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

Сучасні корпоративні мережі характеризуються високою інтенсивністю обміну даними, багаторівневою інфраструктурою, широким використанням хмарних, мобільних та віртуалізованих сервісів. За таких умов збільшується кількість потенційних векторів атак, а традиційні сигнатурні й периметрові механізми не завжди забезпечують належне виявлення нових, модифікованих і малопоширених загроз.

Окремою проблемою для інтелектуальних систем виявлення вторгнень є дисбаланс класів, недостатня представленість рідкісних типів атак та невизначеність рішень класифікатора. Це може призводити до високих агрегованих показників точності за одночасно недостатньої повноти виявлення окремих небезпечних підкласів.

У дисертації запропоновано розглядати мережний трафік не лише як традиційний вектор ознак, а й як сигнал, для якого може бути сформовано частотно-часове представлення. Поєднання соніфікації, спектрального аналізу, двовимірної згорткової нейронної мережі, адаптивного балансування та селективного уточнення рішень утворює логічно завершений напрям дослідження,

спрямований на підвищення точності та збалансованості виявлення комп'ютерних атак.

З огляду на зазначене тема дисертаційної роботи є актуальною, відповідає сучасним задачам кібербезпеки корпоративних мереж та предметній області спеціальності 122 «Комп'ютерні науки».

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

Дисертаційне дослідження виконувалось у рамках науково-дослідної тематики Хмельницького національного університету, зокрема держбюджетної науково-дослідної теми «Система забезпечення стійкості до витоку конфіденційної інформації в корпоративних мережах в умовах впливів комп'ютерних атак» (номер державної реєстрації 0126U002082), в якій здобувач був виконавцем.

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

Наукові положення дисертації сформульовано послідовно і відповідно до поставленої мети. Для розв'язання задач використано методи математичної статистики і теорії ймовірностей, машинного та глибинного навчання, цифрової обробки сигналів, спектрального і частотно-часового аналізу, формування та балансування навчальних вибірок, а також порівняльного експериментального аналізу.

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.

Обґрунтованість результатів забезпечується послідовним переходом від формалізації моделі до експериментальної перевірки її складових. Робота містить кількісне оцінювання метрик якості, порівняння з базовою векторною моделлю та SMOTENC, аналіз помилок і окремий експеримент для каскадної схеми. Така побудова дозволяє простежити внесок кожного етапу у загальний результат.

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

У вступі обґрунтовано актуальність науково-прикладної задачі підвищення точності та збалансованості виявлення комп'ютерних атак, сформульовано мету, об'єкт, предмет, завдання і методи дослідження, визначено наукову новизну та практичне значення.

У першому розділі проаналізовано сучасні системи і методи виявлення вторгнень, сигнатурні, статистичні, поведінкові та інтелектуальні підходи, а також проблеми дисбалансу класів, недостатньої відокремлюваності мережних подій і виявлення рідкісних типів атак.

У другому розділі розроблено модель процесу виявлення комп'ютерних атак на основі частотно-часового представлення мережного трафіку, формалізовано етапи кодування мережних ознак у хвильову форму, побудови спектральних образів та класифікації із застосуванням двовимірної згорткової нейронної мережі.

У третьому розділі представлено метод сигнатурозбережного адаптивного балансування навчальної вибірки та метод підвищення точності у зоні невизначеності прогнозу на основі аналізу помилок базового класифікатора і селективного перевизначення рішень.

У четвертому розділі описано організацію експериментального дослідження та програмну реалізацію, виконано оцінювання базового соніфікаційного підходу, SPAS-балансування і каскадної схеми селективного уточнення рішень. Експериментальна частина підтверджує працездатність запропонованого підходу; для каскадної схеми зафіксовано приблизно одновідсоткове підвищення F1-міри порівняно з базовою соніфікованою моделлю.

Матеріал викладено логічно, структура відповідає поставленим задачам, а висновки узгоджуються зі змістом розділів. За наданими матеріалами перевірки

академічної доброчесності робота є результатом самостійного дослідження здобувача; використані положення інших авторів супроводжуються бібліографічними посиланнями.

5. Практичне значення одержаних результатів

Розроблені моделі та методи утворюють єдиний соніфікаційний конвеєр, який охоплює перетворення мережних ознак у хвильову форму, побудову спектрограм, навчання базового класифікатора, адаптивне балансування навчальної вибірки та селективне перевизначення рішень у τ-зоні невизначеності.

Практичну реалізацію запропонованих підходів виконано програмними засобами, що дає змогу використовувати результати під час створення і модернізації засобів моніторингу безпеки корпоративних мереж.

