УДК 004.056.53:004.021 DOI https://doi.org/10.35546/kntu2078-4481.2025.4.3.15

О. В. КРАЙНЮК
кандидат технічних наук, доцент,
завідувачка кафедри кібербезпеки
Харківський національний автомобільно-дорожній університет
ORCID: 0000-0001-9524-040X

Ю. В. БУЦ
доктор технічних наук, професор,
завідувач кафедри охорони праці та надзвичайних ситуацій
Український державний університет залізничного транспорту
ORCID: 0000-0003-0450-2617

М. М. ПІКСАСОВ
кандидат технічних наук, доцент,
доцент кафедри кібербезпеки
Харківський національний автомобільно-дорожній університет
ORCID: 0000-0001-9487-7273

Н. В. ДІДЕНКО
кандидат технічних наук, доцент,
доцент кафедри кібербезпеки
Харківський національний автомобільно-дорожній університет
ORCID: 0000-0003-3318-438X

Б. О. ПОХОДЕНКО
старший викладач кафедри кібербезпеки
Харківський національний автомобільно-дорожній університет
ORCID: 0000-0002-9995-7077

ФУНКЦІОНАЛЬНЕ МОДЕЛЮВАННЯ ТА АЛГОРИТМІЗАЦІЯ ПРОЦЕСІВ ЗАБЕЗПЕЧЕННЯ КІБЕРСТІЙКОСТІ АВТОМАТИЗОВАНИХ СИСТЕМ ВИДАЧІ ЗІЗ

У статті розглядається актуальна науково-практична проблема забезпечення кіберстійкості та безперервності функціонування автоматизованих систем видачі засобів індивідуального захисту (САВ-ЗІЗ) в умовах деструктивних кібервпливів. В епоху Індустрії 4.0 цифровізація охоплює критичні процеси охорони праці, проте зростання залежності від стабільності мережевого середовища створює ризики блокування доступу до засобів захисту.

Здійснено аналіз вразливостей класичних централізованих архітектур промислового Інтернету речей (IIoT), які характеризуються критичною залежністю від доступності серверної інфраструктури та схильністю до «функціонального паралічу» під час DDoS-атак. Висвітлено обмеження традиційних підходів типу Fail-Secure, які є неприпустимими для критичної інфраструктури безпеки, де пріоритетом є фізична доступність ресурсів, а не блокування доступу.

Методологічною основою дослідження стало функціональне моделювання бізнес-процесів у стандарті IDEF0, що дозволило декомпозувати процес аварійного керування та ідентифікувати критичні вразливості на етапі фіксації транзакцій. Для вирішення виявлених проблем запропоновано гібридну архітектуру та алгоритм адаптивної кіберстійкості, що базується на технології периферійних обчислень (Edge Computing). Це дозволяє децентралізувати логіку прийняття рішень та перенести процес валідації прав доступу безпосередньо на рівень кінцевого обладнання.

Розроблений алгоритм реалізовано на базі скінченного автомата з трьома станами: штатний режим (ONLINE), перехідний режим (DEGRADED) та аварійний режим (OFFLINE). Для захисту цілісності офлайн-транзакцій та протидії фальсифікації даних в ізольованому середовищі застосовано механізм криптографічної інкапсуляції записів з використанням технології хеш-ланцюжків на базі алгоритму SHA-256.

Ефективність запропонованих рішень підтверджено шляхом імітаційного моделювання мовою Python. Результати експерименту засвідчили, що в умовах тривалої атаки на відмову в обслуговуванні розроблена система забезпечує показник доступності сервісу на рівні понад 98%, тоді як класична архітектура демонструє повну зупинку обслуговування. Також доведено ефективність реалізованого протоколу пакетної синхронізації даних, який дозволяє уникнути перевантаження мережі на етапі відновлення зв'язку.

