

Голові разової спеціалізованої
вченої ради PhD 17107
Хмельницького національного
університету
доктору технічних наук,
професору Сергію ЛИСЕНКУ
29016, м. Хмельницький,
вул. Інститутська, 11

ВІДГУК ОФІЦІЙНОГО ОПОНЕНТА

на дисертаційну роботу Віжевського Петра Володимировича
на тему «Методи та засоби виявлення і запобігання витоку даних в
корпоративних мережах згідно еволюційних алгоритмів», подану на здобуття
ступеня доктора філософії з галузі знань 12 Інформаційні технології за
спеціальністю 122 Комп'ютерні науки

1. Актуальність теми дисертаційної роботи.

Витік конфіденційних даних належить до найдорожчих класів інцидентів інформаційної безпеки. Його особливість полягає в тому, що значна частина витоків здійснюється легітимними користувачами через дозволені канали передачі. Традиційні засоби захисту периметра тут не спрацьовують, тому в корпоративних мережах застосовують спеціалізовані системи запобігання витокам даних, які поєднують контентний аналіз документів, контроль каналів та аналіз поведінки користувачів.

Ефективність таких систем обмежується двома чинниками. По-перше, політики безпеки в них є статичними і потребують постійного ручного супроводу, тоді як корпоративне середовище змінюється безперервно: з'являються нові типи документів та ідентифікаторів, змінюються ролі й робочі процеси, поступово дрейфує розподіл характеристик даних. По-друге, застосування методів машинного навчання, яке могло б додати системі адаптивності, породжує проблему пояснюваності: рішення про блокування передачі документа або про підозру щодо співробітника має бути обґрунтоване в термінах, які зрозумілі аудитору і юристу.

Еволюційні алгоритми дають змогу здійснювати глобальний пошук цілісних наборів правил безпосередньо в просторі ознак політики безпеки, зберігаючи інтерпретованість результату, і природно поєднуються з періодичним перенавчанням за сигналом детектора змін. Проте їхнє застосування в задачі запобігання витоку даних (ЗВД) потребує узгодженої формальної моделі процесу, детектора дрейфу, який не залежить від

оперативних міток істинності, та поведінкового профілювання, що враховує індивідуальну норму кожного користувача, а не популяційну.

Отже, актуальною науково-прикладною задачею є підвищення ефективності виявлення та запобігання витокам конфіденційної інформації в корпоративних мережах шляхом розроблення еволюційно-адаптивних методів класифікації документів, адаптації політик і поведінкового профілювання та програмних засобів, що їх реалізують. Зазначена задача відповідає предметній області спеціальності 122 «Комп'ютерні науки», зокрема процесам збору, представлення, обробки, зберігання, передачі та доступу до інформації в комп'ютерних системах.

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 № 1Б-2026 «Система забезпечення стійкості до витоку конфіденційної інформації в корпоративних мережах в умовах впливів комп'ютерних атак» (номер державної реєстрації 0124U001214), в якій автор дисертації є виконавцем.

3. Наукова новизна отриманих результатів.

До основних наукових результатів дисертаційної роботи варто віднести такі:

1) удосконалено модель процесу запобігання витокам даних, яка, на відміну від наявних описових підходів з ізольованим розглядом компонентів ЗВД-системи, об'єднує моделі витоку, корпоративного середовища та даних у єдиній формальній схемі із чітко визначеними точками прикладення адаптивних механізмів, що дає змогу узгоджено проєктувати класифікацію документів, поведінкове профілювання та адаптацію політик як складники одного процесу, а не набір незалежних інструментів;

2) вперше розроблено метод класифікації документів за рівнем конфіденційності на основі генетичного алгоритму, особливістю якого є хромосомне кодування продукційних правил у поєднанні з регуляризацією складності моделі та, на відміну від жадібної індукції правил методом послідовного покриття (CN2, RIPPER) і від генетичного відбору правил із наперед сформованої бази знань, глобальний еволюційний пошук цілісних наборів правил безпосередньо в просторі ознак політик безпеки, що дає змогу отримувати компактний, придатний для аудиту та безпосередньої експертної інтерпретації набір правил із конкурентною якістю розпізнавання і за потреби

відновлювати виявлення нового типу критичних ідентифікаторів одним дописаним експертом правилом без залучення розмічених прикладів;

3) вперше розроблено метод еволюційної адаптації політик ЗВД за умов дрейфу концепції, особливістю якого є детектор змін на основі підтвердженого багатоозначового статистичного тесту, стійкого до поодиноких хибних спрацювань, який, на відміну від класичних детекторів на потоці помилок класифікатора (ADWIN, DDM, EDDM, KSWIN), працює безпосередньо з розподілом вхідних ознак і не потребує оперативних міток істинності, у поєднанні з еволюційним перенавчанням політик, яке, на відміну від інкрементних і ансамблевих схем адаптації, зберігає інтерпретовану структуру набору правил, що дає змогу суттєво зменшити кількість хибних тривог за повного виявлення справжніх змін і втримати точність класифікації в нестационарному потоці;

4) набув подальшого розвитку метод поведінкового профілювання користувачів, який, на відміну від глобальних методів виявлення аномалій з єдиною моделлю нормальної поведінки для всієї сукупності користувачів, ґрунтується на індивідуальному адаптивному профілі кожного користувача з генетичною оптимізацією його конфігурації та ваг ознак, що дає змогу точніше виявляти внутрішніх порушників у межах реалістичного бюджету тривог.

