УДК 004.65 DOI: 10.18372/2073-4751.86.21284

Мельниченко П. І.,
orcid.org/0000-0003-3746-1241,
e-mail: polina.melnychenko@npp.kai.edu.ua

ГІБРИДНИЙ МЕТОД ВИЯВЛЕННЯ АНОМАЛІЙ У ЛОГІЧНИХ КЛАСТЕРАХ КІБЕРВРАЗЛИВОСТЕЙ З ВИКОРИСТАННЯМ АНСАМБЛЮ МОДЕЛЕЙ МАШИННОГО НАВЧАННЯ

Національний університет «Київський авіаційний інститут»

Вступ

Сучасні інформаційні системи стають все більш складними та розподіленими, що супроводжується постійним зростанням кількості кіберзагроз та програмних вразливостей. Збільшення кількості вразливостей, а також їх різнорідність за структурою та змістом створюють серйозні складнощі для своєчасного аналізу та прийняття рішень у галузі кібербезпеки. У цих умовах особливої актуальності набуває завдання автоматичного виявлення аномальних чи потенційно критичних вразливостей. Під аномаліями в даному контексті розуміються випадки, що відрізняються від характерного розподілу вразливостей за ознаками, такими як ступінь критичності, тип уразливості, затронуті компоненти та експлуатаційна можливість. Такі події вимагають пріоритетної уваги, оскільки можуть свідчити про високу ймовірність експлуатації чи масштабного впливу на системи.

Постановка проблеми

Особливого значення в даному контексті набуває завдання логічної кластеризації та структурування даних про вразливості. Кластеризація сприяє виявленню прихованих патернів, наприклад, типів помилок, що повторюються, або схожих експлуатаційних сценаріїв, що робить процес аналізу більш інтерпретованим і стійким до шуму в даних.

Таким чином, актуальність дослідження полягає у необхідності розробки автоматизованого, масштабованого та інтерпретованого методу аналізу вразливостей на основі машинного навчання та логічної кластеризації, що дозволить підвищити ефективність обробки великих потоків даних у галузі кібербезпеки та забезпечити більш точну оцінку рівня загроз.

Аналіз останніх досліджень та публікацій

Використання моделей машинного навчання для виявлення аномалій знайшло відображення у багатьох наукових статтях, а саме: автори статті [1] досліджують прогнозування zero-day атак із використанням ансамблевих моделей машинного навчання, таких як Random Forest, XGBoost та LSTM, однак не враховують гетерогенність (різнорідність) даних, що може призводити до перенавчання на домінуючих класах.

У статті [2] автори використовують моделі IF (Isolation Forest) та OCSVM для оцінювання ефективності методів виявлення аномалій у API журналах, але не враховують ширший спектр джерел кіберзагроз та адаптацію моделей до змін середовища.

У статті [3] розглядається проблема виявлення аномалій у мультимодальних наборах даних. Автором запропоновано гібридний підхід Hybrid AWRED, який поєднує механізми адаптивної реконструкції даних, топологічної кластеризації та регуляризації енергетичних характеристик для підвищення точності виявлення рідкісних аномалій. Однак, запропонований підхід орієнтований переважно на мультимодальні дані та задачі фінансового моніторингу, що обмежує його застосування для виявлення аномалій у інших сферах.

Автори [4] поєднують поведінковий аналіз мережевих даних із семантичним

аналізом вмісту пакетів, що дозволяє не лише виявляти аномалії, а і класифікувати їх за типами кібератак. Разом із тим дослідження зосереджене переважно на мережевому трафіку та семантичному аналізі пакетів, що обмежує застосування підходу для інших типів джерел даних.

У роботі [5] проведено аналіз сучасних підходів до виявлення аномалій мережевого трафіку в інформаційно-комунікаційних системах. Робота має переважно оглядовий характер, та не приділяє достатньої уваги прогнозуванню розвитку аномалій у часових рядах, аналізу залежностей між подіями та використанню процесів самозбудження для моделювання динаміки кібератак.

У статтях [6-8] дослідження аномалій проводиться переважно в мережевому трафіку, та не може бути застосоване до інших сфер.

Проведений аналіз сучасних наукових публікацій показів, що дослідження та виявлення аномалій переважно зосереджені на аналізі мережевого трафіку або в окремих вузьких напрямках. У наявних роботах недостатньо враховано задачі виявлення аномалій на основі даних про вразливості CVE, а також проблему гетерогенності таких даних.

З урахуванням виявлених обмежень, доцільною є розробка гібридного методу виявлення аномалій, що базується на ансамблі моделей машинного навчання (Decision Tree, Random Forest, Gradient Boosting) у поєднанні з методами логічної кластеризації. Запропонований підхід дозволить враховувати семантичну та структурну подібність між вразливостями, що дасть змогу зменшити гетерогенність даних і підвищить точність виявлення аномальних подій.

Мета статті – розробка гібридного методу виявлення аномалій з використанням ансамблю класичних моделей прогнозування та логічної кластеризації.

