THE FORMATION AND DEVELOPMENT HISTORY OF THE LEGAL FOUNDATIONS OF INFORMATION SECURITY POLICY IN THE REPUBLIC OF UZBEKISTAN

Shokirov Boburjon
Student of the faculty of law, Fergana state university
ORCID ID 0009-0009-7151-6294
https://doi.org/10.5281/zenodo.15623269

Annotation

With the development of information technologies in the Republic of Uzbekistan, the issue of ensuring information security has become increasingly relevant. As a result of the rise in cyberattacks, there emerged a need to improve the legal and political foundations of information security. This article analyzes how the categories of information security are reflected in the legislation of Uzbekistan, the main directions of state policy, and the regulations related to the protection of information resources and systems. The article also examines the national strategies of the Republic of Uzbekistan on information security, the powers of state bodies in this area, and the reforms aimed at strengthening cybersecurity. In addition, based on international experience, proposals are developed to improve the effectiveness of information security in the country.

Keywords

Information security, legal foundations, information technologies, cybersecurity, information systems, legal and regulatory documents, information policy.

Introduction

Currently, the development of information technologies is affecting all aspects of human life. The digital economy, e-government systems, online banking services, cloud computing technologies, and other innovative approaches are rapidly penetrating various sectors of society. The widespread use of information technologies, in turn, has made the issue of ensuring information security a pressing concern.

The Republic of Uzbekistan, as one of the countries accelerating the process of digital transformation, is paying great attention to ensuring information security. In recent years, the e-government system has developed in the country, public services have been transferred to electronic formats, online payment systems have been widely introduced in the banking and financial sectors, and the level of information technology use in the industrial and educational spheres has increased. At the same time, this process has led to the emergence of various threats.

Information security is important not only for the protection of personal data, but also for ensuring the stable functioning of state information systems, business entities, and institutions. With the expansion of digital infrastructure, the increase in cybercrimes, unauthorized access to information, fraud, and attacks through malicious software has created the need to develop and strengthen information security policy.

From this point of view, the development and improvement of the legal foundations for ensuring information security in the Republic of Uzbekistan is a pressing issue. This study aims to analyze the existing legal and regulatory documents related to information security, examine international experience, and develop proposals for the further development of national legislation.

The threats arising from information technologies and digital transformation have made ensuring information security an integral part of the national security strategy of the Republic of Uzbekistan. If modern information systems are not protected against cyberattacks, this can lead not only to economic losses, but also to negative impacts on the political and social stability of the state. Therefore, it is necessary to develop legal and institutional mechanisms aimed at strengthening information security and align them with international standards.

Literature review

The issue of ensuring information security is a global problem, and various scientific sources and practical studies need to be analyzed in order to examine it from legal, technical, and organizational perspectives. This section explores literature, regulatory-legal documents, scientific articles, and analytical materials at both national and international levels.
In the Republic of Uzbekistan, there are a number of laws and regulatory documents aimed at ensuring information security, which include the following:

- The Law "On the Principles and Guarantees of Information Freedom" – this law is based on the fundamental principles of ensuring access to information, the use of information resources, and their protection in Uzbekistan.
- The Law “On Electronic Government” – one of the main legal documents governing the digitalization of public services and the control of data exchange.
- The Law “On Electronic Digital Signature” – defines the mechanisms for legalizing electronic document circulation and ensuring authentication.

• The draft Law "On Cybersecurity" – this document covers measures to combat cybercrime, protect information systems, and strengthen information security in Uzbekistan.

In addition, the decisions and decrees of the President and the Government of the Republic of Uzbekistan, such as the "Digital Uzbekistan – 2030" strategy, also serve as important legal foundations for the development of information security.

International experience plays a significant role in the field of information security. In this regard, the following sources are analyzed:

• ISO/IEC 27001 Information Security Management Standard – this international standard is one of the main documents for forming and developing information security policies for organizations and government institutions.

• The European Union's GDPR (General Data Protection Regulation) – one of the most advanced approaches to personal data protection, this regulation defines the principles for managing and securing data.

• The U.S. NIST (National Institute of Standards and Technology) cybersecurity guidelines – include concrete methods for protecting information systems and preventing attacks.

• Recommendations from the UN, ITU (International Telecommunication Union), and other international organizations on information security – strategies aimed at shaping cybersecurity policy and promoting the development of information technologies on a global scale are analyzed.

Methods

The methods used within the framework of this study made it possible to comprehensively assess the current state of information security**.** Theoretical analysis – by examining existing laws, regulatory documents, and scientific research, current problems were identified. Comparative legal analysis – by comparing the experiences of foreign countries with the conditions in Uzbekistan, effective approaches and solutions not yet implemented locally were identified. Empirical research – real-life cases and examples were analyzed to study how legal frameworks function in practice. Expert interviews and surveys – through the opinions and feedback of specialists in the field, relevant problems and proposals for their resolution were gathered. Statistical analysis – threats and trends related to information security were studied in depth. These methods enabled a thorough analysis of the problems in the field of information security and led to the development of concrete proposals for improvement.

