IRSTI 81.93.29
https://doi.org/10.56132/2791-3368-2026-2-66-113-123

G.S. Beketova, N.A. Mukhametbay, K.F. Kharlinsky
Satbayev University, Almaty, Kazakhstan
E-mail: nartaimuhametbai@gmail.com

PROBLEMS OF IMPLEMENTING INFORMATION SECURITY REQUIREMENTS IN INDUSTRIAL CONTROL SYSTEMS

Abstract. This article examines the key challenges associated with implementing information security requirements in industrial control systems. Based on the analysis of scientific publications, international standards, and industry analytical reports, as well as on the author's own analysis and practical experience, the limitations of directly transferring information security requirements developed for corporate information systems to the industrial environment are identified. It is shown that the architectural and operational characteristics of ICS, the priority of availability and continuity of technological processes, and the long life cycle of industrial equipment necessitate the adaptation of information security requirements. The role of an information security management system is substantiated as a tool for risk-oriented adaptation of security requirements and for the implementation of compensating security measures in industrial systems.

Keywords: industrial control systems (ICS), information security, OT cybersecurity, risk-based approach, information security management system, critical infrastructure protection, defense-related infrastructure, national security.

Introduction.

Industrial control systems (ICS) are designed to monitor and control industrial processes in real time with the involvement of an operator. An ICS comprises hardware and software components that provide data acquisition, processing, and transmission, as well as control of actuators at all stages of the technological process. Industrial control systems form the basis for the operation of industrial enterprises and critical infrastructure facilities. Unlike corporate information systems, ICS manage physical processes in real time and are characterized by strict requirements for availability and operational resilience. The relevance of this issue is especially important for critical and defense-related infrastructure. Industrial control systems are used not only in traditional industrial enterprises, but also in facilities that support energy supply, water treatment, fuel storage and distribution, transport infrastructure, and communication systems. Disruption of such technological processes may affect the continuity of essential services, the operational readiness of defense facilities, and the resilience of national security infrastructure. Therefore, the protection of ICS should be

considered not only as a technical information security task, but also as an important element of critical infrastructure protection and national security.

Disruption of ICS operation as a result of information security incidents can lead not only to economic losses, but also to equipment damage, production downtime, and the occurrence of industrial accidents. According to an analytical report by the Expert and Analytical Center InfoWatch, a steady increase in the number of cyber incidents in the ICS segment was recorded in 2022-2024, with a significant proportion of incidents involving violations of the availability of technological processes [1]. International analytical reports also confirm changes in the threat landscape in industrial environments. In particular, reports by Verizon and IBM indicate an increase in attacks related to credential compromise, remote access abuse, and exploitation of network vulnerabilities, which poses a serious threat to industrial control systems [2], [3].

Despite the development of regulatory and methodological documents in the field of information security, the implementation of relevant security requirements in ICS remains a challenging task. A substantial portion of these requirements was developed with the specifics of corporate IT systems in mind and does not fully take into account the architectural and operational characteristics of industrial control systems, as confirmed by both scientific publications and the provisions of international standards [4].

The purpose of this article is to analyze the key challenges associated with implementing information security requirements in industrial control systems and to substantiate the need for their adaptation within the framework of an information security management system.

The scientific novelty of this study is as follows. The paper proposes and validates a risk-oriented approach to adapting information security requirements in ICS, taking into account the operational and technological constraints of industrial control systems. Unlike traditional approaches that assume a formal transfer of information security requirements from corporate IT systems to industrial environments, the proposed model focuses on assessing the acceptability of security measures based on their impact on the availability and resilience of technological processes. The novelty of the approach lies in the formalization of a procedure for the justified deviation from certain information security requirements, followed by the implementation of compensating security measures within the information security management system.

Materials and Methods.

Specific Features of Industrial Control Systems as an Object of Information Security.

Industrial control systems represent hierarchical distributed systems that include programmable logic controllers, SCADA systems, control servers, and industrial data communication networks. Their key characteristic is the control of physical processes in real time and continuous 24/7 operation, which precludes the

possibility of prolonged downtime and experimental changes to security configurations [5].

In accordance with the recommendations of the NIST SP 800-82 standard, the primary security objectives for industrial systems are the availability and integrity of technological process control, whereas information confidentiality, unlike in corporate IT systems, plays a secondary role. A similar approach is reflected in the IEC 62443 series of standards, which define security requirements for industrial communication networks and systems [6].

