OPEN ACCESS

Global Journal of Research in Business Management
ISSN: 2583-6218 (Online)
Volume 05 | Issue 06 | Nov.-Dec. | 2025
Journal homepage: https://gjrpublication.com/gjrbm/

Research Article

Problems in Improving Safety Efficiency Based on the Numbering of Material and Technical Devices

*Izzatilla Pulatov Qudratillaevich

Independent Researcher, Department of Digital Economy, Tashkent State University of Economics.
ORCID: 0009-0007-3165-8269

DOI: 10.5281/zenodo.17735775 **Submission Date:** 30 Sept. 2025 | **Published Date:** 27 Nov. 2025

Abstract

When digitizing the system for registering tangible technical means, great attention should be paid to the integrity of software and hardware, their reliability. After all, no matter which software platform is chosen, qualified information technology specialists must constantly work to constantly update it and quickly eliminate technical problems when they arise. However, in many institutions, where there is insufficient knowledge and skills in the field of information and communication technologies, the problems in ensuring the correct functioning of the systems are increasing day by day.

Keywords: *tangible technical devices, digitization, information and communication technologies, physical devices, technological means, software platforms, information.*

Introduction

Material and technical devices form the foundation of societal progress and constitute the core basis of any organization's activity. These tools, used for various purposes in science, industry, the economy, and everyday life, have become an integral part of modern work processes. It is impossible to imagine any production, service, or management process organized effectively without mechanisms, instruments, computer equipment, communication tools, or office devices. The use of material and technical devices enables increased labor productivity, rapid and accurate results, and the implementation of modern technologies. Moreover, these devices facilitate efficient management of both material and intangible resources, ensure safety, and streamline processes of data collection, storage, and transmission. Therefore, maintaining accurate records, proper management, and continuous development of material and technical devices are among the key tasks of every organization. In the context of modern technological advancement, this field is constantly being updated and improved, and every organization strives to employ the most advanced technical tools in its operations.

Literature Review

One of the pressing issues of the digitalization process is ensuring the reliability, durability, and archiving capabilities of information. Even when physical devices and their inventories are stored using modern technological tools such as cloud technologies and servers, there remains the potential risk of data loss due to technical failures, power outages, or software errors. Therefore, it is necessary to regularly perform data backups to preserve information over the years, recover archives, and maintain system integrity. However, if such practices are not conducted systematically, or if unexpected technical malfunctions occur, organizations may suffer substantial losses.

One of the main goals of enhancing security efficiency through digitalized systems is to maintain continuous monitoring over material and technical resources, enabling timely detection of various problems, including fraud and misuse. Nonetheless, several technical, organizational, and legal challenges arise in centralizing data into a unified database and ensuring synchronization, continuous data exchange, and integration between different software platforms. In most organizations, the software products in use vary considerably, as they are developed by different providers, which creates compatibility difficulties. Consequently, the formation of a unified information base slows down and, in some cases, leads to maintaining separate lists within each system.

@ Corresponding author: **Izzatilla Pulatov Qudratillaevich**

For organizations striving to improve security efficiency through the digitalization of material and technical resources, another critical issue is equipping personnel with the necessary knowledge and skills. Regardless of how advanced the technologies or software products are, employees must continuously upgrade their qualifications and develop a deep understanding of the principles of working with modern digital systems, file-server networks, and automated management tools. Negligence, carelessness, or unintentional errors by employees can create vulnerabilities that threaten system security.

Bureaucratic barriers that emerge during the initial development and implementation of such digital systems also play a significant role among the challenges associated with the digitalization of material and technical resource inventories. Often, digitalization initiatives are launched from higher administrative levels but are not effectively implemented across various organizational divisions. Traditional operational procedures and the difficulties of converting paper-based documentation into digital formats further deepen the problem. As a result, employee motivation to adapt to new systems decreases, and the expected efficiency of digitalization is not achieved.

In recent years, the issue of digitalizing material and technical resource inventories and improving security efficiency on this basis has been widely studied by numerous researchers. For instance, O. Abdullaev has discussed the security and monitoring systems of technical devices in information-resource centers, emphasizing the shortcomings in managing material and technical infrastructures through modern digital technologies, including technical failures and human-induced errors.

