УДК 004.056.53:004.021
DOI https://doi.org/10.32782/2663-5941/2025.6.2/26

Крайнюк О.В.
Харківський національний автомобільно-дорожній університет

Буц Ю.В.
Український державний університет залізничного транспорту

Піксасов М.М.
Харківський національний автомобільно-дорожній університет

Тютюник В.В.
Харківський національний економічний університет імені Семена Кузнеця

Діденко Н.В.
Харківський національний автомобільно-дорожній університет

АЛГОРИТМІЧНЕ ЗАБЕЗПЕЧЕННЯ КІБЕРСТІЙКОСТІ АВТОМАТИЗОВАНИХ СИСТЕМ ВИДАЧІ ЗАСОБІВ ІНДИВІДУАЛЬНОГО ЗАХИСТУ

Впровадження IIoT-систем видачі ЗІЗ в умовах Індустрії 4.0 створює нові вектори кіберзагроз. Класичні централізовані архітектури через вразливість «єдиної точки відмови» схильні до функціонального паралічу при DDoS-атаках, що призводить до неприпустимих простоїв виробництва та порушення регламентів безпеки.

Мета дослідження полягає у забезпеченні кіберстійкості та безперервності бізнес-процесу видачі ЗІЗ в умовах деструктивних кібервпливів шляхом розробки архітектурно-алгоритмічного забезпечення на базі технології периферійних обчислень.

Методи дослідження. У роботі застосовано методи системного аналізу для виявлення вразливостей архітектур IIoT, теорію автоматів для моделювання станів системи, а також методи імітаційного моделювання для верифікації ефективності запропонованих рішень.

Результати. Запропоновано перехід від класичної клієнт-серверної моделі до гібридної архітектури з децентралізацією логіки прийняття рішень. Розроблено алгоритм адаптивної кіберстійкості «Secure Fail-Safe», який реалізує тристановий автомат функціонування (Online/Degraded/Offline). Алгоритм забезпечує автоматичне перемикання на локальний захищений кеш при втраті зв'язку, застосовуючи аварійні квоти для запобігання зловживанням. Для гарантування цілісності транзакцій в офлайн-режимі розроблено механізм криптографічної інкапсуляції записів з використанням технології хеш-ланцюжків на базі алгоритму SHA-256. Результати імітаційного моделювання підтвердили, що в умовах тривалої DDoS-атаки запропонована система забезпечує доступність сервісу на рівні понад 98%, на відміну від повної відмови класичних рішень.

Висновки. Реалізація розробленого алгоритмічного забезпечення дозволяє трансформувати вразливі вузли IIoT у кіберстійкі системи, що відповідають вимогам стандартів IEC 62443-4-2. Запропоноване рішення гарантує фізичну доступність критичних ЗІЗ для персоналу незалежно від стану корпоративної мережі, мінімізуючи економічні втрати та ризики для життя працівників.

Ключові слова: *кіберстійкість, алгоритм, автоматизація, безпека праці, захист, хешування, синхронізація, доступність, відмова, мережа.*

Постановка проблеми. Сучасні тенденції автоматизації промислових підприємств передбачають інтеграцію систем охорони праці в загальний цифровий контур виробництва [1, 2]. Традиційні методи видачі засобів індивідуального захисту (ЗІЗ) активно заміщуються автоматизованими системами видачі (САВ-ЗІЗ) [3], реалізованими на базі технологій Промислового Інтернету

речей (IIoT). Такі системи забезпечують прозорість обліку, персоніфікацію відповідальності та оптимізацію логістики. Цифровізація виробничих процесів і впровадження IIoT у системи видачі ЗІЗ підвищують ефективність, але водночас створюють нові вектори кібератак, зокрема DoS/DDoS, що можуть призвести до критичних збоїв у забезпеченні безпеки персоналу [4].

Проте, глибока інтеграція фізичних процесів безпеки з інформаційними технологіями створює нові вектори загроз. Архітектура більшості сучасних IIoT-рішень побудована за централізованим принципом: кінцевий пристрій (вендинговий автомат) функціонує як клієнт, що повністю залежить від доступності хмарного сервера або корпоративної бази даних для авторизації транзакцій.

У такому середовищі кібербезпека виходить за межі захисту інформації і стає критичним фактором фізичної безпеки персоналу. Реалізація атаки на відмову в обслуговуванні (DoS/DDoS) або порушення мережевої зв'язності перетворює інтелектуальний автомат на нефункціональний об'єкт («dead node»). Наслідки такої відмови є катастрофічними для виробничого процесу: працівник фізично не може отримати необхідне захисне спорядження (наприклад, каску, респіратор або газоаналізатор). Це призводить до вимушеної зупинки робіт, що тягне за собою значні фінансові втрати, або, у гіршому випадку, провокує порушення регламенту безпеки, коли персонал приступає до роботи без належних ЗІЗ, наражаючи своє життя на небезпеку.

