РОЛЬ ШТУЧНОГО ІНТЕЛЕКТУ У ЗАБЕЗПЕЧЕННІ БЕЗПЕКИ ПРОМИСЛОВИХ ОБ'ЄКТІВ

Павленко Вікторія Петрівна[1]

Опубліковано	Секція	УДК
30.06.2025	Економіка	338

DOI: https://doi.org/10.5281/zenodo.17166574

Анотація. У статті розглянуто використання штучного інтелекту (ШІ) для забезпечення безпеки промислових об'єктів на основі аналізу сучасних технологій моніторингу, прогнозування та кібербезпеки. Глобалізація та стрімкий розвиток технологій створили нові виклики для промислових підприємств, які повинні забезпечити високий рівень безпеки у складних умовах. Традиційні методи контролю та діагностики, що базуються на статичних протоколах, ручних перевірках і простих алгоритмах виявлення несправностей, стають дедалі менш ефективними в сучасних умовах. Зростаючий обсяг даних, отриманих з різноманітних сенсорів, пристроїв Індустріального Інтернету Речей та інших систем моніторингу, створює як можливості для вдосконалення контролю, так і ризики, пов'язані з оперативним аналізом і швидким реагуванням на можливі кіберзагрози.

У роботі проведено аналіз існуючих наукових досліджень та практичних розробок у галузі використання ШІ для підвищення безпеки промислових систем. Зокрема, увага приділяється застосуванню кіберфізичних систем, що об'єднують фізичні процеси з кіберкомпонентами. Використання ШІ в таких системах забезпечує раннє виявлення загроз та своєчасне реагування на кібератаки. Проте виклики, пов'язані з адаптацією новітніх технологій до вже існуючих виробничих процесів, залишаються актуальними та вимагають створення нових підходів до обробки гетерогенних даних.

Показано, що інтеграція інтелектуальних алгоритмів у промислові системи безпеки дозволяє значно підвищити точність прогнозування аварійних ситуацій та мінімізувати кількість помилкових спрацьовувань. Завдяки алгоритмам глибинного навчання та аналізу часових рядів можна ефективно виявляти аномальні ситуації задовго до виникнення аварій. Дослідження демонструють, що використання сенсорів вібрації та температури в поєднанні з нейронними мережами сприяє зменшенню часу простою обладнання та запобіганню аваріям.

Зазначено, що актуальність теми зумовлена необхідністю оптимізації промислових процесів за допомогою інтелектуальних систем. Зокрема, забезпечення кібербезпеки набуває особливого значення у зв'язку з високою вразливістю автоматизованих систем до кібератак. Результати дослідження можуть бути використані як основа для розробки нових методик інтеграції ШІ у промислові системи безпеки, що дозволить покращити їхню надійність та адаптивність до змінних умов експлуатації.

[1] Старший науковий співробітник
Український науково-дослідний інститут
спеціальної техніки та судових експертиз
Служби безпеки України
https://orcid.org/0000-0003-2303-0993

Ключові слова: штучний інтелект, безпека промислових об’єктів, прогнозування аварій, автоматизований моніторинг, інтелектуальні системи, кібербезпека.

THE ROLE OF ARTIFICIAL INTELLIGENCE IN ENSURING THE SAFETY OF INDUSTRIAL FACILITIES

Abstract. The article considers the use of artificial intelligence (AI) to ensure the safety of industrial facilities based on the analysis of modern monitoring, forecasting and cybersecurity technologies. Globalization and the rapid development of technologies have created new challenges for industrial enterprises, which must ensure a high level of safety in difficult conditions. Traditional control and diagnostic methods based on static protocols, manual checks and simple fault detection algorithms are becoming less and less effective in modern conditions. The growing volume of data obtained from various sensors, Industrial Internet of Things devices and other monitoring systems creates both opportunities for improving control and risks associated with operational analysis and rapid response to possible cyber threats. The paper analyzes existing scientific research and practical developments in the field of using AI to improve the safety of industrial systems. In particular, attention is paid to the application of cyber-physical systems that combine physical processes with cyber components. The use of AI in such systems ensures early detection of threats and timely response to cyberattacks. However, the challenges associated with adapting the latest technologies to existing production processes remain relevant and require the creation of new approaches to processing heterogeneous data.