Another important feature of industrial control systems is the long life cycle of hardware and software components. In practice, this leads to the operation of legacy operating systems and application software, the updating of which is often impossible without the risk of disrupting the technological process. This issue has been repeatedly highlighted in scientific studies and industry analytical reports [7].

As a result, known vulnerabilities persist in industrial control systems, and their mitigation requires the use of compensating security measures and a risk-oriented approach to the implementation of information security requirements.

Key Problems of Implementing Information Security Requirements in Industrial Control Systems.

Limitations of Software Updates and Vulnerability Management.

In corporate information systems, regular software updates are considered a fundamental requirement of information security. However, in industrial control systems, the installation of updates without prior testing may lead to component incompatibility, failures in controller operation, and loss of control over the technological process. According to industry reports by Dragos and Kaspersky ICS CERT, a significant proportion of incidents in industrial environments are associated with the exploitation of known but unremediated vulnerabilities, the patching of which was postponed for technological reasons [8]. Under conditions where timely vulnerability remediation is not feasible, organizations are forced to compensate for emerging risks through architectural and organizational security measures, including network segmentation, isolation of the technological perimeter, and control of remote access.

Challenges of Deploying Antivirus Protection.

Formal information security requirements typically mandate the use of antivirus solutions. However, the deployment of generic antivirus software in industrial control systems is associated with a high risk of disrupting technological processes.

Automatic file deletion, process blocking, or forced system reboots may result in the interruption of control over technological objects, which is unacceptable in continuous production environments. These risks are examined in detail in analytical materials published by Kaspersky ICS CERT and Positive Technologies [9]. Therefore, both scientific and practical studies emphasize the need to apply specialized security solutions designed for industrial environments, as well as to abandon automatic response modes in favor of controlled and well-documented procedures [10].

Insufficient Segmentation and IT/OT Convergence.

One of the most common causes of incidents in industrial control systems is insufficient segmentation between corporate and technological networks. According to analytical reports by InfoWatch and IBM, a significant number of attacks propagate from the corporate segment into the industrial environment through improperly configured network connections and remote access channels.

The convergence of IT and OT networks without adherence to industrial cybersecurity principles significantly expands the attack surface and increases the likelihood of compromising critical elements of technological control, a concern repeatedly highlighted in CISA recommendations [11].

The implementation of security requirements in industrial control systems requires not only the selection of individual technical controls, but also the correct organization of the interaction between corporate and technological network segments. In modern ICS environments, complete isolation of the technological perimeter is difficult to maintain due to the need for remote maintenance, data exchange with corporate systems, centralized monitoring, and integration with historians and engineering workstations. Therefore, one of the key compensating measures is the creation of a segmented IT/OT architecture with an industrial demilitarized zone.

Figure 1 presents a generalized architecture in which the corporate IT network, industrial DMZ, OT/ICS network, and field level are separated by firewalls and controlled communication channels. This architecture prevents direct access from the corporate network or the Internet to critical ICS components, while still allowing controlled data exchange, monitoring, and vendor maintenance through secure intermediate systems.

As shown in Figure 1, the industrial DMZ acts as an intermediate security layer between the corporate IT network and the OT/ICS network. Systems such as historians, monitoring collectors, patch servers, VPN/PAM solutions, and jump servers are placed in this zone in order to prevent direct interaction between external users and critical control components. Remote vendor access is routed through controlled access mechanisms and should be accompanied by authentication, authorization, session logging, and periodic review of active accounts.

The OT/ICS network contains the main technological control components, including SCADA servers, HMI/operator workstations, engineering workstations, control servers, industrial switches, and PLC/RTU controllers. These components interact with sensors, actuators, motors, pumps, valves, and the physical process at the field level. Direct access from the corporate network to PLCs or field devices must be blocked, while monitoring sensors should collect logs and security events for further analysis. Such segmentation reduces the attack surface and supports the risk-oriented adaptation of information security requirements without disrupting the continuity of technological processes.

Growth of Vulnerabilities and Changes in Attack Vectors.

An analysis of recent industry reports indicates a shift in attack vectors targeting industrial control systems. Whereas infected removable media previously represented the primary source of threats, recent years have seen a predominance of attacks conducted via remote access, credential compromise, and the exploitation of network vulnerabilities. Particular concern is associated with unmanaged and agentless devices, including programmable logic controllers and field devices, for which the deployment of traditional incident detection mechanisms is limited or impractical.

