UDC 004.056.55 **doi:** https://doi.org/10.20998/3083-6298.2025.03.06

Olena Krainiuk[1], Serhii Yevseiev[2], Khazail Rzayev[3], Shayasta Hasanova, Farhad[3]

[1] Kharkiv national automobile and highway university, Kharkiv, Ukraine
[2] National Technical University "Kharkiv polytechnic institute", Kharkiv, Ukraine
[3]Azerbaijan Technical University, Baku, Azerbaijan

# CYBERSECURITY OF ACCOUNTING FOR PERSONAL PROTECTIVE EQUIPMENT: MODELING OF THREATS TO DATA INTEGRITY IN IIOT SYSTEMS

**Abstract. Topicality.** Digitalization of manufacturing requires integrating occupational safety with cybersecurity. Automated PPE dispensing systems (ADS-PPE) handle sensitive IIoT accounting data and are vulnerable to physical tampering, network attacks, and ID cloning. Traditional methods risk errors, financial losses, and safety hazards. Protecting transactional data integrity is essential for business continuity and employee safety. **The subject of study** in the article is methods of ensuring data integrity and confidentiality in the SAB-PPE IIoT system at the stages of user authentication and transaction fixation, considering the specific vulnerabilities of industrial vending machines. **The purpose of the article** is to reduce the cyber risks by substantiating a secure ADS-PPE architecture and identifying critical points that require enhanced cyber protection to ensure the integrity and confidentiality of accounting data. **Results.** A functional IDEF0 model of the ADS-PPE system was developed. Critical elements – device vulnerability and ID compromise were identified as key threats. A multi-layered cybersecurity approach is proposed, including cryptographic hashes or blockchain for data integrity and multi-factor authentication (RFID + PIN/biometrics) with SSL/TLS for secure access. **Conclusion.** Reliable protection of IIoT PPE accounting systems is essential for data authenticity, uninterrupted production, and personnel safety. In production digitalization, occupational safety is tightly linked to cybersecurity.

**Keywords:** industrial Internet of Things (IIoT), cybersecurity, vending machine, data integrity, multi-factor authentication, PPE accounting.

## Introduction

**Problem relevance.** Providing employees with personal protective equipment (PPE) is a critical element of occupational safety and industrial security. Traditional methods of accounting for and distributing PPE, which often rely on manual or partially automated processes, are prone to human error, record-keeping mistakes, and – most importantly – do not ensure prompt and accurate control of distribution limits. These shortcomings not only lead to financial losses but also pose a potential risk of violating safety standards. In addition, dependence on the human factor creates operational barriers, including the need to contact the warehouse, wait for a warehouse employee, and comply with limited access schedules.

The implementation of an Automated PPE Dispensing System (ADS-PPE), realised through vending machines at an industrial enterprise, effectively addresses these problems [1]. The primary advantage is the provision of round-the-clock and uninterrupted access to the required PPE for employees. The system maintains strict and automatic accounting of issuance, controls limits, and promptly generates replenishment or procurement requests.

The modern automated ADS-PPE system operates as an Industrial Internet of Things (IIoT) device, processing and storing critically important accounting information, including the employee and limit database, as well as transaction data. Unlike traditional IT systems, industrial vending complexes are endpoints vulnerable to physical and network unauthorised access, manipulation of issuance limits, and ID badge fraud. Therefore, insufficient cybersecurity of these IIoT devices creates a significant risk to business continuity and enterprise accountability, as breaches in PPE accounting integrity may directly endanger occupational safety.

Providing employees with personal protective equipment (PPE) is a key requirement of occupational safety that is increasingly integrated with digital technologies [2, 3]. The transition to automated PPE accounting and dispensing systems, particularly through vending machines, enhances efficiency but simultaneously introduces new challenges related to data integrity and cybersecurity in the IIoT environment.

## 1. Literature review

### 1.1. Occupational safety and PPE provision: automation requirements

Providing employees with personal protective equipment (PPE) is a fundamental requirement of occupational safety, regulated by both national legislation (the Law of Ukraine *"On Occupational Safety"*) and international standards (e.g., *ILO Convention No. 161*). Modern requirements focus on preventive control and risk minimisation, which necessitate accurate and documented accounting of PPE issuance.

The traditional approach to PPE management, often based on manual records, paper cards, or partially automated warehouse systems, has several critical drawbacks. Operational barriers arise because PPE issuance depends on the warehouse schedule and the availability of the responsible staff member. This causes significant delays and results in the lack of round-the-clock (24/7) access, which is particularly critical for shift-based or continuous production operations.

Additionally, inefficient control mechanisms manifest in the inability to instantly verify issuance limits, which can potentially lead to unauthorised or

 

premature distribution, resulting in both financial losses and safety standards violations. There are also reporting delays, as reports for the Occupational Safety Service (OSS) and management are often generated with a considerable time lag, preventing a timely response to discrepancies or critical shortages.

Functional requirements thus necessitate a transition to an Automated PPE Dispensing System (ADS-PPE). Such a system, implemented through a vending machine, offers critical advantages that address the shortcomings above. Primarily, it ensures continuous access and autonomy by eliminating dependency on warehouse personnel and guaranteeing round-the-clock controlled availability, thereby improving operational efficiency. Furthermore, the system enables strict accounting through instant transaction logging and automated tracking of issuance, which forms the foundation for fraud prevention and enhanced PPE usage discipline.

### 1.2. IIoT-технології у промисловій логістиці: IIoT-архітектура та вендингові рішення

Modern manufacturing necessitates the implementation of automated and digital systems for PPE accounting and control, grounded in scientific and technical principles and compliant with legislative standards [4, 5]. Automation minimises the human factor, ensures 24/7 access to PPE, enables real-time limit control, and allows for instant report generation [4, 6].

Vending technologies have long gone beyond the consumer market. In industry, they are used as Industrial Vending Machines (IVM) for the controlled dispensing of consumables, tools, and, for example, PPE. Such vending machines provide autonomy, continuous access, strict accounting, and fraud reduction, which is particularly important for shift-based and constant production processes [4, 6]. They enable a rapid response to PPE shortages and enhance the discipline of use.

The Automated PPE Dispensing System (ADS-PPE) is a typical example of the Industrial Internet of Things (IIoT), characterised by the following features:

1. Embedded system (Edge Computing). The vending machine itself acts as an intelligent edge device equipped with an embedded processor and mechanisms such as ID readers and inventory sensors [7–10].

