

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

СОБЧУКА Валентина Володимировича

доктора технічних наук, професора,
професора кафедри інтегральних та диференціальних рівнянь
механіко-математичного факультету
Київського національного університету імені Тараса Шевченка
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

Сучасна парадигма розвитку глобального інформаційного простору визначається перманентною інтенсифікацією, децентралізацією та ускладненням архітектури кіберзагроз, спрямованих на корпоративні й державні інформаційно-телекомунікаційні системи. Аналіз релевантних аналітичних звітів провідних інституцій у сфері кібербезпеки свідчить про системне зниження ефективності традиційних сигнатурних та евристичних інструментів захисту (класу IDS/IPS, SIEM) в умовах протидії раніше невідомим деструктивним впливам (атакам типу Zero-day) та комплексним багатоетапним цілеспрямованим загрозам (APT-атакам).

Інтеграція ізольованих мономоделей машинного навчання у контур безпеки часто призводить до виникнення внутрішнього системного протиріччя між детекційною точністю класифікатора та часовою

латентністю його функціонування у високонавантажених мережових середовищах. Крім того, застосування таких підходів нерідко супроводжується деструктивно високим рівнем хибнопозитивних спрацювань.

З огляду на це, науковий пошук, орієнтований на розробку засобів гібридизації гетерогенних ансамблевих архітектур машинного навчання, які здатні забезпечувати операційне детектування атак у режимі реального часу за умови мінімізації обчислювальної складності й ресурсних витрат, є вагомим та актуальним завданням для сучасної галузі кібербезпеки.

Рецензована дисертаційна робота безпосередньо спрямована на вирішення цієї значущої науково-прикладної задачі – створення ефективних методів ідентифікації шкідливої активності в інформаційному контурі організацій. Масштабування кіберінцидентів, безперервна еволюція тактик, технік та процедур (TTPs) злоумисників, а також обмеженість класичних засобів захисту щодо виявлення нетипових аномалій обґрунтовують необхідність модернізації підходів до класифікації мережевого трафіку.

Вибір теми дослідження повністю корелює із сучасними векторами розвитку систем виявлення та запобігання вторгненням. Здобувачем науково ідентифіковано та формалізовано ключові протиріччя предметної області, а саме: компроміс між повнотою детектування та швидкістю ухвалення рішень у реальному часі, а також між генеративною здатністю моделі до узагальнення та її робастністю щодо мінімізації помилок першого роду. Окреслена предметна область характеризується високим ступенем затребуваності як у теоретико-методологічному, так і в безпосередньо прагматичному вимірах.

Обґрунтованість наукових результатів, висновків та рекомендацій

Ступінь обґрунтованості наукових положень, сформульованих у дисертаційному дослідженні, повною мірою відповідає критеріям, що висуваються до кваліфікаційних праць на здобуття наукового ступеня доктора філософії. Автор продемонстрував послідовну та системну дедуктивну архітектуру викладу матеріалу: від теоретико-множинного

обґрунтування вибору конкретного базису методів машинного навчання до етапу інженерної реалізації та емпіричної верифікації на релевантних масивах даних.

Математична формалізація процесу розпізнавання деструктивних інформаційних впливів у вигляді задачі багатокритеріальної оптимізації є коректною. Такий підхід дозволив аналітично визначити цільові функції, сформулювати систему просторових і часових обмежень, а також забезпечити збіжність обчислювальних процедур функціонування системи захисту.

Використання еталонного датасету CSE-CIC-IDS2018 для експериментальної перевірки є обґрунтованим вибором, оскільки цей набір даних широко застосовується у дослідженнях систем виявлення вторгнень. Запропонований багатокритеріальний підхід до відбору оптимальних конфігурацій моделей з використанням фронту Парето та стратегії above-average rule є методологічно коректним і забезпечує об'єктивний вибір найкращої архітектури. Висновки дисертаційної роботи є обґрунтованими та логічно впливають із представлених результатів.

Новизна наукових результатів дослідження

Дисертаційна робота містить результати, що характеризуються науковою новизною та є вагомим внеском у розвиток методів виявлення шкідливої активності. До основних наукових результатів слід віднести такі:

- 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.