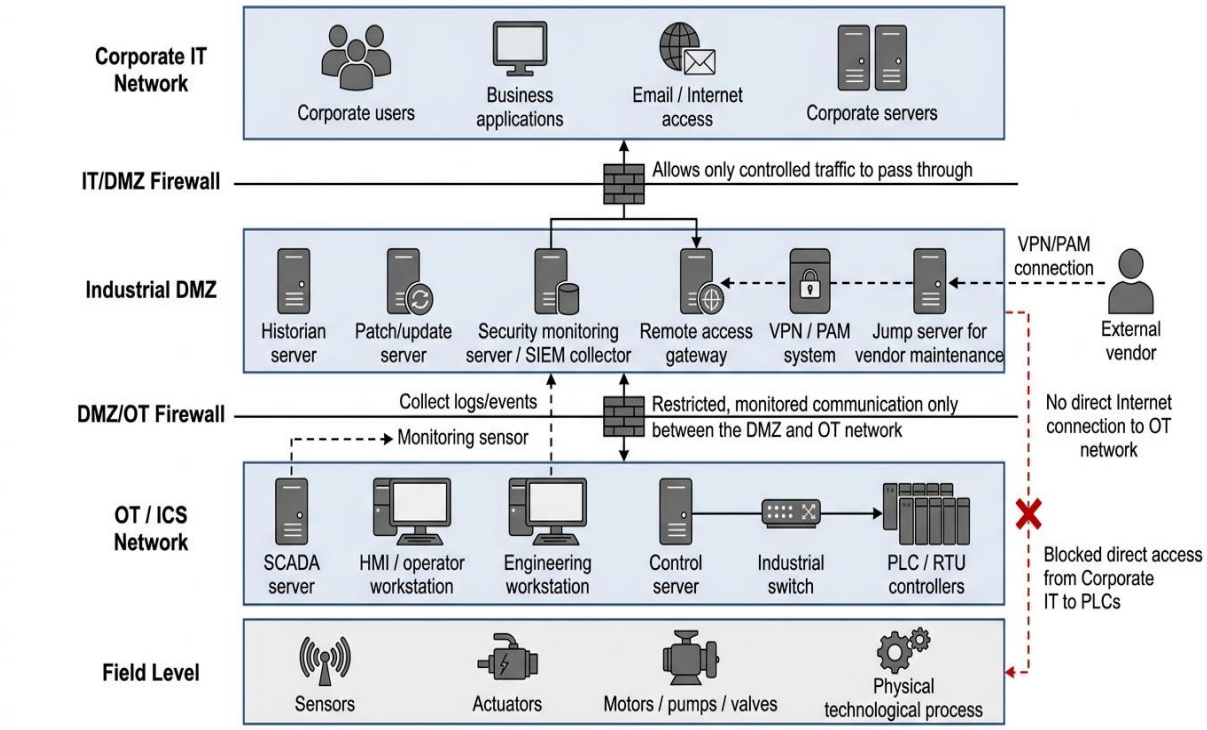

Figure 1 – IT/OT architecture with industrial DMZ and controlled remote access

Human Factor and Organizational Constraints.

The human factor has a significant impact on the level of information security in industrial control systems. According to analytical studies by Verizon and JetInfo, up to 25–30% of incidents in industrial environments are associated with personnel errors, insufficient staff qualification, and violations of established operational procedures [12].

Under these conditions, systematic personnel training, regular knowledge assessment, and the development of an information security culture within a unified management framework become critically important.

Systemic and Organizational Causes of Ineffective Implementation of Information Security Requirements.

An analysis of contemporary practice-oriented sources shows that the key problems in implementing information security requirements in industrial control systems are associated with the mechanical transfer of IT-centric approaches into industrial environments without consideration of operational constraints. The use

of generic security solutions, including antivirus software, active network scanning, and strict authentication mechanisms, may lead to control delays, SCADA system failures, and disruptions to the continuity of technological processes.

The underlying causes of vulnerabilities in industrial control systems are systemic in nature and stem from the multi-level architecture of industrial systems, the long life cycle of equipment, and integration with corporate networks. Formal models of an “isolated technological perimeter” do not reflect actual operating conditions and result in underestimated risk assessments. Organizational factors also play a significant role in the occurrence of incidents, particularly insufficient interaction between information security teams and operational personnel. Decision-making without due consideration of technological requirements reduces the effectiveness of security measures and increases the likelihood of procedural violations. Under these conditions, effective information security for industrial control systems can only be achieved within a risk-oriented information security management system that enables the adaptation of security requirements, the justification of deviations from formal norms, and the implementation of compensating measures without compromising the stability of technological processes.