Основна частина

Гібридний метод виявлення аномалій призначений для підвищення точності виявлення аномалій завдяки запропонованим семантично однорідним кластерам та використанню ансамблю моделей. Схема та кроки методу наведені на рис. 1.

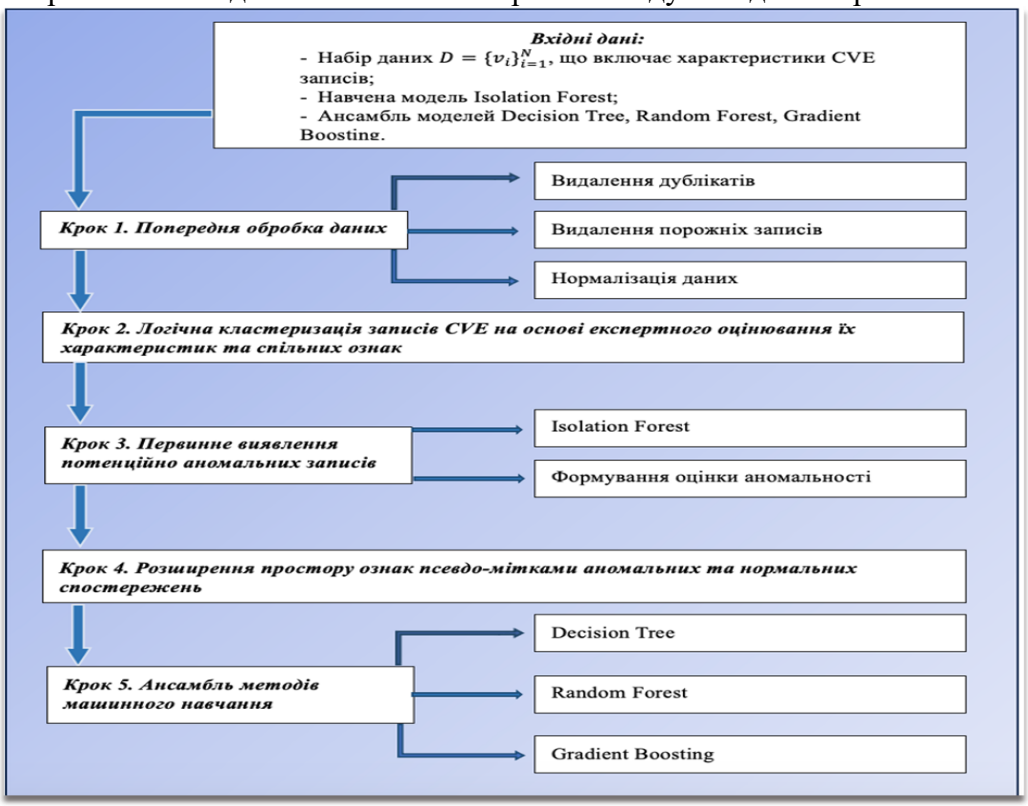

Рис. 1. Схема гібридного методу виявлення аномалій

Вхідними даними для гібридного методу виявлення аномалій у наборі даних про кібервразливості є структуровані характеристики CVE записів, а саме базова

оцінка CVSS, показники експлуатаційності та впливу, рівень критичності, часові характеристики публікації вразливості. Додатково використовується навчена модель Isolation Forest для первинного виявлення потенційно аномальних спостережень, а також ансамбль моделей Decision Tree, Random Forest та Gradient Boosting для подальшого аналізу та уточнення класифікації аномалій.

Перший крок включає попередню обробку та підготовку даних для аналізу. На даному етапі формується набір ознак, що складається з основних характеристик вразливості: значення CVSS, оцінка експлуатаційності, оцінка впливу, числове представлення рівня критичності. Для забезпечення коректної роботи моделей машинного навчання всі ознаки нормалізуються до єдиного масштабу щоб зменшити вплив різниці у числових діапазонах.

Другий крок включає логічну кластеризацію записів CVE на основі експертного оцінювання їх характеристик та спільних ознак.

На третьому кроці до кожного логічного кластера застосовуються модель Isolation Forest для первинного виявлення потенційно аномальних записів. Модель формує оцінку аномальності для кожного запису на основі середньої довжини шляху ізоляції в ансамблі випадкових дерев. На основі отриманих оцінок визначаються записи, які класифікуються як потенційно критичні аномалії.

На четвертому кроці передбачається розширення простору ознак шляхом додавання оцінки аномальності, як додаткової характеристики кожного запису.

П'ятий крок включає застосування ансамблю методів Decision Tree, Random Forest та Gradient Boosting для уточнення класифікації аномалій. Моделі отримують на вході розширений набір ознак та формують остаточний прогноз щодо належності запису до аномального класу. Використання ансамблю методів машинного навчання дозволяє врахувати складні нелінійні залежності між характеристиками вразливостей та підвищує точність виявлення аномалій.