Результати дослідження впроваджено у ТОВ «ІТТ» (акт від 30.06.2026), ПП «Авіві» (довідка від 29.06.2026) та в освітньому процесі Хмельницького національного університету (акт від 26.06.2026).

6. Мова та стиль викладення результатів

Дисертацію написано українською мовою у науковому стилі. Термінологія загалом використана послідовно, математичні та алгоритмічні положення супроводжуються поясненнями, рисунками і таблицями. Виклад дозволяє простежити логіку від постановки задачі до програмної реалізації та експериментальної перевірки.

7. Оприлюднення основних наукових результатів дисертаційної роботи

Основні наукові результати дисертації опубліковано у 5 наукових статтях. Апробацію результатів засвідчено публікацією однієї праці у матеріалах міжнародної конференції, проіндексованої у Scopus, а також доповідями на міжнародних конференціях IntelITSIS-2025, DeSSerT-2025 та ACIT-2026. Також отримано свідоцтво про реєстрацію авторського права на комп'ютерну програму.

Дисертація складається з анотації, змісту, переліку скорочень, вступу, чотирьох розділів, висновків, списку використаних джерел та п'яти додатків. Повний обсяг становить 222 сторінки, у тому числі 167 сторінок основного тексту; список використаних джерел містить 133 найменувань. Робота містить 41 рисунок і 20 таблиць.

8. Недоліки та зауваження до дисертаційної роботи

1. Запропонований підхід інтерпретує статичний вектор мережних ознак як хвильовий сигнал. Така трансформація є оригінальною, однак доцільно було б формальніше показати, які властивості початкового простору ознак гарантовано зберігаються після частотно-амплітудного відображення і які спектральні компоненти можуть бути штучно породжені самим способом кодування.

2. Порядок компонентів у векторі ознак фактично визначає локальну структуру синтезованого сигналу. Було б корисно виконати експеримент з кількома перестановками або групуванням споріднених ознак і показати, наскільки стабільними залишаються спектрограми та метрики класифікації.

3. Мережний трафік у реальних інформаційно-комунікаційних мережах може мати нестаціонарні, самоподібні та довготривало залежні властивості. Доцільно було б окремо деталізувати те, якою мірою запропоноване штучно сформоване частотно-часове подання відображає ці властивості, а не лише взаємне розташування ознак у фіксованому векторі.

4. Експериментальна схема формує сигнал сталої тривалості з вектора сталої розмірності. Для ширшого застосування методу бажано було б окреслити варіант обробки змінної кількості ознак, пропущених значень або потоків, для яких набір характеристик формується динамічно.

5. У роботі обґрунтовано використання двовимірної ЗНМ для спектрограм. Водночас для практичного аналітика важливо пов'язати активні частотно-часові області назад із вихідними характеристиками мережного з'єднання. Доцільно було б доповнити пояснюваність процедурою зворотного відображення вагомих областей спектрограми на конкретні ознаки трафіку.

6. Результати на NSL-KDD підтверджують працездатність підходу, однак межі перенесення моделі на інші домени потребують додаткового дослідження. Доцільно було б перевірити стабільність на реальних pcap/flow-даних іншої організації або хоча б сформулювати критерії, за яких необхідне повторне навчання через зміну статистичних властивостей трафіку.

Зазначені зауваження мають дискусійний та рекомендаційний характер, істотно не впливають на зміст дисертаційної роботи, не знижують достовірності одержаних результатів, її наукової новизни та практичної цінності.

9. Висновок про дисертаційну роботу

На основі викладеного вважаю, що дисертація Семенюка Богдана Васильовича на тему «Моделі та методи виявлення комп'ютерних атак в

корпоративних мережах на основі частотно-часового представлення мережного трафіку», подана на здобуття ступеня доктора філософії, є завершеною самостійною науковою працею, у якій отримано нові науково обґрунтовані теоретичні та експериментальні результати, що в сукупності розв'язують актуальну науково-прикладну задачу підвищення точності та збалансованості виявлення комп'ютерних атак у корпоративних мережах.

За науковим рівнем, практичною цінністю, повнотою апробації, змістом та оформленням дисертаційна робота 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 її автор 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 безпеки інформації та телекомунікацій
Національного технічного університету
«Дніпровська політехніка» Олександра ГЕРАСІНА

Підпис Герасіної О.
засвідчую:
вчений секретар
Вченої ради

НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ «ДНІПРОВСЬКА ПОЛІТЕХНІКА» і.к. 02070743