

РЕЦЕНЗІЯ

рецензента

доктора технічних наук, професора,

директора

Навчально-наукового інституту кібербезпеки та захисту інформації
Державного університету інформаційно-комунікаційних технологій

ІВАНЧЕНКО Євгенії Вікторівни

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

Проблема своєчасного та ефективного виявлення шкідливої активності в інформаційних системах організацій є однією з ключових проблем у сучасній кібербезпеці. Зростання обсягів мережевого трафіку, ускладнення архітектур атак та широке застосування методів обходу традиційних систем захисту показує на те, що організації перебувають під постійним тиском з боку кіберзагроз, що стрімко еволюціонують у кількісному та якісному відношенні. Зростаюча складність кібератак, активне застосування зловмисниками методів обходу традиційних засобів захисту (поліморфний та метаморфний шкідливий код, атаки нульового дня, цілеспрямовані тривалі атаки типу АРТ) зумовлюють нагальну необхідність розробки нових адаптивних методів виявлення шкідливої активності, здатних функціонувати в режимі реального часу.

Важливим стимулом для проведення представленого дисертаційного дослідження є задокументоване протиріччя між зростаючою гетерогенністю

мережевого трафіку та обмеженою узагальнюючою здатністю існуючих моно-класифікаторів на основі машинного навчання. Зокрема, сигнатурні підходи є принципово нездатними виявляти раніше невідомі атаки, аномальні методи страждають від надмірної кількості хибних спрацювань, а поодинокі ML-класифікатори, згідно з теоремою «про відсутність безкоштовних обідів» Д. Волперта, не забезпечують оптимальних результатів на всіх класах задач.

Запропонований у дисертаційній роботі підхід до побудови гібридної системи виявлення шкідливої активності на основі стекінг-ансамблю різнорідних алгоритмів машинного навчання є методологічно виваженим та актуальним. Обрана тема відповідає вимогам часу і пріоритетним напрямкам розвитку науки і техніки в Україні у сфері інформаційних технологій та кібербезпеки, а також узгоджується зі Стратегією кібербезпеки України та міжнародними стандартами ISO/IEC 27001 і NIST Cybersecurity Framework.

Обґрунтованість наукових результатів, висновків та рекомендацій

Наукові результати дисертаційної роботи мають належний рівень обґрунтованості. Дисертант демонструє глибоке розуміння предметної галузі та коректно застосовує математичний апарат для формалізації задачі виявлення шкідливої активності. Обґрунтованість результатів забезпечується поетапним підходом до дослідження: від аналізу існуючих методів до розробки нового методу, його верифікації на стандартизованому датасеті та практичного впровадження.

Вибір CSE-CIC-IDS2018 як тестового датасету є аргументованим – цей набір даних містить актуальний ландшафт кіберзагроз та є загальновизнаним бенчмарком у наукових дослідженнях з виявлення вторгнень. Досягнуті метрики якості (Accuracy 98,07%, F1-score 96,57%) свідчать про ефективність розробленого підходу. Висновки дисертаційної роботи є логічними та відповідають представленим науковим результатам.

Новизна наукових результатів дослідження

Дисертаційне дослідження містить результати, що характеризуються науковою новизною. Зокрема, до вагомих наукових здобутків 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 метакласифікаторі на основі XGBoost для дворівневої стекінг-архітектури, що дає можливість застосовувати різні 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.

Практична цінність отриманих результатів

Практична цінність дисертаційної роботи полягає у розробці повністю готового до впровадження програмного рішення з п'ятимодульною архітектурою. Важливим є те, що автор не лише досягнув теоретичних результатів, а й довів їх до рівня практичної реалізації з конкретними рекомендаціями щодо розгортання, налаштування та підтримки системи.

Використання сучасного технологічного стеку (Python, scikit-learn, XGBoost, LightGBM, CatBoost, Docker/Kubernetes) забезпечує практичну реалізованість розробленого підходу. Час прогнозування 7,16 мс на один мережевий потік відповідає вимогам систем виявлення вторгнень в режимі реального часу та задовольняє потреби сучасних корпоративних мереж.

