчання.

Запропонований у дисертації підхід, що базується на гібридній класифікації з використанням стекінг-ансамблю різнорідних алгоритмів машинного навчання, є закономірною відповіддю на виявлені протиріччя між необхідністю виявлення нових типів атак у реальному часі та обмеженими

можливостями існуючих засобів захисту. Тема дослідження відповідає пріоритетним напрямкам розвитку науки і техніки в Україні, а також вимогам Стратегії кібербезпеки України та міжнародних стандартів ISO/IEC 27001 і NIST Cybersecurity Framework.

2. Обґрунтованість наукових результатів, висновків та рекомендацій

Обґрунтованість результатів дисертаційної роботи забезпечена чіткою постановкою мети та наукового завдання, послідовним виконанням усіх запланованих часткових завдань дослідження та коректним використанням математичного апарату. Автором формалізовано задачу виявлення шкідливої активності як задачу багатокритеріальної оптимізації з цільовою функцією максимізації F1-score при жорстких обмеженнях на рівень хибних спрацювань та час прогнозування.

Достовірність отриманих результатів підтверджується проведенням масштабного експериментального дослідження на еталонному датасеті CSE-CIC-IDS2018, що є загальновизнаним бенчмарком у галузі досліджень систем виявлення вторгнень. Досягнуті показники Accuracy 98,07%, F1-score 96,57% та час прогнозування 7,16 мс є конкурентоспроможними порівняно з аналогічними роботами у цій предметній галузі.

Висновки та рекомендації дисертації є обґрунтованими та впливають з проведеного експериментального дослідження. Практичні рекомендації щодо розгортання програмного рішення (вимоги до апаратного забезпечення, параметри калібрування, процедури підтримки) є конкретними та реалістичними для впровадження в інформаційних системах організацій різного масштабу.

3. Новизна наукових результатів дослідження

Дисертаційна робота містить результати, що характеризуються науковою новизною та мають вагоме значення для розвитку методів

виявлення шкідливої активності. До основних здобутків, що визначають наукову новизну, слід віднести:

1. Вперше розроблено метод виявлення шкідливої активності в інформаційній системі організації на основі гібридної класифікації, який базується на використанні гетерогенного набору базових класифікаторів та мета-класифікаторі на основі XGBoost для дворівневої стекінг-архітектури, що дає можливість застосовувати різноманітні ансамблеві методи машинного навчання у системах виявлення шкідливої активності в режимі реального часу з можливістю динамічного переналаштування класифікаторів.

2. Удосконалено метод комплексної оптимізації вхідного набору даних методу виявлення шкідливої активності в інформаційній системі, який, на відміну від існуючих, поєднує балансування класів (SMOTE), нормалізацію (Min-Max) та зниження розмірності (PCA), що дозволило зменшити обчислювальне навантаження та підвищити точність методу гібридної класифікації.

3. Набув подальшого розвитку метод багатокритеріального вибору оптимальної архітектури системи виявлення шкідливої активності у режимі реального часу, в якому, за рахунок використання послідовного застосування стратегії фільтрації за середніми значеннями та побудови фронту Парето забезпечується баланс між максимальною точністю виявлення шкідливої активності та мінімальними витратами обчислювальних ресурсів.

4. Практична цінність отриманих результатів

Практична цінність дисертаційної роботи є очевидною та підтверджується реальними впровадженнями. Розроблене програмне рішення на основі гібридного методу класифікації прийнято до впровадження в діяльність ТОВ «Євротелеком» та ТОВ «АРВІОМ», а також використано у навчальному процесі Державного університету інформаційно-комунікаційних технологій.

Розроблена п'ятимодульна архітектура програмного рішення (збір даних, інженерія ознак, попередня обробка, гібридна класифікація, реагування) є повністю готовою до інтеграції у сучасні SIEM/SOAR системи. Результати моделювання показали, що виявлення шкідливої активності в інформаційній системі організації на основі гібридної класифікації дозволяє забезпечити приріст точності на 3,87 % та F1-score на 5,11 %, а також скоротити найменший час прогнозування на 76 %. Програмне рішення забезпечує максимальну точність на рівні 0,9807 та мінімальну затримку на рівні 7,16 мс, що задовольняє вимогам до систем виявлення вторгнень реального часу.

