УДК 34.096
МРНТИ 10.19.01

DOI: https://doi.org/10.37788/2025-1/168-172

O.B. Dubovitskaya[1*]
[1]Toraygirov University, Kazakhstan
[*] (e-mail: o.b.d.1970@mail.ru)

On the Issue of Information Security in the Republic of Kazakhstan

Abstract

The main problem: The risk of damage or loss of information in modern information systems requires effective measures to ensure information security, which is especially important for the Republic of Kazakhstan in the face of growing digital threats.

Objective: To analyze the legal and organizational measures for information security in Kazakhstan, with a focus on the role of the Ministry of Digital Development in protecting critical information and personal data.

Methods: A qualitative analysis of regulatory documents and practices in the field of information security was used, including measures for risk management and threat monitoring.

Results and their significance: Key measures for ensuring information security were described, including the establishment of incident response centers and improvements to the legal framework in the field of information security, contributing to the protection of personal data and critical infrastructure in Kazakhstan.

Keywords: information security, cybersecurity, information security policy, personal data, legislation of the Republic of Kazakhstan.

Introduction

With the development of information and communication technologies (ICT), there has been a significant increase in the volume of data being processed, stored, and transmitted through various systems and networks. At the same time, new threats have emerged that can lead to data leakage, distortion, or destruction. Modern technologies, despite their undeniable advantages in accelerating information exchange and improving the quality of interaction between people, also create new opportunities for malicious actors seeking unauthorized access to valuable data, disrupting the operation of critical systems, and causing harm to governmental and commercial structures. In this context, information protection, its integrity, and security have become vital tasks for society.

Information security covers not only protection from external threats, such as hacking attacks, viruses, phishing, and other forms of cybercrime, but also issues related to ensuring the confidentiality, integrity, and availability of data. The threat of data leakage or distortion can have a devastating impact on the functioning of organizations, decrease trust in public and private institutions, and even jeopardize the safety and well-being of citizens.

The issues of information security are of particular importance for the Republic of Kazakhstan, where various sectors of the economy, including digitalization of government management, the banking sector, and commercial organizations, are actively developing. All of these areas are actively implementing the latest ICT to improve efficiency and service quality; however, with this process come growing risks. In the context of global digital transformation, information protection has become an integral part of national security. Losses resulting from breaches in the security of information systems can cause not only financial damage but also harm the country’s reputation on the international stage.

Cyber threats are becoming increasingly sophisticated and diverse, requiring the state, organizations, and individual users to continuously update their knowledge and skills in information protection. This is why ensuring information security is one of the priorities of Kazakhstan's national policy. This includes not only improving legislation related to data protection but also developing the information security infrastructure, training specialists, and conducting large-scale awareness campaigns to educate citizens about the risks and safety measures in the digital space.

Thus, information security issues hold a prominent place in the strategic tasks of societal and economic development in the Republic of Kazakhstan. Given the rapid growth of technologies, it is

essential to effectively respond to challenges and threats, ensuring the protection of vital information at all levels – from personal data to information critical for the functioning of state and private entities.

Materials and Methods

The study utilized a qualitative analysis of legal documents, policies, and practices related to information security in Kazakhstan, focusing on the role of the Ministry of Digital Development, Innovations, and Aerospace Industry, including risk management, the implementation of national cybersecurity strategies, and the protection of critical information and personal data.

Results

Information security can be understood as the protection of information and the supporting infrastructure from deliberate or accidental impacts, whether artificial or natural, that may harm the owners or users of the information, as well as harm the rights and interests of individuals, society, and the state in the information sphere from real and potential threats. It is information security that ensures sustainable development and informational independence, which is a critical factor for any state.

Information security involves maintaining the confidentiality, integrity, and availability of information. Information security is achieved through the implementation of a set of control measures, such as policies, processes, procedures, organizational structures, hardware, and software.

