ВИСНОВОК

про наукову новизну, теоретичне та практичне значення результатів дисертації

на тему «Методи та засоби виявлення і запобігання витоку даних в корпоративних мережах згідно еволюційних алгоритмів»
здобувача наукового ступеня доктора філософії
Віжевського Петра Володимировича
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 «04» вересня 2026 р., протокол № 3.

1. Актуальність теми дослідження. Сучасні корпоративні мережі функціонують в умовах безперервного зростання обсягів оброблюваної інформації та ускладнення ландшафту загроз інформаційній безпеці. Вартість одного інциденту витоку даних у великих компаніях перевищила позначку в 4 мільйони доларів США, при цьому значна частка випадків залишається невиявленою протягом тривалого часу. Перенесення даних та процесів у хмарні середовища, поширення мобільних платформ і гібридних моделей роботи суттєво розширили потенційну поверхню атаки, що зумовлює підвищену увагу дослідників та індустрії до систем запобігання витокам даних (ЗВД). Такі системи покликані контролювати інформаційні потоки, класифікувати документи за рівнем конфіденційності та блокувати несанкціоновану передачу чутливих даних за межі захищеного периметру.

Водночас наявні ЗВД-системи переважно спираються на статичні правила контентного аналізу, що потребують ручного налаштування та не забезпечують автоматичної адаптації до зміни характеру загроз і робочих процесів організації. Методи машинного навчання, що застосовуються для класифікації документів, часто функціонують як «чорні скриньки» і не забезпечують інтерпретованості рішень, необхідної для аудиту безпеки. Проблема дрейфу концепції у потокових даних корпоративних мереж залишається недостатньо дослідженою в контексті ЗВД-систем. Крім того, бракує формальних моделей, які б інтегрували опис витоків, корпоративного середовища та характеристик даних у єдине підґрунтя для побудови адаптивних захисних механізмів.

Перспективним напрямом розв'язання зазначених проблем є застосування еволюційних алгоритмів, які забезпечують глобальний пошук компактних

інтерпретованих наборів правил безпосередньо в просторі ознак політик безпеки, еволюційну адаптацію політик за умов дрейфу концепції без потреби в оперативних мітках істинності та генетичну оптимізацію індивідуальних поведінкових профілів користувачів для виявлення внутрішніх порушників.

Таким чином, актуальною науково-прикладною задачею є підвищення ефективності виявлення і запобігання витокам конфіденційної інформації в корпоративних мережах шляхом розроблення 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.

2. Зв'язок роботи з науковими програмами, планами, темами. Дисертаційне дослідження виконувалось у рамках держбюджетної науково-дослідної теми Хмельницького національного університету № 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. Наукова новизна отриманих результатів полягає у розробленні моделі процесу запобігання витокам даних та методів класифікації документів за рівнем конфіденційності, еволюційної адаптації політик ЗВД за умов дрейфу концепції і поведінкового профілювання користувачів на основі генетичних алгоритмів.

Отримано такі нові наукові результати:

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. Теоретичне та практичне значення результатів дисертації. Теоретичне значення результатів полягає у розвитку моделей і методів інтелектуального виявлення і запобігання витокам конфіденційної інформації в корпоративних мережах на основі еволюційних алгоритмів. Формалізовано модель процесу запобігання витокам даних, що об'єднує моделі витоку, корпоративного середовища та даних у єдиній формальній схемі; підходи до еволюційної індукції інтерпретованих наборів правил класифікації документів за рівнем конфіденційності; механізм виявлення дрейфу концепції на основі підтвердженого багатоознакового статистичного тесту у поєднанні з еволюційним перенавчанням політик; а також засади побудови індивідуальних адаптивних профілів користувачів з генетичною оптимізацією їх конфігурації та ваг ознак.

Практичне значення полягає у розробленні програмного прототипу ЗВД-системи мовою Python із модульною архітектурою, що реалізує запропоновані модель і методи у складі єдиного програмного комплексу. Запропоновані рішення можуть бути використані під час створення і модернізації систем запобігання витокам даних та моніторингу безпеки корпоративних мереж.

За результатами експериментальних досліджень на відкритих корпусах і реальних потоках даних підтверджено, що генетичний класифікатор документів досягає F1-міри 0,826 на корпусі ai4privacy за компактного набору приблизно з п'яти правил; метод поведінкового профілювання на корпусі CERT r4.2 виявляє інсайдерів на робочому бюджеті тривог приблизно у 2,5 раза точніше за глобальні

методи (точність 0,90 у першій двадцятці підозрюваних проти щонайбільше 0,35); правило підтвердження детектора дрейфу зменшує кількість хибних тривог більш як утричі за повного виявлення справжніх змін; адаптація з перенавчанням за сигналом детектора підвищує преквенціальну точність на реальних потоках на 6,6–8,0 % порівняно зі статичною політикою, а еволюційне перенавчання правил на потоках зі структурою політики ЗВД дає 0,851 преквенціальної точності проти 0,739 в інкрементної моделі. У сценарії появи нового типу ідентифікаторів одне дописане експертом правило миттєво відновлює повноту виявлення документів нового типу без жодного розміченого прикладу.

