Registered in Germany Europa Revue Journal
ISSN: 1862-6564 Vol. 6 No. 9 (2026) Published September 30, 2026

ENSURING DATA SECURITY IN DIGITAL INFORMATION PROCESSING: LEGAL AND TECHNICAL ANALYSIS

Tursunov Hojiakbar Hamidullo ugli

Fergana City Specialized Technicum for Individuals with Disabilities Specialist teacher (PhD) Fergana, 150100, Uzbekistan

ORCID: 0000-0002-1280-604X

Email: h.tursunov524@gmail.com

Abstract

This article examines the legal, organizational, and technical aspects of ensuring data security in the process of digital information processing. The study reviews the regulatory framework of the Republic of Uzbekistan formed on the basis of the Law "On Personal Data", the Presidential Decree approving the Cybersecurity Strategy for 2026–2030, and the national standards developed by the "Cybersecurity Center" state unitary enterprise, and situates these developments within the relevant international and national scholarly literature. Statistical indicators of cyber offenses and cyberattacks recorded in the republic over the past five years are analyzed, and their causes and main directions are identified. Based on the research findings, specific proposals are developed for further improving the organizational, legal, and technical mechanisms for ensuring information security. The results of the article are of practical importance for shaping information security policy in state bodies, educational institutions, and commercial organizations.

Keywords

digital information, data security, cybersecurity, personal data, information protection, cyberattack, information technology, legal regulation, literature review.

Introduction

The rapid global development of information and communication technologies, the digitalization of public services, and the increasing integration of virtually every sphere of daily life with the internet have made ensuring data security in the processes of digital information processing, storage, and transmission a matter of pressing importance. Information about individuals has today become not merely a personal matter but a

unique resource of considerable economic value, and this, in turn, has increased the risk of its unlawful use or theft.

In the Republic of Uzbekistan, the development of the digital economy has become one of the priority directions of state policy. However, the rapid pace of digitalization has also led to an expansion of threats in the field of information security. In particular, over the past five years the number of cybercrimes recorded in the republic has grown considerably, and the number of complaints filed by citizens and organizations regarding cyber offenses has increased accordingly. This situation places on the agenda the need to provide the data-processing activities of both state and non-state organizations with robust legal and technical protection systems.

The purpose of this study is to analyze the legal-regulatory framework and the organizational-technical mechanisms that ensure data security in the process of digital information processing in the Republic of Uzbekistan, to assess existing trends on the basis of statistical data, and to develop scientifically grounded proposals for their further improvement.

The objectives of the study are as follows: 1) to analyze the national legislation and standards regulating data security; 2) to examine statistical indicators in the field of cybersecurity; 3) to conduct a comparative analysis with foreign experience; and 4) to develop recommendations for addressing existing problems.

LITERATURE REVIEW

The legal regulation of personal data protection and cybersecurity has attracted considerable scholarly attention both internationally and within Uzbekistan. At the international level, the foundational framework is provided by the Council of Europe's Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Convention No. 108, 1981), which established some of the earliest binding international standards for data protection, and by the European Union's General Data Protection Regulation (GDPR, Regulation (EU) 2016/679), which introduced a comprehensive, rights-based model built on principles such as data minimization, purpose limitation, and restrictions on cross-border data transfer. These instruments are

widely used in the literature as benchmarks against which national data-protection regimes, including Uzbekistan's, are evaluated.

In the technical domain, the international standard ISO/IEC 27001:2013, "Information technology — Security techniques — Information security management systems — Requirements," remains the principal reference framework used in the literature to describe organizational information security management systems and is frequently discussed as a benchmark for institutional certification in both the public and private sectors.

Within Uzbek legal scholarship, Gulyamov and Saidov (2020) examine the broader problems and prospects of legal regulation in the digital economy, providing a foundation for understanding the regulatory environment within which data-security norms operate. Maxkamova (2025) offers a comparative analysis of personal-data-management approaches in Uzbekistan against international standards, highlighting persisting gaps between national practice and global norms. Similarly, studies published in the journal Yurisprudensiya (2026) provide a detailed legal analysis of the Law "On Personal Data" and examine legislative approaches to personal-data protection in the digital environment, drawing on foreign experience to outline directions for national reform. Rajabov (2022) explores the role of cybersecurity within Uzbekistan's public-order and law-enforcement bodies, underscoring the institutional dimension of the problem.

A separate strand of the literature, represented largely by analytical and news publications such as Spot.uz (2022; 2024; 2025), documents the dynamics of cybercrime and cyberattacks within Uzbekistan's national internet segment, offering empirical grounding for policy discussion. Taken together, the existing literature demonstrates a clear division between, on the one hand, works focused on the legal-normative dimension of personal data and cybersecurity regulation and, on the other, works and reports that document the empirical and statistical dynamics of cyber threats. Comparatively few studies integrate both legal and statistical analysis within a single, updated framework that accounts for the most recent legislative changes, including the 2026 amendments to the Law "On Personal Data" and the adoption of the Cybersecurity

Strategy for 2026–2030. This gap in the literature justifies the combined legal-and-technical approach adopted in the present study.

