Міністерство освіти і науки України

Харківський національний університет радіоелектроніки

Кафедра комп'ютерно-інтегрованих технологій, автоматизації, робототехніки та безпекової інженерії

II Всеукраїнська конференція «Інтелектуальні технології цивільної безпеки та робототехнічні системи аварійно-рятувальних робіт»

II All-Ukrainian Conference “Intelligent Civil Safety Technologies and Robotic Systems for Emergency and Rescue Operations”

ICSTRO

2026

I All-Ukrainian Conference

September 17 - 18, 2026

Kharkiv

ЗМІСТ

АВТОМАТИЗОВАНІ СИСТЕМИ ВИЯВЛЕННЯ АНОМАЛІЙ У РОБОТІ ТЕХНОЛОГІЧНОГО ОБЛАДНАННЯ НА ОСНОВІ АНАЛІЗУ ЦИФРОВИХ ПРОТОКОЛІВ ОБМІНУ (MODBUS, DNP3)

Б. І. Кислий, С. В. Сотник
Харківський національний університет радіоелектроніки
Україна, 61166, Харків, пр. Науки, 14
E-mail: bohdan.kyslyi@nure.ua, svetlana.sotnik@nure.ua

Анотація: У роботі досліджено особливості автоматизованого виявлення аномалій у функціонуванні технологічного обладнання шляхом аналізу цифрових протоколів промислового обміну даними Modbus та DNP3. Розглянуто принципи функціонування зазначених протоколів, їх застосування в автоматизованих системах керування технологічними процесами та потенційні кіберзагрози, пов'язані з їх використанням. Проаналізовано сучасні методи моніторингу мережевого трафіку, виявлення відхилень від нормальної роботи обладнання та застосування алгоритмів машинного навчання для своєчасного виявлення аномальної активності. Обґрунтовано доцільність використання автоматизованих систем аналізу промислового трафіку як ефективного засобу підвищення надійності та безпеки кіберфізичних систем.

Ключові слова: кіберфізичні системи, SCADA, Modbus, DNP3, виявлення аномалій, промислова кібербезпека, технологічне обладнання, IDS.

AUTOMATED SYSTEMS FOR DETECTING ANOMALIES IN THE OPERATION OF PROCESS EQUIPMENT BASED ON THE ANALYSIS OF DIGITAL COMMUNICATION PROTOCOLS (MODBUS, DNP3)

B. I. Kyslyi, S. V. Sotnik
Kharkiv National University of Radio Electronics
Ukraine, 61166, Kharkiv, Nauky Ave., 14
E-mail: bohdan.kyslyi@nure.ua, svetlana.sotnik@nure.ua

Annotation: The work examines the characteristics of automated anomaly detection in the operation of process equipment through the analysis of the Modbus and DNP3 industrial data exchange protocols. It examines the operating principles of these protocols, their application in automated process control systems, and the potential cyber threats associated with their use. The paper analyzes modern methods for monitoring network traffic, detecting deviations from normal equipment operation, and applying machine learning algorithms for the timely detection of anomalous activity. It justifies the use of automated industrial traffic analysis systems as an effective means of improving the reliability and security of cyber-physical systems.

Key words: cyber-physical systems, SCADA, Modbus, DNP3, anomaly detection, industrial cybersecurity, process equipment, IDS.

У сучасних умовах цифровізації промисловості кіберфізичні системи та автоматизовані системи керування технологічними процесами широко застосовуються в критичній інфраструктурі. Використання віддаленого доступу, корпоративних і хмарних мереж підвищує ризик несанкціонованого втручання в роботу технологічного обладнання [1-8]. Під **виявленням аномалій** у контексті даного дослідження розуміють процес автоматизованого визначення відхилень параметрів мережевого трафіку та режимів роботи обладнання від встановленої моделі нормального функціонування системи, що може свідчити про кібератаку, технічну несправність або порушення регламенту експлуатації. Своєчасне виявлення таких

відхилень є одним із засобів запобігання аваріям та техногенним надзвичайним ситуаціям на об'єктах критичної інфраструктури, оскільки дозволяє зупинити розвиток інциденту ще на ранній стадії – до настання фізичних наслідків для обладнання, персоналу чи довкілля. Особливу небезпеку становлять промислові протоколи Modbus та DNP3, які широко використовуються для обміну даними. У зв'язку з цим актуальним є застосування автоматизованих систем аналізу промислового трафіку для своєчасного виявлення аномалій та потенційних кіберзагроз як складової забезпечення техногенної та цивільної безпеки.