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», «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 у фахових виданнях України. Апробацію результатів дисертації засвідчено публікацією чотирьох праць у матеріалах міжнародних наукових конференцій, з яких дві проіндексовано в наукометричній базі Scopus. Отримано одне свідоцтво про реєстрацію авторського права на твір (комп'ютерну програму).

У працях, опублікованих у співавторстві, здобувачеві належать такі наукові результати: розроблено метод еволюційної адаптації політик ЗВД за умов дрейфу концепції з підтвердженим статистичним детектором змін; розроблено метод класифікації документів за рівнем конфіденційності на основі генетичного алгоритму з хромосомним кодуванням продукційних правил у складі стратегій виявлення та запобігання витокам даних; розроблено модель системи запобігання витоку даних з еволюційною адаптацією на основі генетичних алгоритмів та її формалізацію; розроблено модель процесу виявлення витоків даних з еволюційною адаптацією, що інтегрує моделі витоку, корпоративного середовища та даних; розроблено метод поведінкового профілювання користувачів на основі індивідуальних адаптивних профілів з генетичною оптимізацією їх конфігурації; реалізовано модуль оцінювання довіри та сформовано список інформації, яку

можна збирати на обчислювальному елементі; розроблено модуль машинного навчання для обфускації; розроблено методи обфускації вихідного коду з використанням штучного інтелекту; розроблено стратегії виявлення та запобігання витокам даних у сучасних корпоративних мережах.

Співавторам належать результати щодо загальної концепції дослідження стратегій виявлення та запобігання витокам даних у сучасних корпоративних мережах та визначення ролі обчислювального елемента на основі його поведінки (Савенко О. С.); формування вимог до моделі (Кравчик Ю. В.); постановки задачі надійних розподілених систем та використання рейтингу обчислювального елементу і бінарного класифікатора для його коригування (Саченко А. О.); розроблення моделі довіри з ролями обчислювальних елементів розподіленої системи та її реалізації (Регіда П. Г.); верифікації моделі та аналізу готових засобів для розгортання бінарного класифікатора (Дрозд А. І.); дослідження технологій обфускації (Головко І., Клейн О.); аналізу стратегій виявлення витоків (Островерхов В.); підготовки експериментальних даних (Маслияк Б.); розроблення підходів штучного інтелекту до застосування в задачі дослідження (Салем А.-Б. М.).

Результати дисертації опубліковано в повному обсязі.

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

Наукові керівники:

доктор технічних наук, професор, професор кафедри комп'ютерної інженерії та інформаційних систем Хмельницького національного університету Савенко Олег Станіславович;

кандидат економічних наук, доцент, доцент кафедри менеджменту та адміністрування Хмельницького національного університету Кравчик Юрій Васильович.

Розглянувши звіт подібності щодо перевірки на плагіат, встановлено, що дисертаційна робота Віжевського П. 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 Віжевського П. 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 10 праць, у тому числі 5 статей у наукових фахових виданнях України, 4 публікації у матеріалах міжнародних наукових конференцій, з яких 2 проіндексовано у 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. Віжевський П. В., Савенко О. С. Еволюційна адаптація політик DLP за умов дрейфу концепції у потокових даних. *Центральноукраїнський науковий вісник. Технічні науки.* 2025. № 12(43), ч. II. С. 9–19. DOI: https://doi.org/10.32515/2664-262X.2025.12(43).2.9-19 – розроблено метод еволюційної адаптації політик ЗВД за умов дрейфу концепції з підтвердженим статистичним детектором змін.

2. Віжевський П. В., Савенко О. С. Стратегії виявлення та запобігання витокам даних у корпоративних мережах згідно генетичного алгоритму. *Information Technology: Computer Science, Software Engineering and Cyber Security.* 2025. № 4. С. 42–56. DOI: https://doi.org/10.32782/IT/2025-4-6 – розроблено метод класифікації документів за рівнем конфіденційності на основі генетичного алгоритму з хромосомним кодуванням продукційних правил.

3. Віжевський П. В., Кравчик Ю. В. Модель системи запобігання витоку даних з еволюційною адаптацією на основі генетичних алгоритмів. *Вісник Хмельницького національного університету. Серія: Технічні науки.* 2025. № 5. С. 429–436. DOI: https://doi.org/10.31891/2307-5732-2025-357-56 – розроблено модель системи запобігання витоку даних з еволюційною адаптацією та її формалізацію.

4. Віжевський П. В., Савенко О. С. Модель процесу виявлення витоків даних з еволюційною адаптацією. *Вимірювальна та обчислювальна техніка в технологічних процесах.* 2026. № 1. С. 270–277. DOI: https://doi.org/10.31891/2219-9365-2026-85-34 – розроблено модель процесу виявлення витоків даних з еволюційною адаптацією, що інтегрує моделі витоку, корпоративного середовища та даних.