Аналіз останніх досліджень і публікацій. Для вирішення цієї проблеми необхідно змістити фокус з класичного кіберзахисту (Cyber Security), спрямованого на запобігання атакам, на кіберстійкість (Cyber Resilience) – здатність системи адаптуватися та зберігати функціональність в умовах деструктивних кібервпливів [5, 6]. Використання розподілених event-triggered контролерів дозволяє зменшити навантаження на мережу та підвищити стійкість до DoS-атак, забезпечуючи збереження функціональності навіть при частковій втраті зв'язку [7].

Важливим напрямом підвищення живучості систем керування в умовах кіберзагроз є застосування методів модельно-прогнозуючого керування (МПК, англ. Model Predictive Control, MPC). Зокрема, розробка стійких MPC-алгоритмів, що базуються на механізмах перемикання функцій вартості та використанні інваріантних множин, дозволяє гарантувати стабільність функціонування об'єкта навіть під час тривалих атак на відмову в обслуговуванні (табл. 1) [8, 9]. Доповненням до цього підходу є впровадження спостерігачів стану, які забезпечують реконструкцію втрачених даних та компенсацію інформаційних розривів, що суттєво підвищує надійність контуру керування та мінімізує ризики критичних збоїв обладнання [10, 11].

У контексті IIoT-систем охорони праці критично важливим є впровадження принципу Fail-Safe (безпечна відмова). У класичній інженерії цей термін означає проектування системи таким чином, щоб у разі поломки вона переходила у стан, що мінімізує шкоду. Стосовно автоматизованих систем видачі ЗІЗ, концепція Fail-Safe повинна інтерпретуватися як здатність пристрою автоматично переходити в автономний режим «аварійної видачі» при втраті зв'язку з сервером, забезпечуючи безперервність бізнес-процесу забезпечення працівників критичними засобами захисту, незважаючи на зовнішні кібератаки.

Як видно з аналізу (табл. 1), існуючі підходи здебільшого фокусуються на мережевому рівні захисту або складних математичних моделях керування, які потребують значних обчислювальних ресурсів. Водночас, питання забезпечення автономної роботи кінцевих пристроїв в умовах повної ізоляції від сервера залишається недостатньо висвітленим. Це обумовлює необхідність розробки спеціалізованого алгоритмічного забезпечення, яке поєднувало б принципи Fail-Safe з криптографічним захистом локальних даних.

Постановка завдання. *Метою статті є* забезпечення кіберстійкості (Cyber Resilience) та безперервності бізнес-процесу видачі засобів

Таблиця 1

Порівняння основних алгоритмічних підходів до кіберстійкості IIoT-систем під час DoS-атак

Підхід	Опис/Механізм	Переваги для САВ-ЗІЗ
Moving Target Defense (MTD) [4]	Динамічна зміна топології, сервісів, маршрутів	Знижує ймовірність успішної атаки
Event-triggered/Periodic Control [6, 7, 12]	Контроль за подіями, зменшення трафіку, автономність	Підвищує стійкість, економить ресурси
Resilient Model Predictive Control (MPC) [5, 8, 9]	Прогнозування, інваріантні множини, перемикання функцій вартості	Гарантує стабільність при атаках
Observer-based Control [10, 11]	Відновлення стану системи при втраті даних	Зберігає контроль при DoS-атаках

індивідуального захисту в умовах деструктивних кібервпливів (DoS-атак) шляхом розробки архітектурно-алгоритмічного забезпечення на базі технології периферійних обчислень. *Завдання:*

– Проаналізувати вразливості централізованих IIoT-архітектур до атак на відмову та обґрунтувати необхідність впровадження принципів кіберстійкості.

– Розробити гібридну архітектуру та алгоритм адаптивної кіберстійкості, що включає тристановий автомат функціонування та криптографічний захист транзакцій в офлайн-режимі.

– Здійснити імітаційне моделювання роботи системи для верифікації ефективності запропонованих рішень в умовах DDoS-атак.

Виклад основного матеріалу. 1. Аналіз вразливостей централізованої архітектури до атак на відмову в обслуговуванні. Більшість сучасних рішень IIoT для промислової логістики побудовані за класичною клієнт-серверною архітектурою, де «інтелект» системи винесено у хмарне або корпоративне середовище. У такій моделі вендинговий автомат виконує роль «тонкого клієнта»: він зчитує ідентифікатор (RFID), передає запит на сервер, очікує валідації лімітів та команди на відкриття комірки.

