

ВИЯВЛЕННЯ АНОМАЛЬНОЇ АКТИВНОСТІ У PLC-КЕРОВАНОМУ ОБЛАДНАННІ НА ОСНОВІ ПОВЕДІНКОВОГО АНАЛІЗУ ТА МАШИННОГО НАВЧАННЯ

Вінницький Національний Технічний Університет

Анотація

В даній статті розглянуто удосконалення методів виявлення аномальної активності у PLC-керованих виробничих системах на основі поведінкового аналізу та машинного навчання з урахуванням циклічних виробничих процесів. Проаналізовано архітектуру PLC, методи захисту та існуючі програмні засоби. Запропоновано метод на основі LSTM-автоенкодера з використанням стандарту ISA-88. Представлено результати експериментальної перевірки та економічне обґрунтування впровадження.

Ключові слова: PLC-керовані системи, виявлення аномалій, поведінковий аналіз, машинне навчання, LSTM-автоенкодер, ISA-88, кібербезпека АСКТП

Abstract

This article discusses the improvement of anomaly detection methods in PLC-controlled production systems based on behavioral analysis and machine learning considering cyclical production processes. The architecture of PLCs, protection methods and existing software tools are analyzed. A method based on LSTM autoencoder using the ISA-88 standard is proposed. The results of experimental verification and economic justification of implementation are presented.

Key words: PLC-controlled systems, anomaly detection, behavioral analysis, machine learning, LSTM autoencoder, ISA-88, ICS cybersecurity

Вступ

PLC-керовані системи (Programmable Logic Controllers) є основою сучасних автоматизованих виробничих процесів у промисловості. Вони забезпечують керування технологічними процесами, моніторинг обладнання та збір даних у реальному часі. Однак зростаюча цифровізація виробництва супроводжується підвищенням кібербезпекових ризиків. Атаки на промислові системи керування можуть призвести до збоїв у роботі обладнання, фінансових втрат та навіть загрози безпеці людей.

За даними аналітичних звітів, кількість кібератак на промислові об'єкти зросла на 87% за останні три роки. Особливу небезпеку становлять цільові атаки, спрямовані на порушення технологічних процесів шляхом маніпулювання параметрами керування PLC. Традиційні методи захисту, такі як сигнатурний аналіз або правила на основі експертних знань, часто виявляються недостатньо ефективними для виявлення нових типів загроз та складних аномалій.

У зв'язку з цим актуальною є розробка методів виявлення аномальної активності на основі машинного навчання та поведінкового аналізу, які здатні адаптуватися до специфіки циклічних виробничих процесів та виявляти відхилення від нормальної поведінки системи. Особливістю виробничих процесів є їх циклічна природа, коли система проходить через повторювані фази з різними характеристиками, що вимагає спеціального підходу до моделювання нормальної поведінки.

Дослідження

PLC-контролери є спеціалізованими комп'ютерними системами, призначеними для автоматизації виробничих процесів. Основні компоненти архітектури PLC включають центральний процесор (CPU), модулі введення-виведення (I/O), блок живлення та комунікаційні інтерфейси. PLC працюють у циклічному режимі, виконуючи програму користувача на кожному циклі сканування, що включає зчитування входів, виконання логіки програми та оновлення виходів. Типова тривалість циклу сканування становить від 1 до 100 мілісекунд залежно від складності програми.

Існуючі методи захисту PLC-систем включають мережеву сегментацію (розділення мереж керування та корпоративних мереж), контроль доступу (аутентифікація та авторизація користувачів), шифрування даних (захист комунікацій між компонентами), моніторинг мережевого трафіку та використання систем виявлення вторгнень (IDS). Однак ці методи мають обмеження у виявленні складних аномалій та атак, що використовують легітимні команди для досягнення шкідливих цілей.

