ISSN: 2181-3906 2026

International scientific journal
«MODERN SCIENCE AND RESEARCH»
VOLUME 5 / ISSUE 4 / UIF:8.2 / MODERNSCIENCE.UZ

CYBERSECURITY ISSUES IN THE IMPLEMENTATION OF ELECTRONIC LOGBOOKS

Vakhobova Raykhona Oktamjon qizi
Master's student, Andijan State Technical Institute.
e-mail: *abdurasulovarayxona76@gmail.com*
Qobulova Nilufarkhon Jalilovna
Professor, Department of Occupational Safety,
Andijan State Technical Institute.
https://doi.org/10.5281/zenodo.19467880

Abstract. *This study is devoted to the issues of ensuring information security and cybersecurity in the process of implementing electronic logbooks. The article highlights the importance of electronic logbooks in improving management and control efficiency and systematizes the main threats associated with them. Using a risk-based approach, assets, threats, vulnerabilities, and consequences were analyzed, and the priority risk factors for electronic logbook systems were identified. The results of the study showed that reliable user authentication, strict access control, recording of change history, the establishment of backup and recovery mechanisms, and the improvement of employee awareness are among the key conditions for ensuring the security of electronic logbooks. The article also develops organizational and technical recommendations necessary for practical implementation.*

Keywords: *electronic logbook, cybersecurity, information security, risk analysis, authentication, role-based access control, audit trail, encryption, backup, incident management.*

Introduction.

The regulatory and legal framework for cybersecurity in the Republic is being developed step by step. In particular, Resolution No. PQ-381 of the President of the Republic of Uzbekistan, dated November 30, 2023, sets out measures aimed at protecting the rights of consumers of digital products and services, as well as strengthening efforts to combat offenses committed through digital technologies [1]. This document also provides a practical basis for strengthening information security and cybersecurity.

In addition, Resolution No. 3513 of the Board of the Central Bank of the Republic of Uzbekistan, dated May 21, 2024, approved regulations on ensuring information security and cybersecurity for payment system operators and payment service providers. These regulations cover requirements related to monitoring, incident detection, protection against attacks, vulnerability management, and incident response [2]. This approach may also serve as a practical model for corporate information systems such as electronic logbooks.

Electronic digital signatures play an important role in ensuring the legal validity and non-repudiation of electronic documents. The Law of the Republic of Uzbekistan No. O'RQ-793, dated October 12, 2022, regulates relations in the field of the use of electronic digital signatures [3]. Therefore, issues of authentication, system integration, and key management are closely connected with cybersecurity. Since electronic logbooks are likely to contain data related to employees, contractors, or other individuals, compliance with the Law of the Republic of Uzbekistan No. O'RQ-547 "On Personal Data," dated July 2, 2019, is also essential [4].

In this regard, special attention should be paid to the purpose of data collection, storage periods, protection methods, and conditions for data transfer.

In recent years, the trend toward the digitalization of document flow and control processes in enterprises has been intensifying. In particular, occupational safety instruction logs, maintenance logs, shift handover logs, defect registers, and quality control records are being converted into electronic form. The main advantage of electronic logbooks is that data become centralized, real-time monitoring becomes possible, evidence can be quickly presented during inspections, and errors caused by the human factor are reduced.

However, an electronic logbook is not merely a digital copy of a paper document. It is an information system connected with networks, servers, databases, user devices, identification mechanisms, and various integrations. For this reason, cybersecurity issues become a central element of its implementation. If security is not properly ensured, the loss, alteration, or leakage of data may lead to the disruption of production processes, undermine the reliability of audit results, and increase risks related to occupational safety accountability.

The relevance of this article lies in the fact that electronic logbooks are often implemented from the perspective of speed and convenience, while in practice many organizations limit themselves to “standard security” settings. Nevertheless, even basic measures such as password policies, role-based access control, audit logs, and regular backups can significantly improve the level of information security.

Methodology.

In this study, the issues of ensuring cybersecurity in the implementation of electronic logbooks were examined using a risk-based approach. Within this approach, the key assets of the information system, the threats affecting them, existing vulnerabilities, and potential consequences are analyzed in an interrelated manner. Such an approach is widely applied in international practice for the development of information security management systems and is consistent with the ISO/IEC 27001 and ISO/IEC 27002 standards. The NIST Cybersecurity Framework 2.0 also recommends a similarly systematic approach for identifying, prioritizing, and managing cyber risks within organizations.