Результатом роботи методу є автоматизоване виявлення локальних прихованих аномальних записів CVE у межах логічних кластерів, що дозволяє підвищити точність аналізу нетипових та потенційно критичних вразливостей.

Проведення експериментального дослідження для оцінки ефективності розробленого гібридного методу виявлення аномалій є ключовим кроком. Реалізація методу була проведена у хмарному сервісі «Google Colab» мовою програмування Python. Дослідження опирається на метрики якості Accuracy, Precision, Recall, F1-score та Log Loss.

В рамках дослідження було використано набір даних [9], що підходять для задачі виявлення аномалій. Дані являють собою набір характеристик CVE: дата публікації CVE, CVSS v3.1, оцінка експлуатаційності, оцінка впливу, CWE, опис вразливості та записуються в наступному вигляді:

$$D = \{v_i\}_{i=1}^{N}, \qquad (1)$$

в якому кожну вразливість можна представити у вигляді $v_i = (t_i, x_i, y_i)$, де t_i – це час виявлення вразливості, $x_i \in \mathbb{R}^d$ – вектор ознак (характеристики CVE), y_i – ціль прогнозування.

Датасет зображено на рис. 2.

	published	cvssMetricV31	SeverityV31	cvss31exploitabilityScore	cvss31impactScore	CWE	Description
111110	2019-01-01 16:29:00.233	6.5	MEDIUM	2.8	3.6	CWE-20	A reachable Object::dictLookup assertion in Po...
111113	2019-01-02 07:29:00.197	7.8	HIGH	1.8	5.9	CWE-532	aria2c in aria2 1.33.1, when --log is used, ca...
111127	2019-01-02 18:29:00.310	9.8	CRITICAL	3.9	5.9	CWE-502	FasterXML jackson-databind 2.x before 2.9.7 mi...
111128	2019-01-02 18:29:00.387	9.8	CRITICAL	3.9	5.9	CWE-502	FasterXML jackson-databind 2.x before 2.9.7 mi...
111138	2019-01-02 18:29:01.277	9.8	CRITICAL	3.9	5.9	CWE-78	On D-Link DIR-818LW Rev.A 2.05.B03 and DIR-860...
...	...	...	...	...	...	...	...
327936	2026-04-21 04:16:13.443	9.8	CRITICAL	3.9	5.9	CWE-78	NewSoftOA developed by NewSoft has an OS Comma...
327940	2026-04-21 07:16:09.547	4.3	MEDIUM	2.8	1.4	CWE-862	The Responsive Blocks – Page Builder for Block...

Рис. 2. Набір даних для виявлення аномалій

Загальна кількість записів складає 194596. Необхідно звернути увагу, що моделі машинного навчання не працюють з порожніми значеннями, тому потрібно впевнитись, що в датасеті відсутні None (Рис. 3).

```
dataset_2.isna().sum()
```

	0
published	0
cvssMetricV31	0
SeverityV31	0
cvss31exploitabilityScore	0
cvss31impactScore	0
CWE	0
Description	0

Рис. 3. Перевірка порожніх значень

Дослідивши розподіл вразливостей (Рис. 4) можна побачити два різких сплески вразливостей у 2020 та 2024 роках. Найбільша кількість вразливостей відноситься до рівнів Medium та High.

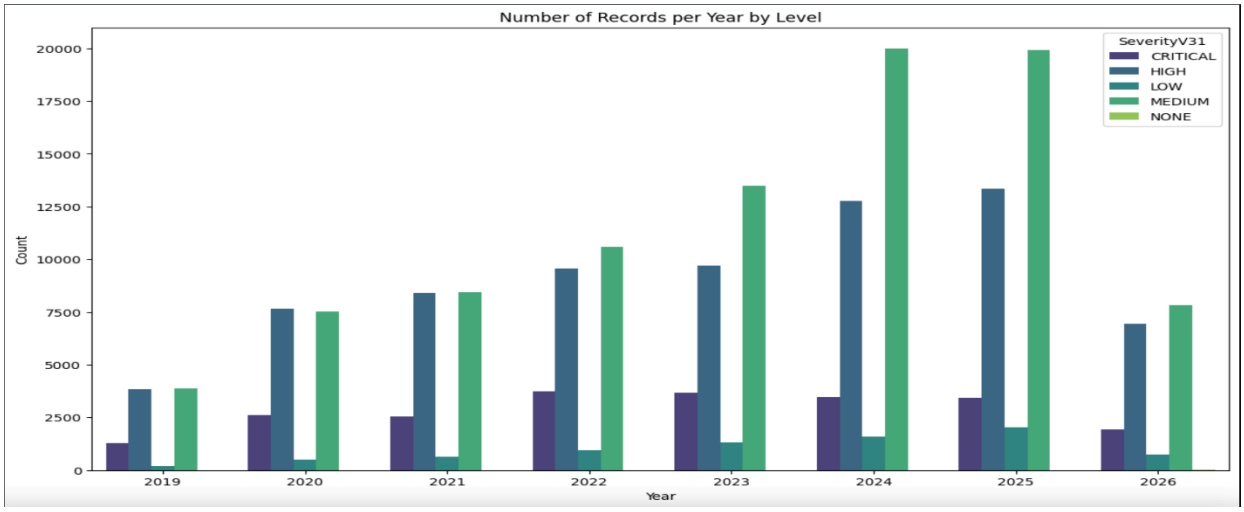

Рис. 4. Кількість записів по роках відповідно до рівнів CVSSv3.1

Використовуючи OWASP Top 10 2025 [10] знаходимо відповідності CWE до класів OWASP.