Ключові слова: *кіберстійкість, промисловий інтернет речей, периферійні обчислення, безпечна відмова, хеш-ланцюжки, доступність сервісу, атаки на відмову, автоматизація процесів, охорона праці, безперервність бізнесу.*

O. V. KRAINIUK
Candidate of Technical Sciences, Associate Professor,
Head of the Cybersecurity Department
Kharkiv National Automobile and Highway University
ORCID: 0000-0001-9524-040X

YU. V. BUTS
Doctor of Technical Sciences, Professor,
Head of the Department of Occupational Safety and Emergency Situations
Ukrainian State University of Railway Transport
ORCID: 0000-0003-0450-2617

M. M. PIKSASOV
Candidate of Technical Sciences, Associate Professor,
Associate Professor at the Department of Cybersecurity
Kharkiv National Automobile and Highway University
ORCID: 0000-0001-9487-7273

N. M. DIDENKO
Candidate of Technical Sciences, Associate Professor,
Associate Professor at the Department of Cybersecurity
Kharkiv National Automobile and Highway University
ORCID: 0000-0003-3318-438X

B. O. POHODENKO
Senior Lecturer at the Department of Cybersecurity
Kharkiv National Automobile and Highway University
ORCID: 0000-0002-9995-7077

FUNCTIONAL MODELING AND ALGORITHMIZATION OF PROCESSES FOR ENSURING CYBER RESILIENCE OF AUTOMATED DISPENSING SYSTEMS FOR PERSONAL PROTECTIVE EQUIPMENT

The article addresses the urgent scientific and practical problem of ensuring cyber resilience and operational continuity of automated personal protective equipment (PPE) dispensing systems under destructive cyber impacts. In the Industry 4.0 era, digitalization covers critical occupational safety processes; however, the increasing reliance on network stability creates significant risks of blocking access to protective equipment during cyber incidents.

The study provides a comprehensive analysis of the vulnerabilities inherent in classic centralized Industrial Internet of Things (IIoT) architectures. These systems are characterized by a critical reliance on server infrastructure availability and susceptibility to "functional paralysis" during Denial-of-Service (DoS) attacks. Specifically, the limitations of traditional Fail-Secure approaches are highlighted, as they are unacceptable for critical occupational safety infrastructure where the physical availability of resources is the priority, rather than access blocking.

The methodological basis of the research is functional modeling of business processes using the IDEF0 standard. This approach allowed for the decomposition of the emergency management process and the identification of critical vulnerabilities at the transaction commitment stage. To address these issues, a hybrid architecture and algorithmic support based on Edge Computing technology are proposed. This enables the decentralization of decision-making logic and transfers the access rights validation process directly to the endpoint level.

The developed adaptive cyber resilience algorithm is implemented based on a three-state Finite State Machine (FSM): normal operation (ONLINE), transitional mode (DEGRADED), and emergency mode (OFFLINE). To protect the integrity of offline transactions and prevent data falsification in an isolated environment, a mechanism of cryptographic record encapsulation using hash chaining technology based on the SHA-256 algorithm is applied.

Simulation results, conducted using Python, confirm the approach's effectiveness. The experiments demonstrated that under conditions of a prolonged DoS attack, the proposed system ensures a service availability rate of over 98%, whereas the classic architecture demonstrates a complete cessation of service. Furthermore, the effectiveness of the implemented batch data synchronization protocol, which prevents network overload during the connection recovery phase, was proven.

Key words: *cyber resilience, Industrial Internet of Things, edge computing, fail-safe, hash chaining, service availability, denial-of-service attacks, process automation, occupational safety, business continuity.*

Постановка проблеми

Актуальність теми. В умовах Індустрії 4.0 (Industry 4.0) цифровізація охоплює критичні бізнес-процеси підприємств, включаючи забезпечення охорони праці. Традиційні методи видачі засобів індивідуального захисту (ЗІЗ) активно заміщуються автоматизованими системами (САВ-ЗІЗ), реалізованими на базі технологій Промислового Інтернету речей (IIoT). Такі системи забезпечують прозорість обліку та персоніфікацію відповідальності. Однак, зростання залежності фізичних процесів безпеки від стабільності кібернетичного середовища створює нові ризики.

Постановка проблеми. Більшість сучасних рішень САВ-ЗІЗ побудовані за централізованою архітектурою, де кінцевий пристрій (вендинговий автомат) критично залежить від доступності серверної інфраструктури. У разі деструктивних кібервпливів (зокрема DoS-атак) або технічних збоїв мережі виникає загроза блокування процесу видачі ЗІЗ. Це призводить не лише до фінансових втрат через простій виробництва, а й до прямого порушення регламентів безпеки персоналу.

