ВИСНОВОК
про наукову новизну, теоретичне та практичне значення результатів дисертації

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

Публічна презентація проведена на кафедрі комп'ютерної інженерії та інформаційних систем Хмельницького національного університету
«07» вересня 2026 р., протокол № 4.

1. Актуальність теми дослідження. Сучасний розвиток корпоративних інформаційних систем супроводжується стрімким зростанням обсягів мережного обміну, ускладненням архітектури цифрової інфраструктури, поширенням хмарних сервісів, віртуалізованих середовищ, віддаленого доступу та розподілених прикладних платформ. Це розширює функціональні можливості корпоративних мереж, але одночасно збільшує кількість потенційних векторів атак, створює передумови для прихованого несанкціонованого доступу, реалізації багатокрокових сценаріїв вторгнення та порушення безперервності функціонування інформаційних систем.

Системи виявлення вторгнень є одним із ключових компонентів кіберзахисту корпоративних мереж. Вони забезпечують збір і попередню обробку телеметрії, виділення інформативних характеристик мережних з'єднань та формування рішення щодо наявності або відсутності зловмисної активності. Водночас традиційні сигнатурні та статистичні підходи не завжди забезпечують необхідну точність за умов складної структури трафіку, появи нових і комбінованих атак, слабкої відокремлюваності нормальних і зловмисних зразків та невизначеності прогнозів у прикордонних випадках класифікації.

Окремою проблемою є дисбаланс класів у наборах даних для навчання систем виявлення атак. Домінування нормального трафіку та недостатня представленість рідкісних підкласів атак зміщують процес навчання в бік мажоритарного класу, можуть формувати завищені оцінки загальної точності та знижують повноту виявлення критично важливих атак. Крім того, пряме векторне подання параметрів мережного з'єднання не завжди дає змогу виявити приховані структурні та міжознакові закономірності, придатні для ефективного використання методів глибинного навчання.

Перспективним напрямом розв'язання зазначених проблем є частотно-часове представлення мережного трафіку, сформоване на основі його соніфікації. Перетворення багатовимірного простору ознак у хвильовий сигнал із подальшим

спектральним аналізом дає змогу отримати структуроване двовимірне подання та застосувати згорткові нейронні мережі для автоматизованого розпізнавання атак. Разом із тим підвищення точності потребує комплексного поєднання інформативного перетворення трафіку, адаптивного балансування навчальної вибірки із збереженням характеристик міноритарних класів та селективного уточнення рішень у зоні невизначеності прогнозу.

Таким чином, актуальною науково-прикладною задачею є підвищення точності та збалансованості виявлення комп'ютерних атак у корпоративних мережах шляхом розроблення моделей і методів частотно-часового представлення мережного трафіку, формування інформативних спектральних ознак, сигнатурозбережного адаптивного балансування навчальної вибірки та селективного перевизначення рішень у зоні невизначеності прогнозу.

2. Зв'язок роботи з науковими програмами, планами, темами. Дисертаційне дослідження виконувалось у рамках держбюджетної науково-дослідної теми Хмельницького національного університету «Система забезпечення стійкості до витоку конфіденційної інформації в корпоративних мережах в умовах впливів комп'ютерних атак» (номер державної реєстрації 0126U002082), в якій автор дисертації був виконавцем.

3. Наукова новизна отриманих результатів. Наукова новизна отриманих результатів полягає у розробленні моделі процесу виявлення комп'ютерних атак та методів частотно-часового перетворення мережного трафіку, сигнатурозбережного адаптивного балансування навчальної вибірки і підвищення точності в зоні невизначеності прогнозу.

Отримано такі нові наукові результати:

1) вперше розроблено модель процесу виявлення комп'ютерних атак на основі соніфікації мережного трафіку, особливістю якої є інтеграція звукового перетворення багатовимірного простору ознак, спектрального аналізу, адаптивного балансування навчальної вибірки та каскадного механізму прийняття рішень у межах узагальненої моделі процесу виявлення атак, що дає змогу узгодити етапи навчання і функціонування моделі та підвищити збалансованість класифікації в умовах дисбалансу класів;

2) розроблено новий метод частотно-часового перетворення мережного трафіку, який, на відміну від відомих векторних підходів до представлення ознак, передбачає інтерпретацію багатовимірного простору параметрів з'єднання як параметрів сигналу з лінійним частотно-амплітудним відображенням і подальшим спектральним аналізом, що дає змогу формувати структуроване 2D-подання трафіку та підвищити інформативність вхідних даних для задачі класифікації атак;

