Голові разової спеціалізованої
вченої ради PhD 17107
Хмельницького національного
університету
доктору технічних наук,
професору Сергію ЛИСЕНКУ

РЕЦЕНЗІЯ

на дисертаційну роботу Віжевського Петра Володимировича
за темою «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 дослідження та її зв'язок із планами наукових робіт Хмельницького національного університету

Корпоративні мережі сьогодні обробляють дедалі більші обсяги інформації, значна частка якої є конфіденційною: персональні дані, фінансові документи, комерційна таємниця, об'єкти інтелектуальної власності. Перенесення робочих процесів у хмарні сервіси, поширення гібридних моделей роботи та особистих пристроїв істотно розширили поверхню атаки і кількість каналів, через які дані можуть залишити захищений периметр.

Системи запобігання витокам даних (ЗВД, DLP) є основним класом засобів протидії таким загрозам. Однак наявні комерційні та дослідницькі рішення переважно спираються на статичні правила контентного аналізу, що потребують ручного налаштування і погано пристосовуються до змін у характері документів, робочих процесах організації та поведінці користувачів. Методи машинного навчання, які могли б надати таким системам адаптивності, зазвичай працюють як непрозорі моделі, а їхні рішення важко пояснити у формі, придатній для аудиту безпеки та обґрунтування дій щодо конкретного співробітника.

Окремою проблемою є дрейф концепції: розподіл ознак документів і закономірності поведінки користувачів у корпоративній мережі змінюються з часом, тому класифікатор, налаштований один раз, поступово втрачає точність. Класичні детектори дрейфу орієнтовані на потік помилок класифікатора, а отже потребують оперативних міток істинності, яких у задачі запобігання витокам практично немає.

Еволюційні алгоритми, зокрема генетичні, є природним інструментом для задач такого типу. Вони дозволяють здійснювати глобальний пошук у просторі наборів продукційних правил, зберігаючи інтерпретовану структуру результату, і водночас придатні для періодичного перенавчання політик безпеки за сигналом детектора змін. Поєднання цих властивостей з індивідуальним поведінковим

профілюванням користувачів дає змогу побудувати ЗВД-систему, яка адаптується до середовища і при цьому залишається зрозумілою для адміністратора безпеки.

Таким чином, тема дисертації, спрямована на розроблення методів та програмних засобів виявлення і запобігання витоку даних у корпоративних мережах на основі еволюційних алгоритмів, є актуальною і відповідає сучасним потребам галузі інформаційних технологій.

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.

2. Формулювання наукової задачі, мети й завдань дослідження

Здобувачем чітко сформульовано протиріччя між потребою динамічного корпоративного середовища в засобах запобігання витокам, здатних безперервно адаптуватися і пояснювати свої рішення, та можливостями наявних ЗВД-систем, які або спираються на статичні правила з ручним налаштуванням, або використовують непрозорі моделі машинного навчання. На основі цього протиріччя визначено об'єкт і предмет дослідження.

Об'єктом дослідження є процес виявлення та запобігання витокам конфіденційної інформації в корпоративних мережах.

Предметом дослідження є методи та програмні засоби виявлення і запобігання витоку даних в корпоративних мережах на основі еволюційних алгоритмів.

Метою дисертаційного дослідження є підвищення ефективності виявлення та запобігання витокам конфіденційної інформації в корпоративних мережах шляхом розробки еволюційно-адаптивних методів класифікації документів, поведінкового профілювання користувачів та оптимізації політик безпеки на основі генетичних алгоритмів, а також програмних засобів, що реалізують ці методи у складі єдиного програмного комплексу.

Для досягнення поставленої мети здобувачем сформульовано такі завдання дослідження:

1) провести системний аналіз відомих методів та платформ запобігання витокам даних, формалізувати їхні функціональні обмеження за критеріями масштабованості, адаптивності та точності класифікації;

2) розробити модель процесу запобігання витокам даних, що інтегрує модель витоку, модель корпоративного середовища та модель даних і враховує характеристики інформаційних ресурсів, профілі

користувачів, рівні конфіденційності, показники довіри та оцінки потенційної шкоди від витоку;

3) розробити метод класифікації документів за рівнем конфіденційності на основі генетичного алгоритму з хромосомним кодуванням продукційних правил, регуляризацією складності моделі та спеціалізованими генетичними операторами;

4) розробити метод еволюційної адаптації політик безпеки за умов дрейфу концепції зі статистичним детектором змін, що забезпечує безперервне вдосконалення правил контентного та контекстного контролю з мінімізацією інтегральної функції втрат;

5) розробити метод поведінкового профілювання користувачів з індивідуальними адаптивними профілями та генетичною оптимізацією складу ознак, їхніх ваг і порогів виявлення аномалій;

6) спроектувати та реалізувати програмний комплекс запобігання витоку з модульною архітектурою і провести експериментальні дослідження запропонованих методів на відкритих корпусах і реальних наборах даних за показниками якості класифікації, інтерпретованості, обчислювальної вартості та стійкості до дрейфу концепції, сформулювати практичні рекомендації щодо інтеграції еволюційно-адаптивних компонентів у наявні корпоративні системи безпеки.

