Голові разової спеціалізованої
вченої ради PhD 17109
Хмельницького національного
університету
доктору технічних наук,
професору Сергію ЛИСЕНКУ
29016, м. Хмельницький,
вул. Інститутська, 11

ВІДГУК ОФІЦІЙНОГО ОПОНЕНТА

на дисертаційну роботу Семенюка Богдана Васильовича
на тему «Моделі та методи виявлення комп'ютерних атак в корпоративних мережах на основі частотно-часового представлення мережного трафіку», подану на здобуття ступеня доктора філософії з галузі знань 12 Інформаційні технології за спеціальністю 122 Комп'ютерні науки

1. Актуальність теми дисертаційної роботи

Розвиток корпоративної IT-інфраструктури супроводжується одночасним ускладненням мережної взаємодії та розширенням поверхні атаки. У практичних умовах засоби моніторингу мають працювати з неоднорідним трафіком, значною кількістю легітимних з'єднань і порівняно малою часткою небезпечних подій. За таких обставин особливої ваги набувають методи, здатні виділяти слабко виражені ознаки атак і зберігати якість розпізнавання для рідкісних класів.

Дисертаційна робота Семенюка Б.В. розглядає цю задачу через нетрадиційне подання мережних характеристик у вигляді сигналу. Перехід до частотно-часової області створює можливість використовувати інструментарій цифрової обробки сигналів та двовимірних нейронних мереж для пошуку закономірностей, які у вихідному векторному просторі можуть бути недостатньо вираженими.

Суттєвою перевагою постановки задачі є те, що автор не обмежується побудовою базового класифікатора. У роботі послідовно розглянуто проблему дисбалансу навчальних даних, аналіз помилок базової моделі та окреме уточнення рішень у зоні невизначеності. Така побудова відповідає практичній логіці сучасних систем виявлення атак, де важливими є не лише середні метрики, а й контроль складних та потенційно небезпечних випадків.

Тому тематика дослідження є своєчасною для засобів забезпечення кібербезпеки корпоративних мереж, а запропонований напрям відповідає предметній області спеціальності 122 «Комп'ютерні науки» та сучасним задачам інтелектуального аналізу мережних даних.

2. Зв'язок роботи з науковими програмами, планами, темами

Дослідження виконувалося в межах наукової тематики Хмельницького національного університету. Зокрема, результати пов'язані з держбюджетною

темою «Система забезпечення стійкості до витоку конфіденційної інформації в корпоративних мережах в умовах впливів комп'ютерних атак» (номер державної реєстрації 0126U002082), до виконання якої здобувач був залучений як виконавець. Тематика дисертації логічно доповнює зазначений напрям досліджень засобами інтелектуального виявлення мережних атак.

3. Оцінка обґрунтованості наукових результатів дисертації, їх достовірності та новизни

Наукові результати одержано на основі поєднання методів аналізу мережного трафіку, цифрової обробки сигналів, машинного та глибинного навчання, а також статистичного оцінювання якості класифікації. Запропоновані рішення перевіряються послідовно: від формування частотно-часового подання до балансування навчальної вибірки та каскадного уточнення складних прогнозів.

До основних результатів, що визначають наукову новизну роботи, належать:

1) вперше розроблено модель процесу виявлення комп'ютерних атак на основі соніфікації мережного трафіку, яка інтегрує звукове перетворення багатовимірного простору ознак, спектральний аналіз, адаптивне балансування навчальної вибірки та каскадний механізм прийняття рішень;

2) розроблено новий метод частотно-часового перетворення мережного трафіку, що передбачає інтерпретацію багатовимірного простору параметрів з'єднання як параметрів сигналу з лінійним частотно-амплітудним відображенням і подальшим спектральним аналізом для формування структурованого 2D-подання;

3) розроблено новий метод сигнатурозбережного адаптивного балансування навчальної вибірки, який зберігає структурні характеристики міноритарного класу та враховує помилки базової моделі під час формування розширеної навчальної множини;

4) розроблено новий метод підвищення точності виявлення атак у зоні невизначеності прогнозу, що формалізує τ-інтервал невизначеності та використовує допоміжну модель для селективного перевизначення помилкових рішень базового класифікатора.