At the first stage of the study, the boundaries and components of the electronic logbook system were defined. The system included user devices, a web application or mobile interface, an application server, a database, identification tools, network infrastructure, integration modules, as well as backup and archival environments. The electronic logbook was considered as a separate information system, and its functional structure was generalized based on practical examples such as occupational safety logbooks, maintenance logs, shift logs, and defect registers. Such boundary-setting helps to more accurately identify threats and select appropriate control measures in subsequent stages.

At the second stage, a data flow analysis of the system was conducted. This included a separate examination of data entry points, transmission channels, processing environments, storage locations, and the backup process. The STRIDE model recommended by Microsoft was used to classify threats. This model covers six major categories of threats: Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, and Elevation of Privilege, and it is widely used in the security analysis of software systems [5].

For electronic logbooks, threats related to record modification, repudiation of user actions, and data disclosure were considered particularly significant.

At the third stage, risk assessment was carried out using a 5×5 matrix. Each threat was evaluated in terms of its likelihood and impact. The impact criteria included disruption of production processes, compromised reliability of evidence for audits and inspections, legal liability risks, data recovery costs, and reputational damage. In addition to the three main principles of information security—confidentiality, integrity, and availability—the criterion of non-repudiation was also applied, since the accurate recording of user actions in electronic logbook entries is important from both legal and managerial perspectives [6]. The law on electronic digital signatures makes this requirement even more relevant in terms of ensuring the reliability and legal validity of electronic documents.

At the fourth stage, control measures were selected and prioritized in order to mitigate the identified risks. These controls were divided into several layers: identification and authentication, access management, application security, network segmentation, data protection, backup and recovery, monitoring, and incident response. This approach corresponds to the principle of defense in depth [7]. Within the framework of NIST CSF 2.0, it is likewise recommended that protection, detection, response, and recovery functions be organized in an interconnected manner.

For identification and authentication, strong password policies, multi-factor authentication (MFA)**,** single sign-on (SSO), and integration with e-IMZO were selected, while RBAC and the principle of least privilege were chosen for access control [7]. In evaluating application security, the OWASP Top 10 list was used as a checklist, including authentication failures, weak access control, injection, and security misconfiguration issues [8]. This approach is especially relevant for electronic logbooks operating through browsers or mobile applications.

In the area of data protection, it was taken into account that electronic logbooks may contain information related to employees or other individuals; therefore, personal data protection requirements were also incorporated into the methodology. Accordingly, the use of protected communication channels during data transmission, encryption during storage, restricted display of sensitive data through masking, and differentiated access rights were предусмотрены [4]. This approach strengthens not only technical security but also legal compliance.

The methodology for monitoring and incident management was developed in accordance with ISO/IEC 27035 and the NIST CSF 2.0 concept [9]. In this context, the stages of incident detection, classification, isolation, impact mitigation, service recovery, and reporting were identified as separate control points. Uzbekistan’s regulatory approach to combating digital offenses and strengthening information security also confirms the importance of monitoring and rapid response.

In practice, many security incidents occur because employees fall victim to phishing attacks, use shared accounts, disclose passwords, or violate internal procedures. Therefore, in addition to technical controls, the study also considered user awareness, short training sessions, phishing simulations, and the simplification of internal guidelines as part of the methodology [8].

At the final stage, a KPI system was proposed to evaluate the effectiveness of the implemented measures.

It included MFA coverage, the number of discrepancies identified during access rights audits, the time required to remediate critical vulnerabilities, the success rate of backup recovery, the number of anomalous events identified in audit logs, and the results of phishing tests. NIST CSF 2.0 also recommends the use of management indicators to measure and improve cybersecurity performance within organizations.

Results.

The study identified six priority risk groups associated with the implementation of electronic logbooks: unauthorized access, alteration or deletion of records, disruption of system availability, leakage of personal and service data, vulnerabilities in integration channels, and abuse by internal employees. These risks are consistent with international application security and information security practices; in particular, similar risk categories are explicitly highlighted in the OWASP Top 10 and ISO/IEC 27002 controls.