Практична цінність отриманих результатів

Практична значущість отриманих дисертантом результатів має чітко виражений прикладний характер і підтверджується актами про реальне впровадження розроблених рішень у діяльність підприємств та організацій. Спроектована п'яти модульна архітектура програмного комплексу є функціонально завершеним програмним рішенням, що адаптоване для інтеграції в існуючі корпоративні системи моніторингу та управління подіями інформаційної безпеки (SIEM/IDS).

Особливо цінним є те, що за результатами моделювання, таке програмне рішення, дозволяє забезпечити приріст точності на 3,87 % та F1-score на 5,11 %, а також скоротити найменший час прогнозування на 76 %, порівняно з відповідними результатами на необробленому датасеті щодо виявлення шкідливої активності в інформаційній системі організації на основі гібридної класифікації. При здійсненні багатокритеріального відбору оптимальних архітектур із використанням стратегії фільтрації за середніми значеннями та побудови фронту Парето 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.

Результати дослідження впроваджено в навчальний процес Державного університету інформаційно-комунікаційних технологій та в діяльність підприємств реального сектору (ТОВ «Євротелеком» та ТОВ «АРВІОМ»), що свідчить про практичну значущість розробленого методу.

Зв'язок роботи з науковими програмами, планами та темами

Дисертаційне дослідження виконане в межах науково-дослідних робіт кафедри систем та технологій кібербезпеки Державного університету інформаційно-комунікаційних технологій, що підтверджує його зв'язок із науковими програмами університету. Тематика роботи узгоджується з пріоритетними напрямками розвитку науки і техніки України у сфері інформаційних технологій та кібербезпеки.

Повнота викладу основних результатів дисертації у публікаціях

Матеріали дисертаційного дослідження пройшли належну апробацію та висвітлення у науковій періодиці. За темою роботи опубліковано 3 статті у провідних фахових виданнях категорії „Б“, одна з яких одноособова та 1 статтю у міжнародному виданні, що входить до наукометричної бази Scopus. Крім того, ключові аспекти дослідження було представлено та обговорено на 3 міжнародних і вітчизняних конференціях, що засвідчує високий рівень публікаційної активності здобувача та репрезентативність апробації його наукових здобутків.

Оцінка змісту дисертації та відповідність встановленим вимогам щодо оформлення

Рецензована дисертація за своєю архітектонікою є завершеною, цілісною науковою працею, що характеризується суворою внутрішньою логікою, послідовністю викладу та чітко структурованим змістом.

У вступній частині роботи наведено вичерпне наукове обґрунтування актуальності обраного напрямку досліджень, коректно та взаємопов'язано дефіновано мету, завдання, об'єкт, предмет, а також методологічну базу наукового пошуку.

Композиційно дисертаційне дослідження складається з чотирьох логічно пов'язаних розділів, які послідовно розкривають архітектуру вирішення поставленої науково-прикладної задачі.

Перший розділ присвячено системному аналітичному огляду сучасного стану кіберзагроз та критичному оцінюванню існуючих засобів захисту. Другий розділ містить теоретико-методологічне обґрунтування та математичну формалізацію запропонованого гібридного методу

класифікації. Третій розділ відображає архітектуру та результати комп'ютерного моделювання й експериментальної верифікації моделей. Четвертий розділ розкриває практичні аспекти інженерної реалізації розробленого програмного комплексу та оцінювання його експлуатаційної ефективності.

Загальні висновки роботи є інформативними, концептуальними й повною мірою відображають сукупність отриманих автором наукових результатів. Зміст дисертаційного дослідження, характер вирішуваних завдань та отримані наукові положення повністю корелюють із сутнісним наповненням паспорта спеціальності 125 «Кібербезпека».

Текстове, графічне та технічне оформлення дисертаційної роботи відповідає чинним державним стандартам та нормативним вимогам, що висуваються до кваліфікаційних наукових праць на здобуття наукового ступеня доктора філософії.