Аналіз підходів. Існуючі дослідження здебільшого фокусуються на криптографічному захисті каналів зв'язку або фізичній безпеці пристроїв. Водночас, недостатньо уваги приділяється формалізації внутрішньої логіки функціонування системи в критичних ситуаціях. Відсутність чітких функціональних моделей, які б описували поведінку системи при втраті зв'язку, ускладнює розробку надійних алгоритмів керування.

Шлях вирішення. Для створення кіберстійкої системи необхідний комплексний підхід, що поєднує функціональне моделювання бізнес-процесів (для виявлення вразливих інформаційних потоків) та алгоритмізацію процедур аварійного керування (для забезпечення безперервності роботи). Використання методології IDEF0 дозволяє декомпозувати процес видачі ЗІЗ та ідентифікувати ті функції, які потребують перенесення на рівень периферійних обчислень (Edge Computing).

Аналіз останніх досліджень і публікацій

Впровадження технологій Індустрії 4.0 у сферу охорони праці актуалізувало питання надійності автоматизованих систем видачі засобів індивідуального захисту (САВ-ЗІЗ). Як зазначається у роботах [1], перехід від ручного обліку до використання IIoT-вендингових автоматів дозволяє оптимізувати логістику та персоніфікувати відповідальність. Однак зростання залежності критичної інфраструктури безпеки від мережевих технологій супроводжується новими викликами.

Аналіз сучасної літератури свідчить, що забезпечення безперервності функціонування таких систем вимагає зміни парадигми захисту. Перехід до Індустрії 4.0 вимагає зміщення акценту з класичного кіберзахисту (запобігання атакам) на забезпечення кіберстійкості – здатності системи адаптуватися та зберігати функціональність під час атак чи збоїв [1].

Серед сучасних рішень виділяються:

– Використання модельно-прогнозуючого керування (англ. Model Predictive Control, MPC) із перемиканням функцій вартості, що дозволяє зберігати стабільність і керованість систем навіть при втраті даних внаслідок DoS-атак [2].

– Застосування спостерігачів стану та нечіткої логіки для компенсації втрат даних та нівелювання невизначеностей у мережевих системах керування [3].

– Впровадження подієво-керованих механізмів, які зменшують навантаження на мережу та підвищують автономність вузлів [4].

Для забезпечення цілісності даних у розподілених системах активно досліджуються технології блокчейну, проте їх імплементація на ресурсно-обмежених пристроях IIoT (до яких належать контролери вендингових автоматів) часто ускладнена через високі обчислювальні вимоги [5, 6].

Попри значний прогрес у теоретичних методах керування для кіберфізичних систем, більшість сучасних рішень орієнтовані на безперервні динамічні об’єкти (енергомережі, транспорт), тоді як дискретні системи обслуговування (наприклад, автоматизовані пункти видачі ЗІЗ) залишаються недостатньо дослідженими щодо алгоритмічної стійкості та кіберстійкості під час DoS-атак [7].

Більшість сучасних підходів (MPC, нечітка логіка, подієво-керовані стратегії) розроблені для безперервних або гібридних систем, де контроль і відновлення функціональності після атак базуються на безперервних моделях [8]. Для дискретних сервісних систем, які мають інші вимоги до доступності та безпеки, такі підходи не завжди застосовні або ефективні.

Існуючі архітектури автоматизованих систем видачі ЗІЗ здебільшого реалізують жорстку клієнт-серверну логіку. У разі DoS-атаки системи переходять у стан Fail-Secure (блокування), що є прийнятним для фінансових терміналів, але неприпустимим для критичної інфраструктури охорони праці, де пріоритетом є фізична доступність ЗІЗ [7]. Відсутні формалізовані алгоритми перемикання в режим Fail-Safe із збереженням цілісності транзакцій.

Огляд сучасних досліджень підкреслює, що більшість рішень зосереджені на виявленні атак, а не на забезпеченні стійкої роботи після їх виникнення. Реалізація гнучких, адаптивних механізмів відновлення для дискретних сервісних систем залишається відкритою проблемою [9].

