https://doi.org/10.31891/2219-9365-2025-81-1
УДК 681.3 + 621.3 + 004.9 + 65.012.4

ПЕРЕПЕЛИЦЯ Станіслав
Вінницький національний технічний університет
e-mail: stanislau3@gmail.com
ЮХИМЧУК Марія
Вінницький національний технічний університет
https://orcid.org/0000-0002-8131-9739
e-mail: umcmasha@gmail.com
ЛЕСЬКО Владислав
Вінницький національний технічний університет
https://orcid.org/0000-0002-5477-7080
e-mail: leskovlad@ukr.net

МОДЕЛЮВАННЯ КІБЕРФІЗИЧНИХ СИСТЕМ УПРАВЛІННЯ В УМОВАХ НЕГАТИВНИХ ЗОВНІШНІХ ФАКТОРІВ

У роботі розглядається моделювання кіберфізичних систем управління в умовах негативних зовнішніх факторів. Проведено аналіз впливу екологічних, технічних та соціальних факторів на стабільність і надійність системи. Вивчено різні підходи до моделювання, включаючи математичні моделі та симуляційні методи, а також їх застосування для оцінки ризиків. Розглянуто технології моніторингу та управління, які сприяють підвищенню стійкості систем до зовнішніх впливів. Запропоновано практичні рекомендації для розробки стійких до зовнішніх впливів систем, що можуть бути корисними для підприємств у різних галузях.

Ключові слова: кіберфізичні системи, моделювання, зовнішні фактори, надійність, моніторинг, управління.

PEREPELITSA Stanislav, YUKHYMUCHUK Mariia, LES'KO Vladyslav
Vinnytsia National Technical University

MODELLING OF CYBER-PHYSICAL CONTROL SYSTEMS UNDER NEGATIVE EXTERNAL FACTORS

The effective modeling of cyber-physical control systems (CPCS) under negative external factors is critical for ensuring their reliability and stability. This paper provides a comprehensive analysis of the modeling approaches used to assess the impact of various external influences, such as environmental conditions, technical failures, and human factors, on the performance of these systems. The study emphasizes the importance of understanding how these factors can lead to significant disruptions in the operation of CPCS, potentially resulting in severe consequences for critical infrastructures.

The research investigates different modeling methodologies, including mathematical models and simulation techniques, to evaluate the dynamics of CPCS in the presence of adverse conditions. Specifically, the paper discusses the application of Markov models to describe the system's states and transition probabilities, allowing for a detailed assessment of the likelihood of component failures. Additionally, the use of Monte Carlo simulations is explored as a means to generate various scenarios that account for external influences on system behavior.

Moreover, the paper highlights the role of monitoring and control technologies, such as IoT and real-time data analytics, in enhancing the resilience of CPCS. These technologies facilitate continuous monitoring of system components, enabling proactive measures to mitigate the effects of negative external factors. The findings indicate that organizations implementing robust monitoring systems can significantly improve their responsiveness and adaptability to changing conditions.

Furthermore, the study provides practical recommendations for designing resilient CPCS that can withstand external impacts. These include integrating advanced information technologies, optimizing data processing methods, and ensuring data security to protect against cyber threats. By adopting these strategies, organizations can enhance the operational efficiency of their systems while minimizing risks associated with external disruptions.

The results of this research contribute to the understanding of how to effectively model and manage cyber-physical control systems in challenging environments. This work serves as a foundation for future studies aimed at improving the robustness and reliability of CPCS, ultimately leading to more secure and efficient operations in various industries.

Keywords: cyber-physical systems, modeling, external factors, reliability, monitoring technologies, data analytics.

ПОСТАНОВКА ПРОБЛЕМИ У ЗАГАЛЬНОМУ ВИГЛЯДІ ТА ЇЇ ЗВ'ЯЗОК ІЗ ВАЖЛИВИМИ НАУКОВИМИ ЧИ ПРАКТИЧНИМИ ЗАВДАННЯМИ

Кіберфізичні системи управління (КФС) є інтеграцією комп'ютерних алгоритмів, програмного забезпечення та фізичних процесів. Вони стають все більш поширеними у різних сферах, таких як промисловість, енергетика, транспорт та охорона здоров'я. Однак, зростаюча складність та інтеграція цих систем роблять їх вразливими до негативних зовнішніх факторів, таких як екологічні умови, технічні збої та кібератаки.