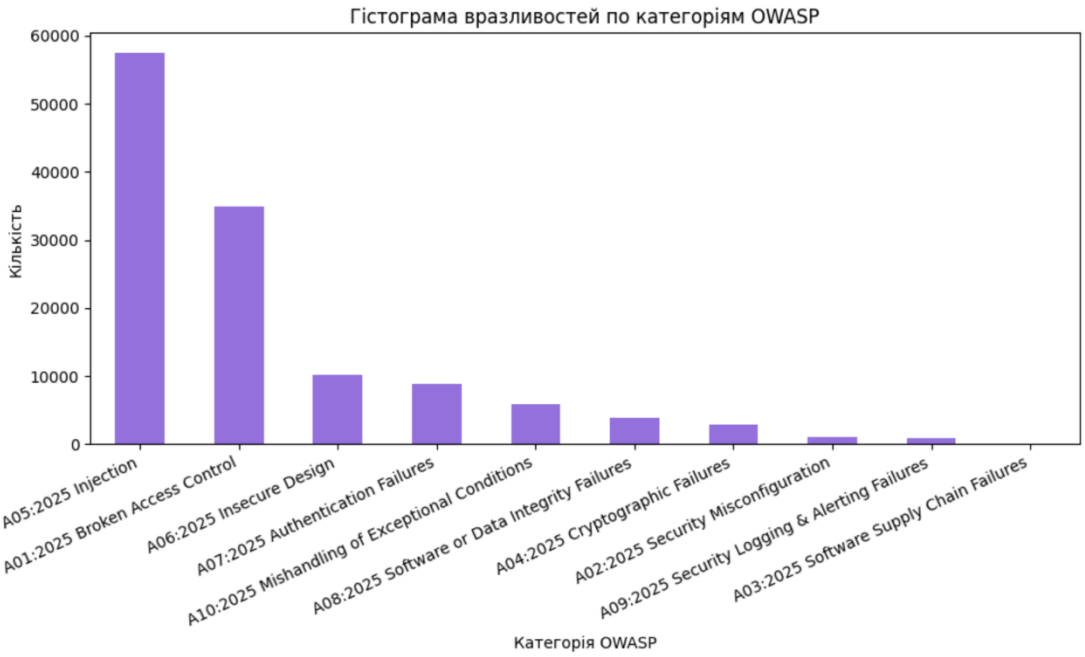

Рис. 5. Гістограма вразливостей по категоріям OWASP Top 10 2025

На рис. 5 можна побачити, що найбільша кількість вразливостей відноситься до категорій A01:2025 Broken Access Control та A05:2025 Injection. Найменша кількість вразливостей у категоріях A09:2025 Security Logging & Alerting Failures. A03:2025 Software Supply Chain Failures, що свідчить про значний дисбаланс вразливостей різних типів. Такий розподіл кількості вразливостей може призвести до перенавчання моделей на домінуючих класах (class imbalance).

З огляду на ці особливості, для забезпечення коректності подальшого аналізу було прийнято рішення зробити логічну (експертну) кластеризацію категорій OWASP, об'єднавши малочисельні та семантично близькі категорії у ширші групи. Такий підхід дозволяє зменшити вплив дисбалансу класів, підвищити статистичну стійкість подальшого аналізу, створити більш послідовну основу для побудови моделі виявлення аномалій.

Логічна кластеризація

Наступним кроком пропонується розбити дані на шість логічних кластерів. Кластер «Broken Access Control» включає в себе вразливості, що пов'язані з неправильною перевіркою прав доступу, що дозволяють користувачам виконувати дії або отримувати дані без відповідних дозволів. Кластер «Injection» включає в себе вразливості, за яких зловмисник може впроваджуваати шкідливі команди або запити (SQLi, XSS) через відсутність валідації вхідних даних. Кластер «Cryptography & Data Protection» – це помилки у шифруванні та захисті даних, що призводять до витоку або компрометації конфіденційної інформації. Кластер «Configuration & Design Weaknesses» – проблеми, спричинені небезпечними налаштуваннями систем або архітектурними помилками, що створюють потенційні точки атаки. Кластер «Authentication and Mishandling Failures» – це вразливості, що пов'язані з помилками автентифікації, керуванням сесіями та неправильною обробкою даних користувача. Кластер «Software Failures» – це загальні програмні помилки (наприклад, переповнення, некоректна обробка винятків), які можуть бути використані для порушення роботи системи або виконання атак.