2. Collection of critical data. The device gathers information about employee identification (RFID, NFC), requests, and the physical state of stock (via inventory sensors). This data is used for access control, inventory tracking, and reporting [7, 9, 11, 12].

3. Communication with the central system (Operational Technology OT network). The vending machine communicates with the central employee and PPE limits database via a network channel, often integrated into the enterprise's operational or corporate network [7, 10, 13, 14].

The architecture of the Automated PPE Dispensing System (ADS-PPE) implements the principles of the Industrial Internet of Things (IIoT) by integrating hardware, software, and analytical components into a unified system. Its operation is based on automatic user identification, centralised limit accounting, and intelligent inventory management.

The interaction process begins with employee identification using an RFID or NFC pass. The contactless technology ensures fast user recognition, minimises the risk of error, and simultaneously performs authorisation. All transactions are linked to a centralised employee database, which stores issuance limits, access rights, and usage history. This database serves as the "single source of truth" for the entire system, ensuring transparency and eliminating double deductions or unauthorised issuance [15, 16].

Inventory management within the system is carried out automatically: the vending unit continuously monitors stock levels, generates replenishment notifications, and synchronises this information with the enterprise's accounting, ERP, or MES systems [15]. This approach ensures uninterrupted PPE availability, reduces administrative overhead, and enhances the efficiency of logistics processes.

A key feature of the Automated PPE Dispensing System (ADS-PPE) is the use of edge analytics, which enables on-device processing of critical data [10]. This minimises network load, accelerates system responsiveness, and enhances reliability in the event of network disruptions. The collected data can be transmitted to cloud-based or corporate environments, where centralised monitoring, efficiency analysis, and management reporting on PPE utilisation are performed.

Data protection is of paramount importance. The system incorporates mechanisms for authentication, access control, encryption, and event monitoring, all of which comply with industrial IIoT cybersecurity standards. These measures ensure the integrity of accounting data and the resilience of the entire infrastructure. Additionally, blockchain technologies can be implemented to strengthen further data immutability and traceability [17–23].

The transparency and accountability of the ADS-PPE are also notable: every user action and inventory change is recorded, which reinforces discipline and reduces the risk of fraud or misuse.

Thus, the Automated PPE Dispensing System functions as an intelligent component of the industrial digital ecosystem, integrating material supply automation with secure data management principles. Fully aligned with contemporary IIoT paradigms, the ADS-PPE operates as a smart edge device that collects critical operational data, integrates seamlessly with OT networks, and ensures an automated, secure, and controlled process of PPE distribution.

### 1.3. The interconnection between occupational safety and cybersecurity

In the context of the digital transformation of industrial environments, the concept of occupational safety has become inseparable from the cybersecurity of the information systems that manage and control personal protective equipment (PPE). Within the Industrial Internet of Things (IIoT) ecosystem, any breach of data integrity or availability directly affects

both the physical safety of employees and the continuity of production processes [24–26].

The Automated PPE Dispensing System (ADS-PPE) operates with mission-critical accounting data, including information on issuance limits and transaction records. These data determine an employee's right to access PPE and confirm the issuance of PPE. Any compromise of data integrity – such as unauthorised modification of issuance limits or deletion of issuance records – can lead to uncontrolled PPE distribution, the creation of hazardous working conditions, and legal risks for the enterprise. Therefore, maintaining the authenticity of transactional records becomes an integral element of the occupational safety management system.

The IIoT infrastructure supporting the ADS-PPE possesses unique vulnerabilities distinct from those of conventional IT systems. The placement of edge devices directly within the production environment introduces risks of physical access and hardware tampering. These edge devices, equipped with processors and embedded software, may be targeted by attacks aimed at seizing control of dispensing mechanisms or manipulating accounting data. Additional risks arise from authentication-level attacks, such as RFID badge cloning or forgery, as well as data compromise during transmission between the vending unit and the central database across the enterprise network [27, 28].

Thus, ensuring the cybersecurity of ADS-PPE systems extends far beyond the protection of informational assets; it represents a critical prerequisite for compliance with occupational safety standards. Robust protection of the IIoT architecture – including user authentication, access control, encrypted communication channels, and transaction monitoring – ensures data integrity, system continuity, and risk reduction for personnel [29].

In this context, cybersecurity emerges as an integral component of the occupational safety management system, and its implementation becomes a key factor in the resilience of the industrial environment. Cybersecurity in IIoT systems is not merely about protecting information – it is a fundamental condition for ensuring workplace safety, reducing personnel risks, and maintaining the operational stability of modern enterprises.

**The purpose of the research**. The purpose of the research. This article aims to justify the architecture of a secure Automated PPE Dispensing System (ADS-PPE) and to identify critical points that require enhanced cybersecurity measures to ensure the integrity and confidentiality of accounting data.

To achieve this goal, the following objectives have been set:

to describe the functional model of the Automated PPE Dispensing System using the IDEF0 methodology (A-0, A0, and detailed blocks);

to define the key data and control elements (ID pass, PPE issuance limits) from the perspective of their cybersecurity criticality;

to analyse potential cyber threats occurring at the stages of identification and authorisation (A1) and instant transaction recording (A2);

to propose measures aimed at ensuring the integrity of transactional data and the confidentiality of accounting information within the IIoT environment.

## 2. Functional model of the PPE issuance system (IDEF0)

The functional model of the Automated PPE Dispensing System (ADS-PPE) represents the interaction between the user, the device, and the enterprise's corporate database. The model is constructed using the IDEF0 methodology, which enables the formalisation of identification, accounting, and control processes for PPE through the precise definition of information flows (Fig. 1, Tables 1 and 2).

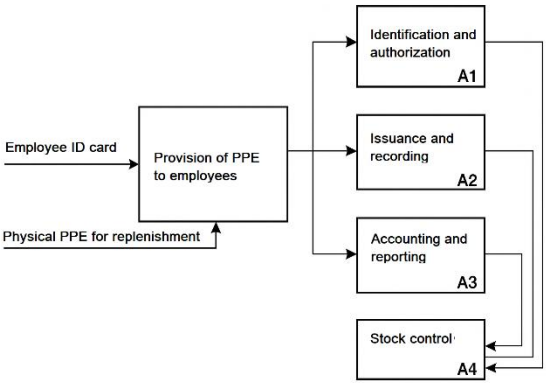


**Fig. 1.** Context diagram IDEF0 of the automated personal protective equipment dispensing system (APPE-PPE)

The context diagram (A-0) describes the overall function "Provision of Employees with PPE", which encompasses the entire cycle from employee identification to reporting and stock control. The primary source of reliable data is the employee and limits database, which ensures centralized management of authorization, accounting, and control.

