American Journal of Open University Education
ISSN **2997-3899** (Online)
Vol. 3, No. 2, July 2026,
Available online at: https://scientificbulletin.com/index.php/AJOUP

Article

Mechanisms for Ensuring Cybersecurity in State Information Systems and Their Effectiveness

Murodova Mehrangiz Umid kizi
English Language Teacher, Cyber University State University
Email: murodovamehrangiz692@gmail.com

Article information:
Manuscript received: 10 Feb 2026; **Accepted:** 27 Mar 2026; **Published:** 26 Apr 2026

Abstract: This article analyzes the mechanisms for ensuring cybersecurity in state information systems, their effectiveness, and the current situation in Uzbekistan. The research is based on a comparative study of the legislative framework of the Republic of Uzbekistan in the field of cybersecurity, global cyber threat statistics, international experience, and the national cybersecurity strategy. The article examines key mechanisms such as the Security Operations Center (SOC) system, vulnerability monitoring, cryptographic protection, information security policy, and staff training, supported by practical examples. The results show that the number of cyberattacks in Uzbekistan increased by 148% in 2022–2023; therefore, strengthening the protection of state systems requires the simultaneous development of technical, legal, and human resource capacities.

Keywords: Cybersecurity, state information systems, cyber threat, cyberattack, information security, SOC, vulnerability, cryptography, digital transformation, Uzbekistan.

Introduction

With the rapid development of digital technologies and the transition of public administration to the e-government system, ensuring cybersecurity in state information systems is becoming not only a technical issue but also a matter of strategic national security. As highly sensitive information such as tax data, citizen registries, medical records, financial transactions, and national security information is stored and processed in electronic systems, the scale and intensity of cyberattacks on state information infrastructure are increasing year by year[1].

On a global scale, in the third quarter of 2024, the number of cyberattacks targeting organizations increased by 75% compared to the same period in 2023, with an average of 1,876 attacks per organization per week recorded (check point research, 2024). The government and military sector ranks second on this list after the education sector, with an average of 2,553 attacks per week on state systems. According to 2024 data, the damage caused by cybercrime to the global economy reached 9.5 trillion u.s. dollars, and this figure is projected to rise to 23 trillion dollars by 2027 (cybersecurity ventures)[2].

Uzbekistan is not excluded from this process. According to the Cybersecurity Center of Uzbekistan, the number of cyberattacks targeting information resources in the **".uz"** domain increased from 4.5 million attacks in 2022 **to** 11 million attacks in 2023**,** recording a 148% increase**.** During 2025, it was also identified that cybercriminals illegally stole 1.9 trillion UZS from Uzbek citizens. Such circumstances require a systematic analysis of the mechanisms for protecting state information systems and evaluating their effectiveness[3].

The purpose of this research is to identify the main mechanisms used to ensure cybersecurity in the state information systems of Uzbekistan, evaluate their effectiveness, and develop scientifically grounded proposals for eliminating weaknesses.The objectives of the research are as follows: to classify the types and directions of cyber threats against state information systems; to analyze the legislative and regulatory framework in Uzbekistan; to assess the effectiveness of technical and organizational protection mechanisms; to study and compare international experience; and to identify problematic aspects and formulate recommendations[4].

Literature Review

An analysis of the scientific literature in the field of cybersecurity shows that this area has become an independent scientific discipline over the last decade. Various authors and international organizations pay great attention to studying the effectiveness of cybersecurity mechanisms.

The Law of the Republic of Uzbekistan "On Cybersecurity" (2022) and the subsequent amendments and additions introduced to it in 2024 (Law No. O'RQ-964) establish the legal foundations for protecting state information systems. This law regulates the mandatory cybersecurity examination of information systems of state bodies, the storage of backup copies of data, and the notification of the authorized body about cyberattacks (Lex.uz, 2022)[5].

In the World Economic Forum report Global Cybersecurity Outlook 2025, 72% of cybersecurity leaders stated that organizational risks have increased, and supply chain attacks and artificial intelligence-based attacks were identified as the main threats. Most specialists consider Zero Trust architecture, multi-factor authentication (MFA), and AI-based monitoring systems as the foundation of future cybersecurity[6].