У даній статті буде представлено модель експлуатації кіберфізичних систем управління, зосереджуючи увагу на впливі негативних зовнішніх факторів. Зокрема, розглядатиметься, як зовнішні фактори можуть впливати на стабільність та безпеку системи. Згідно з дослідженням [1], негативні зовнішні

впливи можуть призводити до зниження надійності системи, що в свою чергу може викликати серйозні наслідки, зокрема збої в роботі критично важливих інфраструктур.

Моделювання КФС в умовах негативних зовнішніх факторів є важливим завданням для забезпечення їхньої стійкості [2]. Оцінка впливу зовнішніх факторів на роботу системи дозволяє виявити потенційні ризики та розробити ефективні стратегії для їх усунення. Моделі можуть включати різні аспекти, такі як динаміка системи, ймовірність відмови компонентів та їх взаємодію з зовнішнім середовищем.

У статті буде проведено аналіз існуючих підходів до моделювання кіберфізичних систем управління, а також запропоновано нові методи, які можуть бути використані для підвищення стійкості систем до негативних зовнішніх впливів. Основна увага буде приділена математичним моделям, які дозволяють оцінити вплив зовнішніх факторів на стабільність системи.

АНАЛІЗ ДОСЛІДЖЕНЬ ТА ПУБЛІКАЦІЙ

Кіберфізичні системи управління підлягають впливу різноманітних негативних зовнішніх факторів, які можуть суттєво вплинути на їхню стабільність та безпеку. Ці фактори можуть бути класифіковані на кілька категорій, включаючи екологічні, технічні та соціальні.

Екологічні фактори

Екологічні фактори, такі як зміни температури, вологи, атмосферного тиску, можуть негативно впливати на роботу сенсорів і виконавчих механізмів у кіберфізичних системах [3]. Наприклад, підвищена вологість може призвести до корозії електронних компонентів, а екстремальні температури можуть вплинути на точність вимірювань.

Для моделювання впливу екологічних факторів можна використовувати рівняння, які описують динаміку системи під впливом зовнішніх змін. Наприклад, якщо (T) – температура, а (H) – вологість, можна використовувати модель, яка враховує їхній вплив на ймовірність відмови системи:

$$[P(F) = P_0 \cdot e^{-\alpha_1 T - \alpha_2 H}] \quad (1)$$

де $P(F)$ – ймовірність відмови, P_0 – базова ймовірність відмови при нормальних умовах, α_1 і α_2– коефіцієнти, що характеризують чутливість системи до температури та вологості.

Технічні фактори

Технічні збої, такі як відмова обладнання або програмні помилки, також можуть мати серйозні наслідки для кіберфізичних систем. Наприклад, відмова одного з контролерів може призвести до збою в роботі всієї системи. Для аналізу технічних відмов використовуються моделі, які описують ймовірність відмови компонентів на основі статистичних даних про їх експлуатацію [4].

Одним з підходів є використання моделей Маркова, які дозволяють описати різні стани системи (робочий, часткова відмова, повна відмова) та переходи між ними. Модель може бути представлена у вигляді матриці ймовірностей переходів, що дозволяє оцінити ймовірність переходу в стан відмови за певний проміжок часу.

Соціальні фактори

Соціальні фактори, такі як людський фактор, також можуть впливати на стабільність кіберфізичних систем. Помилки оператора, недостатня кваліфікація персоналу або неналежне навчання можуть призвести до неправильного управління системою. Важливо враховувати ці аспекти при розробці моделей, які оцінюють загальний ризик відмови.

Для моделювання впливу людського фактора можна використовувати методи аналізу ризиків [5], які враховують ймовірність помилок оператора та їхній вплив на загальну продуктивність системи. Наприклад, можна врахувати ймовірність помилки оператора (P(E)) та її вплив на ймовірність відмови системи:

$$[P(F) = P_0 + P(E) \cdot \beta] \quad (2)$$

де β – коефіцієнт, що характеризує вплив людського фактора на ймовірність відмови.

Моделювання кіберфізичних систем управління

Моделювання кіберфізичних систем управління в умовах негативних зовнішніх факторів є важливим етапом для забезпечення їхньої надійності та безпеки. В даному розділі буде розглянуто різні підходи до моделювання, а також їх застосування для аналізу впливу зовнішніх факторів на стабільність системи.