It has been shown that the integration of intelligent algorithms into industrial security systems can significantly increase the accuracy of predicting emergency situations and minimize the number of false positives. Thanks to deep learning algorithms and time series analysis, it is possible to effectively detect abnormal situations long before accidents occur. Studies show that the use of vibration and temperature sensors in combination with neural networks helps reduce equipment downtime and prevent accidents.

It is noted that the relevance of the topic is due to the need to optimize industrial processes using intelligent systems. In particular, ensuring cybersecurity is of particular importance due to the high vulnerability of automated systems to cyberattacks. The research results can be used as a basis for developing new methods for integrating AI into industrial safety systems, which will improve their reliability and adaptability to changing operating conditions.

Keywords: artificial intelligence, industrial facility safety, accident prediction, automated monitoring, intelligent systems, cybersecurity.

Вступ

Постановка проблеми. Сучасні промислові об’єкти є унікальними комплексними системами, в яких об’єднуються автоматизоване обладнання, комп’ютерні мережі та системи управління, що взаємодіють із фізичним середовищем. Сучасна промисловість стикається з численними викликами у сфері безпеки виробничих процесів.

З одного боку, активне впровадження автоматизації та цифровізації значно підвищує ефективність і продуктивність виробництва, але з іншого — створює нові ризики та загрози. Основні проблеми пов’язані з технічними збоями, кібератаками та людським фактором, які можуть призвести до значних матеріальних втрат, зупинки виробництва або навіть екологічних катастроф.

Автоматизовані промислові системи потребують безперебійного функціонування, але їхня складність збільшує ризик виникнення помилок. Наприклад, збій у системах управління може призвести до критичних аварій або збоїв у виробничих процесах [1, 2].

Крім того, сучасні виробничі системи часто під'єднані до глобальної мережі, що робить їх уразливими до кіберзагроз. Інциденти з несанкціонованим доступом, зловмисним програмним забезпеченням та витоком конфіденційної інформації піддають ризику всю виробничу інфраструктуру. Штучний інтелект (ШІ) є інноваційним інструментом для вирішення цих проблем.

Він дозволяє не лише моніторити стан обладнання та виявляти несправності на ранніх стадіях, але й аналізувати величезні обсяги даних для прогнозування аварійних ситуацій. Однак, попри очевидні переваги, інтеграція ШІ в системи безпеки промислових об'єктів вимагає глибокого аналізу та ретельного планування.

Аналіз останніх досліджень і публікацій. Наукові дослідження, присвячені використанню штучного інтелекту у забезпеченні безпеки промислових об'єктів, мають широкий спектр практичного застосування. Досягнення останніх років охоплюють використання нейронних мереж, алгоритмів машинного навчання, методів глибинного навчання й аналізу часових рядів даних для виявлення аномалій – задовго до виникнення аварійних ситуацій. Зокрема, наукові доробки (Глибовець М.М., Єршова О.Л., Синєгуб П.С., Вострякова В.Ю.) демонструють активний інтерес до застосування алгоритмів машинного навчання для моніторингу стану обладнання та виявлення аномальних ситуацій [3].

Дослідження практичного характеру (Олецький О.В. Бажан Л.І., Махова Г.В.) зосереджуються на використанні глибинного навчання для діагностики технічного стану обладнання. У більшості експериментах використовуються датчики вібрації та температури, а алгоритми нейронних мереж дозволяють виявити ранні ознаки порушень. Такий підхід значно зменшує час простою обладнання та зменшує ризик аварійних ситуацій [4].

Інший напрям дослідження, пропонує новий метод виявлення аномалій у промислових мережах за допомогою алгоритмів кластеризації. Використання методу К-середніх дозволяє виділити незвичні патерни у поведінці промислової системи, що може свідчити про потенційні кібератаки. Виявлення несанкціонованого доступу реалізовується завдяки аналізу журналів активності [5].

Значна кількість науковців акцентує увагу на кіберфізичних системах, що об'єднують фізичні процеси та кіберкомпоненти. Використання ШІ у таких системах забезпечило виявлення загроз на ранніх етапах, що дозволило своєчасно реагувати на кібератаки. Особлива увага приділяється побудові розподілених систем аналізу даних, що дозволяють миттєво реагувати на зміни у стані мережі.