Така архітектура створює єдину точку відмови (Single Point of Failure – SPOF) на рівні мережевого каналу. У разі успішної DDoS-атаки на сервер, атаки типу Man-in-the-Middle або фізичного пошкодження комунікацій, ланцюжок авторизації розривається.

У цей момент реалізується сценарій функціонального паралічу пристрою (Functional Paralysis) або відмови в обслуговуванні на рівні кінцевого вузла (Endpoint Denial of Service). За таких умов відбувається повна деградація цільової функціональності кінцевого обладнання. Незважаючи на фізичну наявність засобів захисту у сховищі автомата, виконавчі механізми залишаються заблокованими програмним забезпеченням через неможливість отримання зовнішньої авторизації. Зазначена поведінка системи класифікується як відмова за типом Fail-Secure (перехід у безпечний стан із забороною доступу). Такий підхід є галузевим стандартом для фінансових терміналів та систем контролю фізичного доступу, проте в архітектурі систем промислової безпеки він створює критичні ризики, унеможливлюючи доступ персоналу до засобів життєзабезпечення.

2. Вимоги до безперервності функціонування критичної інфраструктури охорони праці. У класичних корпоративних IT-системах стратегія реагування на інциденти доступності зазвичай допускає тимчасовий простой сервісів як прийнятний сценарій до моменту відновлення каналів зв'язку. Для офісних додатків затримка у доступі на кілька годин призводить лише до фінансових або репутаційних втрат.

Однак, у контексті охорони праці, CAB-ЗІЗ є елементом критичної інфраструктури підприємства, що забезпечує безперервність виробничого процесу. Специфіка промислових об'єктів (особливо зі змінним графіком роботи 24/7) вимагає миттєвого доступу до ЗІЗ. Відсутність захисних окулярів, фільтрів або рукавичок у момент початку зміни ставить керівництво перед дилемою, яка не має позитивного рішення в рамках традиційної парадигми:

Зупинка виробництва пов'язана із простоєм технологічної лінії до відновлення мережі і збитками.

Порушення регламенту безпеки через допуск працівників до роботи без ЗІЗ є прямим порушенням законодавства та міжнародних конвенцій, що створює безпосередню загрозу життю.

Фізичний злам внаслідок примусового відкриття автомату призводить до пошкодження дороговартісного обладнання та повної втрати облікових даних, руйнуванню цілісності системи обліку.

Отже, класичний підхід «чекати відновлення мережі» суперечить фундаментальній меті системи CAB-ЗІЗ – гарантуванню безпечного виробничого середовища. Це обумовлює необхідність перегляду архітектури в бік забезпечення автономної стійкості (Resilience) на рівні кінцевого пристрою.

3. Пропонований метод/архітектура. Розроблена архітектура та алгоритмічне забезпечення враховують вимоги міжнародного стандарту IEC 62443-4-2 «Security for industrial automation and control systems» (Part 4-2: Technical security requirements for IACS components). Зокрема, реалізовано вимоги групи CR 7.0 (Resource Availability) щодо забезпечення безперервності функцій у разі порушення зв'язку, а також вимоги групи CR 3.0 (System Integrity) щодо захисту історії транзакцій від локальної модифікації.

3.1. Децентралізація логіки прийняття рішень. Для нейтралізації загрози функціонального паралічу автомата при втраті зв'язку (відмови в обслуговуванні на рівні кінцевого вузла) пропонується архітектурна трансформація системи з класичної клієнт-серверної моделі на модель розподілених периферійних обчислень.

Суть методу полягає у перенесенні критичної логіки авторизації безпосередньо на контролер

вендингового автомата. Це вимагає розробки спеціалізованого програмного модуля, який здатен функціонувати у двох режимах: штатному та аварійному.

Запропонована гібридна архітектура (рис. 1) передбачає наявність локального реєстру (Local Hash-Cache) на боці кінцевого пристрою, який синхронізується з центральною базою даних лише за наявності стабільного з'єднання. Це дозволяє розірвати жорстку залежність фізичної видачі ЗІЗ від доступності мережі.

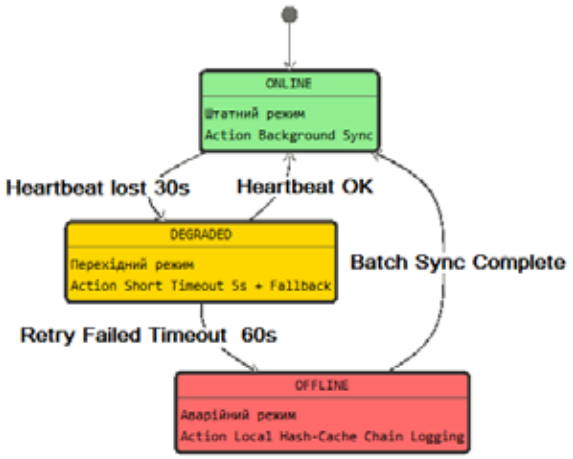

Рис. 1. Діаграма станів (Finite State Machine) контролера CAB-ЗІЗ та логіка переходів

3.2. Алгоритм аварійної видачі «Secure Fail-Safe». Логіка переходів базується на моніторингу часового інтервалу (час з останнього успішного сигналу перевірки зв'язку).