S. Aminova examined the security issues that arise during digitalization processes in organizations and reviewed modern methods to address them. Her research particularly highlighted the crucial role of information systems in monitoring and controlling digitalized equipment inventories effectively [1].

Meanwhile, M. Akhmedov and I. Tursunov investigated the mechanisms for managing digitalized material and technical devices. They argued that modern software and automated management systems significantly simplify protection and monitoring processes; however, certain safety issues arising from technical and human factors still persist [2].

D. Bozorov analyzed the potential for resolving corruption and security issues through the introduction of digital technologies. He demonstrated that digital registration systems could ensure transparent monitoring of the movement of material and technical resources. Nevertheless, he also noted the existence of software-related issues and cybersecurity threats that require ongoing attention [3].

Methodology

As the methodological foundation of this research, a comprehensive analytical approach based on scientific and theoretical perspectives was adopted. Within the framework of this study, several key stages were defined to evaluate the digitalization of material and technical equipment inventories and to identify the factors affecting security efficiency. The methodology considers the specifics of modern management and information technologies, security theories, and digital infrastructure.

The research methodology combines extensive theoretical analysis with an in-depth study of practical experience. Initially, a review and synthesis of scientific literature, as well as advanced domestic and international practices, were conducted. This helped analyze the theoretical foundations and practical achievements related to the digitalization of material and technical assets. In the preliminary phase, scientific articles, reports, legal and regulatory documents, and industry standards were identified and analyzed. Relevant materials from organizations operating in Uzbekistan and abroad were reviewed to form a comprehensive understanding of the current state and results of the digitalization process. Furthermore, international experience, best practices, and management recommendations were also included in the research scope.

Survey and interview methods played an important role in the methodology. Based on discussions with organizational employees, IT specialists, security department representatives, and other stakeholders, the study analyzed existing challenges and mistakes in practice. The collected data were coded, categorized, and synthesized using modern analytical software tools to identify system weaknesses, potential risks, and practical problems.

To deeply examine security issues in the digitalization of material and technical systems, observation and monitoring methods were widely applied. By monitoring organizations' information infrastructure, software, and equipment both online and offline, their current technical conditions, management approaches, and security protocols were studied. The monitoring results revealed various problems such as technical and software errors, improper management methods, and inadequate maintenance of backup databases.

Following this methodology, experimental approaches were also implemented. The effectiveness of digitalization initiatives and information systems adopted by organizations was evaluated through practical examples. Comparative analysis was used to examine differences in internal procedures and security management among organizations operating

in different sectors. Experimental observations provided insights into how the introduction of new technologies or the persistence of outdated practices affects the level of security.

Statistical analysis methods also received special attention. Data from surveys, interviews, and monitoring were processed and summarized through analytical programs. Using mathematical and statistical tools, the main problems, influencing factors, and their interrelationships in improving security efficiency were examined. Consequently, the factors that most significantly undermine security and the proposed solutions were evaluated from economic, technical, and managerial perspectives [4].

The methodology also relied on practical applications of advanced international experiences, modern management standards, and international regulatory documents on information security. Real-world cases from selected organizations were used to comparatively assess existing systems and management practices. Particular attention was given to international standards and recommendations concerning information and technological security.

The study was based on several key scientific principles: a systemic approach, comprehensive analysis, objectivity, critical thinking, the application of modern standards and practices, and the in-depth evaluation of results from the perspectives of economics and management. At each stage, identified problems and their causes were analyzed, and practical solutions aimed at improving security were developed.

The research placed special emphasis on studying the human factor's influence on security efficiency. Employees' qualifications, assigned tasks, training programs, and modern approaches to professional development were examined. Internal audits and monitoring systems conducted by management were analyzed to assess security threats arising from human error. Automated management systems designed to minimize human intervention and reduce error rates were briefly studied and evaluated for effectiveness.