4. Короткий аналіз основного змісту дисертації

Науковий рівень викладення дисертації відповідає вимогам МОН України. Назва дисертації відображає її зміст і відповідає спеціальності 122 Комп'ютерні науки.

У вступі автор пояснює потребу в адаптивному захисті від витоку даних і визначає результати, які виносить на захист. Наведено постановку дослідження, його наукове та практичне значення.

Перший розділ охоплює методи контентного й поведінкового аналізу та їх використання у ЗВД-платформах. Огляд зосереджено на обмеженнях статичних правил, хибних спрацюваннях і пристосуванні засобів захисту до змін корпоративного середовища.

Другий розділ задає формальне середовище роботи запропонованих методів: характеристики документів, учасників інформаційного обміну, каналів і зон безпеки. Модель пов'язує оцінювання чутливості та ризику з вибором захисної дії, а також визначає місце адаптації політик у загальному процесі.

У третьому розділі викладено алгоритмічні результати роботи. Генетичний пошук використано для формування інтерпретованих правил класифікації та добору конфігурації персонального профілю. Для змін у потоці

даних запропоновано детектор із правилом підтвердження, який керує переходом до перенавчання політики.

В четвертому розділі подано матеріал для оцінювання результативності запропонованих рішень. Окремо досліджено класифікацію документів, виявлення інсайдерської активності та адаптацію до дрейфу. Порівняння з базовими методами доповнено аналізом інтерпретованості й часу роботи. Наведено також обмеження експериментів і опис розробленого комплексу програмних засобів.

Завершують роботу узагальнення отриманих результатів та додаткові матеріали, необхідні для ознайомлення з програмними засобами й експериментами. Впровадження підтверджено документами, розміщеними у додатках.

5. Ступінь обґрунтованості наукових положень, висновків і рекомендацій, їх достовірність.

Сформульовані у дисертації наукові положення, висновки та рекомендації є аргументованими. Вони спираються на формальну модель процесу запобігання витокам, побудовану засобами теорії множин, теорії графів і теорії ймовірностей, та на методи еволюційної оптимізації й машинного навчання, застосування яких у роботі є коректним.

Достовірність одержаних результатів підтверджена експериментами на відкритих корпусах і реальних потоках даних із застосуванням перехресної перевірки та довірчих інтервалів, порівнянням із широким колом базових методів (ансамблеві та лінійні класифікатори, класичні детектори дрейфу, глобальні детектори аномалій), апробацією на міжнародних наукових конференціях та практичним впровадженням.

6. Практичні результати роботи

Розроблено програмний комплекс ЗВДЕАГА мовою Python, який реалізує запропоновані методи в модульній архітектурі, що відповідає формальній моделі, і об'єднує класифікацію контенту, поведінкове профілювання, виявлення дрейфу й адаптацію політик. Комплекс зареєстровано як об'єкт авторського права (свідоцтво № 144040).

Експериментально показано, що класифікатор на продукційних правилах дає F1-міру 0,826 на корпусі ai4privacy проти 0,856 у найкращого ансамблевого методу, тобто поступається лише на 3,5 %, але при цьому використовує близько п'яти правил, які безпосередньо читаються в термінах політики безпеки. Персональний поведінковий профіль на корпусі CERT r4.2 виявляє інсайдерів у першій двадцятці підозрюваних з точністю 0,90 проти 0,35 у найкращого з

глобальних детекторів. Правило підтвердження детектора дрейфу зменшує кількість хибних тривог з 2,1 до 0,6 на потік за повного виявлення справжніх змін, а еволюційне перенавчання правил на потоках зі структурою політики ЗВД дає преквенціальну точність 0,851 проти 0,739 в інкрементній моделі.

Теоретичні та практичні результати дослідження впроваджені в ТОВ «ІТТ» (м. Хмельницький, акт від 30.06.2026), ПП «Авіві» (м. Хмельницький, довідка від 29.06.2026), 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 здобувачів спеціальності F7 Комп'ютерна інженерія, зокрема в курсах «Безпека та захист комп'ютерних систем» і «Методології забезпечення якості, надійності, гарантоздатності та безпеки комп'ютерних систем та мереж».

7. Оформлення дисертації, дотримання вимог академічної доброчесності та повнота викладу наукових положень та результатів в опублікованих працях.

Дисертаційна робота складається з анотації, змісту, переліку скорочень, вступу, чотирьох розділів, висновків, списку використаних джерел та семи додатків. Повний обсяг роботи становить 231 сторінку друкованого тексту, з них анотація займає 11 сторінок, зміст 2 сторінки, перелік скорочень 1 сторінку, вступ, розділи та висновки викладено на с. 15-199, список зі 137 використаних джерел займає 15 сторінок, додатки 17 сторінок. Дисертація містить 13 рисунків та 21 таблицю. Оформлення дисертації відповідає вимогам.