У цьому контексті перспективним видається застосування концепції периферійних обчислень, що дозволяє децентралізувати логіку прийняття рішень. Перенесення критичних функцій авторизації безпосередньо на рівень кінцевого обладнання здатне забезпечити необхідну автономність системи під час деструктивних впливів

Важливо зазначити, що організаційно-технічні аспекти впровадження вендингових автоматів та перспективи використання інтелектуальних систем управління безпекою праці вже були обґрунтовані авторами в попередніх працях [10-12]. Проте, якщо раніше акцент робився на функціональній ефективності та автоматизації процесів, то дане дослідження фокусується саме на алгоритмічному забезпеченні їхньої живучості в умовах кібернетичних загроз.

Формулювання мети дослідження

Метою роботи є підвищення рівня кіберстійкості автоматизованих систем видачі ЗІЗ шляхом розробки функціональних моделей та алгоритмічного забезпечення для гарантування безперервності бізнес-процесів в умовах деструктивних кібервпливів. Для досягнення цієї мети передбачається поетапне вирішення комплексу завдань: від функціонального моделювання бізнес-процесів у методології IDEF0 та ідентифікації критичних вразливостей архітектури до розробки алгоритму адаптивного керування («Secure Fail-Safe») з подальшою верифікацією його ефективності шляхом імітаційного моделювання.

Домінуюча централізована архітектура IIoT-систем характеризується критичною залежністю від доступності каналів зв'язку, що створює вразливість типу «єдина точка відмови» (Single Point of Failure). У разі реалізації атак на відмову в обслуговуванні це призводить до функціонального паралічу обладнання та переходу в стан блокування (Fail-Secure), що спричиняє неприпустимі простої виробництва через неможливість видачі засобів захисту. Вирішення зазначеної проблеми вимагає переходу до децентралізованої архітектури на базі периферійних обчислень, яка забезпечить автономне прийняття рішень та реалізацію режиму безпечної відмови (Fail-Safe) в умовах ізоляції від сервера.

Викладення основного матеріалу дослідження

Функціональне моделювання системи в стандарті IDEF0

Для формалізації процесів прийняття рішень в умовах невизначеності (втрати зв'язку) було розроблено функціональну модель системи в методології IDEF0. На відміну від стандартних підходів, де моделюється лише успішний сценарій видачі, дана модель фокусується на декомпозиції процесу аварійного керування.

Декомпозиція процесів верхнього рівня (Діаграма A0). На рівні декомпозиції виділено чотири функціональні блоки, які взаємодіють між собою через інформаційні та керуючі потоки:

– A1 (Ідентифікація та авторизація): Блок отримує дані з RFID-зчитувача. Критичною особливістю є те, що вхідні дані про права доступу можуть надходити з двох джерел: "Центральна база даних" (штатний режим) або локальний захищений реєстр (аварійний режим).

– A2 (Видача та фіксація): Цей блок є вузлом прийняття рішень про фізичну активацію механізму видачі. Він має зворотний зв'язок з блоком A3, що дозволяє буферизувати транзакції при відсутності з'єднання.

– A3 (Облік та звітність): Відповідає за агрегацію даних та формування черги синхронізації (Sync Queue) після відновлення мережі.

– A4 (Контроль залишків): Забезпечує моніторинг фізичної наявності ЗІЗ, запобігаючи помилкам видачі при розсинхронізації баз даних.

Моделювання критичних функцій видачі (Діаграма A2). Деталізація блоку A2 дозволила виявити вразливість на етапі "Миттєва фіксація списання" (A23). У класичній архітектурі цей процес вимагає підтвердження від сервера ("Commit"). У розробленій моделі впроваджено механізм локальної фіксації, де виходом є не просто запис у БД, а криптографічно підписана транзакція, що зберігається в енергонезалежній пам'яті автомата.

Використання CASE-засобу Ramus дозволило верифікувати повноту моделі та гарантувати, що для кожного стану системи (Online/Offline) існує визначений шлях проходження інформаційного потоку, що унеможливлює виникнення стану невизначеного блокування.