RESEARCH METHODOLOGY

In the course of the study, general scientific and special legal research methods were employed. In particular, the formal-legal and systemic analysis methods were used in analyzing regulatory-legal documents; statistical analysis and comparison methods were used in studying statistical data; and the comparative-legal method was used in comparing national experience with international practice. The source base of the study comprised the current legislative acts of the Republic of Uzbekistan, presidential decrees, the official reports of the "Cybersecurity Center" state unitary enterprise and the Central Bank's "CERT-CBU" center, as well as scholarly literature relevant to the topic.

RESULTS AND DISCUSSION

Legal Foundations of Ensuring Data Security

In the Republic of Uzbekistan, relations in the field of personal data protection are regulated by the Law "On Personal Data," adopted on July 2, 2019. Under this Law, any information recorded electronically, on paper, and/or on another physical medium that relates to a specific natural person or allows that person to be identified is regarded as personal data. The Law vests the state with the authority to maintain a unified state register of personal data databases, to establish the required level of their protection, and to issue mandatory instructions for eliminating violations of the law.

On March 26, 2026, significant amendments and additions were introduced to this Law, establishing a mandatory requirement to store biometric and genetic data, as well as the data of users of telecommunication operators' services, within the territory of the republic. Such data may be processed abroad only where the foreign state is recognized as ensuring an adequate level of protection or where contractual guarantees consistent with international standards are in place. This approach reflects the strengthening principle of data localization and is consonant with the experience of the European Union's General Data Protection Regulation (GDPR).

On March 10, 2026, a Presidential Decree approved the country's Cybersecurity Strategy for 2026–2030. Under the Strategy, dedicated cybersecurity units are to be established within the Ministry of Justice, the Ministry of Energy, and the Tax Committee; state bodies are to allocate budgetary and extra-budgetary funds for cybersecurity; and the State Security Service is to conduct regular work to identify deficiencies in national information systems. In addition, the "Cybersecurity Center" state unitary enterprise has developed a series of national standards (including O'zMSt 810:2025, O'zMSt 838:2026, and O'zMSt 840:2026) establishing requirements for data-leakage prevention systems, intrusion-detection tools, and anti-malware software, which serve to introduce unified technical requirements across both state and private organizations.

Statistical Trends in the Field of Cybersecurity

Official statistical data of recent years indicate that cyber offenses in the republic are increasing at a rapid pace. While in 2019 a total of 863 cybercrimes of 18 types committed through information technologies were recorded, in the most recent reporting year more than 58,000 such crimes of 62 types were identified — that is, over the course of five years the number of cybercrimes increased more than 68-fold, while the number of complaints filed by citizens and organizations on such matters grew 34-fold. During this period, cybercriminals misappropriated more than 1.9 trillion so'm from citizens, of which nearly 603 billion so'm relates to the most recent reporting year alone.

The dynamics of cyberattacks directed at the national internet segment likewise present an alarming picture: whereas in 2022 more than 4.5 million attacks were carried out against domestic resources, in the following year this figure exceeded 11 million, a 2.4-fold increase. At the same time, the number of confirmed cybersecurity incidents fell from 235 in 2022 to 158 in 2023 — a decrease of 32 percent — which attests to the growing effectiveness of prevention and monitoring systems. According to expert analysis, the principal causes of successful hacking attacks are the untimely elimination of vulnerabilities in web applications (in approximately 72 percent of cases) and the use of weak passwords (in approximately 25 percent of cases).

It is particularly notable that attacks directed at state information systems account for more than half of all attacks (approximately 52.7 percent), followed by the information and communication technology, finance, and energy sectors. This underscores the need to classify critical information infrastructure objects separately and to apply enhanced protective measures to them. Uzbekistan's rise from 93rd place in 2017 in the Global Cybersecurity Index (GCI) to a considerably higher position in subsequent assessments likewise indicates that reforms carried out in this direction are producing positive results, although the level achieved still remains considerably below that of the world's leading states.

Technical Mechanisms for Ensuring Data Security

In the process of digital information processing, data security is ensured along three principal organizational-technical directions: maintaining confidentiality (preventing unauthorized persons from accessing data), preserving integrity (protecting data from unauthorized alteration), and ensuring availability (guaranteeing the uninterrupted operation of the system). In practice, these tasks are addressed through encryption algorithms, two-factor authentication, intrusion detection and prevention systems (IDS/IPS), backup-copying systems, and firewalls.

The practice of implementing international standards at the level of state bodies in Uzbekistan is also expanding. In particular, the Ministry of Justice has introduced the ISO/IEC 27001 international information security management system standard, which has been certified by an internationally accredited body. Extending this practice to other state bodies and large organizations would help bring information-protection processes into conformity with international requirements and foster a culture of information security among staff. At the same time, the "CERT-CBU" cybersecurity center within the Central Bank's structure performs a coordinating function in preventing fraudulent operations in banking and payment systems and in detecting and promptly responding to cybersecurity threats, reflecting the emergence of a sector-specific oversight model within the financial sector.

