DOI https://doi.org/10.32689/maup.it.2026.2.13
УДК 004.8
JEL Classification: C 45, C 63, C 44

АДАПТАЦІЯ ІНФОРМАЦІЙНО-ЕКСТРЕМАЛЬНОЇ ІНТЕЛЕКТУАЛЬНОЇ ТЕХНОЛОГІЇ ДО АНАЛІЗУ ВЕЛИКИХ ДАНИХ НА ПРИКЛАДІ ЖУРНАЛІВ ПОДІЙ OFFICE 365

К. Є. Шамонін, Д. В. Прилепа

ADAPTATION OF INFORMATION-EXTREME INTELLIGENT TECHNOLOGY TO BIG DATA ANALYSIS ON THE EXAMPLE OF OFFICE 365 EVENT LOGS

Kiril Shamonin, Dmytro Prylepa

Анотація

Об'єктом дослідження є інтелектуальна система підтримки прийняття рішень (СППР) для виявлення кіберзагроз у журналах аудиту хмарної платформи Microsoft Office 365, орієнтована на умови малого та середнього бізнесу (МСБ).

Проблема, що вирішувалася, полягає у відсутності доступних інструментів виявлення прихованих кібератак для організацій, що не мають у штаті великої команди фахівців з кібербезпеки. Існуючі рішення на базі глибокого навчання вимагають значних обчислювальних ресурсів і є непрозорими «чорними скриньками», рішення яких аналітик без профільної підготовки не здатен ні перевірити, ні пояснити керівництву.

Суть отриманих результатів полягає у розробці 4-етапного конвеєра попередньої обробки O365 IEI-Pipeline та синтезі СППР на засадах IEI-технології. Повний цикл обробки 93 379 рядків телеметрії займає 6,4 секунди на стандартному обладнанні. Синтезована СППР досягла нульової помилки другого роду (β = 0) на етапі навчання та ідентифікувала приховану атаку Data Exfiltration у 61,1 % тестових векторів без жодного хибного спрацювання на нормальному трафіку.

Ключовою відмінністю є інтерпретованість рішень: кожне попередження системи пояснюється через конкретні відхилення поведінкових ознак від еталону норми у бінарному просторі, що дозволяє IT-спеціалісту загального профілю зрозуміти причину спрацювання без глибоких знань з машинного навчання. Система належить до класу Explainable AI, на відміну від непрозорих Transformer-архітектур.

Результати пояснюються інформаційним критерієм Кульбака та оптимізованою системою контрольних допусків, що формує геометрично чіткі межі між класами нормальної поведінки та аномалій.

Практичне використання є доцільним у компаніях МСБ, що використовують Microsoft Office 365, за умов відсутності виділеного SOC-центру: система потребує мінімальних обчислювальних ресурсів, не вимагає спеціалізованої інфраструктури та забезпечує прозору аргументацію кожного рішення для нетехнічного персоналу.

Ключові слова: *інтелектуальний аналіз даних, інформаційно-екстремальна інтелектуальна технологія, оцінювання функціональної ефективності, виявлення аномалій, кібербезпека.*

Abstract

The object of the study is an intelligent decision support system (DSS) for cyber threat detection in Microsoft Office 365 audit logs, designed to meet the operational constraints of small and medium-sized businesses (SMBs).

The problem addressed is the lack of accessible tools for detecting covert cyberattacks in organizations without a dedicated cybersecurity team. Existing deep learning-based solutions demand substantial computational resources and operate as opaque black boxes, whose outputs a non-specialist analyst can neither verify nor explain to management.

The core result is the development of a four-stage preprocessing pipeline, O365 IEI-Pipeline, and the synthesis of a DSS based on Information-Extreme Intelligent Technology (IEIT). The complete processing cycle for 93,379 telemetry records takes 6.4 seconds on standard hardware. The synthesized DSS achieved a zero type-II error rate (β = 0) during the training phase and successfully identified a covert Data Exfiltration attack in 61.1% of test feature vectors with no false positives on normal traffic.

The key distinguishing feature is decision interpretability: every system alert is explained through specific deviations of behavioral features from the reference norm in binary space, enabling a general-purpose IT specialist to understand the reason for each detection without deep knowledge of machine learning. The system belongs to the Explainable AI class, in contrast to opaque Transformer-based architectures.

The results are attributed to the Kullback information criterion and an optimized tolerance control system, which establishes geometrically well-defined boundaries between the normal behavior and anomaly classes.

Practical application is advisable for SMB companies using Microsoft Office 365 in the absence of a dedicated SOC: the system requires minimal computational resources, demands no specialized infrastructure, and provides transparent, human-readable justification for every decision to non-technical staff.

Key words: *intellectual data analysis, information-extreme intellectual technology, functional performance evaluation, anomaly detection, cybersecurity.*

© Шамонін К. Є., Прилепа Д. В., 2026
Стаття поширюється на умовах ліцензії відкритого доступу CC BY 4.0

1. Вступ. Одним із перспективних напрямів підвищення ефективності кіберзахисту корпоративних інформаційних систем, що функціонують за умов апріорної невизначеності та дії неконтрольованих зовнішніх факторів, є розроблення інтелектуальних систем підтримки прийняття рішень (СППР) на засадах машинного навчання. Сучасні підприємства щоденно генерують масиви телеметрії, що підпадають під категорію великих даних (Big Data): журнали доступу SaaS-платформ, події операційних технологій (OT), метрики серверного обладнання та трафік пристроїв IoT.

