https://doi.org/10.31891/2219-9365-2026-85-34
УДК 004.056.53:004.89

ВІЖЕВСЬКИЙ Петро
Хмельницький національний університет
https://orcid.org/0009-0009-4851-0839
e-mail: vizhevskyipv@khmnu.edu.ua
САВЕНКО Олег
Хмельницький національний університет
https://orcid.org/0000-0002-4104-745X
e-mail: savenko_oleg_st@ukr.net

МОДЕЛЬ ПРОЦЕСУ ВИЯВЛЕННЯ ВИТОКІВ ДАНИХ З ЕВОЛЮЦІЙНОЮ АДАПТАЦІЄЮ

У роботі запропоновано узагальнену модель процесу виявлення витоків даних з еволюційною адаптацією, побудовану на інтеграції трьох функціональних складових: класифікації документів за рівнем конфіденційності на основі генетичного алгоритму з IF-THEN правилами, виявлення дрейфу концепції через двовіконний статистичний детектор (критерій Колмогорова-Смірнова та t-тест) й адаптивного поведінкового профілювання користувачів із експоненціальним забуванням. Описано архітектуру DLP-системи. Показано механізм зворотного зв'язку, за яким детектор дрейфу підсилює мутацію в генетичному алгоритмі, а поведінковий модуль коригує порогові значення. Експериментальна оцінка на корпусі розсекречених урядових документів DISC (2 450 документів, три рівні конфіденційності) підтверджує: GA-класифікатор досягає F1 = 0,867, поступаючись ансамблевим методам лише на 5-6 %. при повній інтерпретованості правил, механізм адаптації підвищує prequential F1 на 7,6 %, а поведінковий детектор із генетичною оптимізацією ваг забезпечує FPR = 0,023. Модель зберігає повну інтерпретованість рішень, придатну для аудиту та верифікації експертами з безпеки.

Ключові слова: запобігання витоку даних; генетичні алгоритми; еволюційна адаптація; дрейф концепції; поведінкове профілювання; класифікація документів.

VIZHEVSKYI Petro, SAVENKO Oleg
Khmenlnystskyi National University

A MODEL OF THE DATA LEAKAGE DETECTION PROCESS WITH EVOLUTIONARY ADAPTATION

The paper presents a generalized model of the data leakage detection process with evolutionary adaptation, based on the integration of three functional components: document classification using a genetic algorithm with IF–THEN rules, concept drift detection through a dual-window statistical detector (Kolmogorov–Smirnov test and Student's t-test), and adaptive user behavioral profiling with exponential forgetting. The architecture of the proposed DLP system is described as a modular structure combining content analysis, behavioral monitoring, and adaptive parameter control.

A feedback mechanism is implemented to ensure dynamic adaptation. When the drift detector identifies statistically significant distributional changes in input features, it increases the mutation rate of the genetic algorithm, thereby accelerating the evolution of classification rules. Simultaneously, the behavioral profiling module adjusts decision thresholds according to updated user activity patterns. This coordinated interaction enables the system to adapt to evolving data characteristics and usage scenarios without requiring architectural modifications or retraining from scratch.

Experimental evaluation was conducted on the DISC corpus of declassified government documents (2,450 documents across three security levels). Results demonstrate that the genetic algorithm–based classifier achieves an F1-score of 0.867, trailing ensemble methods by only 5–6% while preserving full interpretability of decision rules. The evolutionary adaptation mechanism increases prequential F1 by 7.6%, confirming its effectiveness under streaming conditions with potential distribution shifts. In addition, the behavioral anomaly detector with genetically optimized feature weights achieves a low false positive rate (FPR = 0.023), improving operational reliability.

The proposed model maintains complete transparency of classification logic, making it suitable for audit, compliance verification, and expert validation in security-sensitive environments. Overall, the integration of evolutionary learning, statistical drift monitoring, and adaptive behavioral analysis forms a robust, interpretable, and practically deployable framework for data leakage prevention systems operating in dynamic organizational contexts.

Keywords: data leakage prevention; genetic algorithms; evolutionary adaptation; concept drift; behavioral profiling; document classificatio.

Стаття надійшла до редакції / Received 30.01.2026
Прийнята до друку / Accepted 22.02.2026
Опубліковано / Published 05.03.2026

ПОСТАНОВКА ПРОБЛЕМИ У ЗАГАЛЬНОМУ ВИГЛЯДІ ТА ЇЇ ЗВ'ЯЗОК ІЗ ВАЖЛИВИМИ НАУКОВИМИ ЧИ ПРАКТИЧНИМИ ЗАВДАННЯМИ

Міграція до хмарних платформ, поширення віддаленої роботи та інтенсивне використання сервісів обміну файлами збільшують кількість каналів, якими конфіденційні дані можуть покинути контрольований периметр організації. Огляд методів DLP [1] показує, що до 35 % випадків компрометації даних спричинені інсайдерами, дії яких часто не відрізнити від легітимної активності.