At the detailed level (A0), the system is divided into four interconnected functional blocks.

The first block (A1 "Identification and Authorization") performs employee recognition via RFID identifier and verifies their right to receive PPE. If the limit is exhausted, a request for supervisor approval is generated (Fig. 2).

*Table 1* – **Structure of IDEF0 flows for the SAV-ZIZ system**

| Flow Type | Element | Purpose / Role in the Model |
|---|---|---|
| *Input* | Employee ID pass | Initiates the process of user identification and authorization. |
| | Physical PPE for replenishment | Provides the material input for the system during stock updates. |
| *Control* | PPE issuance limits | Regulate access rights and restrictions on issuance. |
| | Supervisor's approval | Authorizes over-limit issuance in cases of justified necessity. |
| *Output* | Issued PPE | Represents the physical result of the dispensing process. |

| Flow Type | Element | Purpose / Role in the Model |
|---|---|---|
| | Issuance transaction data | Forms the basis for reporting and analytics. |
| | Issuance report (for the Occupational Safety Service) | Used by the Occupational Safety Service for compliance control. |
| | Replenishment request data | Serves as a signal to initiate procurement or stock replenishment. |
| *Mechanism* | Vending machine | Performs identification, dispensing, and data logging operations. |
| | Employee and limit database | Stores information on access rights, transaction history, and inventory. |
| | IIoT network infrastructure | Provides |

*Table 2* – **Details of IDEF0 functional blocks for the SAV-ZIZ system**

| Block № | Process name | Brief function description | Main data / processed objects | Critical cybersecurity aspects |
|---|---|---|---|---|
| *A1* | Identification and authorization | Verification of the employee's identity and confirmation of the right to receive PPE according to limits or with supervisor approval. | ID card, limit database, supervisor's approval | Protection of identification data, prevention of RFID/NFC token cloning |
| *A11* | Reading ID card | Initiation of the identification process via RFID/NFC employee card reading. | User identifier, issue request | Secure reading, encryption of communication between reader and controller |
| *A12* | Verification of issue limit | Comparison of the employee's request with the current limit data in the database. | Employee limit, PPE type | Protection of database queries, access rights validation |
| *A13* | Requesting / obtaining approval | Generation of an over-limit issue request, its transmission to the supervisor, and receipt of confirmation. | Supervisor's approval, request log | Supervisor authentication, access log control |
| *A2* | Dispensing and recording | Automated physical dispensing of PPE after authorization and immediate database update. | PPE, transaction database | Integrity of transaction records, data backup |
| *A21* | Selection of PPE type and location | Search for required PPE in the system, identification of the corresponding dispenser tray. | User request, PPE catalog | Correct query routing, index validation |
| *A22* | Physical PPE dispensing | Activation of the dispensing mechanism, transfer of PPE to the employee. | Dispenser mechanism, issued PPE | Protection of hardware interface from unauthorized interference |
| *A23* | Instant write-off recording | Recording the issue in the database and updating the employee's limit. | Transaction data | Record hashing, log integrity control |
| *A3* | Accounting and reporting | Aggregation of all transaction data, generation of reports for OHS staff and managers. | Issue data, event logs | Protection of reporting data, change auditing |
| *A31* | Data processing and archiving | Standardization of transaction and event records for long-term storage. | Database archive | Backup, access control to archive |
| *A32* | Report generation for OHS | Creation of periodic reports on PPE issuance, use, and shortages. | Reporting data, report templates | Personal data confidentiality, digital signature |
| *A33* | Sending notifications to supervisor | Automatic notification about issuance events or limits. | Notifications, user data | Protection of message transmission channels, logging |
| *A4* | Stock control and replenishment | Monitoring of inventory status and generation of replenishment requests. | Stock data, normative levels | Protection of sensor data, verification of measurement reliability |
| *A41* | Stock monitoring and reconciliation | Comparison of physical data with database records after each operation. | Sensor readings, accounting data | Telemetry protection, anomaly monitoring |
| *A42* | Replenishment need generation | Generation of a signal indicating inventory shortage. | Stock level data | Signal authenticity control, verification |
| *A43* | Recording of replenishment fact | Registration of received PPE and database update. | New inventory, database | Access control, inventory change logging |

The second block (A2 "Dispensing and Recording") provides the physical issuance of the selected PPE and instant recording of the transaction in the database, ensuring data integrity (Fig. 2).

The third block (A3 "Accounting and Reporting") accumulates data on all events, generates reports for the Occupational Safety Service, and sends notifications to managers.

The fourth block (A4 "Stock Control") monitors inventory levels, compares them with normative thresholds, and automatically generates replenishment requests (Fig. 2).

To summarize the structure of flows and component roles, Table 1 presents the typical elements of the IDEF0 model — inputs, outputs, controls, and mechanisms.

Each process is further detailed in Table 2, revealing the internal logic of subprocesses (A11–A43). This level of detail allows not only the analysis of functional relationships but also the identification of critical cybersecurity points, where integrity, confidentiality, and accuracy of data must be ensured.

Thus, Fig. 1, Table 1, and Table 2 provide a comprehensive understanding of the ADS-PPE system architecture and operational logic, as well as highlight the information nodes most vulnerable from the perspective of IIoT industrial cybersecurity.

From a cybersecurity standpoint, the IDEF0 functional model identifies critical nodes requiring protection of data integrity and confidentiality: the user authentication stage, transactional write-off recording, report transmission, and communication with the database. Any compromise of these processes may result in loss of accounting accuracy, violations of occupational safety standards, or disruptions in production logistics.