5. Віжевський П. В., Савенко О. С. Поведінкове профілювання користувачів та виявлення аномалій на основі генетичного алгоритму. *Системні технології.* 2026. № 1 (162). С. 148–159. DOI: https://doi.org/10.34185/1562-9945-5-162-2026-17 – розроблено метод поведінкового профілювання користувачів на основі індивідуальних адаптивних профілів з генетичною оптимізацією їх конфігурації.

Праці, які засвідчують апробацію матеріалів дисертації

6. Rehida P., Savenko O., Sachenko A., Drozd A., Vizhevski P. A trust model that ensures the correctness of computing in grid computing system. *Proceedings of the 5th International Workshop on Intelligent Information Technologies and Systems of Information Security (IntelITSIS-2024)*, Khmelnytskyi, Ukraine, March 2024. Vol. 3675. P. 388–401. URL: https://ceur-ws.org/Vol-3675/paper28.pdf (Scopus) – реалізовано модуль оцінювання довіри, сформовано список інформації, яку можна збирати на обчислювальному елементі шляхом розширення його функціональності.

7. Golovko I., Savenko O., Vizhevskyi P., Sachenko A. Obfuscation process with machine learning module. 2024 *14th International Conference on Dependable Systems, Services and Technologies (DESSERT)*, Athens, Greece, 2024. P. 1–7. DOI: https://doi.org/10.1109/DESSERT65323.2024.11122185 (Scopus) – розроблено модуль машинного навчання для обфускації.

8. Golovko I., Savenko O., Vizhevskiy P., Klein O., Salem A.-B. M. Obfuscation technologies of high-level source code using artificial intelligence. *Proceedings of the 1st International Workshop on Intelligent & CyberPhysical Systems (ICyberPhyS-2024)*, Khmelnytskyi, Ukraine, June 28, 2024. Vol. 3736. P. 324–338. URL: https://ceur-ws.org/Vol-3736/paper24.pdf – розроблено методи обфускації вихідного коду з використанням штучного інтелекту.

9. Sachenko A., Vizhevskyi P., Savenko O., Ostroverkhov V., Maslyyak B. Modern strategies for data leak detection and prevention in corporate networks. *Modern Data Science Technologies Doctoral Consortium (MoDaST 2025)*, Lviv, Ukraine, June 15, 2025. P. 275–292. URL: https://ceur-ws.org/Vol-4005/paper19.pdf – розроблено стратегії виявлення та запобігання витокам даних у сучасних корпоративних мережах.

Публікації, які додатково відображають наукові результати дисертації

10. Свідоцтво про реєстрацію авторського права на твір (програму) № 144040 Україна. Комп'ютерна програма «Програмний комплекс запобігання витоку даних з еволюційною адаптацією на основі генетичних алгоритмів (ЗВДЕАГА)» / Віжевський П. В., Савенко О. С. Дата реєстрації 04.03.2026. URL: https://iprop-ua.com/cr/ny8dq30b/ – розроблено програмно-алгоритмічне забезпечення програмного комплексу запобігання витоку даних з еволюційною адаптацією.

8. Апробація дисертації. Апробацію основних положень, ідей і висновків дисертаційної роботи проведено на фаховому семінарі кафедри комп'ютерної інженерії та інформаційних систем Хмельницького національного університету. Наукові результати роботи доповідалися на таких конференціях: 5th International Workshop on Intelligent Information Technologies and Systems of Information Security (IntelITSIS-2024), Khmelnytskyi, Ukraine, March 2024; 14th IEEE International Conference on Dependable Systems, Services and Technologies (DESSERT-2024),

Athens, Greece, 2024; 1st International Workshop on Intelligent & CyberPhysical Systems (ICyberPhyS-2024), Khmelnytskyi, Ukraine, June 28, 2024; Modern Data Science Technologies Doctoral Consortium (MoDaST 2025), Lviv, Ukraine, June 15, 2025.

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 Віжевського Петра Володимировича
(прізвище, ініціали здобувача)
«Методи та засоби виявлення і запобігання витоку даних в корпоративних мережах згідно еволюційних алгоритмів»,
(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 «Методи та засоби виявлення і запобігання витоку даних в корпоративних мережах згідно еволюційних алгоритмів»,
(назва роботи)
подану Віжевським Петром Володимировичем
(прізвище, ім'я, по батькові)
на здобуття ступеня доктора філософії, до захисту.

Головуюча публічної презентації,
доктор філософії, доцент,
завідувачка кафедри КПС _____ Ольга ПАВЛОВА
(науковий ступінь, вчене звання, посада) підпис Ім'я ПРІЗВИЩЕ

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

Підпис дійсний
Відділ кадрів