Комерційні DLP-рішення здебільшого спираються на заздалегідь визначені статичні правила та шаблони [1, 2]. Обмеження такого підходу це потреба ручного оновлення правил через зміни бізнес-процесів та неможливість реагувати на дрейф концепції внаслідок зміни поведінки користувачів. Внаслідок зміни проєктів, ролей чи інструментів моделі, навчені на історичних вибірках, поступово деградують [3, 4].

Існуючі дослідницькі підходи зосереджуються або на класифікації контенту, або на поведінковому аналізі, або на адаптації до дрейфу, однак не пропонують усі три складові в рамках єдиного адаптивного процесу [5, 6]. Методи на основі глибокого навчання функціонують як «чорні скриньки», що унеможливлює їх повноцінний аудит та верифікацію.

Це формує потребу в моделі процесу виявлення витоків, яка б комбінувала автоматичну адаптацію до змін у характері загроз, інтерпретованість рішень та інтеграцію контентного й поведінкового аналізу з єдиним еволюційним контуром оптимізації.

АНАЛІЗ ДОСЛІДЖЕНЬ ТА ПУБЛІКАЦІЙ

В дослідженнях запобігання витокам даних акцент поступово зміщується від сигнатурних методів до підходів на основі машинного навчання та поведінкового аналізу. Систематичний огляд [1] виокремлює три покоління DLP-систем: на основі регулярних виразів і ключових слів, на основі класичного ML (SVM, Random Forest) та на основі глибокого навчання. В роботі [2] запропоновано метод на основі DeBERTa-BiLSTM для класифікації чутливих текстових документів, що демонструє високу точність, однак не забезпечує пояснення рішень.

Систему виявлення інсайдерських загроз BRITD [5], що базується на ритмах поведінки з часовою динамікою та індивідуальною адаптацією, доповнюють підходи на основі глибокої кластеризації [6] та гібридних алгоритмів з поєднанням неконтрольованого й контрольованого навчання [7]. Ці методи підвищують точність детекції інсайдерів, проте не інтегрують контентний аналіз документів і не мають механізму еволюційної оптимізації параметрів.

Проблему дрейфу концепції у потокових даних систематизовано в оглядових роботах [3, 4]. Performance-aware детектори відстежують деградацію метрик класифікації, тоді як distribution-based підходи порівнюють статистичні характеристики послідовних часових вікон. Мультиагентний адаптивний підхід для систем виявлення вторгнень [11] демонструє ефективність адаптації до зміни характеру трафіку, а робота [10] поєднує генетичне програмування з інкрементальним навчанням для потокової класифікації під дрейфом.

Генетичні алгоритми (ГА) активно застосовуються у задачах кібербезпеки. Огляд [8] охоплює сучасний стан теорії та практики ГА, включаючи гібридні варіанти із самоадаптацією параметрів. У роботі [9] ГА використано для відбору ознак у системах виявлення вторгнень промислових систем управління, де деревоподібна кластеризація забезпечує різноманітність популяції.

Аналіз літератури засвідчує відсутність підходу, який би поєднував контентну класифікацію з інтерпретованими правилами, поведінкове профілювання та адаптацію до дрейфу.

ФОРМУЛЮВАННЯ ЦІЛЕЙ СТАТТІ

Метою роботи є розробка моделі системи запобігання витоку даних з еволюційною адаптацією, яка не деградуватиме за умов дрейфу концепції та дозволяє аналітику безпеки верифікувати логіку прийняття рішень.

ВИКЛАД ОСНОВНОГО МАТЕРІАЛУ

Модель DLP-системи з еволюційною адаптацією побудуємо за модульним принципом, вона складається з чотирьох функціональних модулів, кожен з яких відповідає за окремий аспект. Визначимо систему формально як кортеж:

$$S = \langle L_C, L_A, L_R, L_E, \Phi \rangle, \tag{1}$$

де L_C – рівень збору даних, L_A – рівень аналізу, L_R – рівень реагування, L_E – рівень еволюційної адаптації, Ф – множина функцій взаємодії між компонентами. Рівень збору даних агрегує інформацію з мережевого трафіку, кінцевих точок, хмарних платформ та систем автентифікації. Рівень аналізу виконує класифікацію документів за ступенем конфіденційності та оцінює відхилення поведінки користувачів від профілю. Рівень реагування реалізує захисні дії – блокування, карантин, сповіщення – на підставі комбінованої оцінки ризику. Рівень еволюційної адаптації функціонує як фоновий процес, що безперервно оптимізує параметри аналітичних моделей та політик безпеки засобами генетичного алгоритму. Узагальнена архітектура запропонованої DLP-системи зображена на рисунку 1.