При цьому, наукові досягнення наголошують на викликах, пов'язаних із сумісністю новітніх технологій з існуючими виробничими процесами, що вимагає розроблення спеціалізованих підходів до обробки гетерогенних даних та створення нових стандартів безпеки.

Таким чином, аналіз літератури свідчить про високу ефективність використання ШІ у промисловій безпеці. Однак, питання надійності та адаптивності таких систем залишаються актуальними. Необхідно розробити стратегії мінімізації помилкових запитів та підвищення точності виявлення аномальних подій.

Вцілому, актуальність цього дослідження зумовлена потребою оптимізації промислових процесів за рахунок інтелектуальних систем. Крім того, забезпечення кібербезпеки набуває особливого значення у зв'язку з високою вразливістю автоматизованих систем до кібератак. Результати цього дослідження можуть бути використані як основа для розробки нових методик впровадження ШІ у промислові системи безпеки.

Мета статті – дослідження використання штучного інтелекту у забезпеченні безпеки промислових об'єктів, за рахунок аналізу сучасних технологій моніторингу, прогнозування та кібербезпеки на основі ШІ.

Результати

Глобалізація та стрімкий розвиток технологій поставили перед підприємствами завдання досягнення високого рівня безпеки в умовах, коли традиційні методи, що базуються на статичних протоколах, ручних перевірках і простих алгоритмах виявлення несправностей, стають менш ефективними. Водночас зростає обсяг даних, що надходять від численних датчиків, пристроїв Індустріального Інтернету Речей та інших систем моніторингу. Цей потік інформації відкриває можливості для покращення контролю, але водночас створює ризик неможливості оперативного аналізу та своєчасного реагування, особливо у разі кіберзагроз, коли зловмисники можуть маніпулювати даними або проникати в системи управління. Отже, існує потреба у впровадженні новітніх технологій із залученням алгоритмів ШІ, здатних адаптуватися до змінних умов, забезпечувати прогнозування потенційних збоїв і критичних ситуації [6].

Сучасні підходи до забезпечення безпеки промислових об'єктів із залученням штучного інтелекту охоплюють кілька основних напрямів, серед яких можна виділити прогнозування аварійних ситуацій, автоматизований моніторинг технологічних процесів, забезпечення кібербезпеки та розробку систем підтримки прийняття рішень. Прогнозування аварійних ситуацій базується на аналізі відомих даних і показників, отриманих із сенсорів, що дозволяє завчасно виявити патерни, які прогнозують можливе виникнення несправностей. Наприклад, глибинні нейронні мережі, такі як LSTM (Long Short-Term Memory) і GRU (Gated Recurrent Units), здатні аналізувати часові ряди даних для виявлення особливостей, які можуть свідчити про майбутнє відхилення від норми. Окрім цього, класичні алгоритми машинного навчання, такі як Random Forest і Support Vector Machines, використовуються для класифікації стану обладнання та виявлення аномалій, а методи прогнозного технічного обслуговування, що включають регресійні моделі типу ARIMA, дозволяють визначити оптимальні моменти для проведення сервісних робіт і запобігання аварійним ситуаціям [4].

Автоматизований моніторинг технологічних процесів забезпечує безперервний збір і аналіз даних у режимі реального часу з різноманітних пристроїв і сенсорів, що дозволяє оперативно виявляти відхилення від нормальної роботи системи. У цьому контексті особливе місце належить використанню нейронних мереж, таких як Autoencoder, які відтворюють отриманий сигнал для виявлення невідповідностей, а також методам кластеризації, як-от K-means і DBSCAN, що дозволяють розподілити дані на групи за нормальними характеристиками та ідентифікувати аномалії. У випадках, коли моніторинг проводиться за допомогою відео або аналізу зображень, згорткові нейронні мережі (CNN) забезпечують можливість ідентифікації візуальних змін, що можуть сигналізувати про несправності або небезпеку, наприклад, появу сторонніх об'єктів поруч із критичними установками.

