International Journal of Scientific Trends- (IJST)
ISSN: 2980-4299
Volume 5, Issue 5, May - 2026
Website: https://scientifictrends.org/index.php/ijst
Open Access, Peer Reviewed, Scientific Journal

Data Breaches and Cyberattacks as a Systemic Threat to Information Security in the Context of Digital Transformation

Khusanova Gulbahor
Master's Student of Tashkent State University of Law,
Media Law Specialization

Abstract
In the context of the rapid development of digital technologies, accompanied by a significant expansion in the scale of collection, storage, and processing of personal data, the issue of ensuring their confidentiality and security is becoming particularly relevant and is emerging as one of the key challenges of the modern information society. This article examines the essential characteristics of data breaches and cyberattacks, provides a comprehensive analysis of their causes and consequences, and also studies a cyber incident that occurred in the Republic of Uzbekistan in 2026. Special attention is paid to identifying systemic vulnerabilities and developing practice-oriented approaches to improving the level of information security of consumers of digital services.

Keywords: Information security, data breach, cyberattacks, personal data, digital transformation, cyber threats, information protection, cyber incidents, data confidentiality, consumers of digital services, government information systems.

Introduction

The digital transformation of modern society is accompanied by the active implementation of information and communication technologies in various spheres of life, including public administration, economic processes, and social communications, which leads to the formation of large-scale arrays of personal data subject to storage and processing in a digital environment. This process, on the one hand, contributes to increasing the efficiency of institutional functioning, but on the other hand, objectively increases risks associated with possible data compromise and violation of the confidentiality of consumers' information.

In the context of the continuous growth of cyber threats, data breaches and cyberattacks are transforming into one of the key problems of modern information security, having a significant impact not only on the stability of technical systems but also on the level of trust of consumers in digital services.

In the Republic of Uzbekistan, information security issues are of particular importance in connection with the active implementation of the state's digital transformation strategy. The development of e-government, digital public services, and integrated information systems requires

strengthening legal and organizational mechanisms for ensuring the information security of consumers.

Theoretical Foundations of the Study

A data breach is understood as the process of unauthorized disclosure or dissemination of confidential information arising as a result of the compromise of information system security. Cyberattacks represent deliberate actions aimed at gaining unauthorized access to data, its modification, or destruction.

According to the research of Yuldashev A.E., information security is considered an integral part of national security of the state, emphasizing the need to create a unified system for its provision in the Republic of Uzbekistan.

Among the key causes of data breaches are vulnerabilities in software, insufficient infrastructure security, the human factor, as well as deliberate actions of malicious actors.

Analysis of a Cyber Incident in Uzbekistan

In Uzbekistan, the legal foundations for data protection are enshrined in the Law of the Republic of Uzbekistan "On Personal Data," which regulates the procedure for processing personal information and the obligations of database operators. The laws "On Informatization" and "On E-Government" are also of significant importance, aimed at regulating digital processes and the functioning of state information systems. The implementation of the "Digital Uzbekistan – 2030" strategy further strengthens the relevance of cybersecurity issues.

Despite the implementation of a set of measures aimed at ensuring the protection of personal data, the current information security system still contains a number of vulnerabilities caused by both technical and organizational-management factors. According to the research results of specialist Z.K. Nazarova from the Center for Digital Economy Research, in 2023, 1,186 vulnerabilities were identified in 677 web resources in the Republic of Uzbekistan, with a significant portion of these shortcomings found in government information systems. These indicators demonstrate the presence of persistent systemic risks in the national digital infrastructure and confirm the need for further improvement of technical protection mechanisms, security auditing, and continuous monitoring of state information resources.

In addition, at the beginning of 2026, a cyber incident was recorded in the Republic of Uzbekistan related to the leakage of personal data of users and consumers of state digital services. Initially, media reports circulated information about the compromise of millions of records; however, it was later established that the scale of the breach amounted to about 60,000 records.

At the same time, these records represented individual data elements rather than unique users and could include such information as names, phone numbers, and other personal data. This incident affected the information systems of state structures and demonstrated the presence of vulnerabilities that could be exploited by attackers to gain unauthorized access to consumer information.

Consequences of Data Breaches

Following the incident, prompt measures were taken to prevent further unauthorized access attempts, strengthen the technical protection of information systems, and update the security

mechanisms of the OneID platform, as well as expand users' capabilities to control the transfer of personal data. At the same time, the incident caused significant public resonance, due to the initial dissemination of information about a possible breach involving millions of citizens' data, as a result of which, even after clarification of the scale of the incident, the level of trust in digital government services was partially undermined.

