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

# РЕЦЕНЗІЯ

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 дослідження та її зв'язок із планами наукових робіт університету*

Задача виявлення комп'ютерних атак у корпоративних мережах належить до класу задач розпізнавання за умов істотної неоднорідності даних. Навчальні вибірки містять класи різної чисельності, окремі типи атак мають близькі статистичні характеристики, а межі між безпечною та небезпечною поведінкою можуть бути нечіткими. За цих умов просте підвищення середньої точності не гарантує належної якості для малопредставлених класів.

У дисертації запропоновано математично й алгоритмічно пов'язану послідовність перетворень: нормований вектор мережних ознак кодується у сигнал, для нього формується частотно-часове подання, після чого спектральний образ аналізується нейронною мережею. Окремими складовими є адаптивне балансування та механізм уточнення прогнозів поблизу межі прийняття рішення.

Такий підхід є новим з погляду формування нового простору ознак, оскільки змінює спосіб представлення початкових даних без зміни самої задачі класифікації. Водночас він вимагає коректного вибору параметрів кодування, STFT, процедури балансування і критерію виділення зони невизначеності, що надає роботі виразну методичну складову частину дослідження.

Актуальність теми також визначається необхідністю підвищення повноти виявлення рідкісних атак і зменшення впливу дисбалансу класів. Розв'язувана задача відповідає предметній області зі стандарту вищої освіти для спеціальності 122 «Комп'ютерні науки».

Дисертаційне дослідження пов'язане з держбюджетною темою Хмельницького національного університету «Система забезпечення стійкості до витоку конфіденційної інформації в корпоративних мережах в умовах впливів комп'ютерних атак» (номер державної реєстрації 0126U002082), у виконанні якої Семенюк Б.В. брав участь як виконавець.

### *2. Формулювання наукової задачі, мети та завдань дослідження*

Об'єктом дослідження є процес виявлення комп'ютерних атак у корпоративних мережах. Предмет охоплює моделі та методи, у яких мережні дані переводяться до частотно-часового представлення, а якість класифікації підвищується за рахунок адаптивного балансування та аналізу помилок. Така конкретизація предмета узгоджується зі структурою дисертації та експериментальною частиною.

Мета роботи полягає у підвищенні точності й збалансованості виявлення атак. Для її досягнення сформовано шість взаємопов'язаних завдань: аналіз існуючих підходів; побудова моделі соніфікаційного представлення; розроблення частотно-часового перетворення; створення методу SPAS; розроблення механізму уточнення рішень у τ-зоні; програмна реалізація та експериментальна перевірка. Послідовність завдань є логічною та забезпечує перехід від теоретичної постановки до кількісної оцінки результатів.

### *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*

У вступі сформовано понятійний і методичний каркас дослідження: обґрунтовано актуальність, поставлено мету, визначено об'єкт, предмет і завдання, наведено положення новизни та практичного значення.

Перший розділ систематизує відомі методи виявлення мережних атак і показує, які обмеження виникають при роботі з дисбалансованими даними та рідкісними класами. Це слугує підставою для вибору напряму подальших перетворень ознак.

У другому розділі подано математичний опис соніфікації та частотно-часового перетворення. Особливу увагу приділено формуванню хвильової форми, параметрам STFT та побудові двовимірного представлення, придатного для обробки згортковою мережею.

Третій розділ розвиває методичну частину роботи: описано SPAS-балансування, аналіз помилок базового класифікатора, побудову τ-зони та правила селективного перевизначення. Ці методи орієнтовані на зменшення впливу нерівномірної представленості класів і невпевнених прогнозів.

У четвертому розділі реалізовано послідовну експериментальну перевірку розроблених рішень. Автор порівнює варіанти представлення даних, оцінює вплив балансування та окремо досліджує каскадну схему, що дає можливість аналізувати внесок кожного компонента.

### *5. Обґрунтованість і достовірність наукових положень, висновків і рекомендацій*

Коректність одержаних результатів підтримується використанням загальноприйнятих метрик класифікації, розділенням даних на незалежні підмножини та відокремленням етапів налаштування від остаточного тестування. Для задачі з дисбалансом класів позитивним є застосування не лише accuracy, а й precision, recall, F1 та аналізу матриць помилок.

Достовірність також забезпечується тим, що запропоновані методи перевіряються не ізольовано від базової моделі: у роботі наведено послідовні порівняння, які дають змогу визначити ефект, що створюють частотно-часове подання, балансування та селективне уточнення. Це робить висновки експериментальної частини аргументованими.