According to an interview given by M. Hakimov, Head of Department at the Cybersecurity Center of Uzbekistan, to Kun.uz in 2024, the main problems in ensuring cybersecurity in state agencies' resources are insufficient traffic filtering and vulnerabilities related to the human factor. This opinion is consistent with international literature in the field of information security—including reports by IBM Security X-Force and Verizon Data Breach Investigations Report—which indicate that in 2023 the human factor was responsible for 60–80% of cyber threats[7].

According to Resolution No. PQ-167 of the President of the Republic of Uzbekistan dated May 31, 2023, additional requirements were established for Critical Information Infrastructure (CII) facilities. Sectors of vital importance such as public administration, defense, banking and finance, energy, healthcare, and transport are designated as CII facilities. Researchers point out that there are certain gaps in assessing the practical implementation of these normative documents, particularly the insufficient development of an independent audit system for verifying security standards (Gazeta.uz, 2022)[8].

At the international level, the National Institute of Standards and Technology Cybersecurity Framework and the International Organization for Standardization/IEC 27001 standards are considered the most common methodological foundations for ensuring cybersecurity in state systems. The NIST framework defines five main functions: Identify, Protect, Detect, Respond, and Recover. The European Union's NIS2 Directive, which entered into force in 2022, has significantly strengthened cybersecurity requirements for critical infrastructure operators and is positively assessed by the scientific community[9].

Research Methodology

This research is based on the methods of comparative analysis, document review, and interpretation of statistical data. The study covers three main directions. The first direction is the analysis of the normative-legal framework. The Law of the Republic of Uzbekistan "On Cybersecurity" (2022), Presidential Decrees No. PF-6007 and PQ-4751 of

2020, Resolution No. PQ-167 of 2023, Law No. O‘RQ-964 of 2024, and the Cybersecurity Strategy of Uzbekistan for 2026–2030, approved in 2026, were analyzed. In addition, international standards such as International Organization for Standardization/IEC 27001, National Institute of Standards and Technology CSF, and the European Union NIS2 Directive were comparatively studied. The second direction is the analysis of statistical data. Reports of the Cybersecurity Center of Uzbekistan (2023 report), the World Economic Forum’s Global Cybersecurity Outlook reports (2023, 2025), as well as data from IBM Security X-Force Intelligence Index, Check Point Research, Gartner, and Cybersecurity Ventures were used. The third direction is comparative analysis. Uzbekistan’s cybersecurity system was compared with the models of Estonia (CERT-EE), South Korea (KISA), Singapore (CSA), and Georgia. The experiences of these countries in rapidly raising their cybersecurity levels were studied. As limitations of the study, it should be noted that some statistical data are not available in open sources, and reports of state bodies are not always publicly disclosed. In addition, the situation in the field of cybersecurity changes very rapidly, requiring the research findings to be updated within a short period of time.

Results And Discussion

The dynamics of cyber threats in uzbekistan show a sharp upward trend. Based on the data recorded by the cybersecurity center of uzbekistan, the following table was developed[10]:

Table 1. Dynamics of Cyber Threats in Uzbekistan (Based on data from the Cybersecurity Center of Uzbekistan and Kun.uz).

Indicator	2021	2022	2023	Growth Rate
Number of cyberattacks on the “.uz” **domain**	~2.1 million	4.5 million	11 million	+148%
Share of phishing attacks	28%	35%	39.6%	+11.6 pp
DDoS attacks	Increased	Increased	Significantly increased	High
Data leakage incidents	Low	Medium	Increased	Rising
Financial damage (trillion UZS)	—	—	1.9 (in 2025)	Significant

According to the geographical distribution of cyberattacks carried out in 2023, the main threats to Uzbekistan’s resources originated from Netherlands (759,502 attacks), the United States (696,671 attacks), and Russia (100,549 attacks). This indicates that cyberattacks are often launched through servers located in third countries, which complicates the issue of attribution (identifying the source of the threat)[11].