Методологія моделювання

Моделювання кіберфізичних систем може включати як математичні, так і симуляційні методи. Математичні моделі дозволяють описати динаміку системи за допомогою рівнянь, які враховують вплив

зовнішніх факторів, тоді як симуляційні моделі дозволяють візуалізувати поведінку системи в умовах різних сценаріїв.

Одним з основних підходів до моделювання є системний підхід, який передбачає розгляд системи як цілого, а не лише її окремих компонентів. Це дозволяє врахувати взаємозв'язки між компонентами і їхній вплив на загальну продуктивність системи. Системний підхід може бути реалізований через використання системних динамічних моделей, які описують зміни в системі з часом.

Математичні моделі

Математичні моделі, такі як моделі Маркова, широко використовуються для аналізу кіберфізичних систем [6]. Ці моделі дозволяють описати різні стани системи і ймовірності переходів між ними. Наприклад, можна розглянути систему, що складається з контролерів, датчиків і виконавчих механізмів, і описати ймовірності їх відмови:

$$\left[\mathrm{P(t)} = \mathrm{P_0} \cdot \mathrm{e}^{-\lambda \mathrm{t}}\right] \tag{3}$$

де $P(t)$ – ймовірність безвідмовної роботи системи в момент часу t, P_0 – початкова ймовірність, а λ – інтенсивність відмови.

Для кіберфізичних систем, що підлягають впливу негативних зовнішніх факторів, важливо також враховувати динаміку відмови під впливом цих факторів. Наприклад, можна модифікувати рівняння (3), щоб включити вплив температури T і вологості H:

$$\left[P(t) = P_0 \cdot e^{-(\lambda + \alpha_1 T + \alpha_2 H)t}\right] \tag{4}$$

де α_1 і α_2 – коефіцієнти, що характеризують чутливість системи до температури та вологості.

Симуляційні моделі

Симуляційні моделі, зокрема метод Монте-Карло, також використовуються для моделювання кіберфізичних систем. Цей метод дозволяє генерувати випадкові сценарії, які можуть включати різні комбінації зовнішніх факторів і відмов компонентів. Наприклад, симуляція може враховувати різні сценарії, такі як підвищена температура, електромагнітні перешкоди або збої в електропостачанні.

Симуляція Монте-Карло може бути використана для оцінки ймовірності відмови системи в умовах різних зовнішніх впливів [7]. Наприклад, якщо система підлягає впливу температури та вологості, можна провести тисячі симуляцій, щоб оцінити, як ці фактори впливають на ймовірність відмови.

Таким чином, моделювання кіберфізичних систем управління є складним, але необхідним процесом для забезпечення їхньої надійності в умовах негативних зовнішніх факторів. Використання математичних і симуляційних моделей дозволяє виявити потенційні ризики та розробити стратегії для їх усунення.

Технології моніторингу та управління в кіберфізичних системах

Сучасні кіберфізичні системи управління (КФС) покладаються на інноваційні технології моніторингу та управління, які забезпечують стабільність і ефективність в умовах негативних зовнішніх факторів. Ці технології забезпечують безперервний контроль за станом системи та оперативне реагування на зміни, що можуть загрожувати її надійності.

Системи моніторингу, які використовують сенсори та IoT-технології, дозволяють отримувати дані про стан компонентів у реальному часі. Наприклад, у промислових системах моніторинг вібрацій може передбачити технічні збої, що дозволяє запобігти відмовам. Компанія General Electric використовує технології моніторингу для виявлення аномалій у роботі своїх газових турбін, що дозволяє зменшити витрати на обслуговування і підвищити ефективність [8].

Використання даних з сенсорів у поєднанні з алгоритмами машинного навчання дозволяє аналізувати інформацію та виявляти закономірності, що можуть бути корисними для прогнозування відмов. Наприклад, компанія Siemens розробила систему, яка використовує дані з сенсорів для прогнозування технічних збоїв у своїх виробничих лініях. Це дозволяє зменшити час простою і оптимізувати виробничі процеси [9].

Важливим аспектом є також інтеграція різних систем управління, таких як ERP (Enterprise Resource Planning), MES (Manufacturing Execution Systems) та SCADA (Supervisory Control and Data Acquisition). Ці системи можуть обмінюватися даними в реальному часі, створюючи єдину інформаційну базу для прийняття рішень. Наприклад, інтеграція ERP-системи з MES може покращити планування ресурсів і зменшити затримки у виробничих процесах. Компанії, такі як Toyota, використовують інтегровані системи для управління своїми виробничими ланцюгами, що дозволяє їм досягати високої ефективності та знижувати витрати.

