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

РЕЦЕНЗІЯ

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

Актуальність теми дослідження та її зв'язок із планами наукових робіт університету.

Захист конфіденційної інформації від витоку є одним із пріоритетів інформаційної безпеки корпоративних мереж (КМ). На відміну від зовнішніх атак, витік даних часто відбувається через легітимні канали (електронна пошта, хмарні сховища, знімні носії, месенджери) і легітимними користувачами, тому засоби мережевого периметра є малоефективними. Системи запобігання витокам даних (ЗВД) вирішують цю задачу шляхом класифікації документів за рівнем конфіденційності, контролю каналів передачі та аналізу поведінки користувачів.

Практика експлуатації ЗВД-систем показує дві сталі проблеми. Перша полягає в тому, що політики безпеки формуються вручну у вигляді статичних правил і швидко застарівають, коли змінюються формати документів, склад підрозділів або робочі процеси. Друга пов'язана з тим, що спроби замінити правила моделями машинного навчання дають системи, рішення яких неможливо пояснити в термінах політики безпеки, а це неприйнятно для аудиту і для обґрунтування блокування конкретної передачі.

Еволюційні алгоритми дозволяють поєднати обидві вимоги. Генетичний пошук у просторі наборів продукційних правил дає інтерпретований результат, а періодичне перенавчання за сигналом детектора змін забезпечує адаптацію до нестаціонарного середовища. Водночас застосування таких підходів до задачі ЗВД потребує формальної моделі, яка узгоджує опис даних, витоку та корпоративного середовища, а також методів, придатних до роботи без оперативних міток істинності, оскільки факт витоку рідко стає відомим одразу.

Отже, розроблення методів і засобів виявлення та запобігання витоку даних у КМ на основі еволюційних алгоритмів є актуальною науково-прикладною задачею в галузі інформаційних технологій.

Дисертаційне дослідження Віжевський П. В. 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.

Формулювання наукової задачі, мети й завдань дослідження.

Здобувачем визначено об'єкт і предмет дослідження відповідно до теми та сформульованого протиріччя. Об'єктом дослідження визначено процес виявлення та запобігання витокам конфіденційної інформації в КМ. Предметом дослідження визначено методи та програмні засоби виявлення і запобігання витоку даних у КМ на основі еволюційних алгоритмів.

Метою дослідження визначено підвищення ефективності виявлення та запобігання витокам конфіденційної інформації в КМ 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 мети Віжевський П. В. сформулював шість завдань, які були розв'язані і подані в дисертації.

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.

Короткий аналіз основного змісту дисертації.

Вступ визначає предмет дослідження та його місце серед задач захисту корпоративних даних. Автор формулює мету і завдання, після чого подає положення наукової новизни та відомості про використання результатів.

Матеріал першого розділу підводить до побудови моделі ЗВД-системи. Розглянуто способи аналізу вмісту документів і поведінки користувачів, особливості мережевого середовища та обмеження наявних платформ. На цій основі визначено напрями подальшої розробки.

Основне теоретичне навантаження припадає на другий розділ. Документ описано через його вміст, ознаки, метадані та чутливість; для інциденту витоку враховано актора, канал передавання й ризик. Окремо задано граф корпоративного середовища із зонами безпеки та точками контролю. Ці описи поєднано у модель процесу з модулями аналізу контенту, профілювання, адаптації політик і прийняття рішень.

Третій розділ переводить модельну постановку в алгоритмічну площину. Для контентного аналізу використано еволюційний пошук набору продукційних правил, для адаптації політик передбачено виявлення дрейфу, а для

поведінкового аналізу сформовано індивідуальні профілі. У кожному випадку визначено параметри, які підлягають оптимізації.

У четвертому розділі перевірено роботу алгоритмів на текстових корпусах, журналах активності користувачів і потокових даних. Поряд із показниками якості розглянуто складність правил, обчислювальні витрати та вплив окремих параметрів. Опис програмної реалізації доповнює експериментальну частину рекомендаціями щодо використання методів.