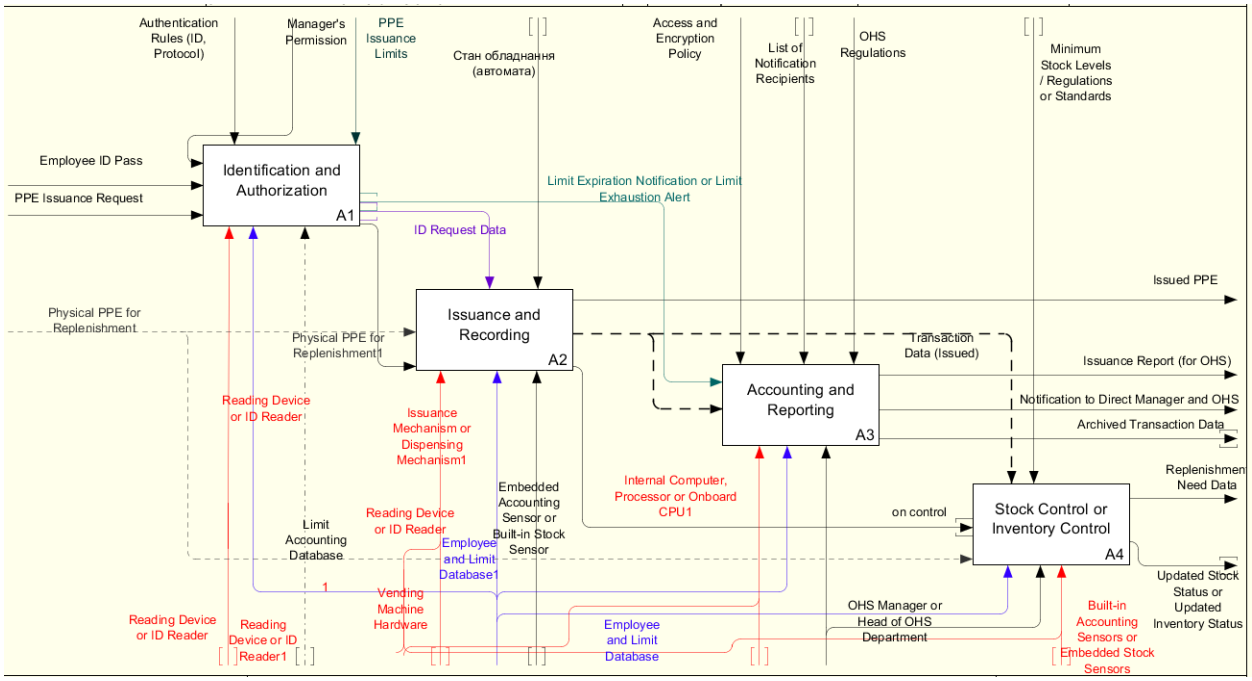


**Fig. 2.** Decomposition of the main process "PPE Issuance Management" (A0) in the Ramus software environment

The constructed context diagram (Fig. 2) allows outlining the overall boundaries of the ADS-PPE system and the interrelationships between the main information flows. To detail its internal logic, a functional diagram at the A0 level was developed, representing the interaction of four core processes: A1 – Identification and Authorisation, A2 – Dispensing and Recording, A3 – Accounting and Reporting, and A4 – Stock Control. The diagram was created using the specialised Ramus software environment, which supports the IDEF0 methodology and enables a clear depiction of the connections between subprocesses, information objects, and control flows (Fig. 2). The use of CASE tools ensures the formalisation of the model and facilitates the subsequent analysis of cyber threats within the system's IIoT architecture.

Thus, the IDEF0 model of ADS-PPE reflects not only the technological logic of the processes but also the cybernetic interdependence between information flows, databases, and physical dispensing mechanisms. The integrity of these connections is a key prerequisite for the reliable operation of the system and, consequently, forms the foundation for integrated occupational safety in a digital manufacturing environment.

## 3. Cybersecurity aspects and threats

The Automated PPE Dispensing System (ADS-PPE) operates as an element of the Industrial Internet of Things (IIoT) infrastructure, integrating hardware devices, software modules, and corporate data networks. This integration ensures continuity of production processes but simultaneously introduces a new level of cyber risks related to the physical location of devices, transmission of confidential information, and integrity of transaction records.

The ADS-PPE architecture includes three main components that are critical from a cybersecurity perspective (Fig. 3).

First, the vending machine, as an endpoint device, contains an embedded computer, RFID reader, and dispensing mechanism, making it vulnerable to physical attacks, unauthorised device connections, and exploitation of hardware interfaces.

Second, the communication channel that transmits data between the vending unit and the accounting database can be targeted for interception, malicious traffic injection, or compromise during the transfer of unencrypted packets.

Third, the employee and limits database, which stores access rights, issuance limits, and transaction

records, serves as a key repository of confidential data and determines the level of trust in the entire system.

The main cybersecurity threats and countermeasures can be described as follows:

Unauthorised access during identification and authorisation (A1). A potential threat is the use of forged or cloned RFID/NFC cards, which could allow an attacker to gain access to the vending unit. To prevent such attacks, it is advisable to implement multi-factor authentication (2FA), combining RFID with a PIN or biometric identifiers, as well as encrypting identifier data at the device level. Additionally, it is recommended to establish an access management policy that records all identification attempts in a security event log.

Data manipulation during dispensing and accounting stages (A2–A3). Vulnerable points include modifying issuance limits or editing transaction records in the database. Such actions may result from external attacks or internal interference. To minimise risks, it is recommended to use cryptographic hash functions or digital signatures for each transaction record, ensuring that data cannot be altered undetectably. It is also essential to implement instantaneous write-off recording at the moment of physical PPE issuance to prevent time windows for manipulation. Automatic duplication of records in a backup database ensures the preservation of transaction history in the event of an incident.