Достовірність висновків підтверджується експериментальним порівнянням кількох варіантів моделі, використанням окремих навчальної, валідаційної та тестової множин, аналізом помилкових рішень і дослідженням поведінки системи в зоні невизначеності. Важливо, що додаткова модель застосовується вибірково, а не замінює базовий класифікатор на всьому просторі даних.

4. Оцінка змісту дисертації, її завершеність та дотримання принципів академічної доброчесності

За структурою дисертація включає анотацію, зміст, перелік скорочень, вступ, чотири змістові розділи, висновки, список використаних джерел і п'ять додатків. Загальний обсяг становить 222 сторінки, основний текст — 167

сторінок з таблицями та рисунками; бібліографія налічує 133 найменування. Ілюстративний матеріал представлено 41 рисунком і 20 таблицями.

Логіка дисертації побудована від аналізу проблеми до експериментального підтвердження запропонованих рішень. У вступній частині визначено науково-прикладну задачу, мету, об'єкт і предмет дослідження, сформульовано завдання та положення наукової новизни.

Перший розділ формує теоретичне підґрунтя роботи: розглянуто підходи до виявлення вторгнень, особливості інтелектуальної класифікації мережних подій та проблеми, пов'язані з рідкісними класами і неоднорідністю даних. Також в цьому розділі здійснено постановку задачі дослідження.

У другому розділі автор переходить до власного способу представлення мережних ознак. Описано їх перетворення у хвильову форму, отримання спектральних образів і використання 2D-CNN для класифікації сформованих частотно-часових представлень.

Третій розділ присвячено підвищенню стійкості навчання до дисбалансу та роботі зі складними прогнозами. В ньому подано сигнатурозбережне адаптивне балансування, аналіз помилок базової моделі та механізм селективного перевизначення рішень.

Четвертий розділ містить програмну реалізацію й експериментальну перевірку складових підходу. Результати дають можливість окремо оцінити базову соніфікаційну модель, ефект SPAS та внесок каскадного уточнення, що підвищує прозорість експериментальної частини.

За матеріалами перевірки академічної доброчесності запозичені положення та результати інших авторів супроводжуються належними бібліографічними посиланнями. Структура роботи є завершеною, а висновки розділів узгоджуються з поставленими завданнями.

5. Практичне значення одержаних результатів

Практична цінність роботи полягає у сформованому програмно-алгоритмічному конвеєрі, який можна використати як основу модуля інтелектуального аналізу мережних подій. Конвеєр включає підготовку ознак, соніфікацію, STFT, класифікацію спектрограм, адаптивне балансування та окреме опрацювання невпевнених прогнозів.

Запропонована архітектура дозволяє розглядати окремі етапи незалежно та, за потреби, замінювати або перенавчати їх без перебудови всього рішення. Це створює передумови для подальшої інтеграції підходу до систем моніторингу корпоративних мереж.

Прикладну спрямованість результатів підтверджують матеріали впровадження у ТОВ «ІТТ», ПП «Авіві» та освітньому процесі Хмельницького національного університету.

6. Мова та стиль викладення результатів

Робота написана українською мовою з дотриманням наукового стилю. Формули, алгоритмічні етапи, таблиці та графічні матеріали використовуються для пояснення запропонованих методів, а основні терміни застосовано послідовно. Загальна структура тексту дає змогу простежити зв'язок між

поставленою задачею, розробленими методами та одержаними експериментальними результатами.