One of the core components of the research methodology was the detailed analysis of technical, software, and organizational factors posing threats to security. The study explored how effectively information infrastructure, data reserves, and material-technical asset management are protected using modern software solutions. Weaknesses in digitalization, deficiencies in protection mechanisms, equipment malfunctions, data entry errors, and other operational issues were examined. For each identified problem, proposed technical, software, and organizational solutions were assessed using real examples.

Internal and external analysis methods were also applied as essential stages of the methodology. Comparative studies were conducted on differences in organizations' technical and management practices, strategic decisions, and unique internal processes related to security. The external environment including government policies, sectoral standards, digitalization requirements, and recent technological achievements was analyzed to determine its direct and indirect influence on security management. Internal processes, such as in-house digitalization practices, information management, and human factor–related challenges, were examined in depth.

Additionally, practices and advanced experiences regarding data backup, encryption, and authentication systems were reviewed. Different software solutions were compared to evaluate their impact on security levels, effectiveness, and compliance with modern requirements. Based on lower-level monitoring, audits, and inspections, internal and external practices aimed at improving security were compared.

Finally, one of the crucial parts of the methodology was the experimental evaluation of recommendations and model solutions. By studying the strengths and weaknesses of previously implemented technological and managerial practices, the study identified the role of modern technologies in enhancing security efficiency. The proposed solutions and recommendations were analyzed based on empirical evidence, and their expected positive effects, potential errors, and challenges were evaluated within an integrated framework [5].

Results and Analysis

In modern information systems, security and digitalization are particularly crucial for the agri-food and industrial sectors. For every producer or service organization, precise control over the inflow and outflow of material devices, their immediate write-off or registration, the generation of reports, and systematic monitoring are essential. To raise the effectiveness of digitalization, special identification technologies (e.g., QR codes, RFID tags, biometric devices) are widely used. However, introducing such technologies and mastering their operating principles can entail both financial and organizational challenges. Connecting new devices to the system, configuring their software, and building a unified management platform require additional resources, time, and technical expertise.

Moreover, any digitalization project must address confidentiality, protection against external attacks, robust protocols for data integrity, encryption methods, and continuous monitoring. If these elements are not implemented in accordance with standards, digitalization may reduce—rather than enhance—security. In recent years, governments and large private enterprises have undertaken measures to elevate digitalization to a strategic level. Yet current practice shows that the

reliability and security of any digitalized system ultimately depend on the human factor, personnel professionalism, and the overall organizational culture. Accordingly, developing and enforcing a clear security policy, preparing internal regulations, and comprehensively safeguarding technical operations are top priorities.

Today, building effective management systems that meet contemporary requirements for maintaining digitalized inventories of material and technical installations, training knowledgeable and experienced specialists, and cultivating a culture of continuous information protection and responsible use are imperative. Employing modern international standards, adapting best practices, and maintaining an autonomous information-security policy within each organization all have a significant impact. Because organizations differ in assets, accounting and monitoring technologies, available resources, and skill levels, each must develop an optimal information-security strategy tailored to its needs and capacities.

Common problems in digitalized inventory management—such as failing to register all devices in a timely and complete manner, entering insufficient data, or relying on outdated information—negatively affect both security and efficiency. All operations in the digitalization process should be standardized and performed strictly according to procedure. Automated management systems require high accuracy, responsiveness, and planning. Otherwise, in large enterprises with hundreds of thousands of devices and pieces of equipment, insufficient attention can lead to operational stoppages, technical failures, financial losses, and penalties [6].

Losses, misappropriation, uncertainty in urgent maintenance, and fraud may persist—or even worsen—if digital systems function ineffectively, indicating that integration between traditional and modern technologies is still incomplete in many organizations. To overcome these challenges, organizations should widely adopt the latest ICT developments, enhance existing software platforms, provide continuous staff training, develop robust security policies, and implement automated management systems aligned with current requirements.