Типовим прикладом є хмарна платформа Microsoft Office 365. Організація зі штатом у 50 користувачів здатна генерувати від 40 000 до 2 000 000 рядків аудит-подій на добу, кожен з яких описується понад 100 різнотипними ознаками: від бінарних маркерів до складних JSON-об'єктів та довільних текстових рядків. Застосування традиційних сигнатурних систем виявлення вторгнень (IDS) або статичних SIEM-правил для аналізу таких слабоформалізованих потоків є вкрай неефективним, а ручний аналіз практично неможливим.

Проблема є особливо гострою для підприємств малого та середнього бізнесу (МСБ), де відсутні виділені SOC-центри та великі команди фахівців з кібербезпеки. За даними аналітичних звітів галузі, понад 60 % кіберінцидентів у секторі МСБ залишаються невиявленими понад 200 днів, що пояснюється не відсутністю даних, а відсутністю інструментів їх інтерпретованого аналізу. Тому розробка доступних, прозорих і ресурсоефективних систем виявлення аномалій є актуальною науково-практичною задачею.

Значна кількість досліджень сфокусована на застосуванні архітектур глибокого навчання, зокрема рекурентних нейронних мереж (LSTM) та моделей Transformer, для аналізу потокової мережевої телеметрії [1, 2, 3]. Проте такі системи характеризуються суттєвими практичними недоліками: вимагають значних обчислювальних ресурсів, є вразливими до змагальних атак (Adversarial ML) і функціонують як непрозорі «чорні скриньки», рішення яких аналітик без профільної підготовки не здатен ні перевірити, ні пояснити керівництву [4, 5].

На противагу методам «чорної скриньки», у сфері практичної кібербезпеки стрімко зростає потреба у прозорому штучному інтелекті (Explainable AI, XAI) [4, 5]. Аналітики SOC-центрів та IT-спеціалісти загального профілю повинні розуміти логічну причину кожного спрацювання системи. Інформаційно-екстремальна інтелектуальна технологія (IEI-технологія) за своєю математичною природою належить до класу XAI: вона дозволяє пояснити кожне рішення СППР через геометрію гіперсферичних контейнерів класів у бінарному просторі ознак [6, 7, 8]. При цьому навчання у редукованому бінарному просторі вимагає на порядки менше обчислювальних ресурсів порівняно з Transformer-архітектурами.

Надзвичайно важливим аспектом роботи з телеметрією Big Data є забезпечення конфіденційності (Privacy-Preserving) [9]. Пряма обробка сирих журналів O365 несе ризики деанонімізації через транзакційні ідентифікатори та кореляційні мітки. Математично обґрунтовані процедури редукції простору ознак виступають не лише інструментом подолання «прокляття розмірності», але й механізмом захисту персональних даних.

Незважаючи на успішне застосування IEI-технології у задачах психоемоційної діагностики [10], розпізнавання електроміографічних біосигналів за розрідженими навчальними матрицями [11], інтелектуального аналізу якості освітнього контенту [12], питання адаптації цього формалізованого апарату до аналізу гетерогенних журналів IT-аудиту залишається недостатньо дослідженим. Зокрема, не розв'язаною є задача подолання феномену Белмана («прокляття розмірності») при застосуванні IEI до масивів Big Data надвисокої розмірності та структурної гетерогенності.

Метою дослідження є підвищення функціональної ефективності розпізнавання аномалій у масивах Big Data шляхом інформаційного аналізу і синтезу СППР у рамках IEI-технології. Це дасть можливість забезпечити інтерпретоване виявлення прихованих кіберзагроз на підприємствах МСБ без необхідності залучення вузькопрофільних фахівців з машинного навчання.

Для досягнення мети були поставлені такі задачі:

1. Розробити метод та алгоритм компонування навчальної матриці з урахуванням структурної гетерогенності ознак розпізнавання та необхідності редукції їх розмірності.

2. Дослідити вплив часової агрегації векторів-реалізацій на формування геометричних меж класів розпізнавання та визначити оптимальну ширину часового вікна τ.

3. Обґрунтувати вибір інформаційного критерію функціональної ефективності (КФЕ) та реалізувати алгоритм паралельної оптимізації системи контрольних допусків (СКД).

4. Здійснити інформаційний синтез СППР та провести її екзаменаційне тестування на прикладі ідентифікації прихованої атаки Data Exfiltration у потоках журналів Office 365.

2. Матеріали та методи. Об'єктом дослідження є процес інформаційного синтезу СППР для виявлення кіберзагроз у масивах телеметрії хмарної платформи Microsoft Office 365.

Основна гіпотеза дослідження полягає в тому, що послідовне застосування евристичної редукції простору ознак, гетерогенного кодування атрибутів та оптимальної часової агрегації векторів-реалізацій дозволяє усунути математичні обмеження IEI-технології в умовах Big Data та забезпечити надійне розведення класів розпізнавання у бінарному просторі ознак.