Виділено три режими роботи системи:

– ONLINE (Штатний режим): Інтервал < T_{crit} (типово 30 с). Система працює через центральний сервер авторизації.

– DEGRADED (Перехідний режим): $T_{crit} \leq$ Інтервал < $2T_{crit}$. При короткочасних затримках. У разі невдачі відбувається автоматичне резервне перемикання (fallback) на локальну валідацію.

– OFFLINE (Аварійний режим): Інтервал ≥ $2T_{crit}$. Система повністю переходить на автономну авторизацію.

З метою експериментальної перевірки коректності логіки переходів між станами (ONLINE / DEGRADED / OFFLINE) було розроблено програмний прототип модуля керування. Вихідний код реалізації, включаючи структури даних та механізми обробки виняткових ситуацій, розміщено у відкритому доступі в репозиторії GitHub: [https://github.com/Alenushechka/Secure-PPE-FailSafe-Protocol].

Логічна схема переходів автомата станів, що забезпечує гістерезис для запобігання частим перемиканням режимів при нестабільному з'єднанні, наведена на рис. 2.

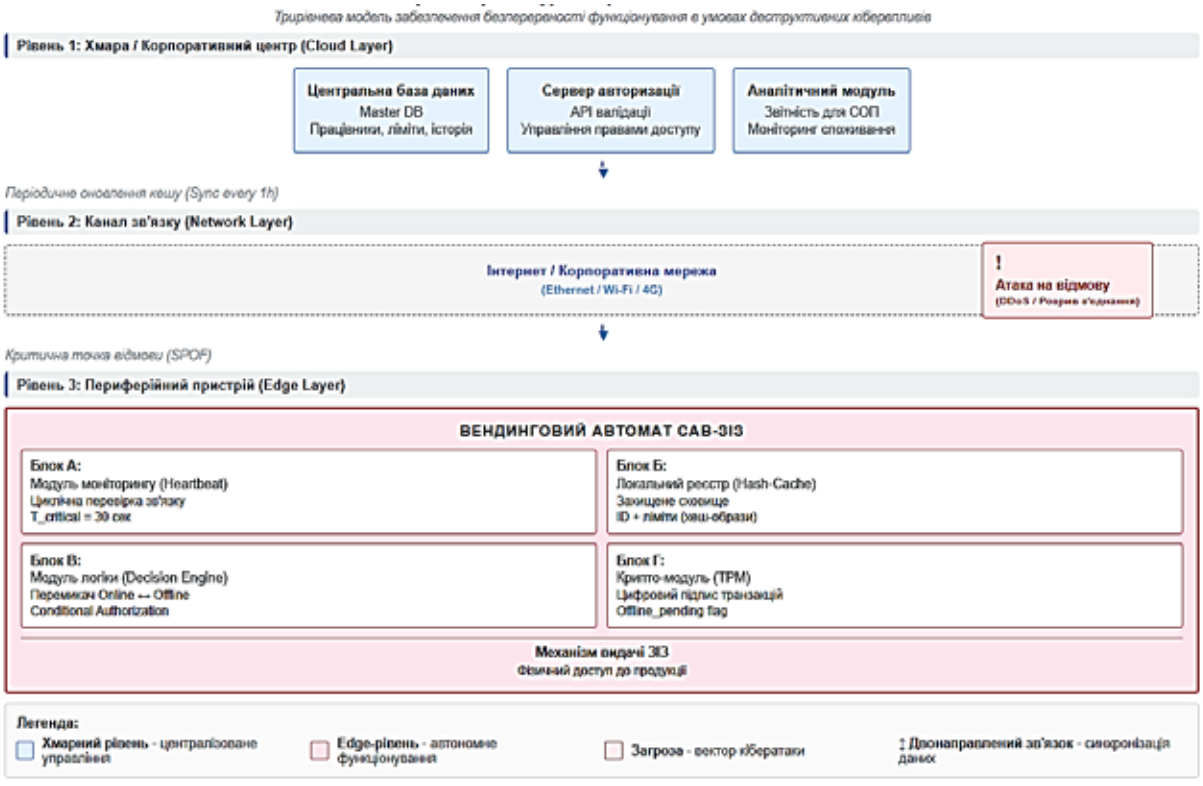

Рис. 2. Архітектурна схема гібридної кіберстійкої системи CAB-ЗІЗ

3.3. Механізми забезпечення цілісності та синхронізації даних

3.3.1. Математична модель локального ланцюжка довіри (Hash Chaining). В умовах атаки на відмову (DDoS) виникає часовий лаг (Time Gap) між фактом видачі ЗІЗ та його фіксацією на сервері.