ISSN 2219-9365

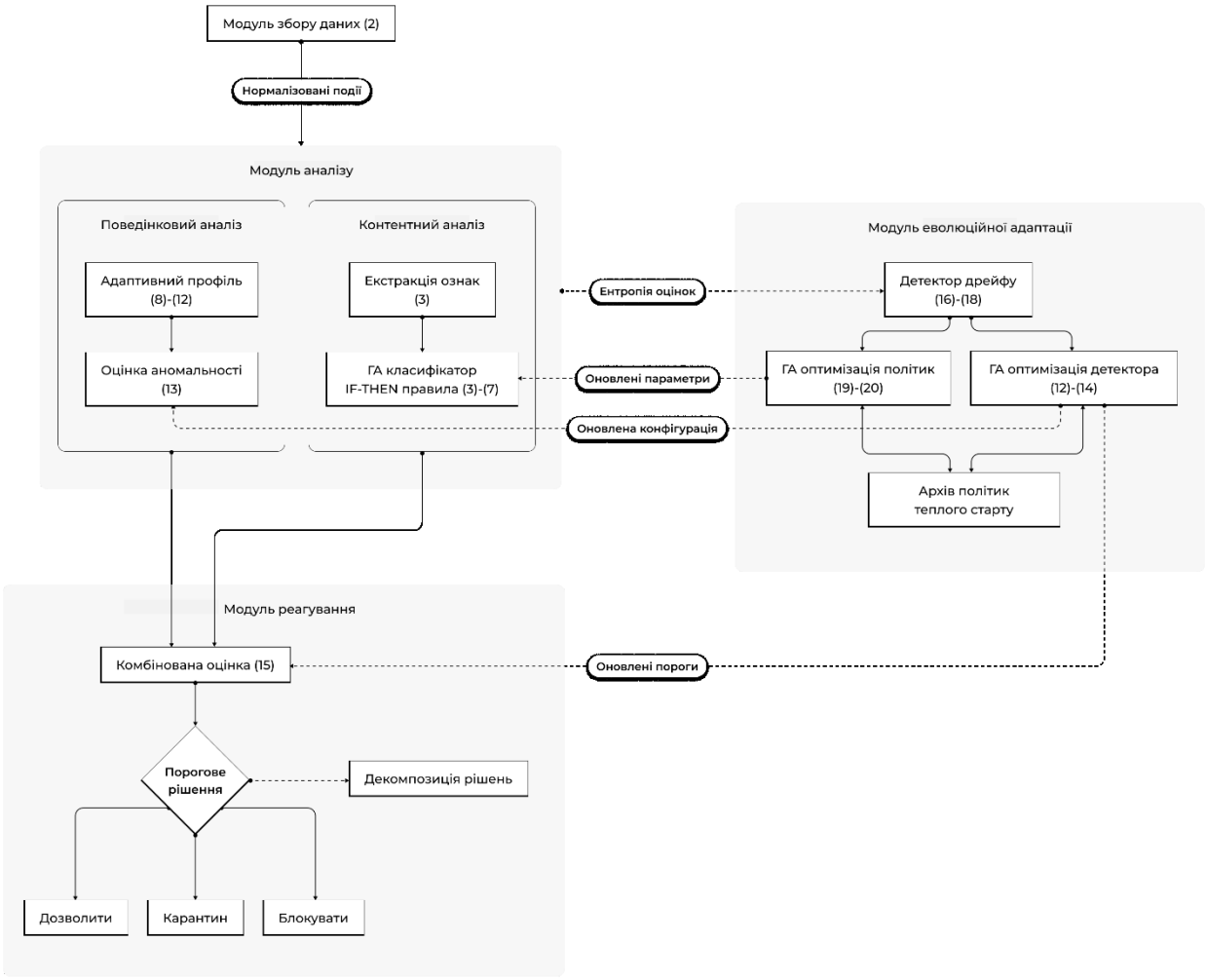

Рис. 1. Архітектура DLP-системи з еволюційною адаптацією

Рівень збору визначимо як множину спеціалізованих колекторів, кожен з яких відповідає за окремий канал надходження даних:

$$L_C = \{C_{net}, C_{end}, C_{cloud}, C_{auth}, C_{email}\}. \quad (2)$$

Мережевий колектор C_{net} здійснює DPI на рівні застосунків аналізуючи HTTP/HTTPS-трафік, поштові протоколи та файлові передачі. Колектор кінцевих точок C_{end} працює безпосередньо на ком'ютерах і серверах, фіксуючи файлові операції, активність буфера обміну, підключення зовнішніх носіїв та друк документів. Хмарний колектор C_{cloud} інтегрується з API інтерфейсами SaaS платформ для моніторингу операцій зі спільними документами, завантажень та наданням доступу. Колектори автентифікації C_{auth} та електронної пошти C_{email} відстежують події входу й вміст повідомлень.

Контентний аналіз базується на класифікаторі, що синтезує набір правил у формі IF-THEN за допомогою генетичного алгоритму. Кожне правило задає умови на конкретні ознаки документа та визначає ступінь належності до певного класу конфіденційності. Такий підхід забезпечує повну інтерпретованість та підтримку коригування правил вручну.

Правило складаємо з кон'юнкції елементарних умов, до якої приєднано цільовий клас та вагу для механізму голосування:

$$r = (C_1 \wedge C_2 \wedge \ldots \wedge C_n) \rightarrow (k, w), \quad (3)$$

Хромосомою кодуємо повний набір правил разом із бінарними прапорцями активності, що дозволяє генетичному алгоритму не лише оптимізувати параметри окремих правил, а й вмикати та вимикати правила:

$$G = \{(r_1, a_1), (r_2, a_2), \dots, (r_K, a_K)\}, \quad a_i \in \{0,1\}. \tag{4}$$

Якість набору правил оцінюємо функцією пристосованості, що враховує точність класифікації та штрафує надмірну складність:

$$F(G) = F_1(G) - \lambda \cdot X(G), \tag{5}$$

де $F_1(G)$ – F1-міра на валідаційній вибірці, $X(G)$ – нормована складність набору правил, λ – коефіцієнт регуляризації, що контролює баланс між точністю та компактністю.

Складність визначаємо як зважену суму кількості активних правил та умов у них:

$$X(G) = \frac{1}{K}\sum_{i=1}^{K} a_i \cdot (1 + \lambda_{cond} \cdot |C_i|). \tag{6}$$

де $|C_i|$ – кількість умов у правилі r_i, λ_{cond} – вага складності умов. Штраф за складність запобігає перенавчанню та сприяє генерації компактного набору правил.

Ініціалізація популяції поєднує два підходи: частина хромосом генерується випадково для забезпечення різноманітності, решта створюється евристично на основі статистик класів:

$$C_f = \big(f, \mu_f - \sigma_f, \mu_f + \sigma_f\big). \tag{7}$$

де μ_f та σ_f – середнє та стандартне відхилення значень ознаки f для документів. Евристичні хромосоми забезпечують «теплий старт» еволюції, оскільки початкові правила вже частково відповідають розподілу даних.

Еволюційний процес використовує турнірну селекцію з розміром турніру 3, одноточковий кросовер із ймовірністю $p_c = 0{,}8$ та мутацію порогових значень із ймовірністю $p_m = 0{,}02$. Елітизм гарантує збереження n_{elite} найкращих хромосом у наступному поколінні.

Поведінковий детектор аномалій будує індивідуальний профіль для кожного користувача на основі наступних ознак: часові патерни активності (розподіл подій протягом доби та тижня), обсяги і типи оброблюваних даних, мережева активність та характеристики контенту.

Оскільки поведінка користувачів змінюється у зв'язку з новими проєктами, обов'язками, профіль має адаптуватися, надаючи більшу вагу нещодавнім спостереженням. Для цього застосовуємо механізм експоненційного забування. Адаптивне середнє значення i-ї ознаки для користувача u в часовий крок k оновлюємо за рекурентною формулою:

$$\mu_i^u(k) = \rho \cdot \mu_i^u(k-1) + (1-\rho) \cdot x_i^u(k), \tag{8}$$

де $\rho \in (0,1)$ – коефіцієнт забування, що визначає швидкість відкидання минулих спостережень, $x_i^u(k)$ – поточне значення ознаки.

