

УДК 004.45:004.942

ДОСЛІДЖЕННЯ МЕТОДІВ ВИЯВЛЕННЯ АНОМАЛІЙ ТА ЗМІЩЕННЯ ДАНИХ (DATA DRIFT) У СИСТЕМАХ МАШИННОГО НАВЧАННЯ

Сорокін С.О.

e-mail: stepan.sorokin@nure.ua

Науковий керівник – канд. техн. наук, доц. Любченко В.А.
Харківський національний університет радіоелектроніки, каф. ІНФ
м. Харків, Україна

This work is devoted to investigating methods for anomaly and data drift detection in machine learning systems. The nature of data drift and anomalies, including covariate shift and concept drift, were considered. An analysis of ensemble methods for outlier detection and statistical metrics for continuous data drift monitoring is carried out. It has been found that combining these approaches within the MLOps architecture forms a reliable protective layer, preventing the silent degradation of intelligent systems in a changing real-world environment.

Актуальність дослідження зумовлена переходом індустрії до дано-центрованого (Data-Centric) підходу. Експлуатація систем машинного навчання (ML) виявила їхню фундаментальну вразливість: ефективність моделі безпосередньо залежить від стабільності вхідних даних. На відміну від традиційного ПЗ, ML-моделі схильні до «тихої деградації» (Silent Degradation). Модель видає прогнози, але їхня точність знижується через порушення гіпотези про ідентичність розподілів (IID). Динаміка реального світу неминуче призводить до відхилень у вигляді епізодичних аномалій та систематичного зміщення даних (Data Drift).

Для ефективного моніторингу необхідно розмежовувати ці відхилення. Аномалії (Outliers) – це точкові, нетипові відхилення у даних, спричинені помилками збору інформації або рідкісними подіями, здатні суттєво спотворити градієнти під час тренування. Системні відхилення поділяються на Covariate Shift (Data Drift), що описує зміну розподілу незалежних вхідних ознак $P(X)$ за умови збереження зв'язку $P(Y|X)$, та Concept Drift – зміну взаємозв'язку між ознаками та цільовою змінною $P(Y|X)$, внаслідок якої вивчені патерни стають нерелевантними.

Для виявлення аномалій (Outlier Detection) та досягнення максимальної робастності рекомендується застосовувати ансамблеві методи (Consensus Scoring). Базові статистичні методи (правило 3σ , міжквартильний розмах IQR) доповнюються алгоритмом Local Outlier Factor (LOF), що аналізує локальну щільність точок. Для обробки великих масивів даних (Big Data) доцільно використовувати Isolation Forest, який ізолює аномалії шляхом випадкового розбиття простору ознак. Механізм консенсусу гарантує маркування точки як аномальної лише за підтвердження більшістю методів ансамблю, що мінімізує хибнопозитивні спрацьовування (False Positives).

Під час промислової експлуатації моделі (Inference) нові дані регулярно порівнюються з референсним датасетом за допомогою статистичних метрик. Дивергенція Кульбака-Лейблера (KL Divergence) оцінює асиметричну втрату інформації при порівнянні розподілів. Робастнішою альтернативою є відстань Вассерштейна (Wasserstein Distance), яка вимірює «вартість» перетворення одного розподілу в інший та демонструє стійкість до зсувів. Індустріальним стандартом оцінки стабільності виступає метрика PSI (Population Stability Index), де значення $PSI > 0.2$ сигналізує про критичний рівень зміщення. Також застосовується тест Колмогорова-Смірнова (K-S Test).

Інтеграція цих методів вимагає створення ізольованого вузла (Data Quality Node) у MLOps-конвеєрі. Життєвий цикл включає Baseline Generation (створення еталонного «сліпка») та Continuous Profiling (потокове обчислення характеристик запитів). Drift Checking Engine автоматизовано порівнює потік із Baseline. У разі виявлення відхилень активується Feedback Loop, ініціюючи сповіщення або автоматичний перезапуск конвеєра перенавчання (Retraining Pipeline).

Висновуючи, застосування ансамблевих методів (таких як Isolation Forest та LOF) на ранніх етапах інгістування даних створює необхідні умови для коректного навчання моделей, допомагаючи алгоритмам фокусуватися на релевантних паттернах, а не на артефактах вибірки. Водночас імплементація надійних статистичних метрик відстані, таких як Wasserstein Distance та PSI, у промисловому середовищі дозволяє організувати ефективну систему раннього попередження про деградацію. Комбінація цих підходів сприяє формуванню комплексного захисного шару в архітектурі MLOps. Це оптимізує процеси підтримки життєвого циклу машинного навчання, підвищує архітектурну надійність інтелектуальних систем та допомагає превентивно адаптувати моделі до мінливих умов реального світу без необхідності ручного втручання на кожному етапі.

Список використаних джерел:

1. Aggarwal C. C. Outlier Analysis. 2nd ed. Cham : Springer, 2017. 484 p.
2. Gama J., Žliobaitė I., Bifet A. A survey on concept drift adaptation // ACM computing surveys (CSUR). 2014. Vol. 46. P. 1–37.
3. Treveil A. et al. Introducing MLOps: How to Scale Machine Learning in the Enterprise. O'Reilly Media, 2020. 275 p.
4. Офіційна документація Evidently AI : вебсайт. URL: <https://www.evidentlyai.com/> (дата звернення: 12.03.2026).