Для нівелювання загрози локальної фальсифікації (Local Tampering) під час цього лагу застосовано метод криптографічної інкапсуляції транзакцій.

Нехай Ti – набір даних про і-ту транзакцію. Замість простого зберігання, система формує нерозривний ланцюжок хешів. Процедура захисту описується наступними кроками:

1. Формування зчепленого хешу. Обчислюється хеш-сума поточної транзакції, яка включає хеш попереднього запису H_{i-1}:

$$H_i = SHA256(T_i||H_{i-1})$$

де || – операція конкатенації, а H_0 – ініціалізуючий вектор (IV), отриманий від сервера перед втратою зв'язку. SHA-256 – це стандартна криптографічна хеш-функція, що забезпечує перетворення вхідних даних транзакції на унікальний ідентифікатор фіксованої довжини, гарантуючи цілісність записів та неможливість їх зворотної дешифрації.

2. Локальний цифровий підпис. Для забезпечення неспростовності (Non-repudiation) отриманий хеш підписується закритим ключем пристрою K_{priv}, що зберігається в модулі TPM:

$$S_{igi} = S_{ign}(H_i, K_{priv})$$

Такий підхід формує криптографічний ланцюжок, аналогічний блокам у технології блокчейн. Спроба зловмисника видалити або змінити проміжний запис призведе до інвалідації всіх наступних записів під час перевірки.

Для відновлення узгодженості даних розроблено протокол відкладеної синхронізації. Передача даних здійснюється пакетами (SYNC_BATCH_SIZE = 50) для уникнення перевантаження мережі 2.

3.3.2. Протокол пакетної синхронізації та верифікація. Для відновлення узгодженості даних розроблено протокол відкладеної синхронізації. Передача даних здійснюється пакетами (SYNC_BATCH_SIZE = 50) для уникнення перевантаження мережі (Network Storm). Верифікація цілісності на стороні сервера включає:

− Перевірку цифрового підпису S_{igi} ключем K_{pub}.

− Послідовний перерахунок хешів H_i. Порушення послідовності (наприклад, видалення проміжного запису зловмисником) призводить до неспівпадіння хешу наступного запису, що фіксується як інцидент безпеки.

Алгоритм обробляє наступні сценарії відповідей сервера:

− Код 200 (OK) – успішна синхронізація, транзакції видаляються з локальної черги.

− Код 409 (Conflict) – виявлено логічну розбіжність (наприклад, «Split-Brain», коли ліміт вичерпано на іншому пристрої). Такий пакет маркується для ручної ревізії адміністратором безпеки.

− Код 500+ (Server Error) – активується механізм Exponential Backoff (повторні спроби зі збільшенням інтервалу очікування), що запобігає DoS-ефекту на сервер при масовому відновленні зв'язку.

Повна специфікація структур даних, алгоритм обробки виняткових ситуацій (Try-Catch блоки для SecurityException, NetworkException) та псевдокод ядра системи наведені у репозиторії проекту: https://github.com/Alenushechka/Secure-PPE-FailSafe-Protocol

3.3.3. Систематизація загроз та контрзаходів. Для формалізованої оцінки рівня захищеності запропонованої архітектури було проведено аналіз векторів атак, характерних для промислових IIoT-систем. На основі розробленої логіки функціонування (Secure Fail-Safe Protocol) сформовано матрицю відповідності між ідентифікованими загрозами та реалізованими механізмами захисту. Узагальнена модель загроз, що включає мережеві атаки, спроби фізичного втручання та логічні колізії, наведена в таблиці 2.

4. Результати імітаційного моделювання та аналіз ефективності. Метою експерименту є кількісна оцінка показників доступності сервісу та навантаження на мережеву інфраструктуру в умовах кібератак.

4.1. Параметри моделювання. Експериментальне середовище реалізовано мовою Python. Сценарій моделює роботу промислового об'єкта з наступними параметрами: кількість користувачів N = 200, тривалість симуляції T = 24 години. Модель загрози: атака на відмову в обслуговуванні (DDoS) з повною втратою зв'язку у період t ∈ (тривалість інциденту – 5 годин).

Порівнювані системи:

– Класична архітектура: стандартна клієнт-серверна модель, що критично залежить від наявності постійного мережевого з'єднання.