During the research process, interviews are conducted with specialists working in the field of information security, legal experts, IT professionals, and representatives of government bodies. Additionally, special surveys are organized to determine the level of public awareness regarding information security.

Discussion and results

The rapid development of information and communication technologies (ICT) in Uzbekistan and their widespread integration into public administration and service delivery systems have made issues related to information security increasingly relevant. The growing number of cyberattacks and intensified hacker activities have created a pressing need to strengthen the legal and political foundations for ensuring information security and to develop them in line with modern requirements.

To date, various challenges have arisen in the process of formulating and implementing state information security policy. These contradictions include the following:

1. The balance between the growing demand for access to information and ensuring information security.

The public's desire for free access to information is steadily increasing. In particular, document exchange over the internet, electronic payments, the provision of information to citizens by state and self-governing bodies, as well as the expanding scope of public and local government services, are becoming more widespread. As information technologies evolve, large volumes of data are disseminated through various technical means, especially mobile devices.

At the same time, state authorities must not only guarantee citizens' freedom to access information but also create conditions to protect their other legal rights and interests. If the state fails to effectively coordinate information flows, this may lead to problems in areas such as the inviolability of personal life and the protection of national interests, ultimately posing a threat to national security.

2. Increasing complexity in controlling information flows under globalization.

The rapid advancement of information technologies and the process of globalization are making the international information exchange system increasingly complex. This situation limits the ability of the state to control

information flows, which in turn may threaten national sovereignty and territorial integrity.

"As the process of globalization continues to intensify worldwide, political measures aimed at protecting the national interests of various actors are also increasing. Without effective state control over the collection, use, and dissemination of information, constitutional rights of citizens may not be adequately protected, and the prevalence of cybercrime may rise," notes Pastukhova [1].

Renowned scholar N.N. Kunyaev commented on this issue as follows: "The development of the global information space creates a need for new legal and organizational measures to protect the state and its citizens from threats posed by foreign states or terrorist organizations" [2].

In response, the Government and Parliament of Uzbekistan have adopted a number of laws and regulatory documents to ensure information security and combat growing cyber threats, based on international standards and national interests.

Among these is the Law "On Telecommunications" adopted on August 20, 1999, which serves as one of the key legal foundations for information security. According to Article 326 of this law: "Individuals and legal entities that damage telecommunications networks or connect to them without authorization shall be held liable in accordance with the law" [3].

In addition, the Law "On the Principles and Guarantees of Freedom of Information" adopted on December 12, 2002, is aimed at ensuring information security in the country. Article 15 of this law outlines the following legal foundations for ensuring information security:

- Implementation of economic, political, and organizational measures to eliminate threats to security in the information sphere;
- Protection of state secrets and prevention of unauthorized use of state information resources;
- Prevention of the dissemination of information that promotes violence or propaganda against the constitutional order;
- Legal measures against the spread of information aimed at promoting terrorism and extremism [4].

The Government of Uzbekistan continues to develop new laws and programs based on international experience to ensure information security. Alongside the development of digital technologies, the formulation of modern strategies in the field of information security remains a priority direction.

In the Republic of Uzbekistan, the rapid development of information technologies has made the issue of ensuring information security increasingly urgent. One of the key laws adopted in this area is the Law "On Informatization," approved on December 11, 2003. Article 19 of this law, titled "Protection of Information Resources and Information Systems," sets out the following core principles and objectives:

- Ensuring the information security of individuals, society, and the state;
- Preventing the leakage, theft, loss, distortion, blocking, falsification, and unauthorized use of information resources;
- Preventing illegal actions such as destruction, blocking, copying, or misrepresentation of information, as well as unauthorized interference with information systems;
- Protecting state secrets and confidential information contained in information resources [5].

This law plays an important role in shaping Uzbekistan's information policy. Chapter 4 of the law outlines the state's informatization policy as follows:

- Expanding the opportunities for every citizen to exercise their constitutional rights to freely receive and disseminate information;
- Ensuring free access to information resources;
- Forming a national information system by developing and improving information resources, technologies, and systems based on international standards;
- Creating favorable conditions for the use of the Internet and international information networks [6].

Additionally, the Law "On Electronic Document Management," adopted on April 29, 2004, is another important legal document related to ensuring information security. Article 17 of this law states the following provision regarding the protection of electronic documents:

"To prevent harm to participants in electronic document circulation or to other legal and natural persons, electronic documents shall be protected in accordance with procedures established by law" [7].