Прийняті спрощення та припущення: усі дані є синтетично сформованими спеціально розробленим генератором, що відтворює структуру O365 Audit Log API зі 108 реальними полями та поведінковий патерн атаки Data Exfiltration. Використання синтетичних даних є галузевим стандартом в академічних дослідженнях з кібербезпеки [1] і обумовлене обмеженнями конфіденційності при роботі з реальними виробничими журналами. Генератор відтворює: гаусовий часовий профіль активності з піком 08:00–18:00; поведінковий патерн атаки Data Exfiltration у вигляді аномального зростання показника FileDownloaded у 11–17 разів. Загальний обсяг вхідного потоку складає 93 379 рядків за 48-годинний період (приблизно 45 000 подій на добу для 8 користувачів). Алфавіт класів розпізнавання: $\Omega = \{\omega_1, \omega_2\}$, де ω_1 – базовий клас нормальної ділової активності, ω_2 – клас аномальної зловмисної поведінки.

Теоретичною основою дослідження слугує математичний апарат IEI-технології, розроблений науковою школою Довбиша А. С. [6, 7, 8]. У рамках цього апарату процес перетворення навчальної матриці дійсних значень у бінарну матрицю здійснюється накладанням системи контрольних допусків (СКД) на кожну і-ту ознаку розпізнавання (1, 2):

$$\overline{Y}_i = \frac{1}{n}\sum_j Y_{1,ij}, \quad VD_i = \overline{Y}_i + \delta, \quad ND_i = \overline{Y}_i - \delta \tag{1}$$

$$X_{k,i}(j) = \begin{cases} 1, & де\ ND_i < Y_{k,i}(j) < VD_i \\ 0, & інакше \end{cases} \tag{2}$$

де δ – ширина поля допусків, що підлягає оптимізації; VD_i та ND_i – верхній та нижній допуски СКД.

Оцінювання функціональної ефективності розбиття простору ознак на класи розпізнавання здійснюється за інформаційною мірою Кульбака [6] (3):

$$E_k = \frac{1}{n}\log_2\left\{\frac{2n - K_2 - K_3 + \varepsilon}{K_2 + K_3 + \varepsilon}\cdot(n - K_2 - K_3)\right\} \tag{3}$$

де n – кількість векторів-реалізацій у навчальній вибірці; K_2 – кількість хибних розпізнавань власних реалізацій; K_3 – кількість хибних розпізнавань чужих реалізацій; ε = 0,1 – параметр регуляризації. Робоча зона КФЕ визначається як сукупність радіусів контейнерів, де достовірності розпізнавання перевищують 0,5, а сам радіус не перевищує міжеталонну відстань.

Для структурно-параметричної ідентифікації СППР застосовано алгоритм паралельного навчання [13]. Оптимальне поле допусків δ* визначається шляхом ітераційного перебору значень, що максимізують усереднений КФЕ по всіх класах (4):

$$\delta^* = \arg\max_\delta\left\{\frac{1}{M}\sum_k \max_{d\in WZ_k} E_k(d)\right\} \tag{4}$$

Для вирішення задачі 1 запропоновано 4-етапний конвеєр попередньої обробки O365 IEI-Pipeline, реалізований у вигляді єдиного Python-скрипту. Вхідний потік характеризується такими параметрами: N = 108 ознак різного типу, 93 379 рядків за 48 годин, 8 суб'єктів моніторингу. Конвеєр долає шість ключових обмежень IEI-технології в умовах Big Data: прокляття розмірності, нечислові ознаки, різні шкали вимірювань, надмірна гранулярність часового ряду, незбалансованість класів та концептуальний дрейф телеметрії.

Статистичний контроль інтенсивності потоку (етап 1) здійснюється за допомогою двох взаємодоповнювальних непараметричних критеріїв. Критерій Вальда–Вольфовіца перевіряє стаціонарність за кількістю серій відносно медіани (5):

$$Z = \frac{R - \mu_R}{\sigma_R}, \qquad p = 2\cdot\left(1 - \Phi(|Z|)\right) \tag{5}$$

де R – кількість серій у вибірці, μ^R і σ^R – теоретичні очікування та середньоквадратичне відхилення. Критерій Фішера порівнює локальну дисперсію ковзного вікна з глобальною дисперсією потоку (6):

$$F = \frac{\sigma^2_{\text{loc}}}{\sigma^2_{\text{glob}}}, \qquad p = 1 - F_{\text{CDF}}(F; df_1, df_2) \tag{6}$$

Тригер аномалії це одночасне виконання умов $p_{WW} < 0{,}05$ та $p_{Fisher} < 0{,}05$ при $\sigma^2_{loc} > \sigma^2_{glob}$.

Евристична редукція простору ознак (етап 2) здійснюється у два кроки. Перший – це видалення за списком виключень (Blacklist): транзакційні ідентифікатори (GUID, CorrelationId, TokenId), технічні метадані версій, вкладені JSON-структури – 44 атрибути. Blacklist-фільтрація виконує подвійну функцію: усуває атрибути без класифікаційного сигналу та видаляє прямі персональні ідентифікатори, реалізуючи базовий механізм Privacy-Preserving [9]. Другий крок – автоматичне видалення атрибутів з нульовою дисперсією (константи та 100 % порожні поля) – 24 атрибути. Результат: зменшення розмірності з N = 108 до N = 32 (скорочення на 70,4 %), оперативна пам'ять зменшується зі 156 МБ до 47 МБ.