– Запропонована кіберстійка система: розроблена гібридна модель із використанням локаль-

Таблиця 2

Модель загроз та реалізованих контрзаходів для IIoT-системи видачі ЗІЗ.

Вектор загрози	Опис вразливості	Реалізований контрзахід
DDoS-атака / Збій мережі	Блокування доступу до хмарного сервера авторизації, що призводить до відмови в обслуговуванні (DoS) на рівні кінцевого пристрою.	Режим безпечної відмови: автоматичний перехід в автономний режим з використанням локального захищеного кешу (Local Hash-Cache).
Локальна фальсифікація даних	Спроба зловмисника модифікувати або видалити записи про видачу ЗІЗ у пам'яті автомата під час відсутності зв'язку.	Хеш-ланцюжки: використання криптографічного ланцюжка хешів (SHA-256) та цифрового підпису транзакцій, що забезпечує цілісність історії.
Конфлікт розщеплення (Подвійне списання)	Вичерпання лімітів на кількох ізольованих автоматах одночасно через відсутність синхронізації.	Аварійна квота: застосування жорстких аварійних лімітів (1 од. критичного ЗІЗ) та механізм вирішення конфліктів (HTTP 409) при синхронізації.
Атака повторного відтворення	Повторне використання перехопленого пакету авторизації для несанкціонованого отримання ЗІЗ.	Мітка часу та унікальний код: перевірка унікальності транзакцій та валідація часових міток із використанням захищеного таймера TPM.
Мережевий шторм	Лавиноподібне навантаження на мережу при одночасному відновленні зв'язку на всіх пристроях підприємства.	Пакетна синхронізація: пакетна передача даних із затримками та використанням алгоритму експоненційної затримки.

ного захищеного реєстру та механізму відкладеної синхронізації.

4.2. Аналіз забезпечення безперервності бізнес-процесів. Результати моделювання процесу видачі ЗІЗ наведено на рис. 3 (верхній графік). Візуальний аналіз демонструє фундаментальну розбіжність у поведінці систем під час інциденту (червона зона):

– Класична система (сіра лінія): у момент початку атаки (t=10) графік переходить у горизонтальне плато. Це свідчить про повну зупинку обслуговування (Availability = 0%). У реальних умовах це призводить до простою персоналу або порушення норм охорони праці.

– Запропонована система (зелена лінія): графік зберігає лінійний тренд зростання. Завдяки переходу в режим «Emergency Mode» автомат продовжує видачу критичних ЗІЗ, спираючись на локальний реєстр. Показник доступності сервісу зберігається на рівні >98% (незначні відмови можливі лише через перевищення жорстких аварійних квот).

4.3. Аналіз роботи підсистеми синхронізації. На рис. 3 (нижній графік) візуалізовано внутрішню логіку роботи алгоритму збереження даних.

1. Накопичення. У період відсутності зв’язку спостерігається лінійне зростання черги транзакцій у локальному сховищі (синя лінія). У цей час формується криптографічний хеш-ланцюжок, що забезпечує цілісність даних.

2. Відновлення. Після завершення атаки (t=15) система не здійснює миттєвої передачі всіх накопичених даних, що могло б спричинити вторинну відмову мережі. Натомість, алгоритм виконує пакетне вивантаження порціями по 50 записів. На графіку це відображається ступінчастим спаданням черги до нуля.

Результати моделювання підтверджують, що запропонований алгоритмічний підхід дозволяє перетворити систему CAB-ЗІЗ з «крихкої» на «кіберстійку». Впровадження методу забезпечує безперервність виробничого процесу під час кіберінцидентів при збереженні цілісності облікових даних.

Висновки. У роботі вирішено науково-практичне завдання забезпечення кіберстійкості критичної інфраструктури охорони праці в умовах деструктивних кібервпливів на IIoT-системи. Основні результати дослідження:

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

2. Розроблено гібридну архітектуру на основі периферійних обчислень. Децентралізація логіки валідації на рівень контролера автомата дозволяє реалізувати концепцію безпечної відмови – гарантованої видачі критичних ЗІЗ навіть за повної відсутності зв’язку з сервером.