In January 2024, three government agencies in Uzbekistan were subjected to cyberattacks. According to the Minister of Digital Technologies, contrary to the initially reported 15 million, nearly 60 thousand citizens’ unique data records were leaked. However, the disclosure of photos of employees of the Ministry of Internal Affairs, data of medical workers from the National Agency for Social Protection, and financial records of the Mortgage Company clearly demonstrated vulnerabilities in state systems[12].

A specific threat landscape has been formed for state information systems. Based on the analysis of international statistical data, the following table was developed:

Table 2. Global Cyber Threat Landscape and Its Impact on State Information Systems.

Threat Type	Share / Frequency	Impact on State Systems	Source
Ransomware	70% of all attacks, 2023	Very high	Sophos / Statista
Phishing	39.6% of email threats	High	Hornetsecurity 2024
DDoS attacks	2,553 per week / government sector	High	Check Point Q3 2024
Data theft / Data breaches	Average loss of $4.88 million	Critical	IBM 2024
Supply chain attacks	30% of breaches	Very high	Verizon 2025
AI-based attacks	Increasing	Emerging threat	WEF 2025

Ransomware attacks pose a particular threat: in 2023, the total amount of losses related to ransom payments reached a record 1.1 billion U.S. dollars. Such attacks targeting critical government infrastructure can paralyze an entire country. A clear example is the HSE ransomware attack on Ireland's healthcare system in 2021, which caused the country's entire medical information system to remain inoperative for weeks[13].

The mechanisms for ensuring cybersecurity in state information systems can be divided into three main groups: technical mechanisms, organizational mechanisms, and legal-regulatory mechanisms[14].

A Security Operations Center (SOC) is an operational center that monitors state information systems 24/7, enabling the real-time detection of threats and prompt response. In Uzbekistan, a National System for Monitoring Cybersecurity Incidents and Responding to Them (national SOC) is being established. In global practice, SOC effectiveness is measured by specific indicators such as Mean Time to Detect (MTTD) and Mean Time to Respond (MTTR). According to IBM Security, organizations that extensively use security automation detect and contain breaches 80 days faster than other organizations[15].

A Vulnerability Management System is the process of regularly identifying, classifying, and eliminating vulnerabilities in state information systems. In Uzbekistan, the State Security Service of Uzbekistan (SSS), with the participation of independent experts, conducts bug bounty competitions to identify vulnerabilities. By mid-2024, 22,254 new vulnerabilities were recorded in the Common Vulnerabilities and Exposures (CVE) database, representing a 30% increase compared to 2023. This highlights the vital importance of the rapid elimination of vulnerabilities[16].

Cryptographic protection tools involve the use of encryption technologies in data transmission and storage. AES-256, RSA-2048, and the modern TLS 1.3 protocols are considered standard for state systems. In Uzbekistan, local cryptographic standards have also been established for state information systems, including O'z DSt GOST-based algorithms[17].

Multi-Factor Authentication (MFA) is currently recognized as one of the most effective cybersecurity tools. According to Microsoft research, the implementation of MFA can prevent 99.9% of phishing attacks. However, according to Arctic Wolf research, 80% of organizations that experienced Business Email Compromise (BEC) attacks did not have

an MFA solution in place at the time of the attack. Therefore, the implementation of MFA in Uzbekistan's state portals is considered a priority task[18].

Intrusion Detection/Prevention Systems (IDS/IPS) are systems that analyze network traffic in real time to detect and block unauthorized access attempts. The fact that insufficient traffic filtering in Uzbekistan has been identified as one of the main causes of cyberattacks (M. Hakimov, 2024) indicates the urgent need for investment in this area.

Zero Trust Architecture is a modern security approach based on the principle of "trust no one, verify everything." In 2023, the global adoption rate of Zero Trust reached 33%. This architecture is particularly important in preventing insider threats and supply chain attacks in state systems.

Information Security Departments. Starting from 2026, specialized cybersecurity departments consisting of four members each will be established within the Ministry of Justice of Uzbekistan, the Ministry of Energy of Uzbekistan, and the State Tax Committee of Uzbekistan. This decision is aimed at creating the necessary human resource base to ensure information security in government agencies[19].