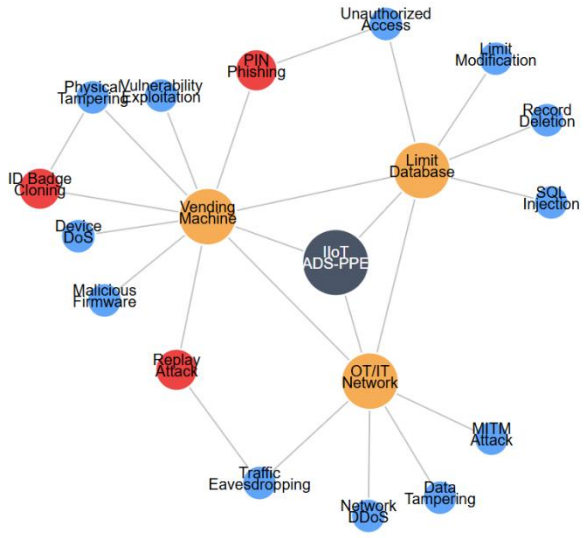


**Fig. 3.** Block diagram of the IIoT ADS-PPE threat model

Attacks on system availability and functionality (A4). In an IIoT environment, a critical aspect is ensuring continuous operation. DDoS attacks or communication failures between the device and the database can block the issuance of PPE, directly affecting employee safety. To protect against such threats, it is necessary to implement redundant communication channels, device health monitoring systems, and automatic notification procedures for the Occupational Safety Service in case of failures or overloads.

Ensuring cybersecurity of ADS-PPE is not an isolated task—it is integrated into occupational safety management as a risk control factor. Any compromise of data integrity or availability in the ADS-PPE system can potentially result in violations of safety standards, as it affects the accuracy of records and the timely provision of protective equipment to personnel. Therefore, an effective cybersecurity strategy should encompass not only technical measures (such as encryption, authentication, and audit) but also procedural aspects – monitoring, incident response, and periodic audits of IIoT device information security.

## 4. Proposed cyber security measures

The developed functional model of ADS-PPE enables the identification of critical points where implementing cybersecurity measures is essential for maintaining data integrity, confidentiality, and availability. An effective security strategy should be based on a comprehensive approach that combines technical, organisational, and procedural solutions, as reflected in the multilayered cybersecurity system (Fig. 4).

Data transmission between the vending machine, the central database, and corporate servers must be conducted using secure SSL/TLS protocols, ensuring encryption of communication channels. Special attention should be paid to encrypting user identifiers (RFID/NFC) and issuance limits, as this data contains confidential personnel information and qualifies as personal data. The use of certificates with mutual authentication prevents Man-in-the-Middle attacks and packet interception.

To prevent tampering with the PPE issuance history, it is advisable to implement digital signatures or a blockchain-based transaction ledger, which ensures that records cannot be altered or deleted without authorisation. This approach creates an immutable digital record that can serve as evidence in incident investigations. Additionally, hashing data at the time of transaction recording ensures the verification of each record upon subsequent access or transfer.

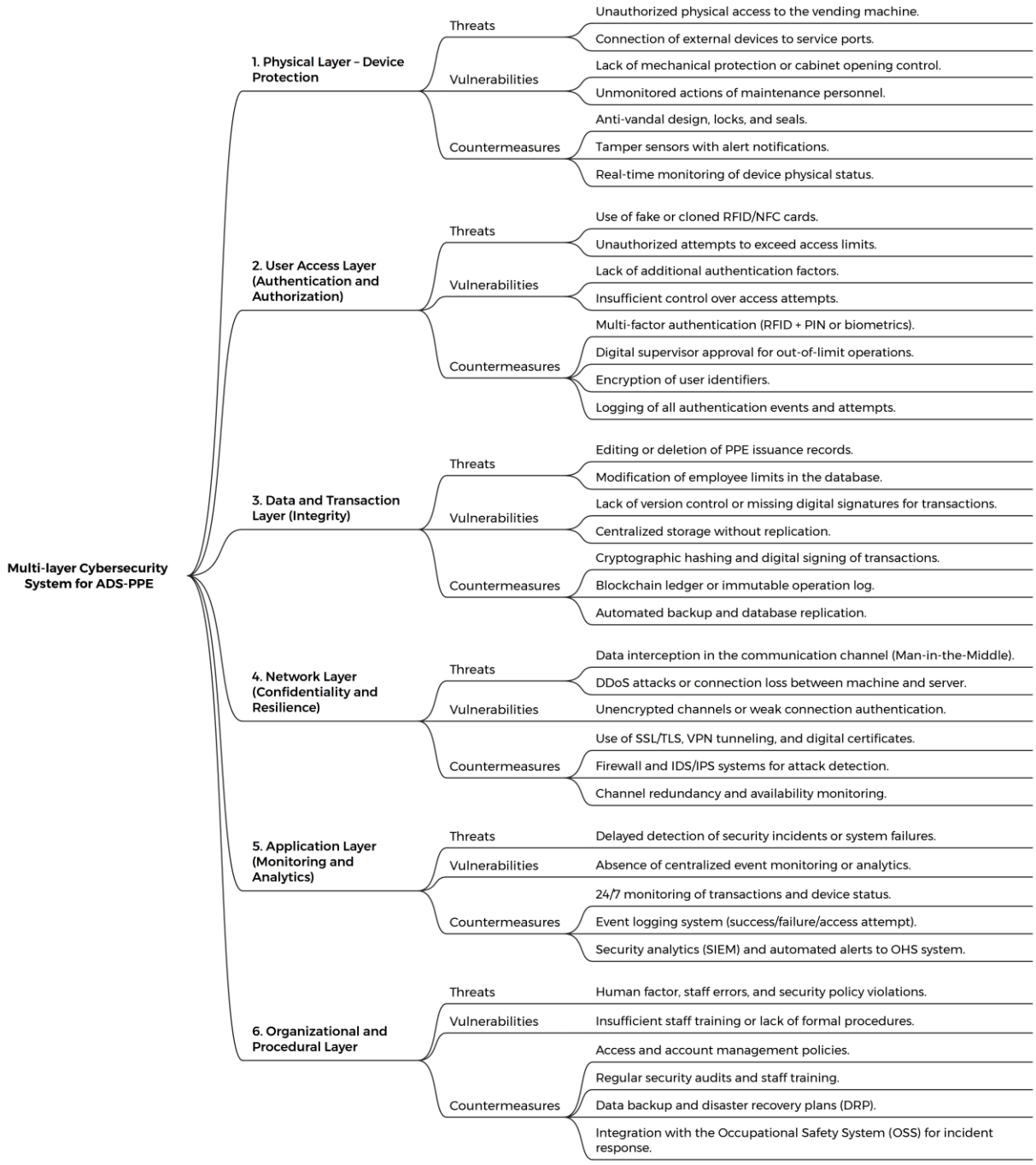


**Fig. 4.** ADS-PPE multi-layered cyber protection system

Since the issuance of PPE is directly tied to access rights, the system must support multi-level authorisation. The optimal solution combines an RFID card with an additional factor, such as a PIN code or biometric identifier. For issuance beyond established limits, a manager approval mechanism is implemented, verified via digital signature or corporate token. This architecture prevents unauthorised elevation of access rights and reduces the risk of internal abuse.