Adaptation of Information Security Requirements within an Information Security Management System.

The analysis conducted demonstrates that the identified problems are systemic in nature and cannot be resolved solely through the deployment of individual technical security controls. Effective information security for industrial control systems is achieved within the framework of an information security management system adapted to the conditions of industrial operation.

An information security management system enables the implementation of a risk-oriented approach, in which the acceptability of specific security measures is determined by their potential impact on the technological process. When the implementation of certain formal security requirements is not feasible, a documented risk assessment is performed and compensating security measures are introduced, including network segmentation, isolation of demilitarized zones, control of remote access, and monitoring of security events.

At the same time, the practical implementation of information security requirements in industrial control systems requires consideration of technological constraints, as well as the prioritization of availability and continuity of production processes. In this regard, the present study proposes and validates a model for adapting information security requirements in industrial control systems based on a risk-oriented approach and the principles of an information security management system.

The proposed risk-oriented model for adapting information security requirements in industrial control systems is presented in Figure 2.

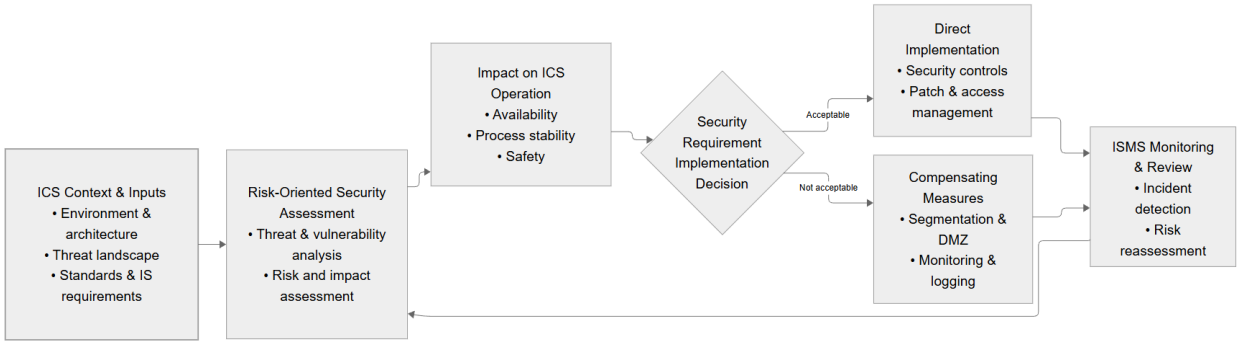

Figure 2 - Risk-oriented model for adapting information security requirements in industrial control systems

Validation of the Model for Adapting Information Security Requirements in Industrial Control Systems.

The validation of the proposed model for adapting information security requirements was conducted based on the results of an information security audit and a pilot project involving the deployment of monitoring and protection tools in the ICS networks of an industrial energy facility. The study examined technological segments of the industrial control system, including servers, operator workstations, engineering stations, network equipment, and data communication channels.

During the information security audit, relevant threats and vulnerabilities characteristic of industrial control systems were identified. It was determined that the most significant risks to ICS are associated with outdated software, the absence of centralized backup mechanisms, the use of unsupported antivirus solutions, the presence of unauthorized network interactions, and the potential for man-in-the-middle attacks (ARP spoofing). The application of the proposed model made it possible to assess the acceptability of implementing security measures with regard to their impact on the availability and resilience of the technological process. In cases where the direct implementation of information security requirements (for example, the deployment of traditional antivirus solutions or software updates) could have disrupted ICS operation, decisions were made to implement compensating measures, including network segmentation, enhanced monitoring, control of network interactions, and security event logging.

As part of the pilot project, a significant number of security events were recorded within the technological network, including events with a high level of criticality. The analysis of network traffic and system logs made it possible to identify previously non-obvious threats, including interactions with external networks under a formally isolated ICS architecture, as well as misconfigurations of individual nodes.

The results obtained confirm the practical applicability of the proposed model for adapting information security requirements and demonstrate the feasibility of using a risk-oriented approach to protect industrial control systems.

Results and Discussion.

As a result of the conducted study and the validation of the proposed approach, the following key results were obtained.

First, it was established that the direct implementation of formal information security requirements developed for corporate IT systems into the industrial ICS environment, without taking technological constraints into account, may lead to reduced control resilience and an increased risk of disrupting the continuity of technological processes.