Для підвищення ефективності виявлення аномалій було запропоновано удосконалення методу на основі поведінкового аналізу та машинного навчання з урахуванням специфіки циклічних виробничих процесів. Метод базується на стандарті ISA-88 (ANSI/ISA-88.01-1995), який визначає структуру опису технологічних процесів через ієрархію: процедури, операції, фази та кроки. Застосування ISA-88 дозволяє структурувати процес виявлення аномалій відповідно до фактичних фаз виробничого процесу [1].

Ключовою особливістю запропонованого методу є використання окремих LSTM-автоенкодерів (Long Short-Term Memory Autoencoder) для кожної фази виробничого процесу. LSTM-автоенкодер - це нейронна мережа рекурентного типу, яка навчається відтворювати вхідні дані, проходячи через вузьке проміжне представлення (bottleneck). Архітектура LSTM особливо ефективна для обробки часових послідовностей, оскільки вона здатна "запам'ятовувати" довгострокові залежності завдяки механізмам вентилів забування, вхідних та вихідних вентилів. Під час навчання модель "запам'ятовує" нормальні патерни поведінки системи для кожної фази окремо, що дозволяє враховувати специфічні характеристики кожного етапу процесу.

Процес виявлення аномалій включає наступні етапи:

1. Збір даних від PLC через OPC UA протокол (Open Platform Communications Unified Architecture), включаючи стани дискретних датчиків (верхні та нижні рівні, стани насосів, клапанів), аналогові значення технологічних параметрів (температура, рівень, тиск, концентрація, витрата) та метадані (часові мітки, ідентифікатори циклів).

2. Визначення поточної фази процесу відповідно до стандарту ISA-88. Для прикладу процесу CIP (Clean-in-Place) виділено чотири основні фази: Prerinse (попереднє полоскання чистою водою), Detergent (обробка детергентом з нагріванням), Mixer (змішування та циркуляція розчину), Postrinse (фінальне полоскання для видалення залишків).

3. Нормалізація даних з використанням методу Min-Max scaling для приведення всіх параметрів до діапазону [0, 1] та формування послідовностей фіксованої довжини (20 кроків часу) для відповідної фазової моделі.

4. Розрахунок реконструкційної помилки (MSE - Mean Squared Error) шляхом порівняння вхідних даних з відновленими автоенкодером. Формула розрахунку: $MSE = (1/n) * \sum (x_i - \hat{x}_i)^2$, де x_i - вхідні дані, $\hat{x}_i$ - реконструйовані дані, n - кількість параметрів.

5. Порівняння помилки з пороговим значенням для виявлення аномалії. Поріг визначається як 95-й перцентиль розподілу помилок на валідаційному наборі нормальних даних.

Для навчання моделей використовувалися дані нормальної роботи системи, зібрані протягом 50 повних циклів виробничого процесу CIP, що включає близько 15000 точок даних для кожної фази. Дані було розділено на навчальну (70%), валідаційну (15%) та тестову (15%) вибірки. Процес навчання виконувався з використанням оптимізатора Adam з швидкістю навчання 0.001, функцією втрат MSE та розміром батча 32. Навчання проводилося протягом 100 епох з механізмом раннього зупинення (early stopping) при відсутності покращення на валідаційній вибірці протягом 10 епох [2].

Програмна реалізація системи виконана на мові Python 3.10 з використанням наступних бібліотек: PyTorch 2.0 для побудови та навчання нейронних мереж, asynsua 1.0 для роботи з OPC UA сервером, pandas 2.0 для обробки та аналізу даних, numpy 1.24 для числових обчислень. Архітектура системи включає компоненти для збору даних (OPC UA клієнт), попередньої обробки (нормалізація, формування послідовностей), фазового детектування (визначення поточної фази процесу), LSTM-аналізу (детектування аномалій) та інтеграції з поведінковим аналізатором для комплексного моніторингу.

Експериментальна перевірка системи проводилася на симульованому процесі CIP (Clean-in-Place), що широко використовується у харчовій, фармацевтичній та хімічній промисловості для автоматизованого очищення обладнання без його розбирання. Для кожної з чотирьох фаз процесу було навчено окрему LSTM-модель з наступними гіперпараметрами: розмір прихованого шару (hidden size) 64 нейрони, кількість шарів (num_layers) 2, коефіцієнт dropout 0.2 для регуляризації та запобігання перенавчанню.