To ensure continuous security monitoring, a comprehensive event logging system must be established that captures successful transactions, failures, access attempts, and configuration changes. Log data should be transmitted to a centralised analytics system (SIEM) or, in a simplified scenario, to the Occupational Safety Service (OSS), which conducts security audits and generates discrepancy reports. Integrating audits with OSS creates synergy between cybersecurity and occupational safety management, enabling a timely response to technical or organisational breaches.

To prevent data loss during failures or attacks, a backup and replication mechanism must be implemented to ensure data integrity and continuity. Automatic duplication of critical records in a secure cloud environment or internal enterprise server guarantees recovery without losing transaction history.

Thus, the proposed measures form a multilayered cybersecurity system for ADS-PPE, covering all stages of the data lifecycle – from user identification to reporting. Their implementation not only reduces the risk of unauthorised actions but also institutionalises occupational safety as an integral part of the enterprise's digital infrastructure.

## Discussion of results

The results obtained highlight the complex interplay between technological processes, data integrity requirements, and cybersecurity challenges within IIoT-based PPE accounting systems. The proposed functional modeling of ADS-PPE using IDEF0 demonstrates that even seemingly simple operational procedures – such as employee identification and automated PPE dispensing – form a multi-layered cyber-physical workflow in which each stage can introduce vulnerabilities. The analysis shows that threats targeting employee identifiers, PPE quota parameters, and real-time transaction records are not only technical issues but also factors that directly influence financial accountability and workplace safety.

The recommended security measures confirm that ensuring data integrity in industrial environments requires more than isolated technical safeguards. Instead, a holistic, multilayered cybersecurity approach – combining cryptographic protection, secure communication protocols, and strengthened authentication – provides the most effective mitigation strategy. The discussion also underscores that IIoT devices remain the weakest link of industrial architectures, making endpoint hardening and protection against physical tampering equally important as network-level mechanisms.

Overall, the study emphasises that secure PPE accounting systems are an integral component of industrial resilience. As production environments continue to digitalise, the interdependence between cybersecurity and occupational safety grows stronger, requiring continuous adaptation of protection mechanisms. Future research directions, including the design of a dedicated cryptographic protocol and exploration of blockchain-based immutable ledgers, offer promising avenues for increasing trustworthiness and transparency in IIoT-driven accounting processes.

## Conclusions

The conducted research focused on developing a substantiated cybersecurity architecture for the Automated PPE Dispensing System (ADS-PPE) within an industrial IIoT environment. The completion of the research objectives led to the following scientifically grounded conclusions:

Based on the IDEF0 methodology, a complete functional model of the ADS-PPE system (A-0 and detailed blocks) was developed, which clearly reflects both the technological logic and the cybernetic interdependencies among all system components.

The analysis identified the employee ID card and PPE issuance limits as critical accounting elements. It was demonstrated that unauthorised manipulation of these data poses a direct threat to both financial logistics and occupational safety within the enterprise.

Potential cybersecurity threats were analysed. Threats specific to IIoT architectures, particularly at the identification and authorisation stage (A1) and the instant transaction recording stage (A2), were systematised. It was found that endpoint vulnerability to physical tampering and compromise of ID cards constitutes a key risk.

Comprehensive cybersecurity measures were proposed. Based on threat analysis, a concept of a multilayered cybersecurity system for ADS-PPE was developed and substantiated.

To ensure the integrity of transaction data, the use of cryptographic hash functions or a blockchain-based ledger was recommended, guaranteeing the impossibility of undetected record modification.

To counter unauthorised access, a requirement for multi-factor authentication (RFID + PIN/biometric) was implemented.

To ensure confidentiality and prevent data interception in networks, the use of secure SSL/TLS protocols was recommended.

Reliable protection of IIoT-based PPE accounting systems is a fundamental prerequisite for ensuring data integrity, uninterrupted production processes, and minimising risks to personnel and equipment.

Prospects for further research include the development and verification of a specific cryptographic protocol for data protection between the endpoint vending device and the central database, as well as the study of integrating distributed blockchain ledgers to create a fully immutable and authenticated transaction log.

Thus, the key conclusion is that in the context of digitalised production, occupational safety is inseparably linked to cybersecurity. Reliable protection of IIoT-based PPE accounting systems is a fundamental condition for ensuring the integrity of critical data, continuity of production processes, and minimisation of risks to personnel.

REFERENCES

1. Krainiuk, O.V., Buts, Y.V., Bogatov, O.I., Lotsman, P.I. and Barbashin, V.V. (2022), "Management of personal protective equipment using vending machines", *The 9th International scientific and practical conference "Study of world opinion regarding the development of science"* Prague, Czech Republic. International Science Group, pp. 672–678, doi: 10.46299/ISG.2022.2.9, URL: https://isg-konf.com/study-of-world-opinion-regarding-the-development-of-science/
2. Krainiuk, O., Buts, Y., Kagramanian, A., Barbashyn, V. and Yatsiuk, M. (2025), "AI-Based Solutions for the Safe Transport of Dangerous Goods in the Context of Ukraine's European Integration", *Intelligent Transport Systems: Ecology, Safety, Quality, Comfort. ITSESQC* 2024. Lecture Notes in Networks and Systems, vol 1335. Springer, Cham., pp. 236–247, doi: https://doi.org/10.1007/978-3-031-87376-8_21