Гетерогенне кодування атрибутів (етап 3) застосовується диференційовано залежно від кардинальності ознак (таблиця 1). Критичним є обмеження OHE до Top-30 категорій: без ліміту атрибут з тисячами унікальних значень породив би тисячі бінарних стовпців і повернув проблему надмірної розмірності.

Таблиця 1

Маршрутизатор методів гетерогенного кодування ознак розпізнавання

Метод кодування	Критерій застосування	Приклади ознак O365
One-Hot Encoding (OHE)	Кардинальність < 30; семантично чіткі категорії	ResultStatus, IsManagedDevice
Частотне кодування (Freq)	Кардинальність > 30; рідкість = аномалія	ClientIP, UserAgent, Operation
Feature Hashing	Нескінченна кардинальність; рядки	SiteUrl, ObjectId, FileName

Часова агрегація векторів-реалізацій (етап 4) здійснюється у вікна фіксованої ширини τ для кожного суб'єкта. Порожні вікна без активності заповнюються нульовим вектором (Zero-Padding), зберігаючи безперервність часового ряду (7):

$$Y_m^{(c)}(\tau) = 0, якщо l \in L : user l = c, tl \in \tau = 0 \quad (7)$$

Рішення щодо класової належності кожного нового вектора-реалізації x_e приймається на основі функції належності (8):

$$\mu_k = 1 - \frac{d\left(\mathbf{x}_k^* \oplus \mathbf{x}_e\right)}{d_k^*} \quad (8)$$

де x^*_k – еталонний вектор k-го класу; d^*_k – оптимальний радіус його контейнера; $\oplus$ – операція XOR (відстань Хеммінга). Рішення: $k^* = \arg\max_k \mu_k$, якщо $\max \mu_k \geq 0$; інакше NAN (поза алфавітом класів).

Обчислювальна реалізація конвеєра виконана мовою Python з використанням бібліотек pandas, numpy та scipy. Паралельна оптимізація СКД реалізована засобами multiprocessing. Тестове середовище: стандартний персональний комп'ютер без спеціалізованого обладнання для машинного навчання.

3. Результати та обговорення.

3.1. Розробка методу компонування навчальної матриці. За результатами реалізації 4-етапного конвеєра попередньої обробки O365 IEI-Pipeline отримано структуровану навчальну матрицю, придатну для обробки засобами IEI-технології. Повний цикл обробки 93 379 рядків × 108 ознак займає 6,4 секунди на стандартному обладнанні.

Ключовим результатом етапу евристичної редукції є зменшення розмірності простору ознак з N = 108 до N = 32 (скорочення на 70,4 %). При цьому міжеталонна відстань Хеммінга, яка при N = 108 вироджувалася до dc → 0 через феномен Белмана, після редукції набула практично значущого рівня dc = 7. На відміну від методів автоматичного відбору ознак на основі взаємної інформації [14] та архітектур глибокого навчання типу Transformer [15], запропонований підхід не потребує навчальних міток на етапі редукції, що є суттєвою перевагою у реальних умовах з обмеженою кількістю розмічених даних.

Схему запропонованого конвеєра наведено на рисунку 1. Важливо, що Blacklist-фільтрація виконує подвійну функцію: усуває атрибути без класифікаційного сигналу та видаляє прямі персональні ідентифікатори (ObjectId, AADTenantId, MailboxOwnerSid), реалізуючи механізм Privacy-Preserving [9]. Це є важливим аспектом при розгортанні системи в умовах дії регуляторних вимог щодо захисту персональних даних.

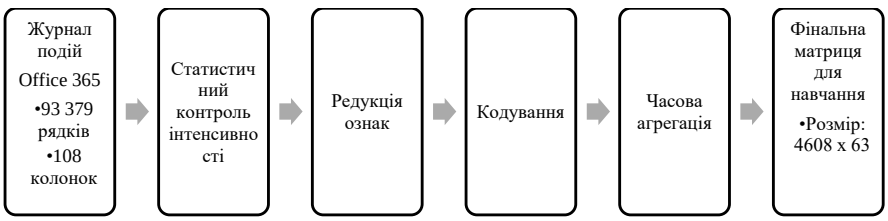


Рис. 1. Конвеєр попередньої обробки O365 IEI-Pipeline

ISSN 2786-5460 (Print), ISSN 2786-5479 (Online)

3.2. Дослідження впливу часової агрегації на якість навчання. Встановлено, що застосування стандартної гранулярності τ = 5 хв є хибним рішенням: поведінка суб'єкта на таких коротких відрізках є вкрай нестабільною, внутрішньокласовий розкид є надмірним, а еталонні вектори двох класів математично збігаються (dc → 0). Таблиця 2 демонструє цю залежність кількісно та обґрунтовує вибір τ* = 2 год як оптимального значення.