Алгоритмізація процесів керування

Якщо функціональна модель IDEF0 визначає вимоги до інформаційних потоків («що має робити система»), то етап алгоритмізації формалізує логіку виконання цих вимог («як система це робить»). Ключовим об'єктом алгоритмізації є блок A1 («Ідентифікація та авторизація»), який відповідає за прийняття рішення про допуск користувача.

Для реалізації концепції кіберстійкості розроблено алгоритм адаптивного керування, який базується на моделі **тристанового скінченного автомата (Finite State Machine)**. Логіка переходів між станами визначається моніторингом часового інтервалу з моменту отримання останнього сигналу перевірки зв'язку (*heartbeat*).

Алгоритм передбачає функціонування системи у трьох режимах:

1. **ONLINE (Штатний режим).** Система має стабільне з'єднання з сервером. Авторизація відбувається через центральну базу даних. У фоновому режимі виконується синхронізація хеш-образів лімітів для підготовки до можливих збоїв.
2. **DEGRADED (Перехідний режим).** Діагностовано нестабільність з'єднання (втрата пакетів або затримка відповіді). Система намагається відновити зв'язок протягом короткого таймауту, перш ніж прийняти рішення про перехід в автономний режим. Це запобігає помилковим перемиканням при короткочасних збоях.
3. **OFFLINE (Аварійний режим).** Фіксується повна втрата зв'язку (наприклад, внаслідок DDoS-атаки). Система переходить на використання локального захищеного реєстру та алгоритму хеш-ланцюжків для фіксації транзакцій.

Графічна інтерпретація розробленого алгоритму та умов переходу між станами наведена на рис. 1.

Рис. 1. Діаграма станів контролера CAB-ЗІЗ та логіка переходів

Такий підхід дозволяє чітко детермінувати поведінку системи у будь-який момент часу, виключаючи невизначеність, характерну для класичних архітектур при збоях мережі.

Програмна реалізація та верифікація

Для перевірки ефективності запропонованих архітектурно-алгоритмічних рішень було розроблено імітаційну модель системи мовою Python. Метою експерименту є кількісна оцінка показників доступності сервісу (Availability) та стійкості до навантажень в умовах кібератак.

Сценарій моделювання відтворює роботу промислового об'єкта з наступними параметрами:

– Кількість користувачів: N = 200.
– Тривалість зміни: T = 24 години.
– Модель загрози: Атака на відмову в обслуговуванні (DDoS) з повною блокадою каналу зв'язку в період t.

Порівняльний аналіз роботи класичної та запропонованої систем наведено на рис. 2.

Графіки демонструють наступні результати:

1. Забезпечення безперервності (верхній графік). Класична система (червона лінія) демонструє повну зупинку обслуговування під час атаки (горизонтальне плато), що означає простий виробництва. Запропонована система (синя лінія) завдяки переходу в режим *Offline* продовжує видачу ЗІЗ, зберігаючи лінійне зростання кількості транзакцій. Показник доступності сервісу становить >98%.
2. Керування навантаженням (нижній графік). Під час атаки транзакції накопичуються у локальному буфері (зростання синьої лінії). Після відновлення зв'язку (t=15) алгоритм не надсилає всі дані миттєво, а використовує механізм пакетної синхронізації (східчасте падіння графіка). Це дозволяє уникнути перевантаження мережі («мережевого шторму») та гарантує стабільність роботи каналу передачі даних.

Таким чином, результати моделювання підтверджують, що алгоритмічне забезпечення на базі тристанового автомата та периферійних обчислень дозволяє гарантувати виконання бізнес-процесів навіть в умовах критичних збоїв інфраструктури.