According to the results of risk prioritization, integrity and non-repudiation were found to be the most critical criteria for electronic logbooks. This is because records in such systems are often used as evidence for internal audits, occupational safety inspections, technical control, or internal investigations. If it is not reliably recorded when a record was created or modified and by whom, the practical and legal value of the logbook decreases [6].

The law on electronic digital signatures also emphasizes the importance of identification and signing mechanisms in ensuring the reliability of electronic documents [3].

According to the practical results, the implementation of MFA ranked among the most effective measures for reducing the risk of unauthorized access. It was noted that the traditional login-and-password model does not provide sufficient protection, especially for web applications, and that unauthorized access becomes easier if user credentials are obtained through phishing or malware. Therefore, multi-factor authentication, particularly for administrators and highly privileged users, was assessed as a protection measure that should be implemented as a priority [10]. The results regarding RBAC (Role-Based Access Control) and the principle of least privilege showed that granting users permissions beyond their functional duties increases internal threats. In electronic logbooks, if roles such as operator, controller, department head, auditor, and administrator are assigned separate and limited privileges, the likelihood of incorrect modification, mass deletion, or unauthorized viewing of records is reduced [7]. For this reason, regular audits of roles and access rights were also identified as an important practical recommendation.

As the most important practical solution for ensuring integrity, the preservation of non-erasable audit trails was recommended. The results showed that the effectiveness of audit logging increases when it is organized in three layers: recording changes through database triggers, storing old and new values in a separate audit table, and forwarding logs to a centralized server or SIEM system [9]. This approach makes it possible to reconstruct user actions later, present the history of changes during inspections, and reduce the likelihood of falsification.

The results concerning data confidentiality showed that electronic logbooks often contain personal data or internal service information. Therefore, the use of protected transmission channels, encryption during storage, masking of certain fields, and differentiated data display based on user roles were selected as the most appropriate measures. This is particularly important for compliance with the requirements of Uzbekistan’s law on personal data [4].

The findings related to system availability showed that for electronic logbooks, creating backup copies alone is not sufficient; it is also necessary to test recovery procedures. For this reason, a backup model close to the 3-2-1 principle, weekly or monthly recovery testing, and at least one offline or immutable copy were recommended. This approach significantly increases the possibility of data recovery, especially in cases of ransomware attacks or server failures.

The results on network security indicated that segmentation and protected administrative access are of particular importance.

Measures such as separating electronic logbook servers from the ordinary office network segment, restricting administrator access exclusively through VPN, and routing logs through a separate protected channel reduce the spread of attacks across the internal network [10]. This result is especially relevant in integrated corporate environments.

The results on application security, in line with OWASP recommendations, showed that protection measures against authentication failures, weak access control, injection, XSS/CSRF, and misconfiguration should be considered mandatory. Since electronic logbook systems are often web-based, validation of user input fields, session management, and API protection directly affect the overall security of the system [8].

Integration security was also identified as one of the key findings. Connection points with ERP, 1C, Active Directory, e-IMZO, and other modules may often become hidden sources of vulnerability. Therefore, it was recommended to use service accounts with limited privileges, store API keys in protected environments, log integration requests, and minimize excessive data exchange [3].

The results also showed that the internal employee factor is a serious source of risk.

The use of shared accounts, insufficient control over administrator activity, and the improper distribution of roles and privileges may lead to intentional or unintentional corruption of records. Therefore, separate logging of administrator activity, two-step approval, segregation of duties, and regular internal audits were identified as effective measures.

As a result of the study, the concept of a “minimum security baseline” was developed for electronic logbooks. It includes measures that should be implemented within the first 30–45 days, such as eliminating shared accounts, enforcing a strong password policy, implementing MFA and RBAC, enabling audit logs, establishing backup procedures, introducing patch management, and providing short awareness training sessions for users.

These measures do not require excessive resources, yet they have a rapid and significant impact on the security level.

To measure the effectiveness of the proposed measures, the following KPIs were recommended: MFA coverage, the number of discrepancies identified in role and access rights audits, the time required to remediate critical vulnerabilities, the success rate of backup recovery, the number of anomalous events detected in audit logs, and the proportion of user errors in phishing tests [10]. These indicators make it possible to manage the security of electronic logbooks not as a one-time project, but as a continuously improving management process.