Таблиця 2

Залежність якості навчання СППР від ширини вікна агрегації τ

Вікно τ	Вект./суб'єкт	dc між класами	Робоча зона WZ	Аномалій (EXAM)	Придатність
5 хв (вихідне)	576	0–1	Відсутня	–	Непридатне
1 год	48	7–8	Вузька (1 рядок)	≈ 50 %	Нестабільне
2 год	36	7	Широка [5..6]	61,1 %	Оптимальне
3 год	16	13	Широка [0..12]	61,1 %	Прийнятне
6 год	8	15	Широка	77,8 %	Мало даних
12 год	4	–	Відсутня	–	Замало даних

Витончені атаки типу Data Exfiltration (Slow and Low) маскуються під нормальну роботу суб'єкта, формують типовий двогорбий денний профіль і є статистично нерозрізненними від нормального трафіку (рисунок 2). Саме такі «тихі» аномалії формують потребу у застосуванні IEI-технології для пошуку прихованих закономірностей у багатовимірному просторі ознак.



Рис. 2. Типовий розподіл потоку подій O365 з двогорбим денним профілем

Агрегація τ* = 2 год дозволяє повністю усунути проблему виродження міжеталонної відстані (dc = 0 при τ = 5 хв → dc = 7 при τ = 2 год) та формує стабільну широку робочу зону КФЕ WZ [5, 6]. Вибір τ = 6 год та τ = 12 год, попри більший dc, є неприйнятним через критично малу кількість векторів-реалізацій (8 та 4 відповідно), що унеможливлює статистично значущу оцінку ефективності. Даний висновок узгоджується з теоретичними положеннями IEI-технології щодо мінімально необхідного обсягу навчальної вибірки [7].

3.3. Інформаційний синтез СППР та оптимізація системи контрольних допусків. Навчання СППР виконано на 2-годинних поведінкових профілях суб'єкта carol.white@contoso.com. Сформовано дві навчальні вибірки: X_1 (базовий клас нормальної ділової активності ω_1, $n_1 = 36$ векторів-реалізацій) та X_2 (клас аномальної поведінки ω_2, $n_2 = 36$ векторів-реалізацій). Кожен вектор-реалізація описується 58 ознаками розпізнавання.

У процесі оптимізації алгоритм ітеративно розширював симетричне поле допусків δ, формуючи СКД на кожну з 58 ознак. Оптимальне поле допусків стабілізувалося на позначці δ* = 8,5. Розрахована міжеталонна кодова відстань Хеммінга dc = 7, оптимальний радіус гіперсферичного контейнера класу атаки d* = 6. Максимальне значення КФЕ досягло Eatk* = 1,0005, що у термінах теорії інформації свідчить про надзвичайно високу інформаційну спроможність обраної системи ознак. Головним результатом є нульове значення помилки другого роду для класу атаки ($K_3 = 0$).

На рисунку 3 показано динаміку показника FileDownloaded у двох тестових класах у парному форматі (тест-норма ліворуч, тест-атака праворуч). Для базового класу середнє значення ознаки становить ≈ 1,39 завантажень за вікно, тоді як на екзаменаційній вибірці Xekz цей показник зростає до ≈ 20,83 (збільшення у 15 разів). Саме такі відхилення виявляються СППР через систему контрольних допусків δ* = 8,5 у бінарному просторі ознак.

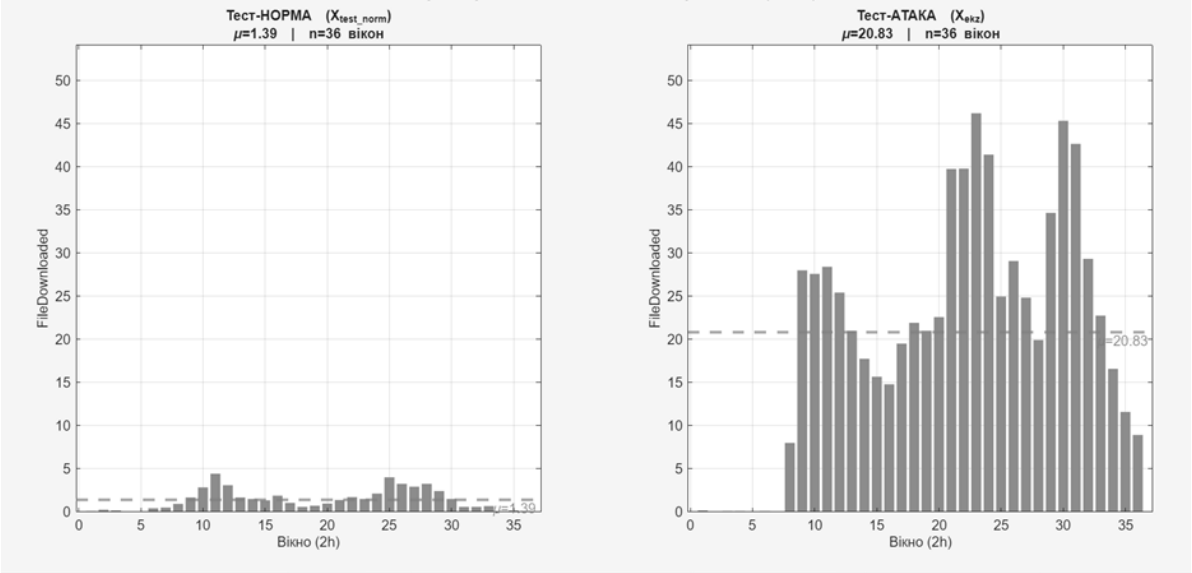


Рис. 3. Ключова ознака атаки: FileDownloaded

Результати синтезу СППР наведено у таблиці 3.