Основу сучасних автоматизованих систем керування технологічними процесами становлять SCADA-комплекси, програмовані логічні контролери (PLC), датчики, виконавчі механізми та мережеві засоби обміну даними. Передача інформації між компонентами системи здійснюється за допомогою спеціалізованих промислових протоколів, серед яких найбільш поширеними є Modbus та DNP3. Коректність та безпека обміну даними за цими протоколами є важливими чинниками стабільного функціонування технологічного обладнання [9].

Одним із найбільш перспективних напрямів підвищення безпеки промислових мереж є використання автоматизованих систем виявлення аномалій (Anomaly Detection Systems). Такі системи здійснюють безперервний моніторинг мережевого трафіку, аналізують параметри обміну даними та виявляють відхилення від нормального режиму роботи обладнання. На відміну від сигнатурних систем виявлення вторгнень, які реагують лише на відомі шаблони атак, системи виявлення аномалій здатні виявляти нові або модифіковані загрози, що раніше не спостерігалися в мережі.

Протокол Modbus є одним із найстаріших і найпоширеніших промислових протоколів обміну даними. Його було розроблено компанією Modicon ще у 1979 році. Популярність протоколу пояснюється простотою реалізації, відкритою специфікацією та широкою підтримкою виробниками обладнання. Проте базова версія Modbus передає дані у відкритому вигляді та не передбачає механізмів автентифікації, шифрування або перевірки цілісності повідомлень. Це створює можливість перехоплення трафіку, підміни команд та несанкціонованого керування обладнанням. Аналіз трафіку Modbus дозволяє виявляти аномальні функціональні коди, нетипові адреси регістрів, різке збільшення кількості запитів, повторювані команди запису та інші ознаки потенційної атаки [10].

Іншим поширеним протоколом промислового обміну є DNP3 (Distributed Network Protocol), який широко застосовується в енергетичних системах, електричних підстанціях, системах диспетчерського керування та телемеханіки. Порівняно з Modbus він має складнішу структуру кадрів і підтримує події, часові мітки та додаткові механізми контролю обміну. Механізми Secure Authentication для DNP3 забезпечують додатковий захист автентичності та цілісності обміну, однак рівень захисту залежить від конкретної реалізації та конфігурації системи. У таких умовах автоматизований аналіз трафіку DNP3 може виявляти аномальні послідовності команд, підозрілі зміни часових міток, нетипову активність окремих пристроїв та інші ознаки несанкціонованого втручання.

Порівняльні характеристики протоколів Modbus та DNP3 і основні ознаки аномальної активності наведено в табл. 1.

Для складніших сценаріїв дедалі частіше застосовуються методи машинного навчання: дерева рішень, випадкові ліси, метод опорних векторів, k-середніх, нейронні мережі та автоенкодери. Такі алгоритми здатні враховувати велику кількість параметрів одночасно та виявляти приховані закономірності в даних. Особливий інтерес становлять автоенкодери, які навчаються відновлювати нормальні дані; якщо похибка відновлення перевищує встановлений поріг, система сигналізує про можливу аномалію.