3. Наукова новизна отриманих автором результатів полягає в наступному:

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 багатоознакового 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 нестаціонарному 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. Аналіз основного змісту дисертації

У вступі обґрунтовано актуальність задачі виявлення і запобігання витокам конфіденційної інформації в корпоративних мережах, проаналізовано результати відомих досліджень за тематикою, сформульовано протиріччя між потребою в адаптивних і водночас пояснюваних засобах захисту та можливостями наявних ЗВД-систем. Визначено об'єкт, предмет, мету і завдання дослідження, наведено основні наукові результати та відомості про їх практичне значення, апробацію і публікації.

У першому розділі здійснено аналіз методів виявлення витоку даних (контентних, контекстних, семантичних, поведінкових, гібридних), особливостей забезпечення безпеки корпоративних мереж і сучасних комерційних та дослідницьких ЗВД-платформ. Узагальнено обмеження розглянутих рішень, обґрунтовано доцільність застосування еволюційно-адаптивних методів і виконано постановку задачі дослідження.

У другому розділі побудовано формальну модель процесу запобігання витокам даних, яка об'єднує модель даних (документ як кортеж вмісту, ознак, метаданих і рівня чутливості, ознаковий простір на основі TF-IDF, шаблонів і метаданих), модель витоку (актор, об'єкт, канал, ризик-модель інциденту з трирівневим рішенням) та модель корпоративного середовища (типізований граф інфраструктури, рольовий доступ, зони безпеки, точки контролю). Композиція моделей утворює модель ЗВД-системи з модулями класифікації контенту, поведінкового аналізу, адаптації політик та прийняття рішень.

У третьому розділі розроблено три методи: метод класифікації документів за рівнем конфіденційності на основі генетичного алгоритму з хромосомним кодуванням правил IF-THEN і регуляризацією складності; метод еволюційної адаптації політик за умов дрейфу концепції з

детектором на основі багатоознакового критерію Колмогорова-Смирнова з правилом підтвердження та перемиканням між режимами експлуатації і дослідження; метод поведінкового профілювання користувачів з експоненційно зваженими індивідуальними профілями та генетичною оптимізацією маски ознак, ваг, порогу і коефіцієнта забування.

У четвертому розділі описано методику експериментального дослідження та результати перевірки методів на корпусах ai4privacy і 20 Newsgroups, корпусі інсайдерських загроз CERT Insider Threat r4.2, потоках RandomRBF, Electricity та INSECTS. Наведено порівняння з відомими методами машинного навчання і детекторами дрейфу, оцінено інтерпретованість, чутливість до параметрів та обчислювальну вартість, описано програмну реалізацію комплексу ЗВДЕАГА мовою Python, сформульовано рекомендації щодо застосування та окреслено обмеження дослідження.

У висновках узагальнено наукові та практичні результати роботи. У додатках наведено список публікацій, таблиці результатів експериментів, фрагменти вихідного коду, опис структури програмного забезпечення та акти впровадження.

5. Обґрунтованість і достовірність наукових положень, висновків і рекомендацій

Наукові положення, висновки та рекомендації дисертації обґрунтовані коректним застосуванням математичного апарату теорії множин і теорії графів для побудови моделі даних, витоку та корпоративного середовища, теорії ймовірностей і математичної статистики для ризик-моделі інциденту та детектора дрейфу, методів еволюційної оптимізації та машинного навчання для розроблення методів класифікації, адаптації політик і поведінкового профілювання.

Достовірність результатів підтверджується експериментальними дослідженнями на загальновідомих відкритих наборах даних (ai4privacy, 20 Newsgroups, CERT Insider Threat r4.2, Electricity, INSECTS, RandomRBF) із застосуванням стандартних метрик якості класифікації, порівнянням із відомими методами та алгоритмами (випадковий ліс, градієнтний бустинг, SVM, ADWIN, DDM, EDDM, KSWIN, Isolation Forest, LOF, One-Class SVM), використанням перехресної перевірки та довірчих інтервалів для основних показників, а також практичним впровадженням розробленого програмного комплексу.

6. Практичне значення одержаних результатів

Розроблено програмний комплекс ЗВДЕАГА мовою Python із модульною архітектурою, який реалізує запропоновані методи у складі єдиної системи і охоплює класифікацію контенту, поведінкове профілювання, виявлення дрейфу та адаптацію політик. Комплекс зареєстровано як об'єкт авторського права.

Експериментальні дослідження показали, що генетичний класифікатор документів досягає F1-міри 0,826 на корпусі ai4privacy за компактного набору приблизно з п'яти правил, при цьому 98-99 % позитивних рішень пояснюється одним чи двома правилами; метод поведінкового профілювання на корпусі CERT r4.2 виявляє інсайдерів у першій двадцятці підозрюваних з точністю 0,90 проти щонайбільше 0,35 у глобальних детекторів аномалій; правило підтвердження детектора дрейфу зменшує кількість хибних тривог у 3,5 раза за повного виявлення справжніх змін на потоках RandomRBF; еволюційне перенавчання політик підвищує преквенціальну точність на реальних потоках на 6,6-8,0 % порівняно зі статичною політикою. Продемонстровано, що за появи нового типу ідентифікатора одне дописане експертом правило відновлює повноту виявлення без розмічених прикладів.