Адаптивну дисперсію оновлюємо аналогічно:

$$(\sigma_i^u(k))^2 = \rho \cdot (\sigma_i^u(k-1))^2 + (1-\rho) \cdot (x_i^u(k) - \mu_i^u(k))^2. \tag{9}$$

Для нормалізованої оцінки відхилення використовуємо z-score:

$$z_i^u(k) = \frac{x_i^u(k) - \mu_i^u(k)}{\sigma_i^u(k) + \varepsilon}. \tag{10}$$

де $\varepsilon > 0$ – мала константа для забезпечення чисельної стійкості

Загальну оцінку аномальності визначимо як зважену суму перетворених z-score за всіма активними ознаками:

$$S_{behavior}(k) = \sum_{i=1}^{m} b_i \cdot w_i \cdot \varphi\big(z_i^u(k)\big), \tag{11}$$

де $b_i \in \{0,1\}$ – індикатор включення i-ї ознаки, $w_i \geq 0$ – вага ознаки, $\varphi(z) = \max(0, z)$ – функція активації, що враховує лише позитивні відхилення (поведінка «більша за норму»).

Конфігурацію детектора (маска активних ознак, ваги та поріг) кодуємо як окрему хромосому, що оптимізується генетичним алгоритмом:

$$G_d = (B, W, \tau, \rho), \tag{12}$$

де $B = (b_1, \dots, b_m)$ – бінарна маска, $W = (w_1, \dots, w_m)$ – вектор ваг, τ – поріг тривоги, ρ – коефіцієнт забування.

Функція пристосованості детектора враховує якість виявлення, хибнопозитивну частку та стабільність потоку тривог:

$$F(G_d) = F_1(G_d) - \alpha \cdot FPR(G_d) - \beta \cdot CV_{alert}(G_d) - \gamma \cdot C(G_d) \quad (21), \tag{13}$$

де FPR – частка хибнопозитивних спрацювань, CV_{alert} – коефіцієнт варіації потоку тривог, α, β, γ – коефіцієнти штрафів. Штраф за волатильність потоку тривог CV_{alert} стимулює стабільне навантаження на аналітиків, запобігаючи ситуаціям, коли тривоги надходять нерівномірними сплесками.

Волатильність визначається як:

$$CV_{alert} = \frac{\sigma_A}{\bar{A}+\varepsilon}, \tag{14}$$

де σ_A – стандартне відхилення кількості тривог за часове вікно, $\bar{A}$ – середня кількість тривог.

Сукупна метрика ризику обчислюється як комбінація поведінкового та контетнтого аналізу:

$$R = \lambda \cdot S_{content} + (1 - \lambda) \cdot S_{behavior}$$

де λ – коефіцієнт балансу між компонентами.

Рівень реагування обирає конкретну дію відповідно до порогових значенн, які є частиною хромосоми політики. Для кожної згенерованої тривоги система обчислює відносний внесок окремих ознак:

$$CN_i^u(k) = \frac{b_i \cdot w_i \cdot \varphi\left(z_i^u(k)\right)}{S^u(k)+\varepsilon}. \tag{15}$$

Ця декомпозиція надає пояснення причин спрацювання детектора: які саме аспекти поведінки користувача відхилилися від норми та наскільки значним є кожне відхилення. Для DLP-систем, де рішення про блокування інформаційного потоку може зупинити критичний бізнес-процес, пояснюваність є операційною необхідністю.

Для виявлення дрейфу розроблено двовіконний статистичний детектор, що поєднує два незалежних джерела сигналу. Перше джерело відстежує невизначеність моделі: для кожної події e_t з оцінкою ризику s_t обчислюємо ентропію розподілу оцінки ризиків:

$$H(e_t) = -s_t \log s_t - (1 - s_t) \log(1 - s_t). \tag{16}$$

Детектор підтримує два ковзних вікна – W_{ref}, що відповідає стабільному періоду, та поточне W_{cur}. Сигнал дрейфу за невизначеністю формуємо на основі порівняння середніх значень ентропії у вікнах:

$$I_{drift}^H = \mathbb{1}\left[\frac{\bar{H}_{cur} - \bar{H}_{ref}}{\sigma_{ref}} > \kappa\right], \tag{17}$$