Таблиця 1 – Порівняльні характеристики протоколів Modbus та DNP3

Характеристика	Modbus	DNP3
Основна сфера застосування	Промислова автоматизація, PLC, SCADA	Енергетика, підстанції, телемеханіка
Структура обміну	Відносно проста	Складніша, підтримує події та часові мітки
Захист у базовій реалізації	Відсутні механізми автентифікації та шифрування	Залежить від реалізації та конфігурації Secure Authentication
Ознаки аномальної активності	Нетипові функціональні коди, адреси регістрів, частота запитів, повторні команди запису	Аномальні послідовності команд, часові мітки, нетипова активність пристроїв
Основні підходи до виявлення	Аналіз трафіку, поведінковий аналіз, машинне навчання (МН)	Аналіз трафіку, поведінковий аналіз, МН

Важливою особливістю промислових мереж є необхідність мінімального впливу системи моніторингу на технологічний процес. Тому значна частина рішень реалізується у пасивному режимі, коли аналізатор лише копіює мережевий трафік через SPAN-порт комутатора або мережевий TAP (Test Access Point) і не втручається у процес обміну даними. Такий підхід дозволяє уникнути затримок у передачі команд керування та зберегти безперервність технологічного процесу.

Автоматизовані системи виявлення аномалій можуть інтегруватися з центрами моніторингу безпеки (SOC), SIEM-платформами та системами керування інцидентами. У разі виявлення підозрілої активності система автоматично формує повідомлення, зберігає мережеві журнали, визначає потенційно уражений сегмент мережі та передає інформацію оператору або засобам автоматичного реагування. Це значно скорочує час виявлення інциденту та підвищує ефективність реагування [11].

Особливу увагу з погляду кібербезпеки потребують промислові протоколи Modbus та DNP3, які широко використовуються для обміну даними. Такі дії можуть залишатися непоміченими протягом тривалого часу та спричиняти приховане погіршення якості продукції або підвищення ризику аварійної ситуації.

Реальність зазначених загроз підтверджується задокументованими інцидентами у критичній інфраструктурі України. Зокрема, у 2022 році угруповання Sandworm здійснило кібератаку на енергетичний об'єкт України, отримавши доступ до операційного технологічного середовища через інфраструктуру, пов'язану зі SCADA-системою, та здійснивши спробу впливу на роботу електричних підстанцій. Для реалізації атаки використовувалися штатні засоби операційного середовища та програмне забезпечення MicroSCADA [12]. Інцидент засвідчив реальність загроз для промислових систем керування та необхідність постійного моніторингу аномальної активності. Подібні випадки засвідчують, що вразливості промислових систем становлять не лише технічну, а й безпосередню загрозу для цивільного населення, оскільки порушення роботи об'єктів енергетики, водопостачання чи теплопостачання може мати каскадний вплив на суміжні системи життєзабезпечення.

Застосування таких систем особливо важливе для об'єктів критичної інфраструктури, де навіть короткочасне порушення роботи обладнання може призвести до масштабних техногенних наслідків. Наприклад, несанкціонована зміна параметрів релейного захисту на підстанції, зміна режиму роботи насосного обладнання або втручання в систему керування котельнею може спричинити аварійну ситуацію, пошкодження обладнання та значні

економічні втрати. Раннє виявлення аномальної активності дозволяє запобігти розвитку інциденту ще до виникнення фізичних наслідків.

Разом із перевагами системи виявлення аномалій мають і певні обмеження. Однією з основних проблем є наявність хибнопозитивних спрацювань, коли нормальна, але рідкісна поведінка обладнання помилково класифікується як атака. Крім того, для якісного навчання моделей необхідно мати достатній обсяг достовірних даних про роботу технологічного процесу, що не завжди можливо для нових або модернізованих виробничих систем.

Перспективним напрямом подальших досліджень є створення гібридних систем, які поєднують сигнатурний аналіз, поведінкове моделювання та методи машинного навчання. Додатково розглядається використання цифрових двійників технологічних процесів для перевірки підозрілих команд у віртуальному середовищі перед їх виконанням на реальному обладнанні. Такий підхід дозволяє підвищити точність виявлення атак та зменшити кількість хибних спрацювань.