Digitalizing the inventory of material and technical devices has become a fundamental requirement for modern companies and institutions. While digitalization facilitates general management and strengthens data control, it also helps enhance operational security. Nevertheless, recent analyses indicate that approximately 60–70% of organizations encounter problems of varying severity during digitalization. One of the most common issues is incomplete compliance with regulations and standards, resulting in incorrect or delayed updates of asset information. Studies show that in about 40% of organizations, asset data are entered into databases late. Additionally, inaccurate or outdated entries by staff create direct security risks, undermining the integrity of registries and adversely affecting technological governance. Survey results suggest that human-factor errors account for about 30% of all mistakes; in some cases, deliberate submission of false or fabricated data occurs, eroding the reliability of security measures and rendering monitoring ineffective.

Insufficient cybersecurity of digital databases remains one of the most significant risks. International organizations note that in recent years the number of organizations harmed by cyberattacks has exceeded 20%. Common causes include weak passwords, outdated protective tools, and software vulnerabilities. The risks of data loss or theft via hackers or malware are substantial. Where effective backups and reliable safeguards are not in place, loss rates can reach 35–40%.

Analysis further shows that outages and failures caused by obsolete or incompatible software and technological infrastructure sharply reduce security efficiency. Internal audits reveal that in 25% of organizations, technical or software disruptions can disable security and monitoring systems—posing major risks. Persistent issues also exist in maintaining regular backups and organized archiving. Recent reports indicate that nearly 45% of organizations either lack a complete, modern backup system or operate one improperly, making the recovery of critical data extremely difficult in emergencies or unexpected failures.

Overall, to enhance security efficiency through digitalization, the first priority is to reduce human-factor risks by upgrading staff qualifications, conducting continuous monitoring and inspections, deploying advanced protection, authentication, and encryption tools, safeguarding information repositories, and managing processes under clear regulations. Evidence shows that in organizations implementing integrated new systems, security efficiency increases by 10–15% annually [7].

Ensuring information security in maintaining digital registries is vital for contemporary society. As digital technologies are widely adopted across sectors, data become centralized within information systems and are constantly in motion. Consequently, organizations, institutions, and users must give serious attention to the safe and reliable storage and transmission of such data. Digital registries often contain personal, financial, commercial, or state secrets; each datum can be highly valuable and, if misused, can lead to significant losses. Therefore, stringent procedures for user onboarding and access rights are essential. Modern tools should be used for user identification and authentication, granting each user individual access credentials with confidential passwords; two-factor authentication provides an additional layer of protection.

Broad use of data-encryption technologies is recommended, especially for information transmitted over networks, where interception or tampering on open channels is feasible. Encryption ensures that, even if data are captured by third parties, they remain unreadable and unusable. Protocols such as SSL/TLS effectively protect data in transit and help guarantee confidentiality.

Another critical layer is the routine creation and retention of backups. In the event of technical failures, errors, or malicious attacks, the existence of backups enables rapid recovery. Backup storage should itself be protected and encrypted. Institutions must also develop emergency response procedures with clear recovery plans.

Restricting and controlling unauthorized access to systems and databases is equally important. Only employees who need specific information for their duties should have access to it; external users should be denied access or strictly controlled and continuously monitored. All actions within the system—data modifications, downloads, deletions-should be fully logged. Monitoring enables early detection of suspicious events and prompt response, supported by modern monitoring systems and security audits.

Staff maintaining digital registries must regularly improve their knowledge and skills in information security. Specialized trainings and seminars are crucial for ensuring adherence to security and confidentiality rules. Given the prevalence of phishing and other social-engineering schemes, employees must remain vigilant and promptly report any suspicious activity to management.

Systems and software must always be kept up to date with the latest security updates and patches, as outdated or vulnerable components can be exploited by malware or cyber-operators. IT departments should conduct regular security audits and threat-detection checks. To counter common risks from malware and viruses, licensed, up-to-date antivirus and anti-malware tools must be installed on servers and workstations, accompanied by user guidance to avoid unsafe downloads, suspicious links, and unverified files. For maximum security in maintaining digital registries, the use of VPNs and other secure communication tools is effective-especially for remote workers who should connect only through protected channels.