3) розроблено новий метод сигнатурозбережного адаптивного балансування навчальної вибірки, який, на відміну від відомих процедур надсемплінгу та підвибірки, характеризується збереженням структурних характеристик міноритарного класу та врахуванням помилок базової моделі під час формування розширеної навчальної множини, що дає змогу зменшити вплив дисбалансу класів на функцію ризику, підвищити повноту виявлення атак і збалансованість класифікації;

4) розроблено новий метод підвищення точності виявлення атак у зоні невизначеності прогнозу, який, на відміну від відомих порогових схем прийняття рішень, передбачає формалізацію τ-інтервалу невизначеності та селективне перевизначення рішень на основі допоміжної моделі, навченої на помилкових прикладах базового класифікатора, що дає змогу зменшити кількість хибнонегативних рішень без порушення принципу незалежності тестової вибірки.

4. Теоретичне та практичне значення результатів дисертації. Теоретичне значення результатів полягає у розвитку моделей і методів інтелектуального виявлення комп'ютерних атак на основі частотно-часового представлення мережного трафіку. Формалізовано послідовність перетворення багатовимірних параметрів мережного з'єднання у хвильовий сигнал і спектральне 2D-подання, підходи до адаптивного формування навчальної множини із збереженням структурних характеристик міноритарних класів, а також механізм каскадного прийняття рішень із виділенням τ-зони невизначеності та застосуванням допоміжної моделі.

Практичне значення полягає у розробленні програмно-алгоритмічного забезпечення, що реалізує єдиний соніфікаційний конвеєр: попередню обробку мережних даних, формування хвильового сигналу, побудову спектрограм, навчання базового двовимірного згорткового класифікатора, сигнатурозбережне адаптивне балансування (SPAS) та селективне перевизначення рішень у зоні невизначеності. Запропоновані рішення можуть бути використані під час створення і модернізації систем моніторингу безпеки корпоративних мереж.

За результатами експериментальних досліджень підтверджено працездатність соніфікаційного підходу як альтернативного каналу подання мережних з'єднань для задачі виявлення вторгнень та ефективність каскадної схеми, що поєднує балансування SPAS, помилково-орієнтоване підсилення проблемних підкласів атак, визначення τ-зони і селективне перевизначення рішень. Застосування запропонованого підходу забезпечило відтворюване покращення якості розпізнавання, а значення F1-міри на тестовій множині зросло приблизно на 1 відсоток порівняно з базовою соніфікованою моделлю.

5. Використання результатів роботи. Теоретичні та практичні результати дослідження впроваджені в ТОВ «ІТТ» (акт від 30.06.2026, м. Хмельницький), ПП

«Авіві» (довідка від 29.06.2026, м. Хмельницький), а також в освітньому процесі Хмельницького національного університету (акт від 26.06.2026) при викладанні дисциплін на кафедрі комп'ютерної інженерії та інформаційних систем для спеціальності F7 Комп'ютерна інженерія, зокрема в курсах «Безпека та захист комп'ютерних систем», «Моделювання та методи оптимізації в наукових та експериментальних дослідженнях», «Методології забезпечення якості, надійності, гарантоздатності та безпеки комп'ютерних систем та мереж».

6. Особиста участь автора в одержанні наукових та практичних результатів, що викладені в дисертаційній роботі.

Повнота викладення матеріалів дисертації в роботах, опублікованих автором. За результатами проведених досліджень основні наукові результати опубліковано у п'яти наукових статтях. Апробацію результатів дисертації засвідчено публікацією однієї праці у матеріалах міжнародної конференції, проіндексованої в наукометричній базі Scopus, та доповідями на двох міжнародних конференціях. Отримано одне свідоцтво про реєстрацію авторського права на твір (комп'ютерну програму).

У працях, опублікованих у співавторстві, здобувачеві належать такі наукові результати: розроблено модель та метод частотно-часового перетворення мережного трафіку на основі соніфікації і формування двовимірного спектрального подання для виявлення комп'ютерних атак із застосуванням двовимірної згорткової нейронної мережі; розроблено метод сигнатурозбережного адаптивного балансування навчальної вибірки; розроблено метод підвищення точності виявлення комп'ютерних атак у зоні невизначеності прогнозу; розроблено модель процесу виявлення комп'ютерних атак на основі частотно-часового представлення мережного трафіку; досліджено вплив синтетичного балансування навчальної вибірки на точність виявлення комп'ютерних атак; розроблено архітектуру програмного забезпечення та програмний код.

