DOI: 10.34185/1991-7848.itmm.2026.01.072

КОНЦЕПТУАЛЬНІ ОСНОВИ ВИЯВЛЕННЯ АНОМАЛІЙ У ПРОМИСЛОВИХ ІНФОРМАЦІЙНИХ СИСТЕМАХ З ВИКОРИСТАННЯМ МАШИННОГО НАВЧАННЯ

Довидовський Е.О.[1] [ORCID], Гуда А.І.[2] [ORCID], Селівьорстова Т.В.[3] [ORCID]

[1]Український державний університет науки і технологій, аспірант, Україна

[2]Український державний університет науки і технологій,

д.т.н., професор, Україна

[3]Український державний університет науки і технологій, к.т.н., доцент, Україна

Анотація. *У роботі розглянуто підходи до виявлення аномалій у промислових інформаційно-управляючих системах із використанням методів машинного навчання. Проаналізовано особливості функціонування сучасних виробничих середовищ та пов'язані з ними ризики інформаційної безпеки, що виникають у процесі цифрової трансформації промисловості та інтеграції інформаційних технологій у виробничі процеси. Основну увагу приділено моделям неконтрольованого навчання, які дозволяють формувати узагальнене уявлення про нормальний стан системи без попереднього маркування даних. Розглянуто принцип роботи автоенкодера як інструмента виявлення відхилень на основі аналізу помилки реконструкції. Запропоновано узагальнену концептуальну схему виявлення аномалій, що базується на порівнянні фактичних і відновлених значень параметрів та дозволяє інтерпретувати відхилення як потенційні порушення нормального функціонування системи. Робота має теоретичний характер і спрямована на систематизацію існуючих підходів.*

Ключові слова: *машинне навчання, аномалії, інформаційна безпека, автоенкодер, промислові системи, поведінковий аналіз.*

У промисловості останніх років інформаційні системи перестали бути допоміжним інструментом і фактично стали частиною виробничого процесу. Це особливо помітно у випадку інтеграції SCADA, сенсорних мереж та систем аналітики, які працюють у постійному режимі збору та обробки даних. З одного боку, це підвищує керованість процесів, з іншого — створює додаткові точки вразливості.

Проблема полягає в тому, що будь-яке відхилення в роботі таких систем не завжди легко інтерпретувати. У реальних умовах складно однозначно

сказати, чи є певна зміна параметрів наслідком нормального технологічного процесу, чи це вже сигнал про збій або зовнішнє втручання. Саме тому завдання виявлення аномалій не зводиться до простої перевірки значень на вихід за межі допустимих інтервалів.

Класичні підходи, які базуються на наперед визначених правилах, у таких умовах швидко втрачають ефективність. Вони добре працюють у стабільних системах, але погано реагують на нові або нетипові сценарії. У цьому контексті логічним виглядає перехід до моделей, які можуть самостійно формувати уявлення про нормальну поведінку системи.

Якщо розглядати промислову систему не як набір окремих параметрів, а як динамічну структуру, то стає очевидним, що її “нормальність” визначається не конкретними значеннями, а скоріше їх взаємозв’язками. Наприклад, певне значення температури може бути допустимим лише за конкретного тиску або навантаження. Саме такі залежності і становлять інтерес у задачі виявлення аномалій.

У цьому сенсі машинне навчання виконує роль інструмента, який дозволяє ці залежності відновити з даних [1,2,5]. Особливо це стосується підходів неконтрольованого навчання, де модель не отримує готових прикладів “нормального” і “аномального”, а змушена самостійно знаходити структуру в даних. Це не завжди дає однозначні результати, але дозволяє уникнути залежності від попередньо підготовлених вибірок.

Одним із найбільш інтуїтивно зрозумілих прикладів такого підходу є автоенкодер [3]. Його часто описують як механізм стиснення і відновлення даних, але у контексті цієї задачі більш важливо інше — здатність моделі “звикати” до певного типу вхідних сигналів. Після навчання вона відтворює знайомі патерни досить точно, тоді як нетипові — значно гірше.