Cyber Security Incident Response Plans (CSIRP) are essential to ensure that every government agency acts according to a clear algorithm in the event of a cyberattack. In Uzbekistan, a procedure has been established for written information exchange with the authorized state body—the Cybersecurity Center of Uzbekistan—within **48 hours** (Resolution No. **PQ-167**, Clause 6, revised edition of 2024). However, international practice shows that merely having a document is not enough; regular exercises and **stress testing** are also necessary.

Employee training and cyber hygiene are equally important. According to IBM Security research, **41%** of cyber threats occur through phishing or social engineering. Therefore, alongside technical tools, continuous employee training and the development of a culture of cyber hygiene are crucial. As emphasized by M. Hakimov, improving the level of information security awareness among citizens and government employees remains an urgent task in Uzbekistan.

Audit and monitoring are important mechanisms in ensuring cybersecurity. In Uzbekistan, procedures have been established for examining the compliance of state information systems and resources with information security requirements; such examinations may be conducted on a mandatory or voluntary basis. In addition, the Cybersecurity Center of Uzbekistan provides services for inspecting websites in the ".uz" domain in accordance with information security requirements[20].

The cybersecurity legislative system in Uzbekistan has been significantly improved in recent years. This evolution can be seen through the following table:

Table 3. Development of Cybersecurity Legislation in Uzbekistan.

Document	Date of Adoption	Main Content
Law "On Cybersecurity"	2022	Main legal framework, examination procedures, concept of Critical Information Infrastructure (CII)
Presidential Decree No. PF-6007	June 15, 2020	Introduction of the state system for protecting information systems
Presidential Resolution No. PQ-4751	June 15, 2020	Further improvement of the cybersecurity system

Presidential Resolution No. PQ-167	May 31, 2023	Improvement of cybersecurity of Critical Information Infrastructure (CII) facilities
Law No. O'RQ-964	September 20, 2024	Strengthening cybersecurity requirements in the banking and financial sector
Cybersecurity Strategy 2026–2030	March 10, 2026	National SOC, bug bounty, workforce training

The Cybersecurity Strategy 2026–2030, approved in 2026, introduced several important innovations: a system for promptly notifying cybersecurity stakeholders about new cyber threats and vulnerabilities will be created; an anti-phishing platform will be launched; communication operators will be obliged to block suspicious calls; and the personal responsibility of heads of government agencies for implementing cyber protection measures will be strengthened.

A comparative assessment of the effectiveness of various cybersecurity mechanisms based on international data is presented in the following table:

Table 4. Evaluation of the Effectiveness of Cybersecurity Mechanisms.

Mechanism	Effectiveness Level	Implementation in Uzbekistan	Recommendation
Multi-Factor Authentication (MFA)	Very high (prevents 99.9% of phishing attacks)	Partially implemented	Expansion required
Employee training	High (prevents 60–80% of threats)	Partial	Regular training courses
SOC / SIEM systems	High (detects 80 days faster)	Being developed	Accelerate implementation
Zero Trust architecture	High (prevents insider threats)	Low	Gradual implementation
Vulnerability scanning	Medium–high	Available (Bug bounty)	Expand
Data encryption	High	Partial	Standardization needed
Backup copies	Medium (3-month requirement established)	Legally regulated	Strengthen monitoring
Audit and certification	Medium	Mandatory examination	Increase independence

The experience of countries with developing digital economies similar to Uzbekistan is of particular importance. Estonia, which has one of the most advanced digital government systems in the world, learned valuable lessons from the cyberattacks of 2007 and successfully developed the X-Road data exchange platform and CERT-EE (Computer

Emergency Response Team). In the Estonian model, "layered defense" and the active involvement of civil society in the national cybersecurity system are considered key principles.

South Korea, through the Korea Internet & Security Agency (KISA), created a cybersecurity monitoring system covering all government agencies. Annual cyberdrills were made mandatory for all public employees. Singapore, under the leadership of the Cyber Security Agency of Singapore (CSA), considers cybersecurity a strategic element of national infrastructure and the economy, and has introduced a model for the integrated protection of Operational Technology (OT) and Information Technology (IT) systems.