Співавторам належать результати щодо обґрунтування доцільності соніфікації мережного трафіку, уточнення постановки експериментального дослідження та апробації результатів; формалізації адаптивного балансування і каскадної схеми селективного уточнення рішень; визначення особливостей проєктування системи виявлення вторгнень і методики її дослідження; організації експериментального дослідження впливу синтетичного балансування; розроблення вимог до програмного забезпечення, його верифікації та окремих алгоритмів.

Результати дисертації опубліковано в повному обсязі.

Дисертаційна робота виконана на кафедрі комп'ютерної інженерії та інформаційних систем Хмельницького національного університету.

Наукові керівники:

кандидат технічних наук, доцент, доцент кафедри комп'ютерної інженерії та інформаційних систем Хмельницького національного університету Корецька Людмила Олександрівна;

доктор філософії, доцент кафедри комп'ютерної інженерії та інформаційних систем Хмельницького національного університету Савенко Богдан Олегович.

Розглянувши звіт подібності щодо перевірки на плагіат, встановлено, що дисертаційна робота Семенюка Б. В. є результатом самостійних досліджень здобувача і не містить елементів плагіату та неправомірних запозичень. Використані ідеї, результати і тексти інших авторів мають посилання на відповідні джерела.

Дисертація характеризується єдністю змісту та відповідає вимогам щодо її оформлення.

Дотримання академічної доброчесності. Дисертаційну роботу Семенюка Б. В. перевірено на текстові збіги відповідно до встановленого в Хмельницькому національному університеті порядку. За результатами аналізу звіту подібності встановлено, що робота є результатом самостійних досліджень здобувача, не містить елементів академічного плагіату та неправомірних запозичень; використані ідеї, результати й тексти інших авторів супроводжуються належними посиланнями.

7. Перелік публікацій за темою дисертації із зазначенням особистого внеску здобувача.

За результатами досліджень опубліковано 7 праць, у тому числі 5 статей у наукових фахових виданнях України, 1 публікацію у матеріалах міжнародної конференції, проіндексовану в наукометричній базі Scopus, та отримано 1 свідоцтво про реєстрацію авторського права на твір (комп'ютерну програму).

Список публікацій здобувача за темою дисертації.

Наукові праці, в яких опубліковані основні наукові результати дисертації

1. Семенюк Б., Каштальян А. Виявлення комп'ютерних атак із використанням 2D-CNN та соніфікації мережного трафіку. *Information Technology: Computer Science, Software Engineering and Cyber Security*. 2025. С. 193–201. DOI: https://doi.org/10.32782/IT/2025-1-26 – розроблено модель та метод частотно-часового перетворення мережного трафіку на основі соніфікації, сформовано двовимірне спектральне подання та проведено експериментальне оцінювання виявлення атак із застосуванням 2D-CNN.

2. Семенюк Б. В., Савенко Б. О. Метод виявлення комп'ютерних атак на основі адаптивності та балансування навчальної вибірки. *Вісник Черкаського державного технологічного університету*. 2026. № 1. С. 34–43. DOI:

https://doi.org/10.62660/bcstu/1.2026.3 – розроблено метод сигнатурозбережного адаптивного балансування навчальної вибірки.

3. Семенюк Б. В., Савенко Б. О. Метод підвищення точності системи виявлення атак у зонах невизначеності на основі аналізу помилок та селективного перевизначення рішень. *Системні технології*. 2026. № 2. С. 99–110. DOI: https://doi.org/10.34185/1562-9945-2-163-2026-09 – розроблено метод підвищення точності виявлення атак у зоні невизначеності прогнозу на основі аналізу помилок та допоміжної моделі.

4. Семенюк Б., Корецька Л. Особливості проєктування та дослідження системи виявлення вторгнень на основі соніфікації мережевого трафіку. *Measuring and Computing Devices in Technological Processes.* 2026. № 1. С. 246–254. DOI: https://doi.org/10.31891/2219-9365-2026-85-31 – розроблено модель процесу виявлення комп'ютерних атак на основі частотно-часового представлення мережного трафіку.

