

РЕЦЕНЗІЯ

доктора економічних наук, професора,
завідувача кафедри управління кібербезпекою та захистом інформації
Навчально-наукового інституту кібербезпеки та захисту інформації
Державного університету інформаційно-комунікаційних технологій

ЛЕГОМІНОВОЇ Світлани Володимирівни

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.

Актуальність теми

Розвиток критичної інформаційної інфраструктури організацій супроводжується зростанням обсягів мережевого трафіку, ускладненням технологічних стеків та підвищенням рівня вимог до безперервності функціонування. У таких умовах ключовою проблемою стає своєчасне та точне виявлення шкідливої активності, яка може призвести до порушення конфіденційності, цілісності та доступності оброблюваних даних.

Традиційні сигнатурні системи виявлення вторгнень не здатні ефективно протидіяти новим типам атак, а окремі класифікатори на основі машинного навчання мають обмежену узагальнюючу здатність. Запропонована в дисертаційній роботі орієнтація на гібридну класифікацію з використанням стекінг-ансамблю різнорідних алгоритмів є логічною та обґрунтованою відповіддю на зазначені виклики. Актуальність роботи підсилюється тим, що для систем, які працюють в режимі реального часу, критичним є не лише точність виявлення, а й мінімізація часу прийняття рішення, що також є предметом дослідження.

Обрана тема є актуальною, своєчасною та відповідає науково-практичним потребам у галузі кібербезпеки. Результати роботи мають теоретичну цінність і практичне значення для вдосконалення систем виявлення вторгнень та підвищення рівня захисту інформаційних систем від сучасних кіберзагроз.

Обґрунтованість наукових результатів, висновків та рекомендацій

Одержані в процесі наукового дослідження результати є достовірними й теоретично обґрунтованими. Об'єкт, предмет та мета роботи логічно пов'язані та чітко окреслюють коло дослідження. Наукові результати викладено послідовно, логічно, що свідчить про застосування системного підходу до вирішення поставленого завдання. Достовірність і обґрунтованість розробленого методу підтверджено результатами проведених експериментів.

Автор опрацьовує повний технологічний ланцюг: від збирання та підготовки даних до навчання ансамблевої моделі, її оптимізації та практичного застосування.

Достовірність наукових положень, висновків і рекомендацій забезпечується узгодженістю теоретичних положень із результатами масштабного обчислювального експерименту. Порівняльний аналіз базових класифікаторів та гібридних стекінгових моделей (у таблицях 3.1–3.4) є методологічно коректним та переконливо демонструє переваги запропонованого підходу. Застосування методів Парето-оптимізації та стратегії *above-average rule* для відбору оптимальної конфігурації є статистично обґрунтованим підходом.

Оцінюючи в цілому викладення матеріалу в роботі, слід відзначити завершену цілісну структуру дисертації, яка надала автору можливість здійснити комплексне дослідження методів виявлення шкідливої активності в інформаційній системі організації на основі гібридної класифікації.

Новизна наукових результатів дослідження

До найбільш суттєвих результатів, що визначають наукову новизну дисертаційного дослідження, слід віднести:

Вперше розроблено метод виявлення шкідливої активності в інформаційній системі організації на основі гібридної класифікації, який базується на використанні гетерогенного набору базових класифікаторів та метакласифікаторі 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.

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.

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.

Отже, зазначені наукові результати формують новий підхід до побудови систем виявлення шкідливої активності, який забезпечує практично значущий баланс між точністю виявлення та вимогами до обчислювальних ресурсів.

Практична цінність отриманих результатів

Основні наукові положення дисертаційної роботи доведено до рівня методичних розробок і практичних рекомендацій, що у своїй єдності можуть покращити процес виявлення шкідливої активності в інформаційних системах організацій.

По-перше, розроблена п'ятимодульна архітектура програмного рішення є функціонально завершеним продуктом, придатним для безпосередньої інтеграції у корпоративні SOC через стандартизовані інтерфейси (REST API, Syslog, CEF).

По-друге, досягнутий час прогнозування 7,16 мс задовольняє вимоги систем виявлення вторгнень в режимі реального часу.

Важливим практичним аспектом є запропонована методика поетапного впровадження системи: від пасивного режиму моніторингу (shadow mode) до активного блокування підозрілого трафіку, що мінімізує ризики помилкового блокування легітимного трафіку на початковому етапі.

Отримані науково-методичні результати дисертаційної роботи використані у практичній діяльності ТОВ “Євротелеком” та ТОВ “APBIOM”, що підтверджує практичну придатність розробленого методу.