The experience of Georgia is one of the most valuable models for Uzbekistan to study, as this country also underwent radical transformation within a short period. After the cyberattacks of 2008, Georgia moved closer to NATO cybersecurity standards within five years, established the CERT-GRENA system, and built a private cloud infrastructure for public services. Based on a comparative study of the experiences of these countries, the following table was developed:

Table 5. Comparative Analysis of International Experience.

Country	Main Cybersecurity System	Best Practice	Applicability to Uzbekistan
Estonia	CERT-EE, X-Road	Layered defense, civil society participation	High
South Korea	KISA	Mandatory cyberdrills, 24/7 monitoring	Medium–High
Singapore	CSA	OT/IT integration, risk rating	Medium
Georgia	CERT-GRENA	Rapid modernization, NATO standards	High
Uzbekistan	Cybersecurity Center	Bug bounty, SOC under development	Development stage

The results of the research indicate that the following major problems exist in Uzbekistan.

The first problem is the shortage of qualified personnel. Globally, there are 3.5 million unfilled cybersecurity jobs (Cybersecurity Ventures, 2024). In Uzbekistan, the lack of qualified cybersecurity specialists is also a serious issue, and the Tashkent University of Information Technologies and other higher educational institutions have only recently begun establishing training programs in this field.

The second problem is limited technical resources. In Uzbekistan, when government agencies do not have their own information security departments, they are allowed to outsource these functions to external contractors (Strategy 2026). However, an important safeguard is that the list of such contractors must be controlled exclusively through the special registry of the State Security Service of Uzbekistan (SSS).

The third problem is the imperfection of coordination and information-sharing systems. A real-time information exchange system on cyber threats among different government agencies has not yet been fully established. This makes it difficult to prevent in time the spread of threats identified in one agency to others.

The fourth problem is that the pace of development of digital services is outstripping the development of security systems. As acknowledged by the Minister of Digital Technologies in 2024, efforts to make services more convenient for citizens have also increased risks. Failure to implement the "Security by Design" principle from the very beginning may become costly later.

The fifth problem is the human factor. Phishing, social engineering, and employees' susceptibility to cyberattacks are among the most common vulnerabilities in state systems. According to IBM Security, the human factor plays a decisive role in 60% of cyber threats.

CONCLUSION

In recent years, significant positive changes have occurred in the field of ensuring cybersecurity in state information systems in Uzbekistan: a comprehensive legislative framework has been established, the Cybersecurity Center of Uzbekistan has been created, a national SOC is being developed, bug bounty programs are being launched, and the Cybersecurity Strategy 2026–2030 was approved in 2026. These developments demonstrate that the country recognizes cybersecurity as a strategic component of national security.

At the same time, the fact that the number of cyberattacks on the ".uz" domain increased by 148% in 2022–2023, that cybercriminals stole 1.9 trillion UZS in 2025, and that cyberattacks on government agencies continue to occur indicates that existing mechanisms are either insufficient or not fully implemented in practice.

Based on the research, the following recommendations are proposed: first, to introduce Multi-Factor Authentication (MFA) and Zero Trust Architecture as standard requirements in all critical state information systems; second, to conduct annual mandatory cyberdrills for employees of government agencies; third, to develop cybersecurity specialist training as a separate field in higher educational institutions; fourth, to establish an automated real-time threat information-sharing system among government agencies; fifth, to make the "Security by Design" principle a mandatory requirement in the development of new digital services; and sixth, to make cybersecurity audit results partially transparent in order to strengthen public oversight.

Cybersecurity is not a one-time project, but a continuous process. As technologies evolve, threats also continue to change; therefore, flexibility, continuous monitoring, and a proactive approach remain decisive factors in protecting state information systems.

