Қоғам & Дәуір

Қазақстан Республикасы Президенті жанындағы Қазақстанның стратегиялық зерттеулер институты

2004 жылдан бастап
әр тоқсан сайын жарық көреді

Бас редактор
Алмас Арзықұлов,
ҚР Президенті жанындағы ҚСЗИ-дің жетекші ғылыми қызметкері

Редакция мекенжайы:
Қазақстан Республикасы,
010000, Астана қаласы,
Бейбітшілік көшесі, 4
ҚР Президенті жанындағы ҚСЗИ

Телефон (7172) 75-20-20
Факс (7172) 75-20-21
E-mail: office@kisi.kz
www.kisi.kz
www.journal-kogam.kisi.kz

Журнал Қазақстан Республикасының Мәдениет, ақпарат және қоғамдық келісім министрлігінде 2003 ж. 19 желтоқсанда тіркеліп, тіркеу туралы № 4526-Ж куәлік берілген.

ISSN 2414-5696 (print)
ISSN 2788-5860 (online)

doi.org/10.52536/2788-5860

Индекс 74007

Журнал саяси ғылымдар саласы бойынша ғылыми еңбектің негізгі нәтижелерін жариялау үшін Қазақстан Республикасы Білім және ғылым министрлігі білім және ғылым саласында сапаны қамтамасыз ету комитеті ұсынатын ғылыми басылымдар тізбесіне енеді.

МАЗМҰНЫ

СОДЕРЖАНИЕ

Қоғам & Дәуір

Қазақстан Республикасы
Президенті жанындағы
Қазақстанның стратегиялық
зерттеулер институты

CONTENTS

Қоғам & Дәуір

Қазақстан Республикасы
Президенті жанындағы
Қазақстанның стратегиялық
зерттеулер институты

2004 жылдан бастап
әр тоқсан сайын жарық көреді

Бас редактор
Алмас Арзықұлов,
ҚР Президенті жанындағы
ҚСЗИ-дің жетекші
ғылыми қызметкері

Редакция мекенжайы:
Қазақстан Республикасы,
010000, Астана қаласы,
Бейбітшілік көшесі, 4
ҚР Президенті жанындағы ҚСЗИ

Телефон (7172) 75-20-20
Факс (7172) 75-20-21
E-mail: office@kisi.kz
www.kisi.kz
www.journal-kogam.kisi.kz

Журнал Қазақстан Республикасының
Мәдениет, ақпарат және қоғамдық
келісім министрлігінде 2003 ж.
19 желтоқсанда тіркеліп, тіркеу туралы
№ 4526-Ж куәлік берілген.

ISSN 2414-5696 (print)
ISSN 2788-5860 (online)

doi.org/10.52536/2788-5860

Индекс 74007

Журнал саяси ғылымдар саласы бойынша
ғылыми еңбектің негізгі нәтижелерін
жариялау үшін Қазақстан Республикасы
Білім және ғылым министрлігі білім және
ғылым саласында сапаны қамтамасыз ету
комитеті ұсынатын ғылыми басылымдар
тізбесіне енеді.

ҒТАХР
11.15.89.

https://doi.org/ 10.52536/2788-5860.2025.86.2.002

Dameli Nyssankuatova [1], ***Nurgul Istmatullaeva*** [2], ***Boma Nuralina*** [3]
[1] *Kazakh National Pedagogical university named after Abay*
Orcid ID: 0009-0007-1392-5861
** e-mail: dameli-1983@mail.ru*
(Almaty, Kazakhstan)
[2] *№231 secondary school KSU,*
teacher of Russian language and literature,
Orcid ID: 0009-0002-3690-6376
(Aral, Kazakhstan)
[3] *International Educational Corporation, Assosiate Professor.*
Orcid ID: 0000-0002-7634-522 X
(Almaty, Kazakhstan)

INFORMATION SECURITY MANAGEMENT: CYBERSECURITY POLICY IN THE MEDIA SPACE

Abstract. In the face of global challenges, Kazakhstan's key strategic resource – information and information technology – plays a crucial role in economic growth and national defense. However, weak information security poses serious risks, including potential leaks of political, economic, scientific, and military data. In today's digital era, strengthening cybersecurity is essential, especially in the media sector, where platforms often become channels for manipulation and misinformation.