Зв'язок роботи з науковими програмами, планами та темами

Тема дисертаційної роботи узгоджується з напрямками науково-технічних досліджень у галузі кібербезпеки та захисту інформаційних систем а також з державними стратегіями і програмами з підвищення кіберстійкості об'єктів критичної інфраструктури. Тема відповідає пріоритетним науковим напрямкам та стандартам ISO/IEC 27001 і NIST Cybersecurity Framework. Дисертаційна робота виконувалась за планами наукової та науково-технічної діяльності ДУІКТ і в межах тематичних НДР кафедри, пов'язаних із виявлення шкідливої активності в інформаційних системах організацій: “Методологія виявлення шкідливих процесів в інформаційних системах” (№ 0121U113613, м. Київ) та “Розробка науково-методичних рекомендацій виявлення шкідливих процесів в інформаційній системі організації” (ТОВ “АЛЬФА-МЕТАЛ”, м. Київ).

Повнота викладу основних результатів дисертації у публікаціях

Основні положення та результати дисертаційного дослідження відображені у 9 наукових працях, серед яких одна стаття опублікована у науковому виданні, що індексується в міжнародній наукометричній базі Scopus, три статті у наукових фахових виданнях України категорії “Б”, дві статті в інших наукових періодичних виданнях та три праці апробаційного характеру за матеріалами міжнародної наукової та науково-практичних конференціях. Тематика публікацій охоплює усі ключові результати роботи: гібридний метод класифікації, оптимізацію датасету, підхід з опорними векторами та виявлення аномалій поведінки. Рівень апробації є достатнім.

Оцінка змісту дисертації та відповідність встановленим вимогам щодо оформлення

Зміст дисертаційної роботи виконаний у логічному зв'язку та послідовності, є цілісним завершеним науковим дослідженням, повністю відповідає означеній темі. Актуальність теми, наукова новизна отриманих результатів і висновки, її практичне значення є доведеними і не викликають сумніву.

Чотири основні розділи послідовно розкривають аналітичний, теоретичний, експериментальний та практичний виміри дослідження. Матеріал викладено у науковому стилі з достатнім рівнем деталізації та аргументації.

Обсяг, структура і стилістичне оформлення дисертації відповідає вимогам МОН України: витримано структуру кваліфікаційної наукової праці, наведено необхідні ілюстративні матеріали, таблиці, перелік публікацій та додатки. Посилання на джерела оформлено коректно.

Недоліки та зауваження

Поряд із позитивною оцінкою, до дисертаційної роботи можна висловити окремі зауваження рекомендаційного характеру:

1) доцільно навести більш детальний аналіз часових характеристик окремих етапів обробки (час нормалізації, час PCA-трансформації, час кожного базового класифікатора та мета-класифікатора окремо), що підвищить відтворюваність результатів та дозволить ідентифікувати вузькі місця у послідовності етапів;

2) бажано розширити обговорення стійкості запропонованого методу до дисбалансу між типами атак у датасеті CSE-CIC-IDS2018 – зокрема, навести аналіз метрик precision та recall окремо для кожного класу атак;

3) у четвертому розділі варто доповнити рекомендації щодо безпеки зберігання та передачі навчальних даних і параметрів моделі, що є важливим аспектом при розгортанні систем кібербезпеки у корпоративних середовищах;

4) бажано приділити увагу у подальших дослідженнях застосуванню методів онлайн-навчання для безперервного оновлення та адаптації моделі до еволюції кіберзагроз без необхідності повного перенавчання.

Втім, наведенні зауваження та дискусійні положення не знижують загальнонаукової та практичної цінності дисертаційної роботи і не впливають на її в цілому позитивну оцінку та можуть бути враховані автором у подальшій роботі.

Висновок

Дисертаційна робота ГАМЗИ Дмитра Євгенійовича на тему “Методи виявлення шкідливої активності в інформаційній системі організації на основі гібридної класифікації” є актуальним, завершеним самостійним науковим дослідженням, що містить науково обґрунтовані результати, які характеризуються елементами наукової новизни та практичною значущістю для галузі кібербезпеки.

Сформульована в дисертації мета досягнута і вирішене важливе наукове завдання щодо розроблення методів виявлення шкідливої активності в інформаційній системі організації на основі гібридної класифікації, яке має важливе значення для теорії та практики захисту інформаційних систем від кібератак, спрямованих на порушення конфіденційності, цілісності та доступності інформації. Відсутність аналогічних рішень робить результати дослідження пріоритетними. Дисертація відповідає спеціальності 125 Кібербезпека і чинним вимогам "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 січня 2022 року № 44, а її автор – ГАМЗА Дмитро Євгенійович, заслуговує на присудження ступеня доктора філософії за спеціальністю 125 Кібербезпека.

Рецензент:

завідувач кафедри управління
кібербезпекою та захистом інформації
доктор економічних наук, професор

Світлана ЛЕГОМІНОВА

"09" червне 2026 р.

Підпис доктора економічних наук, професора С. Легомінової засвідчую.

Учений секретар
Державного університету інформаційно-
комунікаційних технологій



Галина ЄНЧЕВА