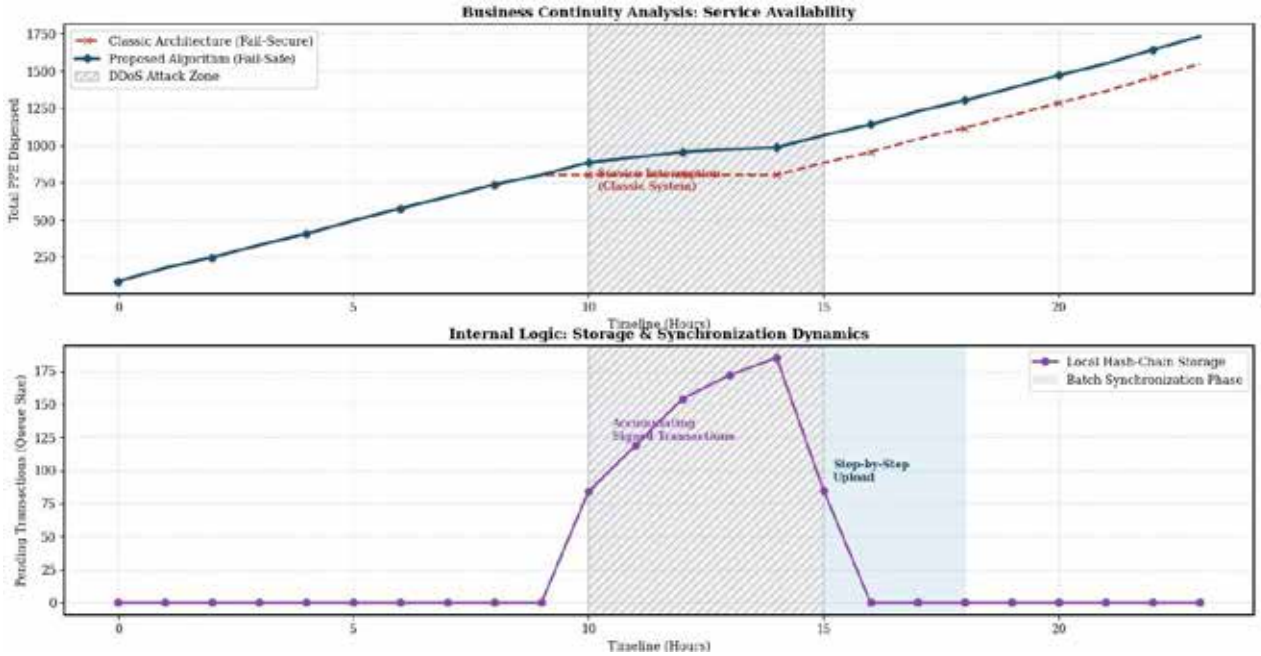

Рис. 2. Результати імітаційного моделювання доступності сервісу (вгорі) та процесу синхронізації даних (внизу)

Висновки

У роботі вирішено актуальне науково-практичне завдання забезпечення кіберстійкості критичної інфраструктури охорони праці в умовах деструктивних кібервпливів на IIoT-системи. Основні наукові та практичні результати дослідження полягають у наступному:

1. Доведено обмеженість класичних архітектур. Встановлено, що традиційна централізована (хмарна) модель авторизації створює критичну точку відмови. Під час DDoS-атак вона діє за принципом безпечного блокування (Fail-Secure), що є неприпустимим для систем промислової безпеки, оскільки призводить до вимушеного простою виробництва та порушення законодавчих норм охорони праці.

2. Розроблено гібридну архітектуру на основі периферійних обчислень. Запропоновано підхід, що передбачає децентралізацію логіки прийняття рішень. Перенесення процесу валідації прав доступу на рівень контролера вендингового автомата дозволяє реалізувати концепцію безпечної відмови – гарантованої видачі критичних засобів захисту навіть за повної відсутності зв'язку з сервером.

3. Створено алгоритм адаптивної кіберстійкості. Розроблений метод базується на тристановому автоматі функціонування (ONLINE / DEGRADED / OFFLINE) та забезпечує автоматичне перемикання на локальний захищений кеш із застосуванням аварійних квот для запобігання конфліктам розщеплення (Split-Brain). Специфікація алгоритму опублікована у відкритому репозиторії GitHub для верифікації логіки обробки винятковых ситуацій.

4. Запропоновано метод захисту цілісності даних. Для протидії локальній фальсифікації в офлайн-режимі розроблено механізм криптографічної інкапсуляції записів з використанням технології хеш-ланцюжків на базі алгоритму SHA-256, що гарантує незмінність історії транзакцій.