3. Krainiuk, O., Buts, Y., Barbashyn, V., Kozodoi, D. and Kozodoi, O. (2024), "Intelektualni systemy upravlinnia bezpekoiu pratsi na osnovi shtuchnoho intelektu: perspektyvy intehratsii v ukrainske zakonodavstva", *Municipal Economy of Cities*, vol. 6(187), pp. 242–251, doi: https://doi.org/10.33042/2522-1809-2024-6-187-242-251
4. Wiek, A., Withycombe, L. and Redman, C. (2011), "Key competencies in sustainability: a reference framework for academic program development", *Sustainability Science*, vol. 6, pp. 203–218, doi: https://doi.org/10.1007/s11625-011-0132-6
5. Fröhlich-Wyder, M., Arias-Roth, E. and Jakob, E. (2019), "Cheese yeasts", *Yeast*, vol. 36, pp. 129–141, doi: https://doi.org/10.1002/yea.3368
6. Grigorescu, S., Trasnea, B., Cocias, T. and Macesanu, G. (2019), "A survey of deep learning techniques for autonomous driving", *Journal of Field Robotics*, vol. 37, pp. 362–386, doi: https://doi.org/10.1002/rob.21918
7. Phade, G., Tribhuvan, A., Vaidya, O. and Gandhe, S. (2021), "Design and Development of Smart Personal Protective Equipment Vending Machine using Internet of Thing", *International Conference on Emerging Smart Computing and Informatics (ESCI)*, pp. 252–257, doi: https://doi.org/10.1109/esci50559.2021.9396775
8. Sánchez, S., Lecumberri, F., Sati, V., Arora, A., Shoeibi, N., Rodríguez, S. and Corchado, J. (2020), "Edge Computing Driven Smart Personal Protective System Deployed on NVIDIA Jetson and Integrated with ROS", *PAAMS 2020. Communications in Computer and Information Science*, vol 1233. Springer, Cham., pp. 385–393, doi: https://doi.org/10.1007/978-3-030-51999-5_32
9. Gallo, G., Rienzo, F., Garzelli, F., Ducange, P. and Vallati, C. (2022), "A Smart System for Personal Protective Equipment Detection in Industrial Environments Based on Deep Learning at the Edge", *IEEE Access*, vol. 10, pp. 110862–110878, doi: https://doi.org/10.1109/access.2022.3215148
10. Mirani, A., Velasco-Hernández, G., Awasthi, A. and Walsh, J. (2022), "Key Challenges and Emerging Technologies in Industrial IoT Architectures: A Review", *Sensors (Basel, Switzerland)*, vol. 22, doi: https://doi.org/10.3390/s22155836
11. Zacharski, A., Samborski, T., Zbrowski, A., Kozioł, S., Mrozek, M. and De Hallenburg, M. (2023), "Disposable personal protective equipment vending machine", *Technologia i Automatyzacja Montażu*, doi: https://doi.org/10.7862/tiam.2023.2.4
12. Muzelak, M. and Skovranek, T. (2022), "Edge computing implementation of safety monitoring system in frame of IIoT", *23rd International Carpathian Control Conference (ICCC),* pp. 125–129, doi: https://doi.org/10.1109/iccc54292.2022.9805918
13. Wu, H., Tian, H., Nie, G. and Zhao, P. (2020), "Wireless Powered Mobile Edge Computing for Industrial Internet of Things Systems", *IEEE Access*, vol. 8, pp. 101539–101549, doi: https://doi.org/10.1109/access.2020.2995649
14. Oñate, W. and Sanz, R. (2023), "Analysis of architectures implemented for IIoT", *Heliyon*, vol. 9, doi: https://doi.org/10.1016/j.heliyon.2023.e12868
15. Kelm, A., Laussat, L., Meins-Becker, A., Platz, D., Khazaee, M., Costin, A., Helmus, M. and Teizer, J. (2013), "Mobile passive Radio Frequency Identification (RFID) portal for automated and rapid control of Personal Protective Equipment (PPE) on construction sites", *Automation in Construction*, vol. 36, pp. 38–52, doi: https://doi.org/10.1016/j.autcon.2013.08.009
16. Moraes, V., De Albuquerque Soares, W., Vasconcelos, B., Zlatar, T. and Barkokébas, B. (2020), "Automated Control on Wearing Personal Protective Equipment", *Revista de Engenharia e Pesquisa Aplicada*, vol. 5, n. 3, pp. 94–101, doi: https://doi.org/10.25286/repa.v5i3.1184
17. Wang, X., Garg, S., Lin, H., Jalil Piran, Md., Hu, J. and Hossain, S. (2021), "Enabling Secure Authentication in Industrial IoT With Transfer Learning Empowered Blockchain", *IEEE Transactions on Industrial Informatics*, vol. 17, pp. 7725–7733, doi: https://doi.org/10.1109/tii.2021.3049405
18. Asaithambi, S., Ravi, L., Devarajan, M., Selvalakshmi, A., Almaktoom, A., Almazyad, A., Xiong, G. and Mohamed, A. (2024), "Blockchain-Assisted Hierarchical Attribute-Based Encryption Scheme for Secure Information Sharing in Industrial Internet of Things", *IEEE Access*, vol. 12, pp. 12586–12601, doi: https://doi.org/10.1109/access.2024.3354846
19. Hu, J., Sun, D., Lu, W., Dong, J. and Wu, H. (2025), "Blockchain-Enabled Distributed Authentication Mechanism for Industrial Device Access", *IEEE Transactions on Industrial Informatics*, vol. 21, pp. 2819–2828, doi: https://doi.org/10.1109/tii.2024.3507201
20. Khalid, U., Asim, M., Baker, T., Hung, P., Tariq, M. and Rafferty, L. (2020), "A decentralized lightweight blockchain-based authentication mechanism for IoT systems", *Cluster Computing*, vol. 23, pp. 2067–2087, doi: https://doi.org/10.1007/s10586-020-03058-6
21. Rathee, G., Ahmad, F., Jaglan, N. and Konstantinou, C. (2022), "A Secure and Trusted Mechanism for Industrial IoT Network Using Blockchain", *IEEE Transactions on Industrial Informatics*, vol. 19, pp. 1894–1902, doi: https://doi.org/10.1109/tii.2022.3182121
22. Yang, Y., Lee, S., Wang, J., Yang, C., Huang, Y. and Hou, T. (2023), "Lightweight Authentication Mechanism for Industrial IoT Environment Combining Elliptic Curve Cryptography and Trusted Token", *Sensors (Basel, Switzerland)*, vol. 23, doi: https://doi.org/10.3390/s23104970
23. Lupascu, C., Lupascu, A. and Bica, I. (2020), "DLT Based Authentication Framework for Industrial IoT Devices", *Sensors (Basel, Switzerland)*, vol. 20, doi: https://doi.org/10.3390/s20092621
24. Arana-Landín, G., Laskurain-Iturbe, I., Iturrate, M. and Landeta-Manzano, B. (2023), "Assessing the influence of industry 4.0 technologies on occupational health and safety", *Heliyon*, vol. 9, doi: https://doi.org/10.1016/j.heliyon.2023.e13720
25. Tsiknas, K., Taketzis, D., Demertzis, K. and Skianis, C. (2021), "Cyber Threats to Industrial IoT: A Survey on Attacks and Countermeasures", *IoT*, vol. 201, doi: https://doi.org/10.3390/iot2010009
26. Cindrić, I., Jurčević, M. and Hadjina, T. (2025), "Mapping of Industrial IoT to IEC 62443 Standards", *Sensors (Basel, Switzerland)*, vol. 25, doi: https://doi.org/10.3390/s25030728
27. Axon, L., Fletcher, K., Scott, A., Stolz, M., Hannigan, R., Kaafarani, A., Goldsmith, M. and Creese, S. (2022), "Emerging Cybersecurity Capability Gaps in the Industrial Internet of Things: Overview and Research Agenda", *Digital Threats: Research and Practice*, vol. 3, pp. 1–27, doi: https://doi.org/10.1145/3503920
28. Dhirani, L., Armstrong, E. and Newe, T. (2021), "Industrial IoT, Cyber Threats, and Standards Landscape: Evaluation and Roadmap", *Sensors (Basel, Switzerland)*, vol. 21, doi: https://doi.org/10.3390/s21113901
29. Tariq, U., Aseeri, A., Alkatheiri, M. and Yu, Z. (2020), "Context-Aware Autonomous Security Assertion for Industrial IoT", *IEEE Access*, vol. 8, pp. 191785–191794, doi: https://doi.org/10.1109/access.2020.3032436