Таблиця 3

Результати синтезу СППР за IEI-технологією

Параметр СППР	Базовий клас X_1	Клас атаки X_2
Кількість векторів-реалізацій n	36	36
Оптимальне поле допусків δ*	8,5	8,5
Міжеталонна відстань dc (Хеммінг)	7	7
Оптимальний радіус контейнера d*	5	6
Максимальне значення КФЕ E* (Кульбак)	0,7898	1,0005
Перша достовірність розпізнавання D_1	0,6111	0,5556
Друга достовірність розпізнавання D_2	0,8889	1,0000
Помилка першого роду α	0,3889	0,4444
Помилка другого роду β	0,1111	0,0000
Робоча зона КФЕ WZ [ds..de]	[5..6]	[6..6]

3.4. Екзаменаційне тестування СППР. З метою двостороннього верифікаційного тестування сформовано дві незалежні тестові вибірки: Xekz (36 векторів-реалізацій із посиленим патерном атаки) та Xnorm (36 векторів-реалізацій нормальної ділової активності). Наявність контрольної тестової вибірки Xnorm є необхідною методологічною умовою: модель із систематичним зміщенням (bias) здатна генерувати хибні рішення про наявність атаки на будь-яких вхідних даних.

На рисунку 4 наведено графіки функцій належності μbase(t) та μatk(t) для обох тестових вибірок. На вибірці Xnorm базова функція належності домінує у всіх вікнах: $\mu base = -0{,}217 \gg \mu atk = -0{,}968$. Жодне вікно не перетинає нульову межу класу атаки: 22 з 36 вікон отримують рішення НОРМА, 14 – NAN. На вибірці Xekz картина симетрично інвертована: $\mu atk = -0{,}111 \gg \mu base = -1{,}111$. У 22 вікнах μatk(t) перетинає нульову межу, генеруючи рішення АТАКА.

Зведені результати двостороннього тестування наведено у таблиці 4.

Двостороннє тестування підтверджує симетричну коректність моделі: СППР однаково впевнено розпізнає обидва протилежних стани. Різниця μatk між двома вибірками складає −0,111 0 (−0,968) = +0,857, що кількісно виражає відстань між станами системи у просторі функцій належності. Генеральна гіпотеза H_1 про наявність стану Data Exfiltration підтверджена через збіг п'яти незалежних індикаторів: 15-кратне зростання FileDownloaded, β_atk = 0, E*_atk > 1,0, вердикт АТАКА у 61,1 % вікон Xekz та нульова частка АТАКА у вибірці Xnorm.

ISSN 2786-5460 (Print), ISSN 2786-5479 (Online)

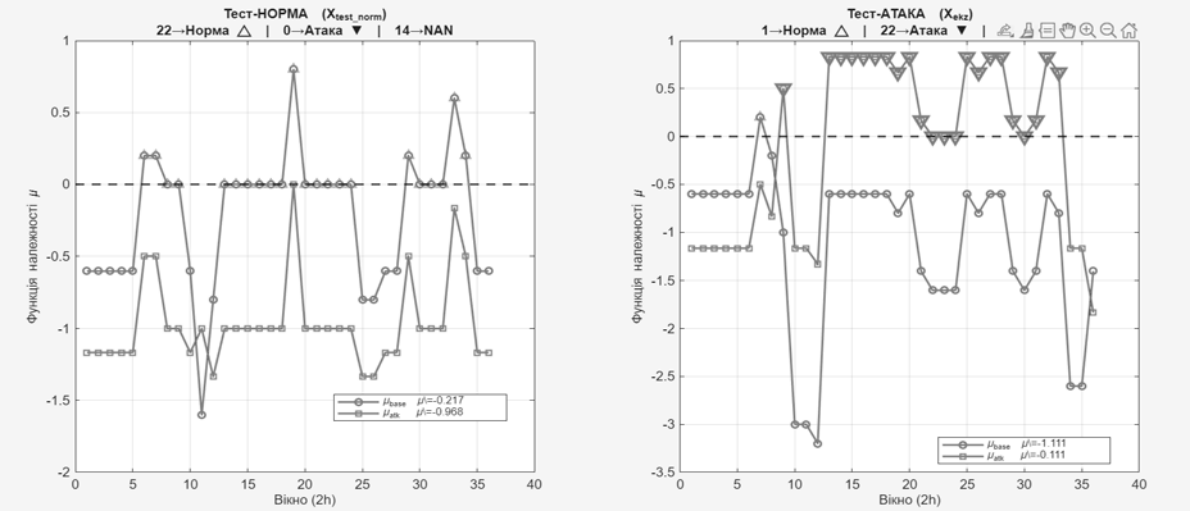


Рис. 4. Функції належності μ(t) для вибірок X_{norm} та X_{ekz}

Таблиця 4

Зведена таблиця результатів двостороннього тестування

Показник	Xnorm (тест-норма)	Xekz (тест-атака)
Кількість вікон n	36	36
Вердикт НОРМА	22 (61,1 %)	1 (2,8 %)
Вердикт АТАКА	0 (0,0 %)	22 (61,1 %)
Поза алфавітом NAN	14 (38,9 %)	13 (36,1 %)
μ̄_base (середнє)	−0,217	−1,111
μ̄_atk (середнє)	−0,968	−0,111
Домінуюча функція	μbase	μatk
FileDownloaded (сер.)	≈ 1,39 файлів/вікно	≈ 20,83 файлів/вікно
Вердикт СППР	НОРМА	АТАКА