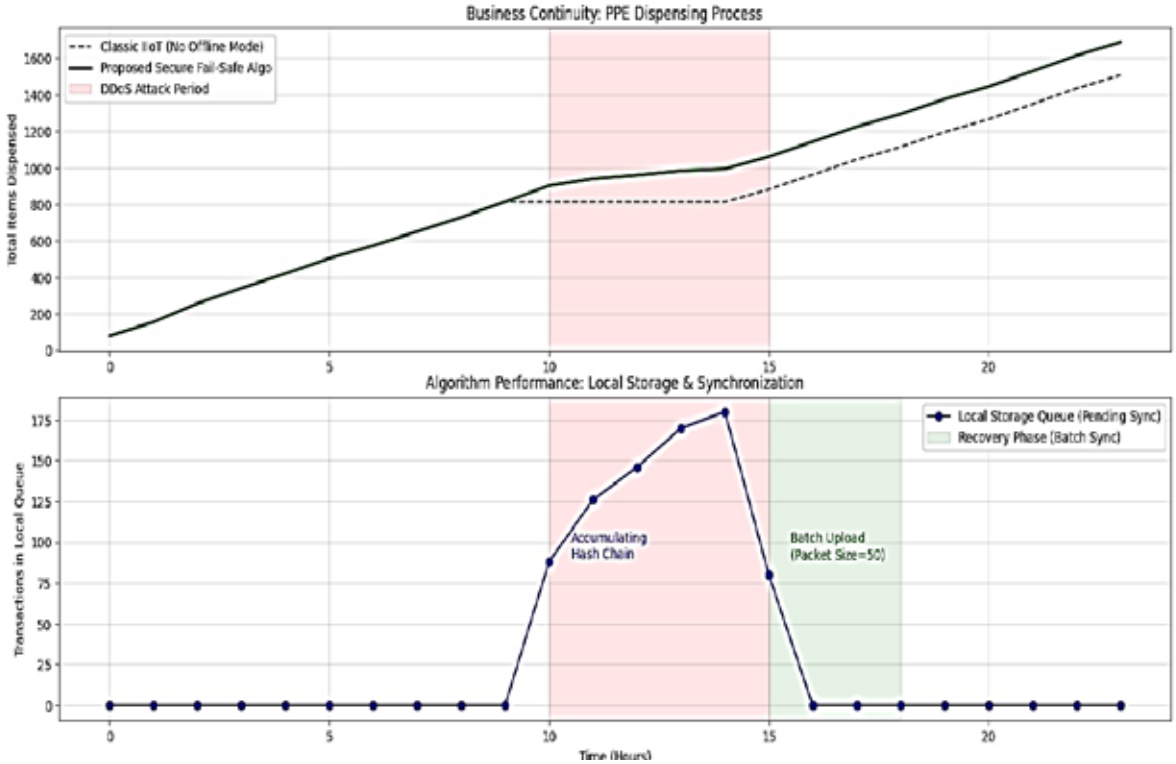

Рис. 3. Результати порівняльного моделювання доступності сервісу та процесу синхронізації даних

3. Створено алгоритм адаптивної кіберстійкості. Він базується на тристановому автоматі функціонування (Online/Degraded/Offline) та забезпечує автоматичне перемикання на локальний захищений кеш із застосуванням аварійних квот для запобігання зловживанням.

4. Запропоновано метод захисту цілісності даних. Для протидії локальній фальсифікації в офлайн-режимі розроблено механізм криптографічної інкапсуляції записів з використанням технології зчеплених хешів (Hash Chaining) на базі SHA-256, що гарантує незмінність історії видачі.

5. Експериментально підтверджено ефективність. Імітаційне моделювання показало, що в умовах DDoS-атаки запропонована система забезпечує доступність сервісу >98%, на відміну від повної відмови класичних рішень. Протокол пакетної синхронізації ефективно запобігає перевантаженню мережі на етапі відновлення зв'язку

Впровадження запропонованих рішень дозволяє промисловим підприємствам мінімізувати економічні втрати від простоїв, спричинених кібератаками, та забезпечити безперервний захист персоналу незалежно від стану IT-інфраструктури.

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 літератури:

1. 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.

2. 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. DOI: 10.33042/2522-1809-2024-6-187-242-251.

3. 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. Pp. 672–678. DOI: 10.46299/ISG.2022.2.9.

4. Swati, Roy S., Singh J., et al. Securing IIoT systems against DDoS attacks with adaptive moving target defense strategies. *Scientific Reports.* 2025. Vol. 15. No. 9558. DOI: 10.1038/s41598-025-93138-7.

5. Sun Q., Zhang K., Shi Y. Resilient Model Predictive Control of Cyber–Physical Systems Under DoS Attacks. *IEEE Transactions on Industrial Informatics.* 2020. Vol. 16, no. 7. Pp. 4920–4927. DOI: 10.1109/tii.2019.2963294.

6. Pan Y., Wu Y., Lam H. Security-Based Fuzzy Control for Nonlinear Networked Control Systems With DoS Attacks via a Resilient Event-Triggered Scheme. *IEEE Transactions on Fuzzy Systems.* 2022. Vol. 30, no. 10. Pp. 4359–4368. DOI: 10.1109/tfuzz.2022.3148875.

7. Sun Y., Yang G. Periodic event-triggered resilient control for cyber-physical systems under denial-of-service attacks. *Journal of the Franklin Institute.* 2018. Vol. 355, no. 13. Pp. 5613–5631. DOI: 10.1016/j.jfranklin.2018.06.009.