Received (Надійшла) 13.11.2025
Accepted for publication (Прийнята до друку) 25.11.2025

ВІДОМОСТІ ПРО АВТОРІВ/ ABOUT THE AUTHORS

**Крайнюк Олена Володимирівна** – кандидат технічних наук, доцент, Харківський національний автомобільно-дорожній університет, Харків, Україна;
**Olena Krainiuk** – PhD, Associate Professor, Kharkiv national automobile and highway university, Kharkiv, Ukraine;
e-mail: olenakrainiuk@khadi.kharkov.ua; ORCID Author ID: https://orcid.org/0000-0001-9524-040X;
Scopus ID: https://www.scopus.com/authid/detail.uri?authorId=59134516300.

**Євсеєв Сергій Петрович** – доктор технічних наук, професор, завідувач кафедри кібербезпеки, Національний технічний університет "Харківський політехнічний інститут", Харків, Україна;
**Serhii Yevseiev** – Doctor of Technical Sciences, Professor, Head of Cyber Security Department, National Technical University "Kharkiv polytechnic institute", Kharkiv, Ukraine;
e-mail: Serhii.Yevseiev@gmail.com; ORCID Author ID: https://orcid.org/0000-0003-1647-6444;
Scopus ID: https://www.scopus.com/authid/detail.uri?authorId=57190440690.

**Рзаєв Хазаїл Нураддін огли -** доктор технічних наук, професор, кафедра комп'ютерних технологій, Азербайджанський технічний університет, Баку, Азербайджанська Республіка;
**Khazail Rzayev** - Doctor of technical sciences, Professor, Department of Computer Technology, Azerbaijan Technical University, Baku, Azerbaijan;
e-mail: xezail.rzayev@aztu.edu.az; ORCID Author ID: https://orcid.org/0000-0001-9272-4302;
Scopus ID: https://www.scopus.com/authid/detail.uri?authorId=57204042636.

**Гасанова Шаяста Фархад кизи** – старший викладач, кафедра комп'ютерних технологій, Азербайджанський технічний університет, Баку, Азербайджанська Республіка;
**Shayasta Hasanova** - Head teacher at the Department of "Computer Technologies", Azerbaijan Technical University, Baku, Azerbaijan;
e-mail: xezail.rzayev@aztu.edu.az; ORCID Author ID: https://orcid.org/0009-0003-4801-2270.

## КІБЕРБЕЗПЕКА ОБЛІКУ ЗІЗ: МОДЕЛЮВАННЯ ЗАГРОЗ ЦІЛІСНОСТІ ДАНИХ У IIOT-СИСТЕМАХ

О.В. Крайнюк, С.П. Євсеєв, Х.Н. Рзаєв, Ш.Ф. Гасанова

**Анотація. Актуальність.** Цифровізація виробництва вимагає інтеграції охорони праці з кібербезпекою. Автоматизовані системи видачі ЗІЗ (CAB-ЗІЗ, ADS-PPE) обробляють чутливі облікові дані IIoT і є вразливими до фізичного втручання, атак у мережі та клонування ID-проходів. Традиційні методи обліку супроводжуються ризиком помилок, фінансових втрат та загроз для безпеки персоналу. Захист цілісності транзакційних даних є ключовим для забезпечення безперервності виробництва та безпеки працівників. **Предмет дослідження** – методи забезпечення цілісності та конфіденційності даних у IIoT-системі CAB-ЗІЗ на етапах аутентифікації користувача та фіксації транзакцій із врахуванням специфічних вразливостей промислових торгових автоматів. **Мета статті** – зменшення кіберризиків шляхом обґрунтування безпечної архітектури CAB-ЗІЗ та визначення критичних точок, що потребують посиленої кіберзахисту для забезпечення цілісності та конфіденційності облікових даних. **Результати.** Розроблено функціональну модель IDEF0 системи CAB-ЗІЗ. Виявлено критичні елементи: вразливість пристроїв та можливість компрометації ID-проходів як ключові загрози. Запропоновано багаторівневий підхід до кібербезпеки, включно з використанням криптографічних хеш-функцій або блокчейну для забезпечення цілісності даних та багатофакторної аутентифікації (RFID + PIN/біометрія) із застосуванням SSL/TLS для безпечного доступу. **Висновок.** Надійний захист IIoT-систем обліку ЗІЗ є необхідною умовою для автентичності даних, безперервності виробництва та безпеки персоналу. У контексті цифровізації виробництва охорона праці тісно пов'язана з кібербезпекою.

**Ключові слова:** промисловий Інтернет Речей (IIoT), кібербезпека, вендинговий автомат, цілісність даних, багатофакторна аутентифікація, облік ЗІЗ.