Недоліки та зауваження

Попри загальну високу якість, безперечну теоретичну та практичну цінність рецензованого дослідження, з метою підвищення його наукової та методичної значущості доцільно висловити такі зауваження й рекомендації:

- 1) У другому розділі, присвяченому математичній формалізації та побудові компонентів системи захисту, автору варто було б надати більш глибоке теоретичне обґрунтування вибору конкретної функції ядра (*kernel function*) для алгоритму опорних векторів (SVM) у складі первинного пулу базових класифікаторів. Роботу суттєво збагатив би порівняльний аналіз операційної ефективності та детекційної точності системи при використанні різних типів ядер (лінійного, поліноміального, радіально-базисного) на досліджуваному масиві даних.
- 2) Досліджуючи процедури попередньої обробки даних, здобувач детально описує механізм балансування класів. Водночас у тексті дисертації бажано було б розширити аналіз чутливості та оцінити вплив варіативності параметра k (кількості найближчих сусідів) в алгоритмі *SMOTE* на якість генерації синтетичних зразків та, як

наслідок, на фінальні метрики робастності всього гібридного ансамблю.

- 3) Для більш глибокого розуміння специфіки функціонування розроблених моделей аналітичний складник роботи доцільно було б доповнити детальним експліцитним аналізом матриць плутанини (*confusion matrix*) у розрізі кожної окремої категорії атак, представлених в еталонному датасеті CSE-CIC-IDS2018. Це дозволило б чітко ідентифікувати специфічні класи деструктивних впливів, для яких запропонований стекінг-метод демонструє гранично низьку або, навпаки, максимальну селективну здатність.
- 4) Перспективним напрямом подальшого розвитку представленого авторами підходу є дослідження можливостей його адаптації та масштабування для аналізу аномалій у зашифрованому мережевому трафіку без його попередньої дешифрування, що є критично актуальним завданням в умовах повсюдного домінування сучасних криптографічних протоколів (зокрема, TLS 1.3).
- 5) При аналізі математичного апарату, наведеного у другому розділі дисертації, виявлено певні методологічні неточності у використанні математичної символіки. Зокрема, у деяких формулах не зовсім вдало обрано індексацію, оператори підсумовування та межі сумування. Вказане зауваження, зважаючи на те, що дисертація виконана за технічною спеціальністю 125 «Кібербезпека», а не за фізико-математичним профілем, є некритичним, має характер технічного недогляду і не спотворює сутнісний зміст запропонованих моделей.

Висловлені зауваження та побажання мають переважно дискусійний або рекомендаційний характер, покликані окреслити вектори для подальших наукових пошуків здобувача і жодним чином не знижують загальну високу позитивну оцінку теоретичних, методичних та прикладних результатів дисертаційного дослідження.

Висновок

Дисертаційна робота Гамзи Дмитра Євгенійовича відповідає чинним вимогам, які встановлені у «Порядку підготовки здобувачів

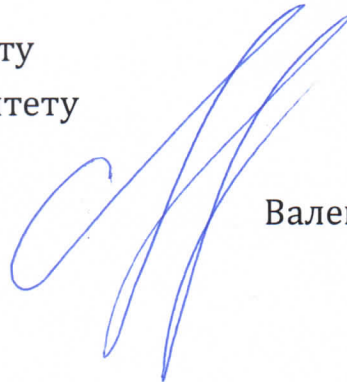
вищої освіти ступеня доктора філософії та доктора наук у закладах вищої освіти (наукових установах)», затвердженого постановою Кабінету Міністрів України від 19 травня 2023 року № 502, та «Порядку підготовки здобувачів вищої освіти ступеня доктора філософії та доктора наук у закладах вищої освіти (наукових установах)», що затверджений постановою Кабінету Міністрів України від 12 січня 2022 р. № 44 (зі змінами від 08 квітня 2025 року № 426).

Дисертаційна робота Гамзи Дмитра Євгенійовича на тему «Методи виявлення шкідливої активності в інформаційній системі організації на основі гібридної класифікації» є самостійним завершеним науковим дослідженням, результати якого мають наукову новизну та практичну значущість для розвитку методів кібербезпеки.

За змістом, рівнем наукової новизни, обґрунтованістю висновків і практичною цінністю отриманих результатів 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:

професор кафедри інтегральних
та диференціальних рівнянь,
механіко-математичного факультету
Київського національного університету
імені Тараса Шевченка,
доктор технічних наук, професор



Валентин СОБЧУК

«10» червня 2026 р.



проф. В. Собчук
завіряю
О. Милинко