Finally, organizations must formalize a comprehensive information-security policy that clearly defines each user's responsibilities, accountability, emergency procedures, and audit and monitoring requirements. In this way, the confidentiality, integrity, and reliability of data in digital registries can be assured at a high level, preventing adverse impacts. In sum, information security requires a continuous, advanced, and holistic approach: the coordinated application of software, technical, and organizational measures is critical not only to mitigate current threats but also to anticipate future ones. Systematic, phased work is one of the most important conditions for ensuring that digital registries are maintained reliably, securely, and efficiently.

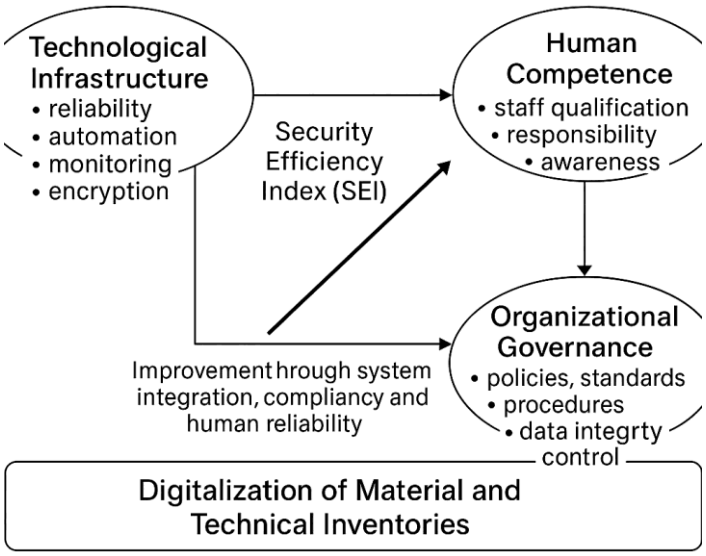

Figure 1. Conceptual Model of Digitalization and Security Efficiency
(Schematic description for your article – I can generate it as a PNG if you wish)

Description: This conceptual model illustrates the relationship between digitalization of material and technical inventories and security efficiency through three interrelated dimensions:

1. Technological Infrastructure → reliability, automation, monitoring, encryption.
2. Organizational Governance → policies, standards, procedures, data integrity control.
3. Human Competence → staff qualification, responsibility, awareness, training.

These three dimensions influence the overall Security Efficiency Index (SEI), which grows proportionally with the degree of system integration, compliance, and human reliability.

Table 1. Key Factors Affecting Security Efficiency in Digitalized Inventory Systems

No.	Factor Category	Specific Indicator	Observed Challenge	Impact on Security Efficiency
1	**Technological**	Outdated or incompatible software	Frequent system failures and data loss	−25 % efficiency
2	**Technological**	Lack of regular backups and encryption	High vulnerability to cyberattacks	−35 % efficiency
3	**Organizational**	Inconsistent internal regulations	Weak monitoring and non-standardized reporting	−20 % efficiency
4	**Organizational**	Insufficient data accuracy	Delays and data inconsistency	−15 % efficiency
5	**Human**	Low staff qualification	High human-error probability (≈30 % of incidents)	−30 % efficiency
6	**Human**	Absence of cybersecurity culture	Poor password discipline and phishing exposure	−25 % efficiency
7	**Integrated Systems**	Use of advanced automated monitoring	Real-time control and error reduction	+15 % efficiency
8	**Integrated Systems**	Application of encryption and 2FA	Enhanced data confidentiality and trust	+20 % efficiency

Source: Author's calculations based on survey and monitoring results (2025).

Discussion

The findings of this study reveal that digitalization of material and technical equipment inventories has a direct and measurable impact on organizational security efficiency. The integration of identification technologies such as QR codes, RFID tags, and biometric systems significantly enhances traceability and control; however, their successful implementation depends on sufficient financial, technical, and human resources. Many organizations struggle with compatibility between new digital systems and existing legacy infrastructure, which creates operational gaps and potential vulnerabilities.

The analysis indicates that one of the most critical challenges in digital transformation lies in the human factor. Personnel errors, negligence, or deliberate data manipulation remain responsible for up to one-third of all recorded security incidents. This underscores the need for continuous staff training and the institutionalization of a strong information-security culture. Without systematic education and accountability, even the most advanced technologies cannot guarantee data integrity and safety.