Discussion.

The analysis conducted shows that, in the implementation of electronic logbooks, the primary focus is often placed on functional convenience, rapid reporting, and the simplification of

control procedures, while cybersecurity requirements may remain a secondary concern. However, international approaches strongly emphasize the necessity of integrating security from the very beginning of the design and implementation of information systems.

The results of the study identified integrity and non-repudiation as the most important security criteria for electronic logbooks. This can be explained by the practical role of such systems: they are not merely tools for storing information, but also serve as evidentiary sources for audits, internal investigations, occupational safety supervision, and internal management decisions. Therefore, it is essential that it be reliably recorded by whom, when, and how a record was created or modified. The law on electronic digital signatures also highlights the importance of identification and verification mechanisms in ensuring the reliability of electronic documents [3].

The current regulatory and legal framework of Uzbekistan also indirectly and directly supports the need for the secure implementation of electronic logbooks. Presidential Resolution No. PQ-381 establishes measures aimed at combating offenses committed through digital technologies and protecting consumer rights [1]. Resolution No. 3513 of the Central Bank sets out more specific requirements for monitoring, protection, vulnerability management, and the strengthening of information security regimes [2]. Although this regulation was developed for payment systems, its approaches are also applicable to internal corporate electronic logbook systems, especially in terms of monitoring, logging, incident response, and data protection.

The issue of handling personal data also occupies an important place in the discussion.

Electronic logbooks may contain employees' full names, positions, dates of instruction, disciplinary records, or other personal data related to technical service activities.

Therefore, when implementing such systems, it is necessary to take into account not only information security requirements but also the requirements for personal data protection [4]. This, in turn, requires practical measures such as strict access control, collection of data in the minimum necessary volume, definition of retention periods, and limitation of excessive visibility of sensitive information.

Overall, the findings of the study and the analysis of the literature confirm that cybersecurity in the implementation of electronic logbooks should not be viewed as a separate technical module, but rather as an integral part of management, legal compliance, and operational stability. It is precisely this approach that transforms electronic logbooks from a convenient digital tool into a reliable, legally valid, and secure management system for the enterprise.

Conclusion.

The implementation of electronic logbooks significantly optimizes management and control processes within an enterprise. However, introducing them without appropriate security measures creates new cyber risks. The results of the study showed that the most important requirements for electronic logbook systems are to ensure the integrity, non-repudiation, confidentiality, and availability of data.

A security architecture organized on the basis of a risk-based approach and the defense-in-depth principle makes it possible to use electronic logbooks in a stable and reliable manner. In particular, the combined use of measures such as MFA, RBAC, audit logs, backup procedures, segmentation, and incident management provides the greatest practical effect.

Thus, taking cybersecurity issues into account at the very initial stage of implementing electronic logbooks ensures not only the organization's information security, but also its legal compliance, audit readiness, and operational stability.

REFERENCES

1. Resolution of the President of the Republic of Uzbekistan No. PQ-381, dated November 30, 2023, "On measures to protect the rights of consumers of digital products (services) and strengthen the fight against offenses committed through digital technologies."
2. Resolution of the Board of the Central Bank of the Republic of Uzbekistan No. 3513, dated May 21, 2024, "On approval of the Regulation on ensuring information security and cybersecurity in the payment systems of payment system operators and payment service providers."
3. Law of the Republic of Uzbekistan No. O'RQ-793, dated October 12, 2022, "On Electronic Digital Signature."
4. Law of the Republic of Uzbekistan No. O'RQ-547, dated July 2, 2019, "On Personal Data."
5. Microsoft. STRIDE Threat Modeling Approach. An approach to classifying threats into Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, and Elevation of Privilege.
6. ISO/IEC 27001:2022. *Information security management systems — Requirements.*
7. ISO/IEC 27002:2022. *Information security, cybersecurity and privacy protection — Information security controls.*
8. OWASP Top 10: 2025. *Web application security risks.*
9. ISO/IEC 27035-1:2023. *Information security incident management — Principles and process.*
10. NIST Cybersecurity Framework (CSF) 2.0, 2024. *Identify–Protect–Detect–Respond–Recover approach.*