Впровадження результатів у навчальний процес ДУІКТ та в діяльність реальних підприємств підтверджує практичну значущість отриманих результатів.

Зв'язок роботи з науковими програмами, планами та темами

Дисертаційна робота виконана в межах науково-дослідних робіт кафедри систем та технологій кібербезпеки ДУІКТ. Тематика дослідження відповідає сучасним пріоритетам розвитку кібербезпеки та узгоджується з вимогами Стратегії кібербезпеки України та міжнародних стандартів у сфері захисту інформаційних систем.

Повнота викладу основних результатів дисертації у публікаціях

Основні результати дисертаційного дослідження відображені у 9 наукових працях, серед яких 3 опубліковані у спеціалізованих фахових виданнях, затверджених наказом МОН України, 1 опубліковано у закордонному науковому виданні, що індексується в Scopus. За матеріалами виступів на науково-технічних конференціях опубліковано 3 тези доповідей. Публікації охоплюють усі ключові аспекти роботи: гібридний метод класифікації, оптимізацію датасету, метод виявлення на основі опорних векторів та методику виявлення аномалій поведінки користувачів. Рівень апробації є достатнім.

Оцінка змісту дисертації та відповідність встановленим вимогам щодо оформлення

Дисертація є цілісним завершеним науковим дослідженням. Структура роботи є логічною та відповідає загальноприйнятим вимогам. Виклад

матеріалу ведеться у науковому стилі, ілюстративні матеріали (рисунки, таблиці) наочно відображають отримані результати та сприяють кращому розумінню запропонованих підходів.

Оформлення дисертаційної роботи відповідає встановленим вимогам до кваліфікаційних наукових праць на здобуття ступеня доктора філософії. Посилання на літературу оформлено коректно.

Недоліки та зауваження

Загалом позитивно оцінюючи наукове та практичне значення дисертаційної роботи, слід вказати на окремі зауваження рекомендаційного характеру:

1) у другому розділі доцільно більш детально обґрунтувати підхід до формування вектора мета-ознак при стекінгу – зокрема, розглянути альтернативу використання ймовірностей класів проти прогнозованих міток для навчання мета-класифікатора;

2) бажано включити до порівняльного аналізу в третьому розділі результати застосування глибоких нейронних мереж (DNN/LSTM) на тому ж датасеті, оскільки вони є прямими конкурентами запропонованого підходу;

3) доцільно навести аналіз важливості ознак після PCA-трансформації (наприклад, через SHAP-значення для компонент) для кращого розуміння інформативності головних компонент у контексті виявлення конкретних типів атак;

4) у четвертому розділі варто деталізувати рекомендований сценарій оновлення моделі при виявленні концептуального дрейфу, включаючи пропоновані статистичні тести та порогові значення для ініціювання перенавчання.

Наведені зауваження не знижують загальної позитивної оцінки та можуть бути враховані в подальших дослідженнях.

Висновок

Дисертаційна робота ГАМЗИ Дмитра Євгенійовича на тему «Методи виявлення шкідливої активності в інформаційній системі організації на основі гібридної класифікації» є завершеним самостійним дослідженням, що містить науково обґрунтовані результати, які мають теоретичне та практичне значення для підвищення ефективності захисту інформаційних систем організацій.

За рівнем наукової новизни, обґрунтованістю висновків, практичною цінністю та відповідністю оформлення 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».

Рецензент:

Директор Навчально-наукового

інституту кібербезпеки та захисту інформації,

доктор технічних наук, професор

 Євгенія ІВАНЧЕНКО

Підпис доктора технічних наук, професора Є. Іванченко засвідчую.

Учений секретар

Державного університету інформаційно-

комунікаційних технологій

«09» червня 2026 р.



Галина ЄНЧЕВА