Забезпечення кібербезпеки на промислових об'єктах вимагає інтеграції сучасних методів аналізу мережевого трафіку для виявлення потенційних загроз і аномальної активності. В цьому напрямі алгоритми глибокого навчання, зокрема Deep Neural Networks і CNN, застосовуються для аналізу потоків даних та виявлення ознак підозрілої активності у мережі, що може свідчити про кібератаки. Також ефективними є методи безнаглядувального навчання, такі як Isolation Forest, які допомагають виявити інциденти, що істотно відрізняються від нормальної роботи системи, а інтеграція технологій блокчейну з класичними підходами забезпечує підвищену стійкість до маніпуляцій даними та несанкціонованого доступу.

Розробка систем підтримки прийняття рішень із залученням ШІ дозволяє інтегрувати аналіз даних і візуалізувати результати таким чином, щоб працівники могли оперативно отримувати обґрунтовані рекомендації щодо управління ризиками. Серед застосовуваних підходів – експертні системи на основі нечіткої логіки, що дозволяють враховувати ситуації, коли традиційні алгоритмічні моделі недостатньо ефективні, а також ансамблеві моделі, які комбінують результати роботи декількох алгоритмів, таких як нейронні мережі, регресійні моделі та дерева рішень, для отримання комплексної оцінки стану об'єкта. Важливим напрямком є впровадження технологій Explainable AI (XAI), які забезпечують прозорість прийняття рішень, надаючи користувачам розгорнуте пояснення алгоритмічних висновків, що сприяє підвищенню довіри та якості прийняття рішень у кризових ситуаціях.

На практиці впровадження технологій штучного інтелекту демонструє свою ефективність у різних галузях. Наприклад, на виробничих підприємствах галузі машинобудування системи ШІ використовують для аналізу температурних показників, вібраційних характеристик і інших технологічних параметрів, що дозволяє своєчасно виявити відхилення від норми та запобігти можливим аварійним станам. У енергетичному секторі застосування ШІ сприяє оптимізації графіків технічного обслуговування завдяки оперативному аналізу даних у режимі реального часу, що значно знижує ризики несподіваних збоїв. Водночас інноваційні рішення знаходять застосування і в нафтогазовій промисловості, де застосування систем штучного інтелекту дозволяє контролювати стан обладнання, оперативно виявляти витоки чи інші аномалії, а також у хімічній галузі, де ефективний моніторинг критичних технологічних параметрів є запорукою запобігання екологічним катастрофам.

Сучасна інтеграція ШІ зіткнулася з рядом викликів. Одним із найважливіших є проблема обробки гетерогенних даних, що генеруються численними пристроями, і необхідність створення алгоритмів, здатних працювати з різнобічними форматами інформації. Крім того, складність інтерпретації рішень алгоритмів ШІ, які часто функціонують за принципом "чорного ящика", вимагає розробки методик, що забезпечать прозорість і зрозумілість результатів для фахівців і керівників. Також не можна недооцінювати виклики, пов'язані з кібербезпекою, оскільки самі системи штучного інтелекту можуть стати об'єктом атак, що вимагає постійного моніторингу їхнього функціонування та оперативного вдосконалення захисних механізмів. Нарешті, успішна інтеграція інноваційних технологій потребує модернізації існуючих інфраструктур, значних інвестицій у навчання персоналу та адаптації організаційних процесів до нових технологічних умов.

У перспективі розвитку технологій штучного інтелекту визначальним напрямком залишається створення гібридних моделей аналізу даних, які об'єднують переваги статичних правил і динамічних алгоритмів машинного навчання. Особливе значення набуває впровадження систем, що використовують методи гібридного навчання, здатні ефективно працювати як в умовах обмежених даних, так і під час раптових змін зовнішнього середовища. Інтерактивні системи управління ризиками, що працюють у режимі реального часу, сприяють оперативному реагуванню на критичні події та дозволяють автоматизувати процеси прийняття рішень. Як бачимо, поєднання інженерії, аналітики даних та кібербезпеки, є ключовим для розробки комплексних рішень, що забезпечують високий рівень безпеки промислових об'єктів.

Стає очевидним, що комплексне дослідження ролі штучного інтелекту у забезпеченні безпеки промислових об'єктів демонструє не лише величезний потенціал новітніх технологій, але й вказує на необхідність подальшої інтеграції інноваційних розробок у виробничі процеси. Поєднання теоретичних концепцій із практичними кейсами відкриває нові можливості для оптимізації управління ризиками та створення

систем, які здатні оперативно реагувати на сучасні виклики й загрози, забезпечуючи високий рівень безпеки критичних об'єктів і сприяючи подальшій модернізації галузі.