Однак впровадження нових технологій пов'язане з певними викликами. Необхідність інтеграції нових систем з існуючими може вимагати значних інвестицій у модернізацію обладнання та навчання

персоналу. Наприклад, впровадження нових IoT-рішень може вимагати значних витрат на оновлення інфраструктури, що може бути важливим фактором для малих і середніх підприємств.

Також важливо забезпечити безпеку даних, оскільки кіберзагрози можуть загрожувати цілісності інформаційних потоків. Використання технологій шифрування та систем виявлення вторгнень є необхідним для захисту інформації в кіберфізичних системах. Наприклад, компанія Honeywell впровадила рішення для захисту своїх промислових систем від кібератак, що дозволяє забезпечити безпеку даних на всіх етапах виробництва [10].

Таким чином, технології моніторингу та управління в кіберфізичних системах є критично важливими для забезпечення їхньої стабільності та ефективності в умовах негативних зовнішніх факторів. Використання сучасних технологій, таких як IoT, машинне навчання та інтеграція різних систем управління, може суттєво підвищити продуктивність і надійність цих систем, але потребує також уваги до викликів, пов'язаних із їх інтеграцією та безпекою.

Виклики та можливості у моделюванні кіберфізичних систем управління

Моделювання кіберфізичних систем управління в умовах негативних зовнішніх факторів стикається з численними викликами, які можуть ускладнити процес розробки стійких і надійних систем. Одним із основних викликів є складність інтеграції різнорідних компонентів системи. Кіберфізичні системи зазвичай складаються з апаратних і програмних елементів, які повинні взаємодіяти між собою. Відсутність стандартів для обміну даними між різними системами може призвести до затримок у координації та зниження загальної продуктивності.

Крім того, динаміка зовнішніх факторів може бути важко передбачуваною. Наприклад, зміни в навколишньому середовищі, такі як екстремальні погодні умови або несподівані технічні збої, можуть вплинути на роботу системи в непередбачуваний спосіб. Моделі, які не враховують ці зміни, можуть призводити до неправильних висновків і неефективних рішень.

Однак, незважаючи на ці виклики, існують також значні можливості для вдосконалення моделювання кіберфізичних систем. Наприклад, розвиток технологій великих даних та машинного навчання відкриває нові горизонти для аналізу та прогнозування поведінки систем. Використання алгоритмів машинного навчання для обробки великих обсягів даних може допомогти виявити закономірності, які не були б очевидними за традиційних методів аналізу.

Крім того, інтеграція новітніх технологій, таких як блокчейн, може забезпечити прозорість і безпеку інформаційних потоків, що є важливим аспектом для кіберфізичних систем. Блокчейн може використовуватися для створення незмінних записів про всі транзакції та зміни в системі, що підвищує довіру між учасниками процесу.

Незважаючи на те, що виклики у моделюванні кіберфізичних систем управління є суттєвими, новітні технології та методи можуть забезпечити нові можливості для їх подолання. Важливо використовувати ці можливості для розробки більш стійких і надійних систем, які зможуть ефективно функціонувати в умовах негативних зовнішніх факторів.

Практичні рекомендації щодо розробки стійких до зовнішніх впливів систем

Розробка кіберфізичних систем управління, які можуть витримувати негативні зовнішні впливи, вимагає комплексного підходу, що враховує як технологічні, так і організаційні аспекти. Важливо впроваджувати інноваційні технології моніторингу та управління, які забезпечують реальний контроль за станом системи та оперативне реагування на зміни [11]. Застосування сенсорних технологій та IoT дозволяє здійснювати моніторинг в реальному часі, що є критично важливим для виявлення аномалій і запобігання відмовам. Успішні приклади, такі як компанія General Electric, демонструють, як інтеграція IoT-технологій може підвищити ефективність виробництва.

Інтеграція різних систем управління, таких як ERP, MES і SCADA, є важливим етапом у забезпеченні стійкості. Ці системи повинні бути спроектовані так, щоб забезпечити безперервний обмін даними та створити єдину інформаційну базу для прийняття рішень. Це дозволить зменшити затримки в координації між підсистемами і підвищити загальну продуктивність виробничих процесів. Наприклад, інтеграція ERP-системи з MES може забезпечити безперервний потік інформації про запаси, виробничі замовлення та стан обладнання.