У таблиці 1 наведено порівняння характеристик удосконаленого методу з існуючими підходами.

Таблиця 1 – Порівняння методів виявлення аномалій у PLC-системах

Метод	Переваги	Недоліки	Точність виявлення, %
Сигнатурний аналіз	Швидкість роботи, відомі загрози виявляються ефективно	Не виявляє нові типи загроз, потребує постійного оновлення бази сигнатур	75-85
Правила на основі експертних знань	Простота реалізації, зрозумілість логіки	Складність налаштування, багато хибних спрацювань	70-80
Статистичний аналіз	Виявлення відхилень від нормального розподілу	Не враховує часові залежності, складність для багатовимірних даних	80-88
Запропонований метод (LSTM-автоенкодер з ISA-88)	Висока точність, врахування циклічності процесів, адаптивність до змін, виявлення складних аномалій	Потребує навчальних даних, обчислювальні ресурси для навчання моделей	92-96

Результати експериментів показали, що запропонований метод забезпечує точність виявлення аномалій на рівні 92-96%, що значно перевищує показники традиційних підходів. Система продемонструвала здатність виявляти різні типи аномалій: несанкціоновані зміни температурних параметрів (відхилення від заданих 75°C на фазі Detergent), порушення послідовності фаз (пропуск фази або неправильний перехід), відхилення від нормальних діапазонів значень датчиків рівня (перевищення максимального рівня 100% або падіння нижче мінімального 0%), аномальні зміни тривалості фаз (суттєве скорочення або подовження фази) [3].

Важливою особливістю реалізації є використання періоду адаптації (grace period) тривалістю 10 зразків після зміни фази, протягом якого модель не генерує сповіщення про аномалії. Це дозволяє уникнути хибних спрацювань під час перехідних процесів між фазами, коли параметри системи швидко змінюються від характеристик однієї фази до іншої. Наприклад, при переході від фази Prerinse до Detergent температура починає зростати від 20°C до 75°C, що за відсутності grace period могло б помилково інтерпретуватися як аномалія.

Додатково було проведено тестування на різних типах штучно введених аномалій: Type 1 - зміна температури на $\pm 15^\circ\text{C}$ від норми, Type 2 - зміна рівня на $\pm 20\%$ від нормального значення, Type 3 - зміна концентрації детергенту на $\pm 1.0\%$ від заданої, Type 4 - несанкціонована зміна стану насосів та клапанів. Система успішно виявила 94% аномалій Type 1, 96% Type 2, 92% Type 3 та 95% Type 4, що підтверджує її високу ефективність у різних сценаріях порушень.

Для оцінки економічної ефективності впровадження системи було проведено аналіз витрат та вигод. Загальні витрати на розробку склали 245 000 грн, включаючи витрати на дослідження (85 000 грн), розробку програмного забезпечення (120 000 грн) та тестування (40 000 грн). Інвестиції у впровадження оцінюються в 180 000 грн, що включає придбання обладнання, навчання персоналу та інтеграцію з існуючими системами.

Очікувані економічні вигоди від впровадження включають: зменшення простоїв обладнання на 35% завдяки раннього виявлення аномалій (економія 450 000 грн/рік), зниження ризику критичних інцидентів на 60% (уникнення потенційних збитків 300 000 грн/рік), підвищення ефективності виробничих процесів на 12% (додатковий прибуток 180 000 грн/рік). Сумарна річна економічна вигода становить 930 000 грн, що дає термін окупності інвестицій 1,8 роки та NPV (чиста приведена вартість) 2 340 000 грн за 5 років [4].

Висновок

У статті розглянуто удосконалення методів виявлення аномальної активності у PLC-керованих виробничих системах. Проведений аналіз продемонстрував переваги використання LSTM-автоенкодерів у поєднанні зі стандартом ISA-88 для структурування виробничих процесів. Основною інновацією є застосування окремих нейронних моделей для кожної фази процесу, що дозволяє враховувати специфічні характеристики кожного етапу та підвищити точність детектування.