Підсумкові висновки співвідносять одержані результати із завданнями дослідження. Додатки містять деталізацію експериментів, матеріали програмної реалізації, публікації та документи про впровадження.

Обґрунтованість і достовірність наукових положень, висновків і рекомендацій.

Наукові висновки та рекомендації, подані в дисертації, обґрунтовані коректним використанням теорії множин для формалізації документа, категорій конфіденційності та ознакового простору, теорії графів для моделі корпоративного середовища із зонами безпеки та точками контролю, теорії ймовірностей і математичної статистики для ризик-моделі інциденту та статистичного детектора дрейфу, методів еволюційної оптимізації для побудови методів класифікації, адаптації політик і профілювання. Достовірність підтверджено експериментами на відкритих корпусах і реальних потоках даних, порівнянням з відомими методами, використанням перехресної перевірки та довірчих інтервалів, а також практичним впровадженням, яке засвідчило відповідність теоретичних положень результатам застосування.

Практичне значення отриманих результатів.

Розроблено програмний комплекс ЗВДЕАГА, який реалізує запропоновані методи у модульній архітектурі та може бути під’єднаний до поштового або проксі-шлюзу для класифікації контенту і до SIEM-системи для поведінкового профілювання. Класифікатор на продукційних правилах забезпечує F1-міру 0,826 на корпусі документів з персональними даними за приблизно п’яти правил, що безпосередньо читаються в термінах політики безпеки; персональний поведінковий профіль виявляє інсайдерів у 2,5 раза точніше за глобальні детектори аномалій на робочому бюджеті тривог; детектор дрейфу з правилом підтвердження скорочує кількість хибних тривог у 3,5 раза, а еволюційна адаптація політик підвищує преквенціальну точність на 6,6-8,0 % на реальних потоках і зберігає інтерпретований набір правил.

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».

Особистий внесок здобувача

Здобувачем розроблено моделі процесу запобігання витокам даних, методи класифікації документів, еволюційної адаптації політик і поведінкового профілювання на основі генетичних алгоритмів та їх програмна реалізація. Основні наукові результати дисертаційної роботи отримані здобувачем самостійно. 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).

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.).

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.

Зауваження.

У результаті розгляду дисертації сформовано наступні зауваження та рекомендації.

1. Зв’язок між оцінками чутливості документа за формулами (2.3), (2.7) і (2.24) (с. 51, 53, 65) та оцінкою модуля класифікації за формулою (2.55) (с. 96) у розділі 2 пояснено лише словесно, без узагальнювальної схеми, яка показувала б послідовність застосування цих співвідношень під час обробки документа.

2. У рекурсивному правилі обчислення чутливості складеного документа (формули (2.6)-(2.7), с. 52-53) припущення про скінченність структури вкладень і відсутність циклів явно не зазначено, а випадок документа без вкладених компонентів окремо не описано.

3. Функції оцінювання чутливості структурованих даних і ймовірності витоку подано лише в узагальненому вигляді (формула (2.20), с. 62-63; формула (2.34), с. 75); числового прикладу вибору цих функцій та обчислення відповідних оцінок для конкретного документа і події його передавання в роботі немає.

4. У моделі корпоративного середовища (формули (2.40) і (2.49), с. 82, 91-92) компоненти, що описують структуру та інтеграційні зв’язки системи, і величини, які безпосередньо входять до правил авторизації та оцінювання ризику (формули (2.50)-(2.52), с. 92-93), явно не розмежовано, що ускладнює перехід від опису середовища до кількісної моделі.

5. У формальному описі модуля прийняття рішень (формула (2.62), с. 99-100) поряд із захисною дією передбачено числову оцінку впевненості, проте її практичне призначення, зокрема яку додаткову інформацію вона надає адміністратору під час перегляду рішення системи, у роботі не пояснено.

6. При розгляді ознакового простору документа (с. 54-61) вибір TF-IDF, n-грам і шаблонних ознак не зіставлено з нейромережевими векторними поданнями текстів з погляду пояснюваності правил та обчислювальних витрат, тому міркування автора щодо вибору ознак розкрито не повністю.

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

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

Підпис дійсний
Відділ кадрів

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