Overall, this cyber incident demonstrated that even relatively limited data breaches can lead to increased fraud risks, reduced trust in digital institutions, and the need for accelerated modernization of state information system protection mechanisms.

Data breaches have a complex negative impact on various levels of the social system. At the individual level, they create risks of fraud, including phishing attacks and digital identity theft. At the level of organizations and the state, the consequences are expressed in reputational losses and a decrease in trust from consumers and users.

In the context of the development of analytical technologies, data breaches can be used for modeling consumer behavior, which increases potential threats.

Causes and Vulnerabilities

The key causes of data breaches are deficiencies in the information security system, including lack of regular software updates, weak access control, API vulnerabilities, and low personnel training levels.

According to Ross Anderson, most vulnerabilities are associated not so much with technical defects as with errors in system design and operation, which emphasizes the importance of organizational factors.

According to Yuldashev A.E., a significant problem remains the fragmentation of existing information protection mechanisms, where individual subsystems operate separately and do not form a holistic cybersecurity model.

Measures to Ensure Information Security

Based on the conducted analysis, it can be assumed that preventing data breaches requires a comprehensive approach combining technological and organizational measures.

At the state level, it is necessary to introduce information security standards and develop cyber threat monitoring systems. Organizations are recommended to apply data encryption, multi-factor authentication, and train employees in secure handling of consumer information.

According to NIST recommendations, an effective cybersecurity system should be based on continuous monitoring, risk management, and rapid incident response.

Conclusion

In recent years, Uzbekistan has achieved significant progress in the field of cybersecurity, reflecting a targeted state policy aimed at implementing digital technologies in various sectors of the economy and ensuring information protection in the digital environment. The adoption of the laws "On Personal Data" and "On Cybersecurity" has become an important stage in forming a regulatory framework aimed at protecting personal information, reducing cyber threats, and strengthening the resilience of national information systems.

At the same time, the ongoing activity of cyberattacks indicates the presence of a number of problems, including a shortage of qualified specialists, vulnerabilities in public and private digital systems, insufficient coordination between responsible structures, low levels of digital literacy among users, and the need for additional investment in the development of information security infrastructure.

Thus, data breaches and cyberattacks remain among the most significant threats in the context of digital transformation, while the experience of Uzbekistan shows that even relatively small incidents can reveal systemic weaknesses in the digital ecosystem. In this regard, effective counteraction to these risks is possible only through the implementation of a comprehensive approach combining technical, organizational, and legal measures, as well as being oriented toward the long-term development of a national cybersecurity system and the protection of consumer interests.

References

1. Law of the Republic of Uzbekistan “On Personal Data” No. ZRU-547 dated July 2, 2019.
2. Law of the Republic of Uzbekistan “On Informatization” No. ZRU-560-II dated December 11, 2003.
3. Law of the Republic of Uzbekistan “On E-Government” No. ZRU-395 dated December 9, 2015.
4. Law of the Republic of Uzbekistan “On Cybersecurity” No. ZRU-764 dated April 15, 2022.
5. Decree of the President of the Republic of Uzbekistan on the Development Strategy “Digital Uzbekistan – 2030”.
6. Yuldashev A.E. On improving the system of ensuring information security in the Republic of Uzbekistan.
7. Nazarova Z.K. Analysis of the level of cybersecurity development in Uzbekistan.
8. IBM Security. Cost of a Data Breach Report 2024. — Armonk: IBM Corporation, 2024.
9. ISO. ISO/IEC 27001:2022 Information Security, Cybersecurity and Privacy Protection — Information Security Management Systems — Requirements. — Geneva: International Organization for Standardization, 2022.
10. Kaspersky. Cybersecurity Trends Report 2024. — Moscow: Kaspersky Lab, 2024.
11. Daryo.uz. Not 15 million, but 60 thousand: clarification on the data breach of Uzbekistan citizens. — 2026.
12. The Cyber Express. Uzbekistan cyberattack limited to 60K records. — 2026.
13. Anderson Ross. Security Engineering: A Guide to Building Dependable Distributed Systems. 2nd ed. — Indianapolis: Wiley Publishing, 2008.
14. NIST. Framework for Improving Critical Infrastructure Cybersecurity. Version 1.1. — Gaithersburg: National Institute of Standards and Technology, 2018. National Institute of Standards and Technology, 2018.