ВИСНОВКИ. Отже, автоматизований аналіз промислового трафіку Modbus та DNP3 дозволяє виявляти відхилення від нормальної моделі функціонування технологічного обладнання та своєчасно формувати ознаки потенційних кіберінцидентів. Встановлено, що поєднання аналізу параметрів та часових характеристик обміну з алгоритмами машинного навчання розширює можливості виявлення як відомих, так і нетипових сценаріїв несанкціонованого втручання. Застосування пасивного моніторингу забезпечує контроль промислового трафіку без безпосереднього впливу на технологічний процес. Водночас ефективність таких систем залежить від якості моделі нормальної поведінки та навчальних даних, а наявність хибнопозитивних спрацювань потребує подальшого вдосконалення методів аналізу. Перспективним напрямом є поєднання сигнатурного аналізу, поведінкового моделювання та машинного навчання, зокрема із застосуванням цифрових двійників технологічних процесів.

ЛІТЕРАТУРА

1. Nevliudov, I., & et al. (2026). Implementing Industry 5.0 technologies in civil safety emergency systems for intelligent management. Scientific Forum: Theory and Practice of Research: Collection of Scientific Papers «SCIENTIA» with Proceedings of the XII International Scientific and Theoretical Conference, July 17, 2026. San Francisco, USA: International Center of Scientific Research, pp. 337-339

2. Ievtushenko, V. I., & et al. (2026). Evolution of SCADA architecture: from centralized models to cloud-based solutions. Computer-integrated technologies, automation and robotics 2026: Proceedings of III st All-Ukrainian Conference, Kharkiv, May 14-15, 2026: Thesises of Reports, pp. 49-53

3. Bielyi, Y., & et al. (2026). Implementing a Secure Data Transmission Channel Based on Mesh VPN Under Limited IPv4 Addressing. International Journal of Academic Information Systems Research (IJAISR), Vol. 10, Issue 6, pp. 30-37

4. Sotnik, S. (2026). Performance and Simulation-Based Comparison of IoT Access Control Systems Using ESP32, Arduino Uno, and Raspberry Pi Pico W. Applied Cybersecurity & Internet Governance, Vol. 5, №1, pp. 1-32. DOI: 10.60097/ACIG/221089

5. Taran, A., et al. (2026). Impact of 5G/6G Networks on the Development of IOT, Robotics, and Autonomous Systems. Low Latest and Mass Connection of Devices. All-Ukrainian Conference “Intelligent Civil Safety Technologies and Robotic Systems for Emergency and Rescue Operations” (ICSTRO-2026) February 12-13, 2026, pp. 114-118

6. Marunich, R., & et al. (2026). Security Analysis of Protocols for Integration With Access Control System. All-Ukrainian Conference “Intelligent Civil Safety Technologies and Robotic Systems for Emergency and Rescue Operations” (ICSTRO-2026) February 12-13, 2026, pp. 59-63

7. Mandrykov, K., & et al. (2026). Comparative Analysis of Industrial Data Transmission Protocols (IIOT) in Automation Systems. All-Ukrainian Conference “Intelligent Civil Safety Technologies and Robotic Systems for Emergency and Rescue Operations” (ICSTRO-2026) February 12-13, 2026, pp. 49-53

8. Cherednichenko, T., & et al. (2025). Features of automatic working time control systems. Manufacturing & Mechatronic Systems 2025: Proceedings of IX st International Conference, Kharkiv, October 25-26, 2025: Thesises of Reports, pp. 54-57

9. Rahman, W., & et al. (2025). Modbus/DNP3 Over TCP/IP implementation on TMDSCNCD28388D and Arduino with Simulink HMI for Iot-based cybersecure electrical systems. International Journal of Business and Economics Insights, 5(3), 494-522

10. Varol, M., & et al. (2025). An intrusion detection system for critical infrastructures: Modbus approach. Engineering Applications of Artificial Intelligence, 162, 112410.

11. Tilbury, J., & et al. (2024). Humans and automation: Augmenting security operation centers. Journal of Cybersecurity and Privacy, 4(3), pp. 388-409

12. Russia’s Sandworm hackers behind power blackouts in Ukraine amid massive missile strikes. cybersecurity help. Режим доступу: https://www.cybersecurity-help.cz/blog/3602.html**.** (Дата звернення 06.08.2026)