5. Експериментально підтверджено ефективність методу. Результати імітаційного моделювання показали, що в умовах тривалої DDoS-атаки (5 годин) запропонована система забезпечує показник доступності сервісу на рівні понад 98%, тоді як класична архітектура демонструє повну зупинку обслуговування. Реалізований протокол пакетної синхронізації довів свою ефективність у запобіганні перевантаженню мережі на етапі відновлення зв'язку.

Практичне значення роботи полягає у можливості мінімізації економічних втрат промислових підприємств від простоїв, спричинених кібератаками, та забезпеченні безперервного захисту персоналу незалежно від стану IT-інфраструктури.

Перспективи подальших досліджень. Подальша робота буде спрямована на апаратну реалізацію прототипу модуля на базі платформи ESP32 з використанням апаратного шифрування та дослідження методів машинного навчання для виявлення аномальної поведінки користувачів в офлайн-режимі.

Список використаної літератури

1. Lezzi M., Corallo A., Lazoi M., Nimis A. B Measuring cyber resilience in industrial IoT: a systematic literature review. *Management Review Quarterly*. 2025. URL: https://doi.org/10.1007/s11301-025-00495-8.

2. Yang H., Dai L., Ma Y., Li Q., Xia Y. Resilient MPC With Switched Cost Functions for Cyber-Physical Systems Against DoS Attacks. *IEEE Transactions on Systems, Man, and Cybernetics: Systems* 2025. Vol. 55. P. 4444–4457. https://doi.org/10.1109/tsmc.2025.3555826.

3. Tang X., Zhao K., Qu H., Wang J. Adaptive event-triggered efficient output feedback model predictive control for networked interval type-2 T–S fuzzy system with data loss. *International Journal of Robust and Nonlinear Control*. 2023. Vol. 34. P. 1673–1695. https://doi.org/10.1002/rnc.7049.

4. Wang Y., Zhu F. Consensus Control for Nonlinear Multi-Agent Systems. *IEEE Transactions on Automation Science and Engineering*. 2025. Vol. 22. P. 10470–10483. https://doi.org/10.1109/tase.2024.3524258.

5. Dildar M., Khan A., Abbasi I., Akhtar R., Ruqaishi K., Sarwar S. End-to-End Security Mechanism Using Blockchain for Industrial Internet of Things. *IEEE Access*. 2025. Vol. 13. P. 20584–20598: https://doi.org/10.1109/access.2025.3535821.

6. Oh T. Blockchain-Enabled Security Enhancement for IoT Networks: Integrating LEACH Algorithm and Distributed Ledger Technology. *Journal of Machine and Computing.* 2025: https://doi.org/10.53759/7669/jmc202505038.

7. Segovia-Ferreira M., Rubio-Hernán J., Cavalli A., García-Alfaro J. Survey on Cyber-Resilience Approaches for Cyber-Physical Systems. *ACM Computing Surveys.* 2023. Vol. 56. P. 1–37: https://doi.org/10.1145/3652953.

8. Liu S., Trivedi A., Yin X., Zamani M. Secure-by-Construction Synthesis of Cyber-Physical Systems. *Annu. Rev. Control*. 2022. Vol. 53. P. 30–50. https://doi.org/10.1016/j.arcontrol.2022.03.004.

9. Bakirtzis G., Sherburne T., Adams S., Horowitz B., Beling P., Fleming C. An ontological metamodel for cyber-physical system safety, security, and resilience coengineering. *Software and Systems Modeling.* 2020. Vol. 21. P. 113–137: https://doi.org/10.1007/s10270-021-00892-z.

10. Крайнюк О. В., Буц Ю. В., Барбашин В. В., Яцюк М. В. Використання штучного інтелекту для управління безпекою праці. *Комунальне господарство міст. Серія: Технічні науки та архітектура*. 2023. № 6(180). С. 207–214. https://doi.org/10.33042/2522-1809-2023-6-180-207-213

11. Крайнюк О., Буц Ю., Барбашин В., Козодой Д., Козодой О. Інтелектуальні системи управління безпекою праці на основі штучного інтелекту: перспективи інтеграції в українське законодавство. *Комунальне господарство міст.* 2024. № 6(187). С. 242–251. https://doi.org/10.33042/2522-1809-2024-6-187-242-251.