Порівняно з підходами на базі LSTM та Transformer-архітектур [1, 2, 3], синтезована СППР демонструє принципово різну обчислювальну складність: повний цикл навчання та тестування на стандартному персональному комп'ютері не перевищує кількох хвилин, тоді як навчання глибоких моделей потребує виділеного GPU та десятків годин. При цьому кожне рішення СППР може бути пояснене через аналіз бітової маски відхилень від еталонного вектора, що є принциповою перевагою для IT-спеціалістів без глибокої підготовки з машинного навчання.

До обмежень дослідження слід віднести такі аспекти: по-перше, навчання виконувалося на синтетичних даних одного суб'єкта, тому для промислового впровадження необхідна валідація на реальних виробничих журналах декількох організацій; по-друге, алфавіт класів розпізнавання обмежений двома класами (M = 2), що не охоплює весь спектр можливих кіберзагроз; по-третє, поточна реалізація передбачає ковзне перенавчання при концептуальному дрейфі телеметрії, що вимагає визначення оптимальної стратегії перенавчання для конкретного виробничого середовища.

4. Висновки. Розроблено та програмно реалізовано 4-етапний конвеєр попередньої обробки телеметрії O365 IEI-Pipeline. Застосування евристичної редукції дозволило зменшити розмірність простору ознак з N = 108 до N = 32 (−70,4 %), ефективно подолавши феномен Белмана та зберігши семантичну інформативність навчальної матриці. Повний цикл обробки понад 90 000 рядків виконується за 6,4 секунди на стандартному обладнанні без спеціалізованого апаратного забезпечення. Відмінністю від підходів автоматичного відбору ознак є те, що редукція не потребує навчальних міток, що є практичною перевагою в умовах обмеженої розмітки.

Експериментально доведено та математично обґрунтовано, що часова агрегація векторів-реалізацій є критичним етапом підготовки навчальної матриці. Встановлено, що агрегація з вікном τ* = 2 год повністю усуває проблему виродження міжеталонної відстані (dc = 0 при τ = 5 хв → dc = 7 при τ = 2 год) та формує стабільну широку робочу зону КФЕ WZ [5, 6]. Цей результат є конкретною кількісною рекомендацією для практичного розгортання системи в умовах O365.

Здійснено інформаційний синтез СППР на базі паралельного алгоритму навчання. Оптимізація СКД ($\delta^* = 8{,}5$) та радіусів контейнерів ($d^*_{base} = 5$, $d^*_{atk} = 6$) за критерієм Кульбака забезпечила ідеальне розділення класів на етапі навчання ($\beta = 0$, $E^*_{atk} = 1{,}0005$). Значення КФЕ понад одиницю підтверджує достатню інформаційну спроможність синтезованої системи ознак для розрізнення класів нормальної поведінки та атаки.

Проведене двостороннє екзаменаційне тестування синтезованої СППР підтвердило її функціональну ефективність та відсутність систематичного зміщення. Система успішно ідентифікувала приховану атаку Data Exfiltration на незалежній тестовій вибірці з достовірністю 61,1 % (22 з 36 векторів-реалізацій) при нульовій частці хибних рішень АТАКА на вибірці нормальної активності. Симетрія функцій належності ($\Delta\mu = 0{,}857$) та часток NAN (36–39 %) підтверджують збалансованість двокласового детектора.

Запропонований підхід є предметно-незалежним: без зміни математичного ядра IEI-технології він може бути поширений на аналіз журналів промислових систем (OT/SCADA), хмарної інфраструктури (AWS CloudTrail) та мережевої телеметрії (NetFlow). Перспективним напрямом подальших досліджень є розширення алфавіту класів розпізнавання ($M \geq 5$) шляхом включення додаткових патернів кібератак (Lateral Movement, Privilege Escalation, Brute Force) та реалізація механізмів адаптивного перенавчання при концептуальному дрейфі телеметричних даних.

Конфлікт інтересів. Автори декларують, що не мають конфлікту інтересів стосовно даного дослідження, в тому числі фінансового, особистісного характеру, авторства чи іншого характеру, що міг би вплинути на дослідження та його результати, представлені в даній статті.

Фінансування. Дослідження проводилося без фінансової підтримки.

Доступність даних. Дані будуть надані за обґрунтованим запитом.

Використання засобів штучного інтелекту. Автори підтверджують, що не використовували технології штучного інтелекту при створенні представленої роботи.

Внесок авторів. К. Є. Шамонін: концептуалізація, методологія, програмна реалізація, проведення досліджень, написання оригінального тексту; Д. В. Прилепа: наукове керівництво, верифікація результатів, редагування, загальне управління дослідженням.