Таким чином, інтеграція технологій ШІ з традиційними системами безпеки створює потужний інструмент, який виявляє нові патерни поведінки, часто невидимі при використанні класичних методів. Цей процес супроводжується вирішенням низки технічних проблем: необхідністю обробки гетерогенних даних, інтеграції з застарілими системами, а також забезпеченням високого рівня кібербезпеки. Одним із серйозних викликів залишається «чорна скринька» потужних алгоритмів, що ускладнює розуміння логіки прийняття рішень і вимагає впровадження підходів для їх прозорості (наприклад, Explainable AI (XAI)).

Висновки

Застосування штучного інтелекту у забезпеченні безпеки промислових об'єктів є ключовим напрямом інноваційного розвитку сучасної промисловості. Завдяки інтеграції ШІ з традиційними системами моніторингу та безпеки з'являється можливість створювати нові рішення, що забезпечують проактивний підхід до управління ризиками. Основними напрямами забезпечення безпеки із залученням ШІ є прогнозування аварійних ситуацій, автоматизований моніторинг технологічних процесів, забезпечення кібербезпеки та розробка систем підтримки прийняття рішень.

Прогнозування аварійних ситуацій дозволяє аналізувати великі обсяги даних, виявляти закономірності та передбачати ймовірність аварійних подій. Це дозволяє вчасно реагувати на потенційні загрози та знижувати ризики збоїв. Автоматизований моніторинг технологічних процесів забезпечує безперервний контроль роботи обладнання, виявлення відхилень та аномалій, що сприяє зниженню кількості непередбачуваних зупинок. У контексті кібербезпеки, системи ШІ можуть автоматично ідентифікувати підозрілу активність, аналізувати аномалії у мережевому трафіку та блокувати потенційні загрози у режимі реального часу. Крім того, інтелектуальні системи підтримки прийняття рішень допомагають оператору аналізувати складні ситуації та пропонувати оптимальні варіанти дій на основі великого обсягу даних, що знижує людський фактор у критичних ситуаціях.

Отже, інтеграція штучного інтелекту у системи безпеки промислових об'єктів дозволяє значно підвищити рівень захищеності виробництва, зменшити ризики аварій та кіберзагроз. Подальше вдосконалення технологій ШІ сприятиме створенню адаптивних та самонавчальних систем безпеки, що реагуватимуть на виклики сучасної промисловості.

Література:

1. Бергер А.Д. Прийняття інноваційних маркетингових рішень на підприємствах харчової промисловості. Ринкова економіка: сучасна теорія і практика управління. 2023. Том 22. Вип. 1 (53). DOI: https://doi.org/10.18524/2413-9998.2023.1(53).288739

2. Єршова О.Л., Бажан Л.І. Штучний інтелект – технологічна основа цифрової трансформації економіки. Статистика України. 2021. No 3. С. 47–55.

3. Крайнюк О. В. SWOT-аналіз впровадження цифрових технологій для забезпечення безпеки праці / О. В. Крайнюк, Ю. В. Буц, В. В. Барбашин // Комунальне господарство міст. – 2021. – № 3 (163). – С. 234–238. – DOI: 10.33042/2522-1809-2021-3-163-234-238.

4. Махова Г.В., Вострякова В.Ю. Штучний інтелект в підприємництві: можливості та перспективи використання. Економіка та підприємництво: зб.

наук. пр./ редкол.: І. М. Рєпіна (голов. ред) та ін. М-во освіти і науки України, Київ. нац. екон. ун-т ім. Вадима Гетьмана. Київ : КНЕУ, 2022. Вип. 49.

5. Howard J. Artificial intelligence: Implications for the future of work / J. Howard // American Journal of Industrial Medicine. – 2019. – Vol. 62 (11). – P. 917–926. – DOI: 10.1002/ajim.23037

6. Shneiderman B. Human-Centered Artificial Intelligence: Reliable, Safe Trustworthy / B. Shneiderman // International Journal of Human–Computer Interaction. – 2020. – Vol. 36 (6). – P. 495–504. – DOI: 10.1080/10447318.2020.1741118.