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. Особистий внесок здобувача

Основні наукові результати, що виносяться на захист, отримано автором самостійно. Здобувачу належать: удосконалена модель процесу запобігання витокам даних, що об'єднує моделі витоку, корпоративного середовища та даних; метод класифікації документів за рівнем конфіденційності на основі генетичного алгоритму з хромосомним кодуванням продукційних правил; метод еволюційної адаптації політик ЗВД за умов дрейфу концепції з підтвердженим багатоознаковим статистичним детектором; метод поведінкового профілювання користувачів з індивідуальними адаптивними профілями; архітектура та програмна реалізація комплексу ЗВДЕАГА, планування і проведення експериментів. У працях, опублікованих у співавторстві, внесок здобувача конкретизовано у вступі до дисертації, і він відповідає змісту наукових результатів роботи.

8. Апробація матеріалів дисертації

Основні положення та результати дисертаційної роботи доповідались і обговорювались на міжнародних наукових конференціях та семінарах: 5th International Workshop on Intelligent Information Technologies and Systems of Information Security (IntelITSIS-2024, м. Хмельницький, березень 2024 р.); 14th IEEE International Conference on Dependable Systems, Services and Technologies (DESSERT 2024, м.

Афіни, Греція, 2024 р.); 1st International Workshop on Intelligent & CyberPhysical Systems (ICyberPhyS 2024, м. Хмельницький, червень 2024 р.); Modern Data Science Technologies Doctoral Consortium (MoDaST 2025, м. Львів, червень 2025 р.).

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).

9. Структура та обсяг дисертації

Дисертаційна робота складається з анотації, змісту, переліку умовних 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.

10. Зауваження

У результаті розгляду дисертації сформовано наступні зауваження та рекомендації.

1. Огляд методів у підрозділі 1.1 (с. 27-32) і таблиця 1.1 (с. 33-34) подають розглянуті підходи одним переліком без групування за призначенням і способом аналізу даних, тому алгоритми виявлення, засоби адаптації та моделі організації захисту, які розв'язують різні завдання, зіставляються в одному ряду.

2. У першому завданні дослідження (с. 18) названо критерії масштабованості, адаптивності та точності класифікації, однак після таблиць 1.1 і 1.2 показники, за якими ці властивості оцінюються в роботі, не пояснено, а посилання на відповідні формальні визначення в розділах 2 і 3 не наведено.

3. Обґрунтування вибору генетичного алгоритму (с. 34-35) не містить зіставлення з іншими еволюційними підходами саме для задачі побудови продукційних правил, зокрема за зручністю кодування правил і збереженням їхньої інтерпретованості.

4. У комбінованій ініціалізації популяції (с. 124-125) поєднано правила жадібного покриття, евристичні та випадково сформовані правила, однак співвідношення цих частин, зокрема орієнтовні частки жадібного покриття й евристичних правил, у роботі не обґрунтовано, що ускладнює перенесення схеми на інші корпуси документів.

5. У підрозділі 1.4 (с. 43-46) мета та завдання дослідження повторюють відповідні положення вступу, тоді як зв'язок між результатами порівняння ЗВД-систем у таблиці 1.3 та обраними напрямами дослідження розкрито стисло.

Втім, зазначені зауваження суттєво не впливають на загальний, доволі високий рівень проведеного дослідження і не знижують його наукової та практичної цінності.

11. Загальний висновок

Вважаю, що дисертаційна робота Віжевського Петра Володимировича на тему «Методи та засоби виявлення і запобігання витоку даних в корпоративних мережах згідно еволюційних алгоритмів» містить нові науково обґрунтовані теоретичні та експериментальні результати в галузі знань 12 Інформаційні технології, які в сукупності забезпечують розв'язання актуальної науково-прикладної задачі підвищення ефективності виявлення та запобігання витокам конфіденційної інформації в корпоративних мережах на основі еволюційно-адаптивних методів.

Дисертаційна робота «Методи та засоби виявлення і запобігання витоку даних в корпоративних мережах згідно еволюційних алгоритмів», яка подана на здобуття ступеня доктора філософії, за своїм науковим рівнем та практичною цінністю, змістом та оформленням 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 за спеціальністю 122 Комп'ютерні науки.

Рецензент,
кандидат технічних наук, доцент,
доцент кафедри комп'ютерної інженерії
та інформаційних систем
Хмельницького національного
університету _____ Андрій НІЧЕПОРУК

«Підпис Андрія НІЧЕПОРУКА засвідчую»:
Проректор з наукової роботи
Хмельницького національного
університету _____ Олег СИНЮК