REFERENCES

[1]Law of the Republic of Uzbekistan "On Cybersecurity," Apr. 15, 2022. [Online]. Available: https://lex.uz/docs/5949704

[2] Decree of the President of the Republic of Uzbekistan "On the Cybersecurity Strategy 2026–2030," Mar. 10, 2026. [Online]. Available: https://www.gazeta.uz/oz/2026/03/17/stategy/

[3] Resolution No. PQ-167 of the President of the Republic of Uzbekistan, "On additional measures to improve the system of ensuring cybersecurity of critical information infrastructure facilities," May 31, 2023. [Online]. Available: https://lex.uz/docs/-6479190

[4] Law of the Republic of Uzbekistan No. O'RQ-964, "On amendments and additions to certain legislative acts in connection with improving legislation in the field of cybersecurity," Sep. 20, 2024. [Online]. Available: https://lex.uz/docs/-7108720

[5] Cybersecurity Center of Uzbekistan, *Cybersecurity Report 2023*. [Online]. Available: https://csec.uz/uz/

[6] M. Hakimov, "Cyberattacks on information resources in Uzbekistan increased 2.4 times," *Kun.uz*, Mar. 29, 2024. [Online]. Available: https://m.kun.uz/news/2024/03/29/ozbekistondagi-axborot-resurslariga-kiberhujumlar-24-barobarga-oshdi

[7] Spot.uz, "Cybersecurity departments will be established in the Ministries of Justice and Energy and the Tax Committee," Mar. 11, 2026. [Online]. Available: https://www.spot.uz/oz/2026/03/11/cybersecurity-departments

[8] Gazeta.uz, "Information systems of state bodies will undergo mandatory cybersecurity expertise," Apr. 17, 2022. [Online]. Available: https://www.gazeta.uz/oz/2022/04/17/cyber-security/

[9] Sputnik Uzbekistan, "Uzbekistan's cybersecurity strategy until 2030 was discussed," Mar. 17, 2026. [Online]. Available: https://oz.sputniknews.uz/20260317/uzbekistan-kiberxavfsizlik-strategiya-muhokama-56325873.html

[10] Ministry for Development of Information Technologies and Communications, "Cybersecurity Center proposed new information systems," *Kun.uz*, Apr. 25, 2020. [Online]. Available: https://kun.uz/uz/news/2020/04/25/akt-vazirligi-ozkomnazorat-va-kiberxavfsizlik-markazi-2ta-yangi-axborot-tizimini-yaratish-togrisida-taklif-berdi

[11] World Economic Forum, *Global Cybersecurity Outlook 2025*. Davos, Switzerland: WEF, 2025. [Online]. Available: https://www.weforum.org/publications/global-cybersecurity-outlook-2025/

[12] Check Point Research, *A Closer Look at Q3 2024: 75% Surge in Cyber Attacks Worldwide*, 2024. [Online]. Available: https://blog.checkpoint.com/research/a-closer-look-at-q3-2024-75-surge-in-cyber-attacks-worldwide/

[13] IBM Security, *Cost of a Data Breach Report 2024*. Armonk, NY, USA: IBM Corporation, 2024. [Online]. Available: https://www.ibm.com/reports/data-breach

[14] Cybersecurity Ventures, *Top 10 Cybersecurity Predictions and Statistics for 2024*. [Online]. Available: https://cybersecurityventures.com/top-5-cybersecurity-facts-figures-predictions-and-statistics-for-2021-to-2025/

[15] Gartner, *Security and Risk Management Market Data 2024*. Stamford, CT, USA: Gartner Inc., 2024. [Online]. Available: https://www.gartner.com/en/information-technology/insights/cybersecurity

[16] Cobalt, *Top Cybersecurity Statistics for 2024*. [Online]. Available: https://www.cobalt.io/blog/cybersecurity-statistics-2024

[17] National Institute of Standards and Technology, *Cybersecurity Framework (CSF) 2.0*, 2024. [Online]. Available: https://www.nist.gov/cyberframework

[18] European Union Agency for Cybersecurity, *NIS2 Directive Implementation Guidelines*. Athens, Greece: ENISA, 2023. [Online]. Available: https://www.enisa.europa.eu/topics/cybersecurity-policy/nis-directive-new

[19] TechTarget, *35 Cybersecurity Statistics to Lose Sleep Over in 2026*. [Online]. Available: https://www.techtarget.com/whatis/34-Cybersecurity-Statistics-to-Lose-Sleep-Over-in-2020

[20] SentinelOne, *Key Cyber Security Statistics for 2026*. [Online]. Available: https://www.sentinelone.com/cybersecurity-101/cybersecurity/cyber-security-statistics/