Отже, для досліджуваного датасету $D = \{x_i\}_{i=1}^{n}$, в якому кожен запис x_i має відповідну OWASP категорію з множини категорій $A = \{A_1, A_2, \ldots, A_m\}$, де $m = 10$, вводимо правило φ, яке відносить кожну

початкову категорію OWASP до одного з логічних кластерів K:

$$\varphi: A \to \{1, \dots, K\} \quad (2)$$

де K – кількість логічних кластерів, а функція φ повертатиме номер кластера.

Визначаємо множину записів, що потрапляють у кластер C_k, як:

$$C_k = \{x_i \in A | \varphi(OWASP(x_i)) = k\} \quad (3)$$

Та отримаємо:

$$\bigcup_{k=1}^{K} C_k \quad (4)$$

Тоді функція φ для кожної категорії OWASP матиме наступний вигляд:

$$\begin{aligned} &\varphi(A_1) = 1 \\ &\varphi(A_5) = 2 \\ &\varphi(A_4) = 3, \varphi(A_9) = 3 \\ &\varphi(A_2) = 4, \varphi(A_6) = 4 \\ &\varphi(A_7) = 5, \varphi(A_{10}) = 5 \\ &\varphi(A_3) = 6, \varphi(A_8) = 6 \end{aligned} \quad (5)$$

де 1 – це кластер $C_1 = \{A_1\}$ «Cluster 1: Broken Access Control», 2 – це кластер $C_2 = \{A_5\}$ «Cluster 2: Injection», 3 – це кластер $C_3 = \{A_4, A_9\}$ «Cluster 3: Cryptography & Data Protection», 4 – це кластер $C_4 = \{A_2, A_6\}$ «Cluster 4: Configuration & Design Weaknesses», 5 – це кластер $C_5 = \{A_7, A_{10}\}$ «Cluster 5: Authentication and Mishandling Failures», 6 – це кластер $C_6 = \{A_3, A_8\}$ «Cluster 6: Software Failures».

Виконавши кластеризацію отримаємо наступний розподіл даних (Рис. 6). Вразливості, що відносяться до категорії Other, не враховуються у даному дослідженні, оскільки вони не відносяться до Webвразливостей.

Запропонована логічна кластеризація дозволяє зменшити дисбаланс класів, сформувати семантично однорідні групи вразливостей та створити передумови для ефективного застосування ансамблю моделей класичного аналізу даних.

Дослідження аномалій

Пропонується підхід, заснований на двох етапах, в якому на першому етапі застосовується Isolation Forest для оцінки ступеня аномальності спостережень, а на другому етапі отримані оцінки інтегруються в розширений простір ознак та використовуються ансамблем класичних моделей машинного навчання для покращення класифікації.

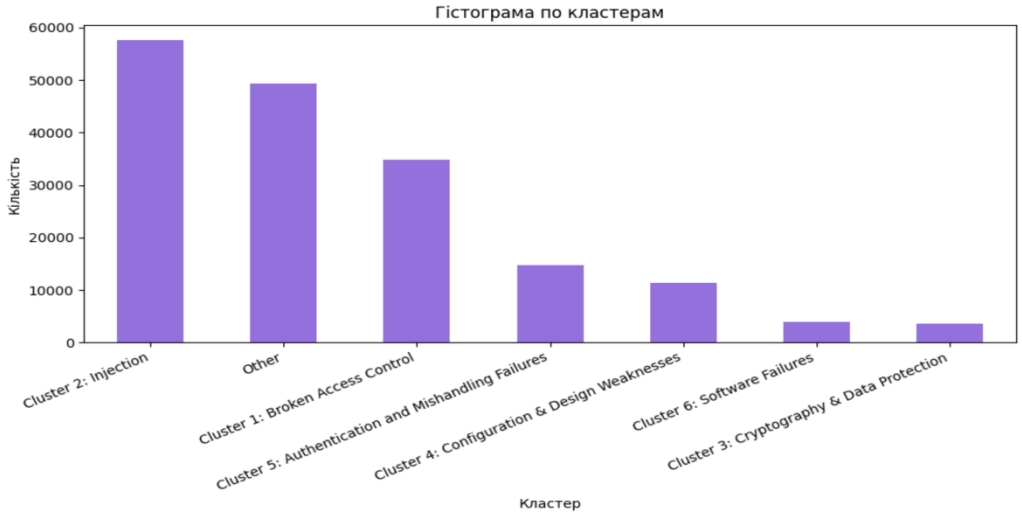

Рис. 6. Гістограма розподілу логічних кластерів

Маючи матрицю ознак $X \in \mathbb{R}^{n \times d}$ відповідно до формули (1), стандартизуємо ознаки $z_{ij} = \frac{x_{ij} - \mu_j}{\sigma_j}$, де x_{ij} – значення j-тої ознаки для i-го об'єкту, μ_j – середнє значення j-тої ознаки в усій вибірці, σ_j – стандартне відхилення.