5. Зв'язок роботи з науковими програмами, планами та темами

Дисертаційна робота виконана в межах науково-дослідних робіт «Методологія виявлення шкідливих процесів в інформаційних системах» (№ 0121U113613) та «Розробка науково-методичних рекомендацій виявлення шкідливих процесів в інформаційній системі організації» (ТОВ «АЛЬФА-МЕТАЛ», м. Київ). Тематика дослідження відповідає пріоритетним напрямкам розвитку науки і техніки в Україні та узгоджується із Законом України «Про основні засади забезпечення кібербезпеки України».

6. Повнота викладу основних результатів дисертації у публікаціях

Основні положення та результати дисертаційного дослідження відображені у 9 наукових працях, серед яких 6 наукових статей (3 – у спеціалізованих фахових виданнях, затверджених МОН України, 1 – у закордонному виданні, що індексується в Scopus, 2 – у інших виданнях України) та 3 тези доповідей на науково-практичних конференціях. Рівень апробації результатів є достатнім для підтвердження наукового внеску здобувача та відповідає вимогам до дисертацій на здобуття ступеня доктора філософії.

7. Оцінка змісту дисертації та відповідність встановленим вимогам щодо оформлення

Дисертація є цілісною завершеною науковою працею, у якій витримано логіку наукового дослідження. Перший розділ містить ґрунтовний аналіз проблематики та класифікацію існуючих методів виявлення шкідливої активності. Другий розділ присвячено розробці гібридного методу класифікації з математичною формалізацією моделі. У третьому розділі проведено комплексне експериментальне дослідження. Четвертий розділ систематизує результати у вигляді архітектури програмного рішення та рекомендацій щодо впровадження.

Зміст дисертаційної роботи відповідає заявленій темі та спеціальності. Оформлення відповідає вимогам до кваліфікаційних праць на здобуття ступеня доктора філософії.

Недоліки та зауваження

Поряд із позитивною оцінкою дисертації доцільно відзначити окремі зауваження рекомендаційного характеру:

1) у третьому розділі бажано деталізувати опис процедури підбору гіперпараметрів базових класифікаторів та мета-класифікатора, включаючи метод оптимізації та кількість ітерацій крос-валідації, що підвищить відтворюваність результатів;

2) доцільно розширити порівняльний аналіз з іншими сучасними гібридними підходами до виявлення вторгнень, представленими в літературі за останні 2–3 роки, для більш повного контекстування досягнутих результатів;

3) перспективним є висвітлення питань стійкості запропонованого методу до адверсаріальних атак, зокрема до цілеспрямованого «отруєння» навчальних даних, що є актуальним для систем кібербезпеки;

4) у четвертому розділі варто деталізувати процедуру моніторингу концептуального дрейфу та автоматичного перенавчання моделі в умовах еволюції кіберзагроз.

Зазначені зауваження мають рекомендаційний характер і не знижують загальної цінності дисертаційної роботи.

Висновок

Дисертаційна робота Гамзи Дмитра Євгенійовича на тему «Методи виявлення шкідливої активності в інформаційній системі організації на основі гібридної класифікації» є завершеним самостійним науковим дослідженням, у якому отримано нові науково обґрунтовані результати, що мають теоретичне та практичне значення для сфери кібербезпеки.

За змістом, рівнем наукової новизни, обґрунтованістю висновків та практичною значущістю дисертація відповідає вимогам до дисертацій на здобуття наукового ступеня доктора філософії, а її автор заслуговує на присудження наукового ступеня доктора філософії за спеціальністю 125 – «Кібербезпека».

Офіційний опонент:

Кандидат технічних наук, доцент,
завідувач кафедри кібербезпеки
та комп'ютерної інженерії Київського національного університету
будівництва і архітектури

« 12 » 06 2026 р

Максим ДЕЛЕМБОВСЬКИЙ

Підпис к.т.н., доц. Делембовського М.М. засвідчую:
Секретар Вчений ради Київського національного університету
будівництва і архітектури

« 12 » 06 2026 р



Микола КЛИМЕНКО