7. Оприлюднення основних наукових результатів дисертаційної роботи

Результати дисертаційного дослідження відображено у п'яти наукових статтях. Окрему частину апробації становить публікація у матеріалах міжнародної конференції, що індексується у Scopus. Результати роботи також представлялися на конференціях IntelITSIS-2025, DeSSerT-2025 та ACIT-2026. Крім публікаційної апробації, результати програмної реалізації подано одним авторським свідоцтвом про реєстрацію права на комп'ютерні програми.

Наукові публікації автора повністю відповідають темі дисертації та підкріплюють її результати. Отже, зміст дисертації та її основні результати пройшли належну апробацію та повною мірою відображені в опублікованих працях автора.

8. Недоліки та зауваження до дисертаційної роботи

1. У дисертації продемонстровано переваги запропонованого підходу на контрольованому експериментальному наборі даних. Для практичного використання в корпоративній мережі доцільно було б чіткіше сформулювати модель потенційного зловмисника, зокрема, його можливості щодо зміни мережних ознак, маскування активності або формування аномального трафіку в контексті того, які з них враховуються, а які виходять за межі дослідження.

2. Перехід від первинного мережного потоку до фіксованого вектору ознак є важливою частиною прикладного контуру, але в роботі основний акцент зроблено вже на сформованих ознаках. Доцільно було б детальніше описати вимоги до flow-агрегації, часових вікон та обробки неповних записів, щоб однозначно відтворити вхідний тракт у реальній системі моніторингу.

3. Для каскадного механізму критичною є якість оцінки невизначеності базового класифікатора. Було б корисно окремо показати калібрування вихідних імовірностей 2D-CNN та перевірити, як зміна калібрування впливає на розмір τ-зони і частку рішень, що передаються допоміжній моделі.

4. У практичних системах кіберзахисту ціна пропущеної атаки та ціна хибної тривоги істотно відрізняються. Доцільно було б доповнити аналіз сценарієм з ваговою функцією втрат або ризику, де вибір робочої точки класифікатора і меж τ визначається не лише F1-мірою, а й пріоритетом безпеки конкретного середовища.

5. Після розгортання системи статистичні характеристики трафіку та склад атак неминуче змінюються. Варто було б формалізувати критерій, за яким система визначає потребу в оновленні базової чи допоміжної моделі, а також описати безпечний цикл перенавчання, що не допускає деградації якості на раніше відомих класах.

6. Оскільки запропонована система працює з даними, що можуть бути цілеспрямовано спотворені атакуючим, перспективним є окреме дослідження її стійкості до evasion-сценаріїв. Зокрема, доцільно оцінити, які мінімальні зміни

вихідних мережних характеристик здатні істотно змінити спектральний образ і чи зберігає каскадна схема перевагу за таких впливів.

Зазначені зауваження мають дискусійний і рекомендаційний характер та не ставлять під сумнів основні наукові результати дисертації, коректність проведених експериментів і практичну цінність запропонованих рішень.

9. Висновок про дисертаційну роботу

Проведене дослідження є цілісною науковою роботою, у якій поєднано методи обробки сигналів і машинного навчання для розв'язання задачі виявлення комп'ютерних атак. Запропоновані моделі та методи мають наукову новизну, пройшли експериментальну перевірку й отримали програмну реалізацію, а наведені результати достатньо повно характеризують внесок здобувача у розв'язання поставленої науково-прикладної задачі.

Дисертаційна робота за своїм науковим рівнем, практичною цінністю, змістом та оформленням відповідає вимогам Порядку присудження ступеня доктора філософії та скасування рішення разової спеціалізованої вченої ради, затвердженого постановою Кабінету Міністрів України № 44 від 12 січня 2022 року (зі змінами), а Семенюк Богдан Васильович заслуговує на присудження ступеня доктора філософії з галузі знань 12 Інформаційні технології за спеціальністю 122 Комп'ютерні науки.

Офіційний опонент,
кандидат технічних наук, доцент,
доцент кафедри кібербезпеки
Західноукраїнського національного університету _____ Степан ІВАСЬЄВ

Підпис Степан Васьєв
Завіряю: Начальник загального відділу Анна Семен,