Даний крок приводить всі ознаки до однієї шкали (від 0 до 1), що дає можливість моделі коректно порівнювати ознаки не виділяючи якусь окрему.

Отримаємо нормалізований простір $Z = \{z_1, z_2, \dots, z_n\}$.

Дані будуємо ансамбль випадкових дерев Isolation Forest, який розраховує для кожного об'єкту аномальну оцінку (score):

$$s_i = f_{IF}(z_i) \quad (6)$$

Лістинг

```
from sklearn.ensemble import IsolationForest
model_if = IsolationForest(
   n_estimators=200,
   contamination=0.05,
   random_state=42
)
labels = model_if.fit_predict(X)
```

На основі параметру contamination = 0.05 виділяється множина потенційних аномалій: $A = \{x_i : s_i > \tau\}$, які необхідно додати в датасет як нову ознаку $x'_i = (x_i, s_i)$ та сформувати розширений простір ознак $X' \in \mathbb{R}^{n\times(d+1)}$.

Для кожного логічного кластера було застосовано модель визначення аномалій Isolation Forest, на основі якої сформовано псевдо-мітки аномальних та нормальних спостережень. Результат представлено в табл. 1.

Таблиця 1 Характеристика набору даних для кластерів

Характеристика	Кластер 1 Broken Access Control	Кластер 2 Injection	Кластер 3 Cryptography & Data Protection	Кластер 4 Configuration & Design Weaknesses	Кластер 5 Authentication and Mishandling Failures	Кластер 6 Software Failures
Розмірність набору даних	34825	57540	3681	11336	14753	3881
Кількість не аномальних значень	33085	54656	3497	10767	14013	3684
Кількість аномалій	1740	2877	184	567	737	194
Розподіл класів	Нормальні 95 %, аномалії 5 %	Нормальні 94,98 %, аномалії 5,02 %	Нормальні 95,01 %, аномалії 4,99 %	Нормальні 94,98 %, аномалії 5,02 %	Нормальні 94,98 %, аномалії 5,02 %	Нормальні 94,92 %, аномалії 5,08 %

Далі отримані результати використовувалися для навчання (Таблиця 2) ансамблю моделей машинного навчання Decision Tree, Random Forest та Gradient Boosting з метою побудови ефективної класифікаційної моделі для швидкого виявлення аномалій без необхідності повторного застосування вихідного алгоритму.

Таблиця 2 Параметри моделей машинного навчання

Модель	**Гіперпараметри**
Decision Tree	dt_model = DecisionTreeClassifier(max_depth=8, random_state=42)
Random Forest	rf_model = RandomForestClassifier(n_estimators=300, max_depth=10, random_state=42, n_jobs=-1)
Gradient Boosting	gb_model = GradientBoostingClassifier(n_estimators=300, learning_rate=0.05, max_depth=5, random_state=42)

Для оцінки якості побудованих моделей були використані метрики Accuracy, Precision, Recall, F1-score та Log Loss. Результати оцінки кожного кластера представлені у табл. 3.

Таблиця 3. Показники якості ансамблю моделей

Модель	**Accuracy**	**Precision**	**Recall**	**F1-score**	**Log Loss**
Кластер 1 Broken Access Control					
Decision Tree	0,9821	0,8770	0,6666	0,7575	0,2203
Random Forest	0,9852	0,8976	0,7310	0,8058	0,0694
Gradient Boosting	0,9871	0,8904	0,7904	0,8374	0,0342
Кластер 2 Injection					
Decision Tree	0,9789	0,7927	0,7963	0,7945	0,7594
Random Forest	0,9856	0,9671	0,7444	0,8413	0,0434
Gradient Boosting	0,9860	0,9861	0,7380	0,8442	0,0388
Кластер 3 Cryptography & Data Protection					
Decision Tree	0,9249	0,4275	0,6326	0,5102	2,7044
Random Forest	0,9659	0,8333	0,5612	0,6707	0,2355
Gradient Boosting	0, 9375	0,4965	0,7448	0,5959	0,1277
Кластер 4 Configuration & Design Weaknesses					
Decision Tree	0,9829	0,8700	0,8259	0,8474	0,6156
Random Forest	0,9856	0,9958	0,7531	0,8576	0,0684
Gradient Boosting	0,9869	0,9880	0,7816	0,8727	0,0419
Кластер 5 Authentication and Mishandling Failures					
Decision Tree	0,9663	0,5920	0,6572	0,6229	1,2129
Random Forest	0,9833	0,8227	0,7735	0,7974	0,0442
Gradient Boosting	0,9845	0,7774	0,8899	0,8299	0,0404
Кластер 6 Software Failures					
Decision Tree	0,9497	0,5000	0,5773	0,5358	1,8124
Random Forest	0,9637	0,5944	0,8762	0,7083	0,4125
Gradient Boosting	0,9108	0,3563	0,9587	0,5195	0,4374

Отримані результати показують, що якість моделей доволі сильно варіюється в залежності від розміру вибірки. У кластерах з великим обсягом даних (кластер 1 Broken Access Control та кластер 2 Injection) найкращі результати демонструє модель Gradient Boosting, оскільки має найбільш збалансоване співвідношення Precision та Recall, а також максимальне значення F1-score при мінімальному значенні Log Loss. Такий результат свідчить про здатність моделі ефективно вловлювати складні нелінійні залежності даних.