12. Крайнюк О. В., Буц Ю. В., Богатов О. І., Лоцман П. І., Барбашин В. В. Управління засобами індивідуального захисту за допомогою вендингових автоматів. *The 9th International scientific and practical conference "Study of world opinion regarding the development of science*". 2022. P. 672–678. URL: https://doi.org/10.46299/ISG.2022.2.9.

References

1. Lezzi, M., Corallo, A., Lazoi, M., & Nimis, A. (2025). Measuring cyber resilience in industrial IoT: A systematic literature review. Management Review Quarterly. DOI: 10.1007/s11301-025-00495-8

2. Yang, H., Dai, L., Ma, Y., Li, Q., & Xia, Y. (2025). Resilient MPC with switched cost functions for cyber-physical systems against DoS attacks. IEEE Transactions on Systems, Man, and Cybernetics: Systems, 55, 4444–4457. DOI: 10.1109/tsmc.2025.3555826

3. Tang, X., Zhao, K., Qu, H., & Wang, J. (2023). Adaptive event-triggered efficient output feedback model predictive control for networked interval type-2 T-S fuzzy system with data loss. International Journal of Robust and Nonlinear Control, 34, 1673–1695. DOI: 10.1002/rnc.7049

4. Wang, Y., & Zhu, F. (2025). Distributed hybrid dynamic event-triggered consensus control for nonlinear multi-agent systems. IEEE Transactions on Automation Science and Engineering, 22, 10470–10483. DOI: 10.1109/tase.2024.3524258

5. Dildar, M., Khan, A., Abbasi, I., Akhtar, R., Ruqaishi, K., & Sarwar, S. (2025). End-to-end security mechanism using blockchain for Industrial Internet of Things. IEEE Access, 13, 20584–20598. DOI: 10.1109/access.2025.3535821

6. Oh, T. (2025). Blockchain-enabled security enhancement for IoT networks: Integrating LEACH algorithm and distributed ledger technology. Journal of Machine and Computing. DOI: 10.53759/7669/jmc202505038

7. Segovia-Ferreira, M., Rubio-Hernán, J., Cavalli, A., & García-Alfaro, J. (2023). A survey on cyber-resilience approaches for cyber-physical systems. ACM Computing Surveys, 56, 1–37. DOI: 10.1145/3652953

8. Liu, S., Trivedi, A., Yin, X., & Zamani, M. (2022). Secure-by-construction synthesis of cyber-physical systems. Annual Reviews in Control, 53, 30–50. DOI:10.1016/j.arcontrol.2022.03.004

9. Bakirtzis, G., Sherburne, T., Adams, S., Horowitz, B., Beling, P., & Fleming, C. (2020). An ontological metamodel for cyber-physical system safety, security, and resilience coengineering. Software and Systems Modeling, 21, 113–137. DOI:10.1007/s10270-021-00892-z

10. Krainiuk, O. V., Buts, Yu. V., Barbashin, V. V., & Yatsiuk, M. V. (2023). Use of artificial intelligence for occupational safety management. Komunalne hospodarstvo mist. Seriia: Tekhnichni nauky ta arkhitektura, (6(180)), 207–214. DOI: 10.33042/2522-1809-2023-6-180-207-213

11. Krainiuk, O., Buts, Yu., Barbashin, V., Kozodoi, D., & Kozodoi, O. (2024). Intelligent occupational safety management systems based on artificial intelligence: Prospects for integration into Ukrainian legislation. Komunalne hospodarstvo mist, (6(187)), 242–251. DOI: 10.33042/2522-1809-2024-6-187-242-251

12. Krainiuk, O. V., Buts, Yu. V., Bohatov, O. I., Lotsman, P. I., & Barbashin, V. V. (2022). Management of personal protective equipment using vending machines. In The 9th International scientific and practical conference "Study of world opinion regarding the development of science" (pp. 672–678). International Science Group. DOI: 10.46299/ISG.2022.2.9

Дата першого надходження рукопису до видання: 11.11.2025
Дата прийнятого до друку рукопису після рецензування: 08.12.2025
Дата публікації: 31.12.2025