Це можна інтерпретувати як непряму оцінку відповідності поточного стану системи її типовій поведінці [4]. Якщо відновлення відбувається з помилкою, яка помітно перевищує звичайний рівень, це дає підстави вважати, що система перебуває у нетиповому режимі. Формально така помилка часто задається через середньоквадратичне відхилення (1):

$$L = \frac{1}{n}\sum_{i=1}^{n}(x_i - \hat{x_i})^2, \tag{1}$$

де x_i — фактичне значення параметра системи у момент часу i, $\hat{x_i}$ — відповідне значення, відновлене моделлю, n — загальна кількість спостережень. Величина L відображає середній рівень розбіжності між реальною поведінкою системи та тією, яку модель вважає типовою.

Однак у практичному сенсі важливе не саме значення функції, а спосіб інтерпретації її змін. Вибір порогового рівня, при якому відхилення вважається аномалією, не є універсальним і зазвичай визначається емпірично.

Якщо спробувати узагальнити логіку роботи такої системи, то вона виглядає як послідовний процес: спочатку дані приводяться до зручного вигляду, далі формується модель, яка описує нормальний стан, і вже потім нові спостереження порівнюються з цим описом. При цьому кожен із етапів може впливати на кінцевий результат, іноді навіть сильніше, ніж сама модель.

Окремо варто звернути увагу на те, що поняття аномалії в подібних задачах не є жорстко визначеним. У реальних системах часто трапляються перехідні режими, які формально відрізняються від «нормальних», але не є помилковими. Це створює ситуацію, коли модель повинна балансувати між чутливістю до відхилень і стійкістю до варіацій.

Інші підходи, такі як кластеризація або ізоляційні методи, вирішують подібну задачу інакше, але загальна ідея залишається тією ж [5,6]. Вони також намагаються виділити структуру даних і знайти елементи, які цій структурі не відповідають.

Висновки

Розглянутий підхід до виявлення аномалій базується на досить простій ідеї: замість того, щоб шукати конкретні ознаки загроз, доцільніше описати нормальну поведінку системи і відслідковувати відхилення від неї. Методи машинного навчання, зокрема автоенкодери, надають інструменти для реалізації такого підходу без жорсткої прив’язки до попередньо визначених сценаріїв.

При цьому слід враховувати, що ефективність подібних рішень значною мірою залежить від контексту застосування. Теоретично описана схема може бути реалізована різними способами, і її практична цінність визначається не лише вибором моделі, але й якістю даних та коректністю інтерпретації результатів.

ЛІТЕРАТУРА / REFERENCE

1. Goodfellow I., Bengio Y., Courville A. Deep Learning. Cambridge: MIT Press, 2016. URL: https://www.deeplearningbook.org
2. Chandola V., Banerjee A., Kumar V. Anomaly Detection: A Survey. ACM Computing Surveys. 2009. Vol. 41, No. 3. P. 1–58. DOI: 10.1145/1541880.1541882
3. Hinton G. E., Salakhutdinov R. R. Reducing the dimensionality of data with neural networks. Science. 2006. Vol. 313. P. 504–507. DOI: 10.1126/science.1127647
4. Aggarwal C. C. Outlier Analysis. 2nd ed. Springer, 2017. DOI: 10.1007/978-3-319-47578-3
5. Ahmed M., Mahmood A. N., Hu J. A survey of network anomaly detection techniques. Journal of Network and Computer Applications. 2016. Vol. 60. P. 19–31. DOI: 10.1016/j.jnca.2015.11.016
6. Goh J., Adepu S., Junejo K. N., Mathur A. A dataset to support research in the design of secure water treatment systems (SWaT). International Conference on Critical Information Infrastructures Security. 2016. DOI: 10.1007/978-3-319-71368-7_25

CONCEPTUAL FOUNDATIONS OF ANOMALY DETECTION IN INDUSTRIAL INFORMATION SYSTEMS USING MACHINE LEARNING

Eduard Dovydovskyi, Anton Guda, Tetiana Seliverstova

Abstract. *The paper provides a conceptual overview of anomaly detection in industrial information systems with a focus on machine learning methods. The discussion emphasizes unsupervised approaches for modeling normal system behavior and detecting deviations without predefined attack patterns. The work is descriptive and aims to clarify the underlying principles rather than present experimental validation.*

Keywords: *machine learning, anomaly detection, cybersecurity, autoencoder, industrial systems, behavioral analysis*