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

РЕЦЕНЗІЯ

на дисертацію 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 дослідження та її зв'язок із планами наукових робіт університету

Для корпоративної мережі виявлення атаки має цінність лише тоді, коли рішення може бути отримане своєчасно та використане в подальшому реагуванні. Сучасна інфраструктура генерує значні обсяги телеметрії, а події безпеки відрізняються за частотою, критичністю та характером прояву. Через це засоби виявлення повинні поєднувати достатню точність із контрольованою кількістю хибних спрацювань.

Робота Семенюка Б.В. пропонує розглядати мережні ознаки через їх частотно-часове представлення та використовувати спектрограми як вхід для 2D-CNN. Такий підхід розширює традиційний набір методів аналізу трафіку та створює додатковий рівень представлення, на якому можуть виявлятися відмінності між нормальними й атакувальними подіями.

Практично важливо, що дослідження охоплює не один алгоритм, а весь ланцюжок прийняття рішення: підготовку даних, формування спектрального образу, базову класифікацію, компенсацію дисбалансу і повторний аналіз невпевнених прогнозів. Це дозволяє оцінювати систему не лише як модель машинного навчання, а як потенційний компонент засобу мережного моніторингу.

Ураховуючи актуальність автоматизованого аналізу телеметрії безпеки та потребу в кращому виявленні малопоширених атак, тема дисертації є значущою і відповідає профілю спеціальності 122 «Комп'ютерні науки».

Зміст роботи узгоджується з напрямом держбюджетної теми Хмельницького національного університету «Система забезпечення стійкості до витоку конфіденційної інформації в корпоративних мережах в умовах впливів комп'ютерних атак» (держреєстрація 0126U002082). У межах цієї тематики здобувач виконував дослідницькі завдання, пов'язані з аналізом і виявленням зловмисної мережної активності.

2. Формулювання наукової задачі, мети та завдань дослідження

Науково-прикладна задача сформульована як підвищення точності та збалансованості виявлення комп'ютерних атак у корпоративних мережах. Об'єктом є процес виявлення атак, а предметом – моделі та методи, що поєднують частотно-часове подання трафіку, балансування навчальних даних і уточнення рішень класифікатора.

Мета та завдання роботи взаємно узгоджені. Спочатку автор аналізує існуючі системи й обмеження класичних підходів, далі формує власне подання даних, розробляє методи для проблемних класів і невизначених рішень, а завершальним етапом є програмна реалізація та експериментальна оцінка. Така послідовність є доцільною з точки зору побудови прикладної системи для засобів забезпечення кібербезпеки.

3. Наукова новизна отриманих результатів

Наукова новизна результатів дисертаційного дослідження визначається такими положеннями:

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.

4. Короткий аналіз основного змісту дисертації

Вступ окреслює проблематику виявлення атак і обґрунтовує необхідність підвищення якості роботи з рідкісними та складними подіями. Тут визначено основні поняття, мету, завдання та очікуваний науковий результат.

Перший розділ містить огляд методів і систем виявлення вторгнень з акцентом на обмеження сигнатурних та інтелектуальних підходів. Значна увага приділена дисбалансу класів і проблемам оцінювання якості в умовах нерівномірних вибірок.

Другий розділ описує основний соніфікаційний конвеєр: перетворення мережних характеристик у сигнал, виконання STFT і отримання спектрограми, яка надалі класифікується 2D-CNN. Це є базою для наступних удосконалень.

Третій розділ зосереджений на підвищенні якості для складних прикладів. У ньому запропоновано SPAS для формування збалансованішої вибірки та каскадний механізм, який використовує інформацію про помилки базової моделі для уточнення прогнозів у τ-зоні.

Четвертий розділ демонструє реалізацію методів і результати експериментів. Наведене роздільне оцінювання етапів дозволяє порівнювати базовий і вдосконалені варіанти системи та визначати, на якому етапі досягається покращення показників.

5. Обґрунтованість і достовірність наукових положень, висновків і рекомендацій

Висновки дисертації базуються на результатах програмних експериментів та кількісних метриках. Порівняння виконуються на однаково сформованих вибірках, що зменшує вплив сторонніх факторів на оцінку внеску окремих методів. Аналіз помилок доповнює агреговані показники і дає змогу оцінити поведінку системи на складних класах.

Прикладна перевірка не обмежується демонстрацією одного показника. Автор аналізує роботу базової моделі, балансування і каскадного уточнення окремо, а також наводить програмну реалізацію. Сукупність цих матеріалів є достатньою для підтвердження працездатності запропонованого підходу.