де $\bar{H}_{ref}$, $\bar{H}_{cur}$ – середні значення ентропії у відповідних вікнах, σ_{ref} – стандартне відхилення у референтному вікні, κ – поріг чутливості. Друге джерело сигналу моніторить зміни у розподілі ознак через двовибірковий тест Колмогорова-Смирнова для кожної ознаки f_j у парі вікон. Фінальний бінарний сигнал дрейфу формуємо як диз'юнкцію обох джерел:

$$I_{drift} = I^{H}_{drift} \vee I^{KS}_{drift}, \tag{18}$$

що забезпечує виявлення як деградації впевненості моделі, так і зміни розподілу ознак. Для запобігання хибним спрацюванням через випадкові флуктуації застосовується механізм підтвердження: адаптація активується лише після k послідовних детекцій дрейфу (типово $k = 3$), що є необхідною ціною за стабільність системи. Після виявлення дрейфу система ініціює еволюційну оптимізацію політик. Політику DLP-системи кодуємо як хромосому з параметрами реагування та навчання:

$$P = (\tau_q, \tau_b, W, \rho, \eta, \mu_0, \mu_1), \tag{19}$$

де τ_q – поріг карантину, τ_b – поріг блокування, $W = (w_1, \dots, w_5)$ – ваги складових цільової функції, ρ – параметр затухання, η – швидкість навчання, μ_0 та μ_1 – базова та додаткова інтенсивність мутації відповідно.

Якість політики оцінимо функцією пристосованості:

$$F(P) = \sum_{j=1}^{5} w_j \cdot J_j(P), \tag{20}$$

де J_1 – частка хибнонегативних спрацювань, J_2 – частка хибнопозитивних спрацювань, J_3 – затримка обробки подій, J_4 – складність політик, J_5 – стабільність потоку сповіщень. Цей набір критеріїв відображає компроміс: жорсткі політики знижують ризик витоків, але генерують надмірну кількість хибних тривог, які збільшуватимуть навантаження на аналітиків.

При виявленні дрейфу інтенсивність мутації автоматично збільшується, що розширює область пошуку в просторі параметрів:

$$\mu = \mu_0 + \mu_1 \cdot I_{drift}. \tag{21}$$

Підвищена мутація зберігається протягом перехідного періоду, достатнього для адаптації популяції до нових умов.

Окремим механізмом є архів політик із теплим стартом. Система зберігає політики, що продемонстрували високу ефективність за різних умов, разом із описом цих умов (розподіл типів подій, рівень активності, характеристики трафіку). При виявленні дрейфу архів перевіряється на наявність політики, ефективної за аналогічних обставин. Якщо така знайдена, вона включається до початкової популяції, що значно прискорює адаптацію до повторюваних патернів [10].

Для експериментальної оцінки обрано корпус DISC [12] – колекцію з 2 450 розсекречених урядових документів, розподілених за трьома рівнями конфіденційності: "UNCLASSIFIED" (963 документи), "SECRET" (1 341) та "TOP SECRET" (146). Документи охоплюють три тематичні напрямки: зовнішню політику щодо Афганістану, китайсько-американські відносини (1960–1998) та матеріали епохи Маркоса на Філіппінах (1965–1986). Задача класифікації за реальними грифами секретності безпосередньо відповідає задачі DLP-системи

Таблиця 1

Порівняння якості класифікації

Метод	Precision	Recall	F1
Запропонований	0,873	0,861	0,867
Random Forest	0,921	0,915	0,918
Gradient Boosting	0,929	0,922	0,925
SVM	0,894	0,881	0,887
Naive Bayes	0,842	0,798	0,819

Ласифікатор досягає F1 = 0,867, поступаючись ансамблевим методам (Random Forest 0,918; Gradient Boosting 0,925) на ~5– 6 в.п., проте випереджаючи Naive Bayes (0,819). SVM демонструє F1 = 0,887, що лише на 2 в.п. вище за запропонований метод. Перевагою GA-класифікатора є повна інтерпретованість: результат навчання – компактний набір правил типу «ЯКЩО tf-idf(‘classified’) > 0,04 ТА tf-idf(‘embassy’) > 0,02, ТО SECRET (вага 0,79)», що може бути безпосередньо верифікований аналітиком.

Механізм адаптації до дрейфу концепції перевірено на потоці даних із п’ятьма точками дрейфу різних типів: три раптових (sudden), одна поступова (gradual) та одна інкрементальна (incremental). Для оцінки механізму адаптації порівняно дві конфігурації: статичну модель (навчену на початковому вікні без подальшого оновлення) та адаптивну модель із запропонованим двовіконним детектором дрейфу та еволюційною оптимізацією.

Таблиця 2

Результати адаптації до дрейфу концепції

Конфігурація	Послідовне F1	Стандартне відхилення
Без адаптації	0,831	0,142
З адаптацією	0,894	0,098

Адаптивна модель забезпечує приріст послідовної F1 на 7,6 % (з 0,831 до 0,894) та зниження стандартного відхилення з 0,142 до 0,098. Статистичний детектор (KS-тест + t-тест) виявив 4 з 5 точок дрейфу (Recall = 0,80): усі раптові та інкрементальну, тоді як поступовий дрейф було виявлено із затримкою, що зумовлено повільною зміною розподілу. F1 детекції = 0,571. Поведінковий профілювальник із генетичною оптимізацією ваг досягає F1 = 0,449 при FPR = 0,023, тоді як фіксований профіль демонструє FPR = 0,991.