Another law aimed at ensuring information security is the Law "On the Protection of Information in Automated Banking Systems," adopted on April 4, 2006. Article 5 of this law provides for the following:

- Development of rules for information protection and ensuring compliance with them;

• Implementation of information security measures in automated banking systems and establishment of oversight over these processes;

• Organization of specialized information protection services [8].

Among the key legal documents related to ensuring transparency of information in the country is the Law "On the Openness of Activities of State Authorities and Administration," approved on May 5, 2014. According to Article 6 of this law, access to information about the activities of state bodies is carried out in accordance with legal restrictions. Specifically, if the information includes state secrets or other confidential data protected by law, its disclosure may be limited [9].

Furthermore, the Law "On Personal Data," adopted on July 2, 2019, established an essential legal foundation for the protection of personal information. Article 28 of this law outlines the following requirements:

• Disclosure or dissemination of personal data without the subject's consent or without a legal basis is prohibited;

• Confidentiality of personal data is a mandatory requirement, and any person or organization using such data must comply with these rules;

• Any person or organization in possession of personal data must not disclose or disseminate this data to third parties [10].

The above-mentioned laws form the legal basis for ensuring information security, protecting personal data, and enhancing the security of state information systems in Uzbekistan.

Conclusion

Information security holds significant importance as a component of the national security of the Republic of Uzbekistan. In recent years, legislation adopted by the government has served to strengthen the national information security system. However, the acceleration of globalization and technological advancement has led to the emergence of new cyber threats. Therefore, it is essential to further improve the legal framework for ensuring state-level information security, expand international cooperation, and implement modern technologies for protecting information systems.

Although the national legal framework has established certain foundations for ensuring information security, alignment with international standards remains necessary. In particular, updating existing legislation on personal data protection, the development of the digital economy, and the prevention of cybercrime is of vital importance.

International experience demonstrates that ensuring information security requires the establishment of mandatory standards, strong cooperation between the public and private sectors, and a high level of public awareness regarding cybersecurity. In this regard, international frameworks and instruments such as ISO/IEC 27001, the NIST Cybersecurity Framework, and the GDPR play a key role.

While Uzbekistan's legal foundation for information security defines clear concepts, its practical application and monitoring systems need to be further strengthened. In particular, it is necessary to enhance the qualifications of law enforcement agencies and IT specialists and to develop comprehensive strategies to combat cybercrime.

Based on the findings of this study, the following recommendations are proposed:

- ✓ **Strengthening the Legal Framework** – Develop new draft laws on information security and harmonize existing legislation with international standards.
- ✓ **Improving Cybersecurity Literacy Among Citizens** – Introduce cybersecurity courses in schools and higher education institutions and conduct public awareness campaigns through mass media.
- ✓ **Developing a National Information Security Strategy** – Adopt a long-term, state-level strategy aimed at ensuring information security across the country.
- ✓ **Enhancing Public–Private Sector Cooperation** – Involve private sector actors in cybersecurity regulation processes and provide training to improve their competencies.

Strengthening Mechanisms to Combat Cybercrime – Develop specific legal measures against cybercrime and ensure their effective implementation in practice.

References:

1. Pastukhova, N.B. State Sovereignty in the Era of Globalization // Journal of Russian Law, 2006. – No. 5. – [Electronic resource] – SPS Garant.
2. Kunyaev, N.N. Information Security as an Object of Legal Regulation in the Russian Federation // Legal World, 2008. – No. 2. – [Electronic resource] – SPS Consultant Plus.
3. Law of the Republic of Uzbekistan "On Telecommunications". August 6, 2024 – https://lex.uz/docs/-7283071

4. Law of the Republic of Uzbekistan “On the Principles and Guarantees of Freedom of Information”. December 12, 2002, No. 439-II – https://lex.uz/docs/-52268
5. Law of the Republic of Uzbekistan “On Informatization”. Adopted on December 11, 2003, No. 560-II // Bulletin of the Oliy Majlis of the Republic of Uzbekistan, 2004, No. 1–2, Article 10.
6. Law of the Republic of Uzbekistan “On Informatization”. December 11, 2003 // National Database of Legislation, April 21, 2021, No. 03/21/683/0375 – https://lex.uz/docs/-83472
7. Law of the Republic of Uzbekistan “On Electronic Document Circulation”, No. 611-II. April 29, 2004 – https://lex.uz/docs/-165079
8. Law of the Republic of Uzbekistan “On the Protection of Information in the Automated Banking System”. April 4, 2006 – https://lex.uz/ru/docs/-4763600
9. Law of the Republic of Uzbekistan “On the Openness of Activities of Public Authorities and Administration”, No. 369. Adopted on May 5, 2014 – https://lex.uz/docs/2381133
10. Law of the Republic of Uzbekistan “On Personal Data”, No. O‘RQ-547. July 2, 2019 – https://lex.uz/docs/-4396419