At the same time, experts particularly emphasize problems such as the shortage of qualified cybersecurity personnel, the absence of developed internal information-

security rules in many organizations, and the commissioning of new information systems without adequate testing. These shortcomings ultimately heighten the risk that vulnerabilities within the system will lead to the loss of the personal data of citizens and organizations.

PROBLEMS AND PROPOSALS

On the basis of the analysis conducted, the following proposals have been developed:

1) to expand the system for training qualified personnel in information security in state bodies and educational institutions, including by incorporating applied cybersecurity modules into the curricula of specialized technicums and colleges;

2) to establish, through strict legislative regulation, a mandatory security assessment for all state information systems prior to their launch;

3) to encourage the phased introduction of international information security standards such as ISO/IEC 27001 within organizations;

4) to establish ongoing public-awareness initiatives aimed at improving citizens' digital literacy, in particular their ability to use complex passwords and recognize phishing attacks;

5) to further develop separate, enhanced monitoring and rapid-response systems for critical information infrastructure objects.

Conclusion

In conclusion, ensuring data security in the process of digital information processing is becoming an inseparable part of the construction of a modern rule-of-law state. In the Republic of Uzbekistan, the legal-regulatory framework in this field has been considerably improved in recent years: legislation on the protection of personal data has been strengthened, a national cybersecurity strategy has been adopted, and unified national standards for technical protection tools have been developed. At the same time, statistical indicators showing the rapid growth in the number of cybercrimes and cyberattacks confirm the need to further strengthen existing protection systems. Only through the harmonized implementation of legal, organizational, and technical measures, together with the enhancement of personnel capacity and the expansion of the

population's digital literacy, can a sustainable level of data security be achieved in the process of digital information processing.

REFERENCES:

1. Law of the Republic of Uzbekistan "On Personal Data" ["Shaxsga doir ma'lumotlar to'g'risida"gi Qonun], No. O'RQ-547, July 2, 2019.

2. Decree of the President of the Republic of Uzbekistan "On Approving the Cybersecurity Strategy of the Republic of Uzbekistan and Improving the System for Preventing Cybercrime," No. PF-38, March 10, 2026.

3. "Cybersecurity Center" State Unitary Enterprise. Collection of National Standards in the Field of Cybersecurity (O'zMSt 810:2025, O'zMSt 816:2025, O'zMSt 838–841:2026). Tashkent, 2026.

4. Central Bank of the Republic of Uzbekistan, "CERT-CBU" Cybersecurity Center. Information Digest on Activities Carried Out in 2024. Tashkent, 2025.

5. Gulyamov, S.S., Saidov, A.H. (2020). Problems and Prospects of Legal Regulation in the Digital Economy [Raqamli iqtisodiyotda huquqiy tartibga solish muammolari va istiqbollari]. Tashkent: TSUL Publishing House.

6. Maxkamova, M. (2025). Comparative Analysis of Personal Data Management: Uzbekistan and International Standards [Shaxsiy ma'lumotlarni boshqarishning qiyosiy tahlili]. Society and Innovations [Jamiyat va innovatsiyalar], Special Issue 09, pp. 84–91.

7. Legal Analysis of the Law of the Republic of Uzbekistan "On Personal Data" [O'zbekiston Respublikasining "Shaxsga doir ma'lumotlar to'g'risida"gi qonunining huquqiy tahlili]. Yurisprudensiya, 2026, No. 1 (vol. 6), pp. 132–144.

8. Legislation on the Protection of Personal Data in the Digital Environment: Foreign Experience and National Prospects [Raqamli muhitda shaxsga doir ma'lumotlarni himoya qilish sohasidagi qonunchilik]. Yurisprudensiya, 2026, No. 1 (vol. 6), pp. 145–155.

9. Rajabov, O.O. (2022). The Role of Cybersecurity in the Law Enforcement Bodies of the Republic of Uzbekistan. Uzbekistan–China: Development of Cultural, Historical, Scientific and Economic Relations, vol. 2, Special Issue, pp. 522–526.

10. Cybercrimes in Uzbekistan Increased 9.1-fold in 2024 [2024-yilda O'zbekistonda kiberjinoyatlar 9,1 barobarga oshdi]. Spot.uz, May 29, 2025.

11. Analysis of the Dynamics of Cyberattacks on Uzbekistan's Internet Segment [O'zbekiston internet segmentida kibertajovuzlar dinamikasi tahlili]. Spot.uz, February 13, 2024.

12. Annual Cybersecurity Report 2021 [2021-yilgi kiberxavfsizlik yillik hisoboti]. Spot.uz, March 3, 2022.

13. European Union. Regulation (EU) 2016/679 of the European Parliament and of the Council on the Protection of Natural Persons with regard to the Processing of Personal Data (General Data Protection Regulation). Official Journal of the European Union, L 119, 2016.

14. Council of Europe. Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS No. 108), 1981.

15. ISO/IEC 27001:2013. Information Technology — Security Techniques — Information Security Management Systems — Requirements. International Organization for Standardization, 2013.