У дисертації не виявлено текстових запозичень і використання наукових результатів інших науковців без посилань на відповідні джерела.

За результатами дисертаційного дослідження опубліковано 10 наукових праць, у тому числі 5 статей у наукових фахових виданнях України категорії Б, 4 праці у матеріалах міжнародних наукових конференцій, з яких 2 опубліковано у виданнях, що індексуються наукометричною базою Scopus, а також одержано свідоцтво про реєстрацію авторського права на комп'ютерну програму «Програмний комплекс запобігання витоку даних з еволюційною адаптацією на основі генетичних алгоритмів (ЗВДЕАГА)» (№ 144040 від 04.03.2026).

Усі наукові положення і результати дисертації повністю викладено в опублікованих працях.

8. Мова та стиль дисертаційної роботи

Текст дисертаційної роботи викладено в логічній послідовності, українською мовою, з використанням усталеної термінології. Дисертація містить достатню кількість ілюстративного матеріалу: схем, рисунків, таблиць.

Мова викладу, стиль та оформлення роботи відповідають вимогам до наукових праць.

9. Зауваження та дискусійні положення щодо змісту дисертації

1. Автор зазначає в дисертації, що зі збільшенням кількості ознак простір пошуку генетичного алгоритму істотно зростає, а при кількості ознак понад кілька тисяч ефективність пошуку може знижуватися. Водночас питання практичної масштабованості методу для великих корпоративних інформаційних систем досліджено недостатньо. На мою думку, доцільним було б навести експериментальні результати для різної кількості ознак та обсягів даних.

2. Запропонований генетичний класифікатор оптимізує правила вже сформованого ознакового простору, тому якість результату безпосередньо залежить від релевантності вибраних ознак. Автор це обмеження визнає, однак питання автоматичного формування або адаптивного відбору ознак не є центральною частиною запропонованого методу. У зв'язку з цим виникає питання щодо стійкості методу до зміни складу ознак у реальному корпоративному середовищі.

3. Експериментальна перевірка проведена на кількох відкритих корпусах і потоках даних, зокрема ai4privacy, 20 Newsgroups, CERT Insider Threat r4.2, Electricity, INSECTS та RandomRBF. Разом із тим виникає питання, наскільки результати, отримані на таких benchmark-наборах, можуть бути безпосередньо перенесені на конкретні корпоративні мережі, де структура документів, політики доступу та поведінка користувачів можуть істотно відрізнятися.

4. Запропонований метод еволюційної адаптації політик є одним із центральних результатів роботи. Водночас сам автор зазначає, що детектор із правилом підтвердження доцільніше застосовувати за відносно дискретних змін концепції, тоді як за неперервного високовимірного дрейфу рекомендується моніторинг якості класифікації. Отже, перспективним напрямом є розширення методу для складніших сценаріїв комбінованого та поступового дрейфу.

5. Індивідуальні профілі користувачів є цікавою особливістю запропонованого методу. Водночас у практичній системі кількість користувачів корпоративної мережі може бути дуже значною. Тому потребує додаткового дослідження питання обчислювальної та інформаційної вартості підтримки індивідуальних профілів для десятків або сотень тисяч користувачів.

Однак, зазначені зауваження істотно не впливають на зміст дисертаційної роботи та не знижують її наукову новизну та практичну цінність.

10. Висновки щодо дисертації в цілому

На основі викладеного вище вважаю, що дисертація Віжевського Петра Володимировича на тему «Методи та засоби виявлення і запобігання витоку даних в корпоративних мережах згідно еволюційних алгоритмів», що подана на здобуття ступеня доктора філософії, є завершеною самостійною науковою працею, у якій отримано нові науково обґрунтовані результати, що в сукупності розв'язують актуальну науково-прикладну задачу підвищення ефективності виявлення та запобігання витокам конфіденційної інформації в корпоративних мережах. За актуальністю, науковою новизною, практичною цінністю, змістом та оформленням дисертація 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», затвердженого постановою Кабінету Міністрів України від 12 січня 2022 р. № 44 (зі змінами, внесеними згідно з постановами Кабінету Міністрів України № 341 від 21.03.2022, № 502 від 19.05.2023, № 507 від 03.05.2024), а її автор, Віжевський Петро Володимирович, заслуговує на присудження ступеня доктора філософії з галузі знань 12 Інформаційні технології за спеціальністю 122 Комп'ютерні науки.

Офіційний опонент,
доктор технічних наук, доцент,
професор кафедри автоматизованих
систем управління Національного університету
«Львівська політехніка»



Наталія ЛИСА

«Підпис Наталії ЛИСОЇ засвідчую»

Вчений секретар
Національного університету
«Львівська політехніка»

к.т.н., доцент

«28» 09 2026 р.



Юрій ЯТЧИШИН