Second, a model for adapting information security requirements in industrial control systems was developed and validated. The model is based on a risk-oriented assessment of the acceptability of security measures and the application of compensating measures in cases where the implementation of specific requirements is not feasible.

Third, within the pilot project, it was demonstrated that even under a formally isolated technological network architecture, information security events are recorded in industrial control systems, indicating the presence of hidden network interactions and underestimated attack vectors. This result confirms the inadequacy of assumptions regarding the complete isolation of the technological perimeter in the absence of continuous monitoring.

Fourth, the practical applicability of using an information security management system as a tool for aligning information security requirements with the operational characteristics of industrial control systems was confirmed. This approach enables the justification of deviations from formal security requirements and the reduction of overall risk without compromising the technological process.

Conclusion.

Within the framework of this study, the main problems of implementing information security requirements in industrial control systems were analyzed, taking into account the architectural, technological, and operational characteristics of ICS. It was established that the direct transfer of information security requirements used in corporate information systems to the industrial environment is not always acceptable, since such measures may create additional risks for the availability, resilience, and continuity of technological processes.

The main result of the work is the development and practical validation of a risk-oriented model for adapting information security requirements in ICS. The proposed model makes it possible to assess security measures not only from the standpoint of formal compliance with requirements, but also with regard to their possible impact on the technological process. In cases where the direct implementation of certain requirements may disrupt the operation of an industrial system, the model provides for justified deviation from formal norms and the application of compensating security measures, including network segmentation, the use of an industrial DMZ, remote access control, security event monitoring, and logging of critical actions.

The practical validation of the model based on audit materials and a pilot project confirmed its applicability in real industrial conditions. The obtained results revealed hidden network interactions, configuration errors, outdated software, and other underestimated attack vectors, which confirms the need for continuous monitoring and regular risk assessment.

Thus, the proposed approach makes it possible to adapt information security requirements to the conditions of ICS without compromising the reliability and continuity of technological processes. The results of the study can be used to protect industrial enterprises, critical infrastructure facilities, and defense-related systems.

REFERENCES

1. InfoWatch Expert and Analytical Center. (2024). Trends in the development of cyber incidents in industrial control systems. https://www.infowatch.ru/sites/default/files/analytics/files/tendentsii-razvitiya-kiberintsidentov-asu-tp-za-dve-tysyachi-dvadtsat-chetyvertiy-god.pdf

2. Verizon. (2024). The report on the investigation of data leaks for 2024. https://www.verizon.com/business/resources/reports/2024-dbir-data-breach-investigations-report.pdf

3. IBM. (2024). The X-Force Threat Analysis Index 2024. https://newsletter.radensa.ru/wp-content/uploads/2024/03/IBM-XForce-Threat-Intelligence-Index-2024.pdf

4. Kravchuk A. Yu., Kotova N. A., Anichkin I. I. (2022). Modern approaches to information security in industrial control systems. Innovation and Investments, № 3.

5. NIST SP 800-82. Guide to Industrial Control Systems (ICS) Security. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r2.pdf

6. IEC 62443. Industrial communication networks – Network and system security. https://www.isa.org/standards-and-publications/isa-standards/isa-iec-62443-series-of-standards

7. ARinteg. (n.d.). Information security in industrial control systems. https://arinteg.ru/solutions/zashchita-asu-tp/

8. Dragos. (n.d.). OT Cybersecurity Year in Review. https://www.dragos.com/blog/dragos-8th-annual-ot-cybersecurity-year-in-review-is-now-available

9. Kaspersky ICS CERT. (n.d.). Analytical reports on threats to industrial control systems. https://ics-cert.kaspersky.com/publications/reports/2025/09/11/threat-landscape-for-industrial-automation-systems-q2-2025/

10. Positive Technologies. (n.d.). Industrial Cybersecurity reports. https://ptsecurity.com/research/analytics/kiberugrozy-dlya-promyshlennosti-industrial-iot/#id6

11. CISA. Recommended Cybersecurity Practices for Industrial Control Systems.https://www.cisa.gov/sites/default/files/publications/Cybersecurity_Best_Practices_for_Industrial_Control_Systems_508.pdf

12. JetInfo. (n.d.). Security problems of industrial networks. https://www.jetinfo.ru/pochemu-bezopasnost-promyshlennyh-setej-na-10-let-otstaet-ot-korporativnyh-standartov/