References:

1. Ring, M., Wunderlich, S., Scheuring, D., Landes, D., & Hotho, A. (2019). A survey of network-based intrusion detection data sets. Computers & Security, 86, 147–167. https://doi.org/10.1016/j.cose.2019.06.005

2. Hindy, H., Brosset, D., Bayne, E., Seeam, A., Tachtatzis, C., Atkinson, R., & Bellekens, X. (2020). A taxonomy of network threats and the effect of current datasets on intrusion detection systems. IEEE Access, 8, 104650–104675. https://doi.org/10.1109/ACCESS.2020.2994it

3. Yin, C., Zhu, Y., Fei, J., & He, X. (2017). A deep learning approach for intrusion detection using recurrent neural networks. IEEE Access, 5, 21954–21961. https://doi.org/10.1109/ACCESS.2017.2762418

4. Khan, N., Ahmad, K., AlTamimi, A., Alani, M. M., Bermak, A., & Khalil, I. (2025). Explainable AI-based intrusion detection systems for Industry 5.0 and adversarial XAI: a systematic review. Information, 16(12), 1036. https://doi.org/10.3390/info16121036

5. Mohale, V. Z., & Obagbuwa, I. C. (2025). A systematic review on the integration of explainable artificial intelligence in intrusion detection systems. Frontiers in Artificial Intelligence, 8, 1526221. https://doi.org/10.3389/frai.2025.1526221

6. Moskalenko, V. V., & Dovbysh, A. S. (2016). Vstup do informatsiinoho analizu i syntezu infokomunikatsiinykh system [Introduction to information analysis and synthesis of infocommunication systems]. Sumy State University [in Ukrainian].

7. Dovbysh, A. S., & Myronenko, M. I. (2025). Osnovy mashynnoho navchannia [Fundamentals of machine learning]. Sumy State University [in Ukrainian].

8. Shelekhov, I. V., & Prylepa, D. V. (2025). Metodychni vkazivky dlia kursovoi roboty z dystsypliny «Systemnyi analiz ta teoriia pryiniattia rishen» [Methodical guidelines for coursework in system analysis and decision theory]. Sumy State University [in Ukrainian].

9. Koo, J., Kang, G., & Kim, Y.-G. (2020). Security and privacy in Big Data life cycle: a survey and open challenges. Sustainability, 12(24), 10571. https://doi.org/10.3390/su122410571

10. Prylepa, D. V. (2023). Informatsiino-ekstremalna intelektualna tekhnolohiia diahnostuvannia emotsiino-psykhichnoho stanu liudyny [IEIT for diagnosing the emotional and psychological state of a person]. Extended abstract of candidate's thesis. NTU «KhPI» [in Ukrainian].

11. Pyatachenko, V., & Dovbysh, A. (2023). Information-extreme machine learning of a hand prosthesis control system for EMG biosignal recognition using a sparse training matrix. Kompiuterni nauky, (2), 10. https://doi.org/10.32782/1995-0519.2023.2.10 [in Ukrainian].

12. Shelekhov, I. V., Prylepa, D. V., Khibovska, Yu. O., Shamonin, K. Ye., & Dorenskyi, O. P. (2025). IEIT for intelligent analysis of educational content quality in higher education. Central Ukrainian Scientific Bulletin. Technical Sciences, 12(43) (1), 58–72 [in Ukrainian].

13. Drofa, V. O. (2016). Optymizatsiia kontrolnykh dopuskiv na oznaky rozpiznavannia pry mashynnomu navchanni [Optimization of control tolerances for recognition features in machine learning]. Visnyk NTU «KhPI». Systemnyi analiz, upravlinnia ta informatsiini tekhnolohii, (45), 29–33 [in Ukrainian].

14. Chandrashekar, G., & Sahin, F. (2014). A survey on feature selection methods. Computers & Electrical Engineering, 40(1), 16–28. https://doi.org/10.1016/j.compeleceng.2013.11.024

15. Vaswani, A., Shazeer, N., Parmar, N., Uszkoreit, J., Jones, L., Gomez, A. N., Kaiser, Ł., & Polosukhin, I. (2017). Attention is all you need. Advances in Neural Information Processing Systems, 30, 5998–6008. https://proceedings.neurips.cc/paper_files/paper/2017/file/3f5ee243547dee91fbd053c1c4a845aa-Paper.pdf

Відомості про авторів

Англ.	Укр.
Kiril Shamonin Postgraduate Student at the Department of Computer Science, Faculty of Electronics and Information Technologies, Sumy State University kirilshamonin@gmail.com ORCID: 0009-0004-9771-7629	Шамонін Кіріл Євгенович аспірант кафедри комп'ютерних наук, факультет електроніки та інформаційних технологій, Сумський державний університет kirilshamonin@gmail.com ORCID: 0009-0004-9771-7629
Dmytro Prylepa Candidate of Technical Sciences, Senior Lecturer at the Department of Computer Science, Faculty of Electronics and Information Technologies, Sumy State University d.prylepa@cs.sumdu.edu.ua ORCID: 0000-0002-4022-5496	Прилепа Дмитро Вікторович кандидат технічних наук, старший викладач кафедри комп'ютерних наук, факультет електроніки та інформаційних технологій, Сумський державний університет d.prylepa@cs.sumdu.edu.ua ORCID: 0000-0002-4022-5496

Дата надходження статті: 06.05.2026
Дата надходження виправленої версії статті: 25.06.2026
Дата прийняття статті: 06.07.2026
Дата публікації статті: 26.10.2026