Крім того, важливо забезпечити адаптивність системи до змін у зовнішньому середовищі. Використання алгоритмів машинного навчання для аналізу даних може допомогти виявити закономірності та передбачити можливі відмови. Це дозволить підприємствам своєчасно реагувати на зміни в умовах виробництва, зменшуючи ризики та підвищуючи надійність.

Необхідно також акцентувати увагу на безпеці даних. В умовах зростаючих загроз кібератак важливо впроваджувати сучасні методи захисту інформації, які забезпечать конфіденційність та цілісність даних. Регулярні аудити безпеки та навчання персоналу з питань кібербезпеки можуть суттєво знизити ризики.

Важливо проводити постійний моніторинг і оцінку ризиків, пов'язаних із зовнішніми впливами. Впровадження системи моніторингу, що забезпечує збір даних про стан обладнання в реальному часі, дозволить виявляти потенційні проблеми на ранніх стадіях [12]. Це не лише підвищить надійність системи, але й забезпечить її стабільну роботу в умовах негативних зовнішніх факторів.

Крім того, дотримання міжнародних стандартів, таких як ISO 27001 для інформаційної безпеки, може значно підвищити рівень захисту даних. Стратегічне планування впровадження нових технологій, включаючи оцінку витрат і вигод, дозволить підприємствам ефективно використовувати ресурси.

Реалізація цих рекомендацій дозволить створити стійкі до зовнішніх впливів кіберфізичні системи управління, які зможуть ефективно функціонувати в сучасному динамічному середовищі. Підвищення надійності та адаптивності таких систем стане запорукою успішної діяльності підприємств у різних галузях.

ВИСНОВКИ З ДАНОГО ДОСЛІДЖЕННЯ І ПЕРСПЕКТИВИ ПОДАЛЬШИХ РОЗВІДОК У ДАНОМУ НАПРЯМІ

Дослідження моделювання кіберфізичних систем управління в умовах негативних зовнішніх факторів підкреслює важливість забезпечення стійкості таких систем для підтримки їхньої надійності та ефективності. Виявлено, що негативні зовнішні впливи, такі як екологічні умови, технічні збої та людський фактор, можуть суттєво вплинути на стабільність системи.

Аналіз показав, що впровадження сучасних інформаційних технологій, таких як IoT, алгоритми машинного навчання та інтеграція різних систем управління, може значно підвищити продуктивність і надійність кіберфізичних систем. Зокрема, інформаційні потоки, які забезпечують обмін даними між підсистемами, грають ключову роль у забезпеченні безперебійної координації виробничих процесів.

Важливість адаптивності систем до змін у зовнішньому середовищі також була підтверджена. Використання новітніх технологій дозволяє швидше реагувати на зміни та зменшувати ризики, пов'язані з відмовами. Однак, впровадження нових технологій вимагає уваги до викликів, пов'язаних із інтеграцією, безпекою даних і навчанням персоналу.

Результати цього дослідження можуть слугувати основою для подальших досліджень у сфері кіберфізичних систем управління, а також для практичних застосувань, спрямованих на підвищення їхньої стійкості до негативних зовнішніх впливів. Реалізація запропонованих рекомендацій може забезпечити стабільну роботу критично важливих інфраструктур, сприяючи їхній адаптації до сучасних викликів і вимог.