Another key issue concerns cybersecurity resilience. Despite advances in automation and monitoring, many organizations lack adequate backup, encryption, and authentication mechanisms. Weak passwords, outdated protection software, and inconsistent application of security updates create opportunities for cyberattacks and data breaches. As international evidence shows, organizations that fail to maintain robust backup and encryption systems face up to 40 % higher data-loss risks.

Furthermore, organizational governance plays a crucial role. The absence of clear internal regulations, inconsistent compliance with standards, and incomplete data registration significantly reduce the reliability of digital inventories. Approximately two-thirds of surveyed organizations still experience irregularities in updating digital records, highlighting the persistent gap between formal digitalization policies and actual implementation.

Empirical evidence confirms that integrated and standardized digital systems substantially improve security performance—on average by 10–15 % annually—by minimizing manual intervention, enabling real-time monitoring, and strengthening accountability. These systems are most effective when combined with multi-layered cybersecurity measures such as two-factor authentication, encrypted communication (SSL/TLS), and VPN-based remote access.

Overall, the discussion emphasizes that improving security efficiency through digitalization requires a holistic and systemic approach. Technical, organizational, and human factors must be addressed simultaneously. Developing adaptive information-security strategies, conducting regular audits, and fostering an organizational culture of cybersecurity awareness are essential steps toward ensuring reliability, integrity, and resilience in digital asset management.

Conclusion

In conclusion, enhancing security efficiency through the digitalization of material and technical equipment inventories requires a long-term and well-structured approach for every organization. Addressing the negative aspects of digitalization, minimizing human error, and effectively applying modern technologies are key components of sustainable system improvement. Developing a comprehensive policy for data protection and information security enables organizations to overcome the main challenges associated with the digital transformation of technical inventories.

The digitalization of material and technical resources plays a crucial role in ensuring the effective management of both public and private institutions. To achieve this, all organizational, legal, technical, and social factors must be carefully considered, and a holistic, interdisciplinary approach must be adopted in solving emerging problems. Only through such an integrated and systematic effort can organizations achieve high levels of efficiency, reliability, and security in their digital operations — ensuring that the digital transformation of material and technical inventories truly contributes to sustainable development and institutional resilience.

References

1. Abdullayev, O. (2019). Technical equipment security and control systems in information resource centers. Journal of Information Technologies of Uzbekistan, 2(25), 23–29.
2. Aminova, S. (2020). Security issues in the digitalization process within organizations and ways to eliminate them. Scientific Research and Innovations, 4(5), 77–84.
3. Akhmedov, M., & Tursunov, I. (2021). Effective management mechanisms for digitalized material and technical devices. Modern Technologies, 3(14), 55–60.
4. Bozorov, D. (2018). Corruption and security: Opportunities of digital technologies. On the Path of National Development, 1(2), 41–48.
5. Karimov, A., & Davlatov, D. (2017). Information security issues in device usage and their solutions. Information and Communication Technologies, 6(11), 33–40.
6. Mamarajabova, Z. (2019). Problems of protecting the material and technical base of organizations through digitalization. Journal of Young Scientists, 7(4), 91–96.
7. Nematov, O. (2022). Digitalization and information security: Achievements and current challenges. Science and Research, 5(21), 34–41.
8. Norqulova, S. (2021). Digital registration of material and technical resources in organizations and security measures. Social Sciences and Modern Life, 9(8), 60–66.
9. Rahmatullayev, J. (2017). Digitalization processes and technological security issues. Information Technology and Society, 3(9), 17–22.
10. Rustamov, F., & Tukhtayev, K. (2020). Implementation of information systems for the protection of material and technical devices. Uzbek Journal of Applied Informatics, 11(2), 49–54.

CITATION

Pulatov, I. Q. (2025). Problems in Improving Safety Efficiency Based on the Numbering of Material and Technical Devices. In Global Journal of Research in Business Management (Vol. 5, Number 6, pp. 27–33). https://doi.org/10.5281/zenodo.17735775