Discussion

The Information Security Policy (ISP) represents a set of preventive (precautionary) measures for the protection of information. This applies to both restricted-access information (i.e., classified information) and information processes, and consists of a set of requirements addressed to users of the information systems of the Ministry of Digital Development, Innovations, and Aerospace Industry of the Republic of Kazakhstan, as well as its agencies and subordinate organizations in their activities. It should be noted that the ISP is developed based on the Law of the Republic of Kazakhstan "On Informatization" dated November 24, 2015, and the Government Resolution of the Republic of Kazakhstan "On Certain Measures for Ensuring Information Security in the Republic of Kazakhstan" dated September 14, 2004 [1].

In terms of the Ministry of Digital Development, Innovations, and Aerospace Industry of the Republic of Kazakhstan's specific activities in the field of information security, these include:

– Regulation of the ".KZ" domain space;
– Coordination of critical infrastructure;
– Protection of personal data;
– State control in the field of information security (IS);
– Testing and technical regulation in the field of IS;
– Accreditation of certification centers [2].

The ISP applies to all structural units and infrastructure of the Ministry, its agencies, and organizations under its jurisdiction, and is mandatory for all employees and officials. Moreover, the provisions of the ISP also apply to organizations that interact with the Ministry, its agencies, and subordinate organizations as suppliers and/or consumers of information and services, and may be used in internal regulatory, methodological documents, and contracts [3].

To further improve the situation in the field of information security and personal data protection, the Ministry of Digital Development, Innovations, and Aerospace Industry of the Republic of Kazakhstan (hereinafter referred to as the Ministry) has initiated the delegation of powers to the Committee on Information Security regarding the protection of personal data, conducting audits, and inspections of information system owners processing personal data.

Additionally, test laboratories in the field of information security have been created for the study of malicious code, a national coordination center for information security has been launched, a private computer security incident response service (CERT) has been established, and seven operational information security centers (SOS) have been set up, among other initiatives.

Risk analysis in information security is conducted jointly with the inventory and classification of the information assets of the Ministry, its agencies, and organizations under its jurisdiction. The basis for defining and assessing the consequences of information security risks lies in the information security requirements for information assets and information set forth by the ISP.

Based on the results of risk assessments, priorities are determined for managing and implementing elements of information security, the actions of management regarding the handling of relevant risks, and decisions about expenses for activities stemming from the potential damage caused by a breach of information security [4].

Information intended for publication in public access systems must comply with the legislative requirements of the Republic of Kazakhstan. Protection of critical information must be ensured during its collection and storage. Systems providing the ability to electronically publish information, provide feedback, and input information must be under proper control [4].

To monitor the implementation of ISP requirements, detect unauthorized actions in information processing, and respond promptly to identified threats, regular monitoring and registration of information security events in information systems in the Republic of Kazakhstan are carried out. All relevant legal requirements for monitoring information security events must strictly comply with the legislative requirements of Kazakhstan [5].

Legislative measures in the field of information security aim to create a legal framework in the country that organizes and regulates the behavior of subjects and objects of information legal relations, as well as determining responsibility for violations of established norms.

In the Republic of Kazakhstan, the legislative and regulatory framework in the field of information security includes:

– The Criminal Code of the Republic of Kazakhstan;
– The Code of the Republic of Kazakhstan on Administrative Offenses;
– The Law of the Republic of Kazakhstan "On National Security";
– The Law of the Republic of Kazakhstan "On Informatization";
– The Law of the Republic of Kazakhstan "On State Secrets";
– The Law of the Republic of Kazakhstan "On Personal Data and Their Protection";
– The Law of the Republic of Kazakhstan "On Electronic Documents and Electronic Digital Signature";
– The Law of the Republic of Kazakhstan "On Communication";
– Unified Requirements in the Field of Information and Communication Technologies and Information Security (Government Resolution of the Republic of Kazakhstan No. 832 dated December 20, 2016);
– The Concept of Cybersecurity ("Cyber Shield of Kazakhstan").

The basis for the security of IT infrastructure is the triad of services—confidentiality, integrity, and availability. In this context:

– Confidentiality ensures that information can be read and interpreted only by authorized individuals and processes. An example would be an email message protected from being read by anyone other than the recipient;
– Integrity guarantees that information remains unchanged, accurate, and authentic. For example, measures that ensure an email message is not altered during transmission;
– Availability ensures that authorized users can access and work with the information assets, resources, and systems they need, with the required performance. An example might be access control and ensuring the bandwidth of an email service [6].

