Проблеми та обмеження виявлення аномалій у кіберфізичних системах критичної інфраструктури

УДК 004.056:004.8

Ігор Воробець

Тернопільський національний технічний університет імені Івана Пулюя, ihor_vorobets0809@tntu.edu.ua

Питання безпеки критичної інфраструктури набуває особливої актуальності в умовах сучасних воєнних і кіберзагроз, пов'язаних з російсько-українською війною. Об'єкти енергетики, промисловості, транспорту та зв'язку функціонують на основі кіберфізичних систем (КФС), які забезпечують інтеграцію цифрових алгоритмів керування з фізичними процесами та стають цілями кіберфізичних атак, що можуть призводити до порушення їх функціонування та виникнення аварійних ситуацій.

До причин їх вразливості можна віднести складну ієрархічну структуру, а також використання відкритих мережевих протоколів. Атаки на КФС можуть бути спрямовані не лише на порушення конфіденційності інформації, а й на вплив на фізичний стан об'єктів, що призводить до катастрофічних наслідків - від зупинки виробничих процесів до масштабних техногенних аварій [1]. У зв'язку з цим постає необхідність систем моніторингу для раннього виявлення інцидентів безпеки у таких системах.

Для вирішення цієї проблеми часто застосовуються методи машинного навчання (machine learning, ML), зокрема алгоритми виявлення аномалій, що дозволяють ідентифікувати відхилення від нормального функціонування системи [2], зокрема аномальні зміни технологічних параметрів, несанкціоновану зміну режимів роботи обладнання, підміну даних сенсорів або нетипову мережеву активність.

Завдяки автоматизованому аналізу великих обсягів даних методи ML дозволяють виявляти складні закономірності та відхилення у функціонуванні КФС. Однак їх ефективність обмежується низкою чинників, особливо пов'язаних із підготовкою даних для навчання моделей.

Метою роботи є аналіз проблеми дефіциту даних при навчанні ML-моделей у задачах виявлення аномалій у КФС і систематизація підходів до її вирішення в контексті забезпечення безпеки об'єктів критичної інфраструктури.

Специфіка функціонування таких систем полягає в тому, що реальні аномальні події й інциденти безпеки трапляються рідко та мають різні прояви. Це унеможливлює формування збалансованих наборів навчальних даних, що, у свою чергу, спричиняє зниження здатності моделей до узагальнення і ризик некоректної роботи системи виявлення аномалій.

У доповіді проведено аналіз підходів до вирішення проблеми дефіциту аномальних даних при навчанні ML-моделей для виявлення аномалій. Розглянуті підходи доцільно розділити на дві групи.

Перша група складається з підходів, які мінімізують потребу в аномальних даних для навчання моделей. До них належать методи однокласової класифікації (one-class classification, OCC), відповідно до яких ML-модель навчається на нормальних даних та визначає аномалії як відхилення від

визначеної «норми». Використання методів OCC не вимагає наявності аномальних даних при навчанні моделі та загалом є ефективним для задач із суттєвим дисбалансом даних. Водночас моделі на основі OCC часто показують високу чутливість до змін у даних та підвищену кількість помилкових спрацювань [3]. Також можна розглянути методи навчання з малою кількістю прикладів (few-shot learning, FSL), що дозволяють навчати моделі в умовах обмеженої кількості аномальних даних, здійснюючи формування узагальнених представлень даних й оцінюючи подібність між ними. Основною перевагою методів FSL є можливість виявляти аномалії за обмеженої кількості прикладів аномальних даних. Проте їх ефективність значною мірою залежить від формування представлень і вибору архітектури моделі [4].

Підходи другої групи полягають у штучному розширенні навчальної вибірки шляхом генерування синтетичних аномальних даних. Це можна здійснити за допомогою генеративних моделей, які дозволяють моделювати сигнали у КФС і таким чином створювати нові приклади аномалій. Генеративні моделі дозволяють збільшити кількість і різноманітність аномальних прикладів, однак вони можуть характеризуватися нестабільністю навчання, а синтетичні дані не завжди повною мірою відтворюють статистичні характеристики реальних даних [5].

Таким чином, у доповіді проаналізовано проблему дефіциту навчальних даних як одного з ключових обмежень застосування методів виявлення аномалій для попередження кіберфізичних атак на КФС критичної інфраструктури. Розглянуто підходи до вирішення цієї проблеми, які поділено на дві групи: на основі зменшення залежності від аномальних даних, зокрема методи OCC та FSL, і підходи на основі штучного розширення навчальної вибірки з використанням генеративних моделей.

1. Cyber-physical systems security–a survey / A. Humayed et al. IEEE Internet of Things Journal. 2017. Vol. 4, no. 6. P. 1802–1831. URL: https://doi.org/10.1109/jiot.2017.2703172 (дата звернення: 09.05.2026).
2. Deep learning for anomaly detection: a review / G. Pang et al. ACM Computing Surveys. 2021. Vol. 54, no. 2. P. 1–38. URL: https://doi.org/10.1145/3439950 (дата звернення: 09.05.2026).
3. Seliya N., Abdollah Zadeh A., Khoshgoftaar T. M. A literature review on one-class classification and its potential applications in big data. Journal of Big Data. 2021. Vol. 8, no. 1. URL: https://doi.org/10.1186/s40537-021-00514-x (дата звернення: 09.05.2026).
4. Ntalampiras S., Potamitis I. Few-shot learning for modeling cyber physical systems in non-stationary environments. Neural Computing and Applications. 2022. URL: https://doi.org/10.1007/s00521-022-07903-0 (дата звернення: 09.05.2026).
5. Generative adversarial networks for synthetic data generation: a systematic review of techniques, applications, and evaluation methods / R. Thinakaran et al. International Journal of Innovative Research and Scientific Studies. 2025. Vol. 8, no. 5. P. 286–293. URL: https://doi.org/10.53894/ijirss.v8i5.8655 (дата звернення: 09.05.2026).