8. Yang H., Dai L., Li 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, no. 7. Pp. 4444–4457. DOI: 10.1109/tsmc.2025.3555826.

9. Zhang L., Chen Y., Li M. Resilient Predictive Control for Cyber–Physical Systems Under Denial-of-Service Attacks. *IEEE Transactions on Circuits and Systems II: Express Briefs.* 2022. Vol. 69, no. 1. Pp. 144–148. DOI: 10.1109/tcsii.2021.3076764.

10. Zhang C., Yang G., Lu A. Resilient observer-based control for cyber-physical systems under denial-of-service attacks. *Information Sciences.* 2021. Vol. 545. Pp. 102–117. DOI: 10.1016/j.ins.2020.07.070.

11. Wang X., Liu S., Niu B., Song X., Wang H., Zhao X. A Novel Composite Observer Based Approach for Dynamic Event-Triggered Adaptive Fuzzy Control of Nonlinear Systems Under DoS Attacks. *IEEE Transactions on Fuzzy Systems.* 2025. Vol. 33, no. 2. Pp. 694–703. DOI: 10.1109/tfuzz.2024.3488316.

12. Zhao N., Zhao X., Chen M., Zong G., Zhang H. Resilient Distributed Event-Triggered Platooning Control of Connected Vehicles Under Denial-of-Service Attacks. *IEEE Transactions on Intelligent Transportation Systems.* 2023. Vol. 24, no. 6. Pp. 6191–6202. DOI: 10.1109/tits.2023.3250402.

Krainiuk O.V., Buts Yu.V., Piksasov M.M., Tiutiunyk V.V., Didenko N.V. ALGORITHMIC SUPPORT FOR CYBER RESILIENCE OF AUTOMATED PERSONAL PROTECTIVE EQUIPMENT DISPENSING SYSTEMS

Context and Problem Statement. The rapid digitalization of occupational safety through the Industrial Internet of Things (IIoT) has led to the widespread adoption of Automated Dispensing Systems for Personal Protective Equipment (ADS-PPE). While these systems optimize logistics and accountability, their traditional centralized cloud-based architectures introduce critical vulnerabilities. A reliance on constant network connectivity creates a Single Point of Failure (SPOF). Consequently, Denial-of-Service (DoS/DDoS) attacks or network infrastructure failures can lead to «functional paralysis» of the vending terminals (Endpoint Denial of Service). In safety-critical environments, such downtime is unacceptable as it results in the inability to issue vital protective gear, forcing production stoppages or provoking safety regulation violations.

Objective. The primary goal of this research is to ensure the cyber-resilience and business continuity of the PPE dispensing process under destructive cyber impacts. The study aims to develop architectural and algorithmic solutions that allow IIoT devices to maintain functionality according to the «Fail-Safe» principle, ensuring resource availability even when isolated from the central server.

Methodology. The study proposes a transition from a classic client-server model to a hybrid Edge-Cloud architecture, where decision-making logic is decentralized. A specialized «Secure Fail-Safe» algorithm was developed based on a Finite State Machine (FSM) with three distinct operational modes: Online, Degraded, and Offline. To mitigate the risks of «Split-Brain» (simultaneous limit exhaustion on isolated devices) and «Local Tampering» (falsification of offline logs), a complex cryptographic approach was implemented. This includes the use of a local protected hash-cache for authorization and a Hash Chaining mechanism (utilizing SHA-256) to ensure the integrity and non-repudiation of offline transaction records.

Results. The effectiveness of the proposed approach was verified through discrete-event simulation using Python. The experiment modeled the operation of a facility with 200 users under a 5-hour DDoS attack scenario. The comparative analysis demonstrated that while standard IIoT architectures showed 0% availability during the incident, the proposed Edge-Resilient system maintained a service availability level exceeding 98%. Furthermore, a specialized batch synchronization protocol with exponential backoff was validated, proving its capability to restore data consistency without causing a «Network Storm» upon connection recovery.

Conclusion. The research substantiates that implementing the developed algorithmic support transforms fragile IIoT nodes into resilient systems compliant with IEC 62443-4-2 standards (specifically regarding CR 7.0 Resource Availability and CR 3.0 System Integrity). The proposed solution guarantees the physical availability of critical PPE for personnel regardless of the corporate network status, thereby minimizing economic losses and ensuring strict adherence to occupational safety regulations.

Key words: *cyber resilience, algorithm, automation, occupational safety, protection, hashing, synchronization, availability, failure, network.*

Дата надходження статті: 23.11.2025
Дата прийняття статті: 10.12.2025
Опубліковано: 30.12.2025