Модель Random Forest показує стабільні результати у всіх кластерах, особливо при обмеженому наборі даних (кластер 3 Cryptography & Data Protection та кластер 6 Software Failures), що вказує на її стійкість до перенавчання та гарну узагальнюючу здатність.

Decision Tree показує високі значення Accuracy у деяких випадках, але має менш стабільні результати у метриках Precision та F1-score, що говорить про її схильність до перенавчання та погану здатність до узагальнення даних у порівнянні з іншими моделями.

Таким чином, Gradient Boosting рекомендується розглядати як кращу модель для кластерів з великим обсягом та складної структурою даних, тоді як Random Forest рекомендується для кластерів з обмеженою кількістю даних.

Висновки та перспективи подальших досліджень.

В результаті роботи було розроблено гібридний метод виявлення аномалій з використанням ансамблю класичних моделей прогнозування та логічної кластеризації, що враховує семантичну та структурну подібність між вразливостями, зменшує гетерогенність даних та підвищує точність виявлення аномальних подій.

Порівняльний аналіз моделей показав, що моделі Random Forest та Gradient Boosting забезпечують найбільш стабільні та точні результати класифікації аномалій, при цьому Gradient Boosting демонструє найкращу ефективність на великих вибірках, а Random Forest залишається стійкішим при обмеженому обсязі даних.

Подальші дослідження можуть бути спрямовані на моделювання стохастичної динаміки виникнення аномалій та їх впливу на формування каскадних сплесків вразливостей із застосуванням самозбуджуваних процесів, таких як процес Хоукса, для виявлення прихованих часових закономірностей та залежностей.

Література

1. Ahmed A.F Osman, Mohammed Awad Mohammed Ataelfadiel. Zero-day attack prediction using ensemble machine learning with threat intelligence data. International Journal of Applied Mathematics, Volume 38No. 10s, 2025, 983-1004. ISSN: 1314-8060 (online version)

2. Мартовицький, В., Свиридов, А., Авдєєв, О., Гудзинський, І., & Коротецький, О. (2025). Дослідження методів виявлення аномалій у арі журналах для забезпечення безпеки та надійності програмних систем. Вісник Херсонського національного технічного університету, 2 (1 (92)), 142-148. DOI: https://doi.org/10.35546/kntu2078-4481.2025.1.2.19

3. Довженко, Т. П. (2026). Hybrid awred: синергія адаптивної реконструкції та топологічної кластеризації для виявлення аномалій у мультимодальних даних. Зв'язок, (1), 80-88. DOI: https://doi.org/10.31673/2412-9070.2026.017405

4. Шульга В.П., Іванченко І.С., Рижаков М.М. Математична модель семантичної атрибуції кіберінцидентів у системах виявлення аномалій на основі глибокого навчання. Сучасний захист інформації, 2025, № 3(63), 186-198. DOI: https://doi.org/10.31673/2409-7292.2025.032076

5. Петляк, Н. (2025). Аналіз моделей виявлення аномалій трафіку в сучасних інформаційно-комунікаційних системах та мережах. Вимірювальна та обчислювальна техніка в технологічних процесах, (1), 180–186. DOI: https://doi.org/10.31891/2219-9365-2025-81-21
6. Поночовний, П., & Пепа, Ю. (2025). Реалізація системи захисту серверів з урахуванням аномалій в пакетах. Вимірювальна та обчислювальна техніка в технологічних процесах, (1), 44–51. DOI: https://doi.org/10.31891/2219-9365-2025-81-6
7. Іванченко, Є., Аверічев, І., & Рижаков, М. (2025). Узагальнена модель прогнозування та виявлення кібербезпекових аномалій на основі штучного інтелекту. Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка», 4(28), 529–546. DOI: https://doi.org/10.28925/2663-4023.2025.28.823
8. Є. Ю. Глоба, В. Р. Смірнов, М. С. Нараєвський, В. М. Федорченко. Метод виявлення аномалій в корпоративній мережі. Системи управління, навігації та зв'язку. 2025. No 3, 193-198. Режим доступу: https://www.researchgate.net/publication/396481105_METOD_VIAVLENNA_ANOMALIJ_V_KORPORATIVNIJ_MEREZI METHOD_FOR_DETECTING_ANOMALIES_IN_CORPORATE_NETWORKS
9. National Vulnerability Database. Режим доступу: https://nvd.nist.gov/developers/vulnerabilities
10. OWASP Top 10 2025. Режим доступу: https://owasp.org/Top10/2025/A01_2025-Broken_Access_Control/

Мельниченко П. І.

