УДК 004.8.052

ІНТЕРПРЕТОВАНІ РЕКОНСТРУКТИВНІ МЕТОДИ ВИЯВЛЕННЯ АНОМАЛІЙ У ПОТОКОВИХ ДАНИХ ІНФОРМАЦІЙНИХ СИСТЕМ

Шендрик О.М.
e-mail: oleksii.shendryk@nure.ua
Науковий керівник – д.т.н., доц. Чала О.В.
Харківський національний університет радіоелектроніки, каф. ІСТ
м. Харків, Україна

Modern information systems process large volumes of continuously arriving streaming data and require timely management decisions under strict time constraints. Real-time monitoring of such systems relies on automated anomaly detection methods, among which reconstructive approaches based on autoencoder encoder–decoder architectures are widely used to learn normal data patterns and detect anomalies through increased reconstruction error. However, these approaches face several limitations, including reconstruction inversion (the ability to reconstruct anomalous data), the inability to distinguish concept drift from true anomalies, and the lack of explainability for detected deviations. The proposed approach aims to reduce false alarms and improve detection accuracy while supporting operator situational awareness in monitoring systems such as telecommunications networks, cybersecurity monitoring platforms, and industrial control systems.

Сучасні безперервні складні системи функціонують в умовах постійної генерації потокових даних, що характеризуються високою швидкістю надходження, багатовимірністю та динамічною зміною статистичних властивостей. Такі системи охоплюють промислові об’єкти, телекомунікаційні мережі, сервіси цифрової економіки, медицину та інші масштабні галузі, де своєчасне виявлення аномалій є критичним для забезпечення надійності, безпеки та ефективності функціонування. Традиційні підходи, що базуються на фіксованих правилах або аналізі накопичених даних, не забезпечують необхідної швидкодії та адаптивності, що обумовлює потребу у розробленні нових інтелектуальних методів аналізу потокових даних.

Одним із перспективних напрямів є адаптивно-реконструктивні методи виявлення аномалій, які поєднують здатність моделей глибокого навчання до відновлення нормальних патернів поведінки системи з механізмами динамічної адаптації до змін середовища. Реконструктивна складова таких методів передбачає побудову моделей типу кодувач-декодувач, що формують латентне представлення нормального режиму функціонування системи та оцінюють ступінь відхилення вхідних даних через похибку реконструкції [1].

Сутність адаптивно-реконструктивного підходу полягає у спільному моделюванні двох процесів: відтворення нормальної поведінки та відокремлення аномальних відхилень з урахуванням часової динаміки даних. На відміну від статичних моделей, такі методи враховують контекст спостережень, міжчасові залежності та структурні взаємозв'язки між компонентами системи. Це дозволяє підвищити чутливість до локальних аномалій при одночасному зменшенні кількості хибних спрацювань, спричинених глобальними змінами розподілу даних.

Разом з тим, класичні реконструктивні моделі мають низку обмежень, що знижують їх ефективність у потокових сценаріях. Зокрема, явище інверсії реконструкції призводить до того, що модель може однаково добре відновлювати як нормальні, так і аномальні спостереження, що ускладнює їх розрізнення. Додатковою проблемою є неможливість чіткого розмежування між дрейфом концепцій та істинними аномаліями, що спричиняє збільшення частоти хибних тривог. Крім того, більшість глибинних моделей залишаються недостатньо інтерпретованими, що обмежує їх застосування у критично важливих системах, де необхідна підтримка ситуаційної обізнаності оператора [2].

Подальший розвиток адаптивно-реконструктивних методів передбачає інтеграцію механізмів компенсації зазначених недоліків. Одним із підходів є декомпозиція похибки реконструкції на складові, що відповідають систематичним змінам нормального стану та локальним відхиленням, що дозволяє диференціювати дрейф концепцій і аномалії [3]. Використання багатокомпонентних архітектур з кількома кодувачами або додатковими дискримінаторними модулями забезпечує підвищення точності ідентифікації аномальних патернів. Адаптивне налаштування рівня шуму та порогових значень дозволяє динамічно регулювати чутливість системи до змін у даних [4].

Важливим аспектом є забезпечення інтерпретованості результатів виявлення аномалій. У цьому контексті перспективним є використання нейросимвольних підходів, що поєднують числові моделі глибинного навчання із символьними представленнями знань. Інтеграція онтологічних моделей предметної області дозволяє відобразити результати аналізу у вигляді зрозумілих для оператора пояснень, встановлюючи зв'язок між величиною похибки реконструкції та семантичними характеристиками системи. Формування багаторівневих пояснень, що включають опис, інтерпретацію та причинно-наслідкові зв'язки, сприяє підвищенню довіри до автоматизованих систем моніторингу [5].

Таким чином, адаптивно-реконструктивні методи виявлення аномалій у потокових даних формують новий клас інтелектуальних технологій,

орієнтованих на роботу в умовах невизначеності та динамічних змін. Їх застосування дозволяє забезпечити безперервний аналіз стану складних систем, знизити кількість хибних спрацювань та підвищити точність виявлення критичних відхилень. Практична реалізація таких методів відкриває можливості для створення інтелектуальних систем моніторингу в галузях, де обробка потокових даних у реальному часі є ключовим фактором ефективності.

Список використаних джерел:

1. Birihanu, E., Singh, K., Masrur Ahmed, A., & Workneh, T. C. (2025). Explainable correlation-based anomaly detection for industrial control systems cybersecurity. *Frontiers in Artificial Intelligence*, *8*, Article 1508821. URL: https://doi.org/10.3389/frai.2024.1508821 (дата звернення 10.03.2026).
2. Cao, Y., Xu, X., Zhang, J., Cheng, Y., Huang, X., Pang, G., & Shen, W. (2024). A survey on visual anomaly detection: Challenge, approach, and prospect. *arXiv preprint arXiv:2401.16402*. URL: https://doi.org/10.48550/arXiv.2401.16402 (дата звернення 10.03.2026).
3. Ekle, O. A., & Eberle, W. (2024). Anomaly detection in dynamic graphs: A comprehensive survey. *ACM Transactions on Knowledge Discovery from Data*, *18*(6), 1-32. URL: https://doi.org/10.1145/3669906 (дата звернення 10.03.2026).
4. Fabian, Z., Tinaz, B., & Soltanolkotabi, M. (2024). Adapt and diffuse: Sample-adaptive reconstruction via latent diffusion models. In *Proceedings of the 41st International Conference on Machine Learning* (pp. 12345-12367). PMLR.
5. Gummadi, A. N., Shaik, T., Hussain, T., & Cherukuri, A. K. (2025). A systematic evaluation of white-box explainable AI methods for enhancing anomaly detection in IoT systems. *Internet of Things*, *29*, Article 101186. URL: https://doi.org/10.1016/j.iot.2025.101186 (дата звернення 10.03.2026).