Час навчання GA-класифікатора на DISC (12,3 с) перевищує конкурентів, що зумовлено ітеративною природою еволюційного пошуку. Це обмеження є допустимим: навчання виконується офлайн і одноразово, а класифікація нового документа відбувається за мілісекунди. Адаптація політик виконується інкрементально без повного перенавчання.

Таким чином, запропонована модель є єдиною серед розглянутих, що поєднує конкурентоспроможну точність, повну інтерпретованість та вбудовану адаптивність до дрейфу концепції.

ВИСНОВКИ З ДАНОГО ДОСЛІДЖЕННЯ І ПЕРСПЕКТИВИ ПОДАЛЬШИХ РОЗВІДОК У ДАНОМУ НАПРЯМІ

Розроблено узагальнену модель процесу виявлення витоків даних з еволюційною адаптацією, що інтегрує три складові в єдину модульну архітектуру: класифікацію документів на основі генетичного алгоритму з IF-THEN правилами, двовіконний статистичний детектор дрейфу концепції та адаптивне поведінкове профілювання з експоненціальним забуванням. Формалізовано замкнений контур зворотного зв'язку, де виявлення дрейфу автоматично підсилює мутацію в ГА, а архів ефективних політик забезпечує теплий старт при повторних паттернах.

Експериментальна оцінка на корпусі розсекречених урядових документів DISC підтвердила працездатність моделі. GA-класифікатор досягає F1 = 0,867, поступаючись ансамблевим методам на 5- 6 % при повній інтерпретованості правил. Механізм адаптації підвищує послідовну F1 на 7,6 %. Поведінковий детектор із генетичною оптимізацією забезпечує FPR = 0,023, що на порядки менше за фіксований профіль (0,991). Перспективним напрямком роботи є інтеграція нейромереж для екстракції ознак, що дозволить GA-класифікатору працювати з компактними представленнями ознак замість високорозмірних TF-IDF векторів документів.

Література

1. Herrera Montano I., García Aranda J. J., Ramos Diaz J., Molina Cardín S., de la Torre Díez I. Survey of Techniques on Data Leakage Protection and Methods to address the Insider threat. *Cluster Computing.* 2022. Vol. 25. P. 4289–4302. https://doi.org/10.1007/s10586-022-03668-2

2. Miao W., Zhao X., Zhang Y., Chen S., Li X., Li Q. A Deep Learning-Based Method for Preventing Data Leakage in Electric Power Industrial Internet of Things Business Data Interactions. *Sensors.* 2024. Vol. 24, № 13. Art. 4069. https://doi.org/10.3390/s24134069

3. Bayram F., Ahmed B. S., Kassler A. From concept drift to model degradation: An overview on performance-aware drift detectors. *Knowledge-Based Systems.* 2022. Vol. 245. Art. 108632. https://doi.org/10.1016/j.knosys.2022.108632.

4. Hinder F., Vaquet V., Hammer B. One or two things we know about concept drift – A survey on monitoring in evolving environments. Part A: Detecting concept drift. *Frontiers in Artificial Intelligence.* 2024. Vol. 7. Art. 1330257. https://doi.org/10.3389/frai.2024.1330257.

5. Song S., Gao N., Zhang Y., Ma C. BRITD: behavior rhythm insider threat detection with time awareness and user adaptation. *Cybersecurity.* 2024. Vol. 7. Art. 2. https://doi.org/10.1186/s42400-023-00190-9.

6. Wang J., Sun Q., Zhou C. Insider Threat Detection Based on Deep Clustering of Multi-Source Behavioral Events. *Applied Sciences.* 2023. Vol. 13, № 24. Art. 13021. https://doi.org/10.3390/app132413021.

7. Yi J., Tian Y. Insider Threat Detection Model Enhancement Using Hybrid Algorithms between Unsupervised and Supervised Learning. *Electronics.* 2024. Vol. 13, № 5. Art. 973. https://doi.org/10.3390/electronics13050973.

8. Katoch S., Chauhan S. S., Kumar V. A review on genetic algorithm: Past, present, and future. *Multimedia Tools and Applications.* 2021. Vol. 80. P. 8091–8126. https://doi.org/10.1007/s11042-020-10139-6.