### *6. Практичне значення одержаних результатів*

Результати можуть бути використані у програмних модулях аналізу мережного трафіку, де необхідно працювати з дисбалансованими навчальними даними та контролювати помилки класифікації. Запропоновані процедури описані алгоритмічно і мають програмну реалізацію, що полегшує їх відтворення.

Окреме практичне значення має модульність розробленого конвеєра: соніфікаційне подання, SPAS та каскадний механізм можуть оцінюватися й удосконалюватися окремо. Це дає можливість адаптувати рішення до інших наборів даних без повної зміни методичної основи.

Факт використання результатів підтверджено актами та довідками про впровадження у ТОВ «ІТТ», ПП «Авіві» і навчальному процесі Хмельницького національного університету.

### *7. Особистий внесок здобувача*

Особистий внесок Семенюка Б.В. полягає у формуванні загальної моделі дослідження, розробленні методу частотно-часового представлення мережних ознак, методу SPAS і каскадного механізму уточнення, а також у програмуванні експериментального конвеєра й аналізі отриманих результатів. Для спільних публікацій внесок здобувача конкретизовано у матеріалах дисертації.

### *8. Апробація матеріалів дисертації*

Матеріали роботи пройшли апробацію через публікацію п'яти наукових статей і однієї конференційної праці, проіндексованої у Scopus. Окремі результати доповідалися на міжнародних науковому семінарі IntelITSIS-2025 та наукових конференціях DeSSerT-2025 і ACIT-2026. Програмні результати роботи підтверджені одним свідоцтвом про реєстрацію авторського права.

### *9. Структура та обсяг дисертації*

Робота складається з анотації, змісту, переліку скорочень, вступу, чотирьох розділів, загальних висновків, списку джерел і п'яти додатків. Обсяг дисертації - 222 сторінки, з яких 167 сторінок припадає на основний текст, в який включено рисунки і таблиці. Список літератури містить 133 позицій, у тексті подано 41 рисунок та 20 таблиць.

### *10. Зауваження*

1. У способі формування сигналу початкові мережні характеристики одержують позиції у впорядкованому векторі. Доцільно було б формально визначити, які перетворення порядку ознак залишають результат інваріантним, а які принципово змінюють спектральну картину. Це дозволило б чіткіше окреслити математичні властивості введеного відображення.

2. Параметри короткочасного перетворення Фур'є безпосередньо визначають часову й частотну роздільну здатність спектрограми. Було б корисно доповнити роботу таблицею чутливості до довжини вікна, перекриття та частоти дискретизації, щоб показати область параметрів, у якій якість класифікації залишається стабільною.

3. Для нейронних моделей можливе коливання результатів між незалежними запусками. Оскільки приріст каскадної схеми є помірним, бажано було б подати середні значення метрик і міри розсіювання за кількома ініціалізаціями або застосувати статистичний критерій для порівняння базового і каскадного варіантів.

4. Поняття «сигнатурозбережного» балансування є одним із ключових для SPAS. Доцільно було б ввести числову міру близькості структур міноритарного класу до і після синтетичного розширення та показати, як ця міра пов'язана з підсумковим Recall рідкісних підкласів.

5. Межі $\tau$-зони визначають, які саме приклади передаються на додаткову класифікацію. Для повнішого математичного обґрунтування методу варто було б навести залежність F1, Recall і частки перевизначених прикладів від $\tau$ та описати правило вибору робочого значення без використання тестової множини.

6. За умов значного дисбалансу агрегована F1-міра може приховувати поведінку окремих класів. Доцільно було б для основних експериментальних етапів уніфіковано подати Macro-F1 разом із пер-класовими Recall/F1 та довірчими інтервалами, що зробило б оцінювання ефекту балансування статистично повнішим.

Наведені зауваження спрямовані на поглиблення формального та статистичного обґрунтування роботи. Вони мають рекомендаційний характер і не змінюють позитивної оцінки отриманих наукових результатів.

### *11. Загальний висновок*

Дисертація Семенюка Богдана Васильовича містить завершений цикл наукового дослідження: від формалізації задачі та побудови нового представлення даних до розроблення методів балансування, аналізу невизначеності й експериментальної перевірки. Результати мають достатній рівень обґрунтованості,

а запропоновані методи становлять самостійний внесок у методи інтелектуального виявлення комп'ютерних атак.

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 фізико-математичних наук, доцент,
доцент кафедри комп'ютерної інженерії та інформаційних систем
Хмельницького національного університету Тетяна КИСІЛЬ

«Підпис Тетяни КИСІЛЬ засвідчую»:
Проректор з наукової роботи
Хмельницького національного університету Олег СИНЮК

«___» _____ 2026 р.