5. Семенюк Б., Стецюк Ю. Дослідження впливу синтетичного балансування навчальної вибірки на точність виявлення комп'ютерних атак. *Measuring and Computing Devices in Technological Processes*. 2026. № 2. С. 410–417. DOI: https://doi.org/10.31891/2219-9365-2026-86-48 – проведено дослідження впливу синтетичного балансування навчальної вибірки на точність виявлення комп'ютерних атак.

Праці, які засвідчують апробацію матеріалів дисертації

6. Semeniuk B., Kashtalian A., Martiniuk D., Drozd A., Abdel-Badeeh M. Salem. Detection of computer attacks based on sonification of network traffic. *IntelITSIS'25: The 6th International Workshop on Intelligent Information Technologies & Systems of Information Security*, April 04, 2025, Khmelnytskyi, Ukraine. Pp. 252–263. URL: https://ceur-ws.org/Vol-3963/paper21.pdf (Scopus) – розроблено модель і метод частотно-часового перетворення мережного трафіку, здійснено формування спектрального подання та експериментальну перевірку підходу.

Публікації, які додатково відображають наукові результати дисертації

7. Свідоцтво про реєстрацію авторського права на твір (програму) № 145847 Україна. Комп'ютерна програма «Sonified IDS» / Семенюк Б.В., Нічепорук А.О., Савенко О.С. Дата реєстрації 24.04.2026. URL: https://sis.nipo.gov.ua/uk/search/detail/1925939/ – розроблено програмно-алгоритмічне забезпечення системи виявлення комп'ютерних атак на основі соніфікації мережного трафіку.

8. Апробація дисертації. Апробацію основних положень, ідей і висновків дисертаційної роботи проведено на науковому семінарі кафедри комп'ютерної інженерії та інформаційних систем Хмельницького національного університету. Наукові результати роботи доповідалися на таких конференціях: 6th International

Workshop on Intelligent Information Technologies & Systems of Information Security (IntelITSIS), Khmelnytskyi, Ukraine, April 04, 2025; 15th International Conference on Dependable Systems, Services and Technologies (DeSSerT-2025), Athens, Greece, December 19–21, 2025; 16th International Conference on Advanced Computer Information Technologies (ACIT-2026), Zlin, Czech Republic, September 2–4, 2026.

9. Оцінка мови, стилю та оформлення дисертації. Дисертацію написано грамотною українською мовою. Стиль викладення матеріалів дослідження, наукових положень, висновків і рекомендацій є послідовним, логічним та забезпечує належне сприйняття змісту роботи. Дисертацію оформлено відповідно до вимог, передбачених наказом Міністерства освіти і науки України від 12.01.2017 № 40 (зі змінами, внесеними наказом Міністерства освіти і науки України від 31.05.2019 № 759) «Про затвердження Вимог до оформлення дисертації».

ВВАЖАТИ, що дисертаційна робота _ Семенюка Богдана Васильовича __
(прізвище, ініціали здобувача)
«Моделі та методи виявлення комп'ютерних атак в корпоративних мережах на основі частотно-часового представлення мережного трафіку»,
(назва)
яка подана на здобуття ступеня доктора філософії, за своїм науковим рівнем та практичною цінністю, змістом та оформленням повністю відповідає вимогам пп. 6, 7, 8, 9 «Порядку присудження ступеня доктора філософії та скасування рішення разової спеціалізованої вченої ради закладу вищої освіти, наукової установи про присудження ступеня доктора філософії», затвердженому постановою Кабінету Міністрів України від 12 січня 2022 р. № 44, та відповідає напрямку наукового дослідження освітньо-наукової програми Хмельницького національного університету зі спеціальності 122 Комп'ютерні науки.
(шифр, назва)

РЕКОМЕНДУВАТИ:

Дисертаційну роботу «Моделі та методи виявлення комп'ютерних атак в корпоративних мережах на основі частотно-часового представлення мережного трафіку», _____
назва роботи
подану ___Семенюком Богданом Васильовичем _____
прізвище, ім'я, по батькові
на здобуття ступеня доктора філософії, до захисту.

Головуюча публічної презентації,
доктор філософії, доцент,
завідувачка кафедри КІС
(науковий ступінь, вчене звання, посада)

Підпис дійсний
Відділ кадрів
підпис

Ольга ПАВЛОВА
Ім'я ПРІЗВИЩЕ

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ ХМЕЛЬНИЦЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
ВІДДІЛ КАДРІВ
Ідентифікаційний код 02071234