9. Fang Y., Yao Y., Lin X., Wang J., Zhai H. A feature selection based on genetic algorithm for intrusion detection of industrial control systems. *Computers & Security.* 2024. Vol. 139. Art. 103675. https://doi.org/10.1016/j.cose.2023.103675.

10. Shyaa M. A., Zainol Z., Abdullah R., Anbar M., Alzubaidi L., Santamaria J. Enhanced Intrusion Detection with Data Stream Classification and Concept Drift Guided by the Incremental Learning Genetic

Programming Combiner. *Sensors.* 2023. Vol. 23, № 7. Art. 3736. https://doi.org/10.3390/s23073736.

11. Soltani M., Khajavi K., Jafari Siavoshani M., Jahangir A. H. A multi-agent adaptive deep learning framework for online intrusion detection. *Cybersecurity.* 2024. Vol. 7. Art. 9. https://doi.org/10.1186/s42400-023-00199-0.

12. Bass E., Albanese M., Zampieri M. DISC: A Dataset for Information Security Classification. *Proceedings of the 21st International Conference on Security and Cryptography (SECRYPT).* 2024. P. 175–185. https://doi.org/10.5220/0012763400003767.

References

1. Herrera Montano, I., García Aranda, J. J., Ramos Diaz, J., Molina Cardín, S., & de la Torre Díez, I. (2022). Survey of Techniques on Data Leakage Protection and Methods to address the Insider threat. *Cluster Computing,* 25, 4289–4302. https://doi.org/10.1007/s10586-022-03668-2

2. Miao, W., Zhao, X., Zhang, Y., Chen, S., Li, X., & Li, Q. (2024). A Deep Learning-Based Method for Preventing Data Leakage in Electric Power Industrial Internet of Things Business Data Interactions. *Sensors,* 24(13), 4069. https://doi.org/10.3390/s24134069

3. Bayram, F., Ahmed, B. S., & Kassler, A. (2022). From concept drift to model degradation: An overview on performance-aware drift detectors. *Knowledge-Based Systems,* 245, 108632. https://doi.org/10.1016/j.knosys.2022.108632

4. Hinder, F., Vaquet, V., & Hammer, B. (2024). One or two things we know about concept drift – A survey on monitoring in evolving environments. Part A: Detecting concept drift. *Frontiers in Artificial Intelligence,* 7, 1330257. https://doi.org/10.3389/frai.2024.1330257

5. Song, S., Gao, N., Zhang, Y., & Ma, C. (2024). BRITD: behavior rhythm insider threat detection with time awareness and user adaptation. *Cybersecurity,* 7, 2. https://doi.org/10.1186/s42400-023-00190-9

6. Wang, J., Sun, Q., & Zhou, C. (2023). Insider Threat Detection Based on Deep Clustering of Multi-Source Behavioral Events. *Applied Sciences,* 13(24), 13021. https://doi.org/10.3390/app132413021

7. Yi, J., & Tian, Y. (2024). Insider Threat Detection Model Enhancement Using Hybrid Algorithms between Unsupervised and Supervised Learning. *Electronics,* 13(5), 973. https://doi.org/10.3390/electronics13050973

8. Katoch, S., Chauhan, S. S., & Kumar, V. (2021). A review on genetic algorithm: Past, present, and future. *Multimedia Tools and Applications,* 80, 8091–8126. https://doi.org/10.1007/s11042-020-10139-6

9. Fang, Y., Yao, Y., Lin, X., Wang, J., & Zhai, H. (2024). A feature selection based on genetic algorithm for intrusion detection of industrial control systems. *Computers & Security,* 139, 103675. https://doi.org/10.1016/j.cose.2023.103675

10. Shyaa, M. A., Zainol, Z., Abdullah, R., Anbar, M., Alzubaidi, L., & Santamaria, J. (2023). Enhanced Intrusion Detection with Data Stream Classification and Concept Drift Guided by the Incremental Learning Genetic Programming Combiner. *Sensors,* 23(7), 3736. https://doi.org/10.3390/s23073736

11. Soltani, M., Khajavi, K., Jafari Siavoshani, M., & Jahangir, A. H. (2024). A multi-agent adaptive deep learning framework for online intrusion detection. *Cybersecurity,* 7, 9. https://doi.org/10.1186/s42400-023-00199-0

12. Bass, E., Albanese, M., & Zampieri, M. (2024). DISC: A Dataset for Information Security Classification. In *Proceedings of the 21st International Conference on Security and Cryptography (SECRYPT)* (pp. 175–185). SciTePress. https://doi.org/10.5220/0012763400003767