It should also be noted that methods used to ensure information security in information systems include:

– Prevention;
– Access management;
– Cryptography methods;
– Counteracting malicious software attacks;
– Regulation;
– Compulsion;
– Encouragement.

Conclusion

In conclusion, it can be confidently stated that information security is an integral element of modern society, covering a wide range of aspects, from personal data protection to ensuring national security. In the context of the rapid development of technologies and the widespread adoption of information and communication systems, information protection has gained particular significance. Threats from cybercriminals, terrorism, natural disasters, or even internal user errors are becoming increasingly complex and multifaceted, requiring a comprehensive approach to security issues.

Information security is not merely about protecting data from leaks or losses. It is about safeguarding the rights and interests of all participants in the information space – individuals, organizations, and the state as a whole. It is important to understand that information protection encompasses not only technical but also legal, organizational, and social aspects. An effective

information security system must consider all these components, as well as remain flexible and adaptable to rapidly changing conditions.

To ensure information security, it is necessary to develop a cohesive strategy that includes legislative initiatives, the development of specialized protection technologies, and raising awareness and education among the population. In the context of globalization and active interaction between countries, it is crucial for governmental bodies, private companies, and individual users to be able to operate in a secure digital environment without fear for the safety of their data and resources.

Special attention should be given to national security in the field of information technology. Modern threats, such as cyberattacks on critical infrastructure, can have far-reaching consequences for an entire country. Therefore, protecting information systems becomes a strategically important task for any state. Kazakhstan, like many other countries, is actively implementing measures to protect information, creating the necessary structures and systems to ensure a reliable and secure digital environment.

In conclusion, information security is a key factor in the sustainable development of society and the economy in the modern world. Technologies open new horizons, but at the same time, the number of threats to data and systems is growing. Only a comprehensive approach, including technical, legal, and organizational measures, can provide full information protection and create conditions for the safe use of digital technologies at all levels—from personal use to state governance.

THE LIST OF SOURCES

1 Постановление Правительства Республики Казахстан от 30 сентября 2011 г. № 1128 «О проекте Указа Президента Республики Казахстан «О Концепции информационной безопасности Республики Казахстан до 2016 года» (утвержден) // Электронная база нормативно-правовых актов «Параграф». [Электронный ресурс]. – URL: https://adilet.zan.kz/ rus/docs/P1100001128/history.

2 Официальный сайт Министерства цифрового развития, инноваций и аэрокосмической промышленности РК. [Электронный ресурс]. – URL: https://www.gov.kz/memleket/ entities/ mdai?lang=ru.

3 Махмутов А. Концепция национальной безопасности Казахстана в контексте современных внешнеполитических реалий // Материалы круглого стола «Внешнеполитические перспективы и новые концепты международной стратегии Ка- захстана». Институт мировой экономики и политики при Фонде Первого Президента Республики Казахстан – Лидера Нации. – 2012. – 12 марта.

4 Информация // Казахстан. Национальная энциклопедия. – Алматы: Қазақ энциклопедиясы, 2005. – Т. II. – ISBN 9965-9746-3-2. (CC BY-SA 3.0). [Электронный ресурс].– URL: https://commons.wikimedia.org/w/index.php?title=File:Kazakhstan_National_encyclopedia_(ru)_-_Vol_2_of_5_(2005).pdf&page=484.

5 Дмитриенко Т.А. Обеспечение информационной безопасности и развитие информационной инфраструктуры Республики Казахстан // Информационно- аналитический журнал «ANALYTIC». – 2003. – С. 12-14.

6 Жансултанова Э. Информационная безопасность. [Электронный ресурс]. – URL: https://www.zakon.kz/4931365-informatsionnaya-bezopasnost.html.