ГІБРИДНИЙ МЕТОД ВИЯВЛЕННЯ АНОМАЛІЙ У ЛОГІЧНИХ КЛАСТЕРАХ КІБЕРВРАЗЛИВОСТЕЙ З ВИКОРИСТАННЯМ АНСАМБЛЮ МОДЕЛЕЙ МАШИННОГО НАВЧАННЯ

У роботі запропоновано гібридний метод виявлення аномалій, заснований на логічній кластеризації вразливостей та застосуванні методів машинного навчання. Вихідні дані містять інформацію про вразливість програмного забезпечення, включаючи метрики CVSS, рівні критичності, типи CWE, тимчасові характеристики та приналежність до логічних груп, сформованих на основі OWASP Top Ten.

На першому етапі проводиться аналіз даних та формування додаткових тимчасових характеристик. Далі виконується логічна кластеризація вразливостей, що дозволяє розділити дані на семантично однорідні групи, такі як Broken Access Control, Injection, Cryptography & Data Protection, Configuration & Design Weaknesses, Authentication and Mishandling Failures та Software Failures. Такий підхід дозволяє знизити гетерогенність даних та підвищити якість подальшого аналізу.

На другому етапі застосовується метод виявлення аномалій Isolation Forest, який використовується для виявлення нетипових вразливостей всередині кожного кластера. Отримані результати використовуються як псевдо-мітки для навчання ансамблевих моделей машинного навчання, включаючи Decision Tree, Random Forest та Gradient Boosting. Дані моделі використовуються для класифікації аномалій та оцінки їх передбачуваності на основі простору ознак, що включає CVSS-метрики, оцінку експлуатаційності, оцінку впливу та часові характеристики.

Для оцінки якості моделей використовувалися метрики Accuracy, Precision, Recall, F1-score та Log Loss. Результати експериментів показали, що Gradient Boosting демонструє найкращу якість на великих вибірках, тоді як Random Forest показує стабільніші результати на малих кластерах. Decision Tree має високу інтерпретованість, але схильний до перенавчання та має погану здатність до узагальнення даних у порівнянні з іншими моделями.

Запропонований гібридний метод дозволяє підвищити точність виявлення аномалій завдяки запропонованим семантично однорідним кластерам та використанню ансамблю моделей.

Результати дослідження можуть бути використані у системах моніторингу інформаційної безпеки та управління інцидентами, а також при розробці інтелектуальних систем прогнозування, спрямованих на виявлення аномальних подій та моделювання динаміки поширення вразливостей.

Ключові слова: *виявлення аномалій, кіберзахист, логічна кластеризація, ансамбль моделей машинного навчання, дерево рішень, Random Forest, Gradient Boosting.*

Melnychenko P.

HYBRID METHOD FOR ANOMALY DETECTION IN LOGICAL CLUSTERS OF CYBER VULNERABILITIES USING AN ENSEMBLE OF MACHINE LEARNING MODELS

The article presents the hybrid anomaly detection method based on logical clustering of vulnerabilities and the application of machine learning techniques. The dataset includes information about software vulnerabilities, including CVSS metrics, severity levels, CWE types, temporal characteristics, and assignment to logical groups formed based on the OWASP Top Ten.

At the first stage, data analysis is performed along with the construction of additional temporal features. Subsequently, logical clustering of vulnerabilities is carried out, allowing the data to be partitioned into semantically homogeneous groups such as Broken Access Control, Injection, Cryptography & Data Protection, Configuration & Design Weaknesses, Authentication and Mishandling Failures, and Software Failures. This approach reduces data heterogeneity and improves the quality of subsequent analysis.

At the second stage, the Isolation Forest anomaly detection method is applied to identify atypical vulnerabilities within each cluster. The obtained results are used as pseudo-labels for training ensemble machine learning models, including Decision Tree, Random Forest, and Gradient Boosting. These models are employed for anomaly classification and for evaluating their predictability based on a feature space that includes CVSS metrics, exploitability score, impact score, and temporal characteristics.

Model performance is evaluated using Accuracy, Precision, Recall, F1-score, and Log Loss metrics. Experimental results show that Gradient Boosting demonstrates the best performance on large datasets, while Random Forest provides more stable results on smaller clusters. Decision Tree offers high interpretability but is prone to overfitting and exhibits weaker generalization capability compared to other models.

The proposed hybrid method improves anomaly detection accuracy through the use of semantically homogeneous clusters and an ensemble of models.

The results of the study can be applied in information security monitoring and incident management systems, as well as in the development of intelligent forecasting systems aimed at detecting anomalous events and modeling the dynamics of vulnerability propagation.

Keywords*: anomaly detection, cybersecurity, logical clustering, ensemble learning, decision tree, Random Forest, Gradient Boosting.*

Стаття подана до редакції: 15/05/2026
Стаття прийнята до опублікування: 19/05/2026
Стаття опублікована: 30/05/2026