Гүлжанат Бекетова, PhD, қауымдастырылған профессор, Satbayev University, Алматы, Қазақстан, g.beketova@satbayev.university

Нартай Мухаметбай, магистрант, Satbayev University, Алматы, Қазақстан, nartaimuhametbai@gmail.com

Владислав Харлинский, магистрант, Satbayev University, Алматы, Қазақстан, Kharlinskiy.V@stud.satbayev.university

АВТОМАТТАНДЫРЫЛҒАН ТЕХНОЛОГИЯЛЫҚ ПРОЦЕСТЕРДІ БАСҚАРУ ЖҮЙЕЛЕРІНДЕ АҚПАРАТТЫҚ ҚАУІПСІЗДІК ТАЛАПТАРЫН ЕНГІЗУ МӘСЕЛЕЛЕРІ

Аңдатпа. Бұл мақалада автоматтандырылған технологиялық процестерді басқару жүйелерінде ақпараттық қауіпсіздік талаптарын енгізуге байланысты негізгі мәселелер қарастырылады. Ғылыми жарияланымдарды, халықаралық стандарттарды және салалық аналитикалық есептерді талдау, сондай-ақ автордың жеке талдауы мен практикалық тәжірибесі негізінде корпоративтік ақпараттық жүйелер үшін әзірленген ақпараттық қауіпсіздік талаптарын өнеркәсіптік ортаға тікелей көшірудің шектеулері айқындалды. Автоматтандырылған технологиялық процестерді басқару жүйелерінде архитектуралық және пайдалану ерекшеліктері, технологиялық процестердің қолжетімділігі мен үздіксіз жұмыс істеу басымдығы, сондай-ақ өнеркәсіптік жабдықтың ұзақ өмірлік циклі ақпараттық қауіпсіздік талаптарын бейімдеуді қажет ететіні көрсетілді. Ақпараттық қауіпсіздікті басқару жүйесінің қауіптерге негізделген тәсіл арқылы қауіпсіздік талаптарын бейімдеу және өнеркәсіптік жүйелерде өтемдік қорғаныс шараларын енгізу құралы ретіндегі рөлі айқындалды.

Түйінді сөздер: өнеркәсіптік басқару жүйелері (ӨБЖ), ақпараттық қауіпсіздік, операциялық технологиялардың (ОТ) киберқауіпсіздігі, тәуекелге бағдарланған тәсіл, ақпараттық қауіпсіздікті басқару жүйесі, маңызды инфрақұрылымды қорғау, қорғаныс инфрақұрылымы, ұлттық қауіпсіздік.

Гулжанат Бекетова, PhD, ассоциированный профессор, Satbayev University, Алматы, Казахстан, g.beketova@satbayev.university

Нартай Мухаметбай, магистрант, Satbayev University, Алматы, Казахстан, nartaimuhametbai@gmail.com

Владислав Харлинский, магистрант, Satbayev University, Алматы, Қазақстан, Kharlinskiy.V@stud.satbayev.university

ПРОБЛЕМЫ ВНЕДРЕНИЯ ТРЕБОВАНИЙ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В АВТОМАТИЗИРОВАННЫХ СИСТЕМАХ УПРАВЛЕНИЯ ТЕХНОЛОГИЧЕСКИМИ ПРОЦЕССАМИ

Аннотация. В статье рассматриваются ключевые проблемы внедрения требований информационной безопасности в автоматизированных системах управления технологическими процессами. На основе анализа научных публикаций, международных стандартов и отраслевых аналитических отчетов, а также авторского анализа и практического опыта выявлены ограничения прямого переноса требований информационной безопасности, разработанных для корпоративных информационных систем, в промышленную среду. Показано, что архитектурные и эксплуатационные особенности автоматизированных систем управления технологическими процессами, приоритет доступности и непрерывности технологических процессов, а также длительный жизненный цикл промышленного оборудования обуславливают необходимость адаптации требований информационной безопасности. Обоснована роль системы управления информационной безопасностью как инструмента риск-ориентированной адаптации требований безопасности и внедрения компенсирующих мер защиты в промышленных системах.

Ключевые слова: промышленные системы управления (ПСУ), информационная безопасность, кибербезопасность операционных технологий (ОТ), риск-ориентированный подход, система менеджмента информационной безопасности, защита критической инфраструктуры, оборонная инфраструктура, национальная безопасность.

Received: June 01, 2026
Peer-reviewed: June 22, 2026
Accepted: June 22, 2026