REFERENCES

1 Resolution of the Government of the Republic of Kazakhstan. (2011, September 30). On the draft decree of the President of the Republic of Kazakhstan "On the Concept of Information Security of the Republic of Kazakhstan until 2016" (approved). Retrieved from https://adilet.zan.kz/rus/docs/P1100001128/history [in Russian].

2 Ministry of Digital Development, Innovation, and Aerospace Industry of the Republic of Kazakhstan. Official website. Retrieved from https://www.gov.kz/memleket/entities/mdai?lang=ru [in Russian].

3 Makhmutov, A. (2012). The concept of national security of Kazakhstan in the context of modern foreign policy realities. Materials of the round table "Foreign Political Prospects and New Concepts of Kazakhstan's International Strategy". Institute of World Economy and Politics under the Fund of the First President of the Republic of Kazakhstan – Leader of the Nation, March 12.

4 Kazakhstan. National Encyclopedia. (2005). Vol. II. Almaty: Kazakh Encyclopedia. Retrieved from https://commons.wikimedia.org/w/index.php?title=File:Kazakhstan_National_encyclopedia_(ru)_-Vol_2_of_5_(2005).pdf&page=484 [in Russian].
5 Dmitrienko, T.A. (2003). Ensuring information security and developing information infrastructure in the Republic of Kazakhstan. Information and Analytical Journal "ANALYTIC", 12-14.
6 Zhansultanova, E. (n.d.). Information security. Retrieved from https://www.zakon.kz/4931365-informatsionnaya-bezopasnost.html [in Russian].

О.Б. Дубовицкая[1]
[1]Торайғыров университеті, Қазақстан

Қазақстан Республикасындағы ақпараттық қауіпсіздік мәселесі

Қазіргі ақпараттық жүйелерде ақпараттың зақымдалуы немесе жоғалуының қаупі ақпараттық қауіпсіздікті қамтамасыз ету үшін тиімді шараларды қажет етеді, бұл Қазақстан Республикасында цифрлық қауіп-қатерлердің өсуі жағдайында ерекше маңызды болып табылады.

Қазақстандағы ақпараттық қауіпсіздік бойынша заңдық және ұйымдастырушылық шараларды талдау, сондай-ақ, маңызды ақпарат пен жеке деректерді қорғауда Цифрлық даму министрлігінің рөлін зерделеу.

Ақпараттық қауіпсіздік саласындағы нормативтік құжаттар мен тәжірибелерді сапалық талдау жүргізілді, оның ішінде қауіп-қатерді басқару және мониторинг жүргізу шаралары қарастырылды.

Ақпараттық қауіпсіздікті қамтамасыз ету жөніндегі негізгі шаралар сипатталды, оның ішінде инциденттерге жауап беру орталықтарын құру және ақпараттық қауіпсіздік саласындағы заңнаманы жетілдіру, бұл Қазақстандағы жеке деректер мен критикалық инфрақұрылымды қорғауға ықпал етеді.

Кілт сөздер: ақпараттық қауіпсіздік, киберқауіпсіздік, ақпараттық қауіпсіздік саясаты, жеке деректер, Қазақстан Республикасының заңнамасы.

О.Б. Дубовицкая[1]
[1]Торайгыров университет, Казахстан

О вопросе информационной безопасности в Республике Казахстан

Риск повреждения или утраты информации в современных информационных системах требует эффективных мер по обеспечению информационной безопасности, что особенно важно для Республики Казахстан в условиях роста цифровых угроз.

Анализ правовых и организационных мер информационной безопасности в Казахстане, с фокусом на роль Министерства цифрового развития в защите критической информации и персональных данных.

Использован качественный анализ нормативных документов и практик в области информационной безопасности, включая меры по управлению рисками и мониторингу угроз.

Описаны ключевые меры по обеспечению безопасности информации, включая создание центров реагирования на инциденты и улучшение законодательства в области информационной безопасности, что способствует защите личных данных и критической инфраструктуры в Казахстане.

Ключевые слова: информационная безопасность, кибербезопасность, политика информационной безопасности, персональные данные, законодательство Республики Казахстан.

Date of receipt of the manuscript to the editor: 2025/01/06