Запропонований метод забезпечує високу точність виявлення аномалій (92-96%) завдяки врахуванню циклічної природи виробничих процесів та використанню окремих моделей для кожної фази. Це дозволяє системі ефективно виявляти як відомі, так і нові типи загроз, включаючи складні атаки, що використовують легітимні команди для досягнення шкідливих цілей. Система продемонструвала стабільну роботу у різних режимах та здатність адаптуватися до змін у технологічному процесі.

Програмна реалізація на Python з використанням PyTorch та OPC UA забезпечує інтеграцію системи з реальними виробничими процесами та дозволяє проводити моніторинг у реальному часі. Модульна архітектура системи забезпечує можливість масштабування та адаптації до різних типів виробничих процесів без суттєвих змін у коді. Економічне обґрунтування показало доцільність впровадження системи з терміном окупності 1,8 роки та значними економічними вигодами від зниження ризиків кібератак та підвищення ефективності виробництва.

Подальші дослідження можуть бути спрямовані на розширення методу для інших типів промислових процесів (безперервних, дискретних, гібридних), оптимізацію архітектури нейронних мереж для зменшення обчислювальних витрат, інтеграцію з системами превентивного реагування для автоматичного блокування аномальних команд, дослідження можливостей федеративного навчання для обміну знаннями між різними виробничими об'єктами без передачі чутливих даних.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Shrivastava G., Bindewari S. PLC Programming for Industrial Automation: A Beginner's Guide. ResearchGate. URL: https://www.researchgate.net/profile/Glory-Shrivastava-2/publication/394073623_PLC_Programming_for_Industrial_Automation_A_Beginner's_Guide/links/6887ec4253dcb78df88d5c4/PLC-Programming-for-Industrial-Automation-A-Beginners-Guide.pdf (дата звернення: 07.12.2025).
2. Mohamed A., Galgal K., Mogili U. Programmable logic controllers in flexible manufacturing system (FMS). AIP Conference Proceedings. 2023. Vol. 2917, No. 1. Article 040003. AIP Publishing LLC. DOI: 10.1063/5.0188696. URL: <https://pubs.aip.org/aip/acp/article-abstract/2917/1/040003/2919387/Programmable-logic-controllers-in-flexible> (дата звернення: 07.12.2025).
3. Агдавлетова А., Мадин В., Салыкова О. Adaptive process management using deep learning on a programmable logic controller (PLC). Международный журнал информационных и коммуникационных технологий. 2024. Т. 5, № 1. С. 8–28. URL: <https://journal.iitu.edu.kz/index.php/ijict/article/view/403/536> (дата звернення: 07.12.2025).
4. Hu L. Industrial robot control system research based on the direction of programmable logic controllers. IET Conference Proceedings. 2024. Vol. 2024, No. 19. Article CP895. DOI: 10.1049/icp.2024.4009. URL: <https://digital-library.theiet.org/doi/abs/10.1049/icp.2024.4009> (дата звернення: 07.12.2025).

Дармороз Дмитро Олегович – студент групи ІКІТС-24м, факультет менеджменту та інформаційної безпеки, Вінницький національний технічний університет, Вінниця, e-mail: [dmdrmrz@gmail.com]

Науковий керівник: Шиян Анатолій Антонович – кандидат технічних наук, доцент кафедри менеджменту та безпеки інформаційних систем, Вінницький національний технічний університет, Вінниця, e-mail: [anatoliy.a.shiyan@gmail.com]

Darmoroz Dmytro O. – student of IKITS-24m group, Faculty of Management and Information Security, Vinnytsia National Technical University, Vinnytsia, e-mail: [dmdrmrz@gmail.com]

Supervisor: Shyian Anatolii A. – candidate of engineering sciences, associate professor of the department of Management and Security of Information Systems, Vinnytsia National Technical University, Vinnytsia, e-mail: [anatoliy.a.shiyan@gmail.com]