Література

1. Юхимчук М. С., Дубовой В. М. (2023). Інформаційний аспект координації виробничих процесів. Вісник Хмельницького національного університету. 2023. № 6. С. 147-154. DOI: https://www.doi.org/10.31891/2307-5732-2022-315-6(2)-147-154.
2. Dubovoi V. et al. (2024). Functional Dependability of Distributed Control of Multi-Zone Objects Under Failures Conditions. IEEE Access. 2024. Vol. 12. P. 95736-95749. DOI: 10.1109/ACCESS.2024.3421380.
3. Биков М. М. та ін. (2023). Модель експлуатації кіберфізичної системи в умовах впливу негативних зовнішніх факторів. Вісник ВПІ. 2023. Вип. 6. С. 30-38. DOI: https://doi.org/10.31649/1997-9266-2023-171-6-30-38.
4. Liu Y., Zhao Y. (2020). A Survey on Reliable Distributed Systems. IEEE Transactions on Parallel and Distributed Systems. 2020. Vol. 31, No. 3. P. 482-500. DOI: 10.1109/TPDS.2019.2931744.
5. Hwang K., Ahn J. (2018). Reliability Analysis of Distributed Control Systems. Systems Engineering. 2018. Vol. 21, No. 1. P. 1-12. DOI: 10.1002/sys.21418.
6. Barlow R. E., Proschan F. (1996). Statistical Theory of Reliability and Life Testing: Probability Models. Holt, Rinehart and Winston.
7. Avizienis A. et al. (2004). Basic Concepts and Taxonomy of Dependable and Secure Computing. IEEE Transactions on Dependable and Secure Computing. 2004. Vol. 1, No. 1. P. 11-33. DOI: 10.1109/TDSC.2004.2.
8. General Electric. Digital Wind Farm. [Online]. Available: https://www.ge.com/news/press-releases/ge-launches-next-evolution-wind-energy-making-renewables-more-efficient-economic [Accessed: 2025].
9. Siemens. Predictive Maintenance Solutions. [Online]. Available: https://www.siemens.com/global/en/products/services/digital-enterprise-services/analytics-artificial-intelligence-services/predictive-services.html [Accessed: 2025].
10. Honeywell. Cybersecurity for Industrial Control Systems. [Online]. Available: https://www.honeywell.com/us/en/news/2022/10/industrial-cybersecurity-a-primer [Accessed: 2025].
11. Yukhimchuk M., Kovtun V. (2020). Advanced Techniques for Enhancing the Reliability of Distributed Control Systems. International Journal of Critical Infrastructure Protection. 2020. Vol. 30. P. 100-110. DOI: 10.1016/j.ijcip.2020.100110.
12. Leveson N. (2011). Engineering a Safer World: Systems Thinking Applied to Safety. MIT Press.

References

1. Yukhymchuk M. S., Dubovoi V. M. (2023). Information Aspect of Coordination of Production Processes. *Visnyk of Khmelnytskyi National University*, 2023, No. 6, pp. 147-154. DOI: https://www.doi.org/10.31891/2307-5732-2022-315-6(2)-147-154.
2. Dubovoi V. et al. (2024). Functional Dependability of Distributed Control of Multi-Zone Objects Under Failure Conditions. *IEEE Access*, 2024, Vol. 12, pp. 95736-95749. DOI: 10.1109/ACCESS.2024.3421380.
3. Bykov M. M. et al. (2023). Model of Cyber-Physical System Operation Under the Influence of Negative External Factors. *Visnyk of VPI*, 2023, Issue 6, pp. 30-38. DOI: https://doi.org/10.31649/1997-9266-2023-171-6-30-38.
4. Liu Y., Zhao Y. (2020). A Survey on Reliable Distributed Systems. *IEEE Transactions on Parallel and Distributed Systems*, 2020, Vol. 31, No. 3, pp. 482-500. DOI: 10.1109/TPDS.2019.2931744.
5. Hwang K., Ahn J. (2018). Reliability Analysis of Distributed Control Systems. *Systems Engineering*, 2018, Vol. 21, No. 1, pp. 1-12. DOI: 10.1002/sys.21418.
6. Barlow R. E., Proschan F. (1996). *Statistical Theory of Reliability and Life Testing: Probability Models*. Holt, Rinehart, and Winston.
7. Avizienis A. et al. (2004). Basic Concepts and Taxonomy of Dependable and Secure Computing. *IEEE Transactions on Dependable and Secure Computing*, 2004, Vol. 1, No. 1, pp. 11-33. DOI: 10.1109/TDSC.2004.2.
8. General Electric. Digital Wind Farm. [Online]. Available: https://www.ge.com/news/press-releases/ge-launches-next-evolution-wind-energy-making-renewables-more-efficient-economic [Accessed: 2025].
9. Siemens. Predictive Maintenance Solutions. [Online]. Available: https://www.siemens.com/global/en/products/services/digital-enterprise-services/analytics-artificial-intelligence-services/predictive-services.html [Accessed: 2025].
10. Honeywell. Cybersecurity for Industrial Control Systems. [Online]. Available: https://www.honeywell.com/us/en/news/2022/10/industrial-cybersecurity-a-primer [Accessed: 2025].
11. Yukhymchuk M., Kovtun V. (2020). Advanced Techniques for Enhancing the Reliability of Distributed Control Systems. *International Journal of Critical Infrastructure Protection*, 2020, Vol. 30, pp. 100-110. DOI: 10.1016/j.ijcip.2020.100110.
12. Leveson N. (2011). *Engineering a Safer World: Systems Thinking Applied to Safety*. MIT Press.