6. Практичне значення одержаних результатів

Розроблений підхід може бути використаний як аналітичний модуль у системах моніторингу мережної безпеки. На вхід такого модуля подається сформований набір характеристик мережних з'єднань, а результатом є рішення класифікатора, яке може бути передане у контур подальшої обробки подій.

Практичний інтерес становить можливість окремо налаштовувати базовий класифікатор, процедуру балансування і механізм повторної класифікації невпевнених випадків. Це дозволяє керувати співвідношенням між якістю виявлення та обчислювальними витратами при перенесенні рішення до іншої інфраструктури.

Реальність прикладного використання підтверджується впровадженням результатів у ТОВ «ІТТ», ПП «Авіві» та освітній діяльності Хмельницького національного університету.

7. Особистий внесок здобувача

Здобувачем особисто розроблено ключові складові дослідження: модель соніфікаційного подання, метод частотно-часового перетворення, SPAS і механізм селективного уточнення. Ним також виконано програмну реалізацію, підготовку експериментів і аналіз результатів. Внесок у спільні публікації відображено у вступі дисертації.

8. Апробація матеріалів дисертації

Результати роботи оприлюднено у п'яти наукових статтях і одній публікації в матеріалах міжнародної конференції, що індексована в наукометричній базі Scopus. Доповіді за тематикою дослідження були представлені на міжнародних конференціях IntelITSIS-2025, DeSSerT-2025 та ACIT-2026. Одну програмну розробку зареєстровано як авторське свідоцтво на твір (програму).

9. Структура та обсяг дисертації

Дисертація має традиційну для кваліфікаційної роботи структуру та містить чотири основні розділи, а також вступні матеріали, висновки, бібліографію і п'ять додатків. Загальний обсяг — 222 сторінки, основний текст — 167 сторінок (включно з рисунками і таблицями), список джерел — 133 найменування. Для подання результатів подано 41 рисунок і 20 таблиць.

10. Зауваження

1. Для практичного впровадження доцільно було б чіткіше визначити місце розробленого модуля у типовій архітектурі корпоративного моніторингу: на якому рівні збираються ознаки, де виконується соніфікація та яким компонентом формується остаточна подія безпеки.

2. Робота завершується рішенням про належність події до класу атаки або нормального трафіку. Для інтеграції з SOC корисно було б описати мінімальний формат вихідного повідомлення для SIEM/SOAR: ідентифікатор потоку, оцінку впевненості, ознаку проходження через τ-зону та дані, достатні для подальшого розслідування.

3. Наведені результати характеризують якість класифікації, однак для експлуатації важливо знати ресурсний профіль усього конвеєра. Доцільно було б подати тест навантаження із зазначенням кількості flow-записів за секунду та окремо оцінити внесок підготовки ознак, STFT, 2D-CNN і допоміжної моделі у загальну затримку.

4. У корпоративній мережі телеметрія може бути неповною через втрату пакетів, несправність сенсора або різні налаштування flow-експортерів. Варто було б дослідити деградацію якості за відсутності частини вхідних характеристик та визначити, які ознаки є критичними для стабільної роботи соніфікаційного подання.

5. Каскадна схема формує додатковий рівень прийняття рішення для невпевнених випадків. Для оператора SOC корисно було б пов'язати цей механізм із пріоритезацією інцидентів. Наприклад, виділяти події, які були перевизначені допоміжною моделлю, в окрему чергу для підвищеної уваги аналітика.

6. Експлуатація системи потребуватиме контрольованого оновлення моделей. Доцільно було б описати процедуру версіонування базового класифікатора, SPAS-набору і допоміжної моделі, а також критерії повернення до попередньої версії у разі погіршення показників після оновлення.

Зауваження стосуються переважно питань подальшого практичного впровадження й експлуатації запропонованих рішень. Вони не впливають на позитивну оцінку наукової новизни, достовірності та завершеності дисертаційної роботи.

11. Загальний висновок

Дисертаційна робота містить взаємопов'язаний комплекс моделей, методів і програмних рішень для інтелектуального виявлення мережних атак. Автором показано не лише можливість формування нового частотно-часового представлення, а й способи підвищення якості роботи з дисбалансованими та

невпевненими прикладами. Отримані результати мають як наукове, так і прикладне значення для систем моніторингу безпеки.

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.

Рецензент,
кандидат технічних наук, доцент,
завідувач кафедри кібербезпеки
Хмельницького національного університету _____ Юрій КЛЬОЦ

«Підпис Юрія КЛЬОЦА засвідчую»
Проректор з наукової роботи
Хмельницького національного університету _____ Олег СИНЮК

«___» _____ 2026 р.