This article examines Kazakhstan's cybersecurity policy in the media sphere, focusing on how media influence can generate cyber threats and how these threats might be mitigated. The study analyzes interactions between civil society and political discourse on social media, highlighting the need for accurate, reliable information to counter manipulation.

To address rising threats, the article recommends a multifaceted cybersecurity strategy that includes technical tools such as firewalls and artificial intelligence, staff training, incident response protocols, and stronger legal regulations. A robust regulatory framework is emphasized as a vital element in developing sustainable solutions and protecting national information assets in the digital age.

Key words: *repatriation, migration, polish nationality, adaptation, pole's card, Poland.*

Дәмелі Нысанкуатова, Нұргүл Исматуллаева, Бота Нуралина
АҚПАРАТТЫҚ ҚАУІПСІЗДІКТІ БАСҚАРУ: МЕДИА КЕҢІСТІКТЕГІ КИБЕРҚАУІПСІЗДІК САЯСАТЫ

Аңдатпа. Жаһандық сын-қатерлер жағдайында Қазақстан үшін стратегиялық маңызды ресурс – ақпарат пен ақпараттық технологиялар. Олар елдің экономикалық дамуы мен ұлттық қауіпсіздігін қамтамасыз етуде шешуші рөл атқарады. Ақпараттық қауіпсіздіктің әлсіздігі саяси, экономикалық, ғылыми және әскери деректердің таралуына қауіп төндіреді. Цифрлық дәуірде, әсіресе медиа кеңістігінде, киберқауіпсіздікті қамтамасыз ету ерекше маңызға ие.

Мақалада Қазақстандағы медиа саласындағы киберқауіпсіздік саясаты талданады. Медиа ықпалының киберқауіптердің пайда болуына әсері және оларды болдырмау жолдары қарастырылады. Сондай-ақ азаматтық қоғам мен әлеуметтік желілердегі саяси дискурс арасындағы өзара әрекетке талдау жасалып, ақпараттың шынайылығы мен сапасының маңызы атап өтіледі.

Авторлар ақпараттық қауіпсіздікті қамтамасыз ету үшін техникалық құралдарды, мамандарды оқытуды, инциденттерге әрекет ету протоколдарын және құқықтық реттеуді күшейтуді ұсынады. Ұлттық ақпараттық ресурстарды қорғау үшін орнықты құқықтық база қалыптастырудың өзектілігі көрсетіледі.

Түйін сөздер: *ақпарат; қауіпсіздік; саясат; жаһандану; медиа; киберқауіпсіздік; басқару; ақпараттық технологиялар; цифрлық технологиялар.*

Дамели Нысанкуатова, Нургуль Исматуллаева, Бота Нуралина

УПРАВЛЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ: ПОЛИТИКА КИБЕРБЕЗОПАСНОСТИ В МЕДИА ПРОСТРАНСТВЕ

Аннотация. В условиях глобальных вызовов ключевым стратегическим ресурсом Казахстана выступают информация и информационные технологии, играющие значимую роль в обеспечении экономической стабильности и национальной безопасности. Недостаточная информационная защищённость порождает риски утечки политически, экономически, научно и военно значимой информации. В цифровую эпоху особую актуальность приобретает развитие кибербезопасности, особенно в медийной сфере, где цифровые платформы становятся инструментами дезинформации и манипуляции общественным мнением.

Настоящая статья посвящена анализу политики Казахстана в области кибербезопасности в медиа-пространстве, с акцентом на источники киберугроз и возможные меры их преодоления. Рассматривается взаимодействие гражданского общества и политических дискурсов в социальных сетях, подчёркивается значимость достоверного информационного контента для предотвращения манипуляций.

Предлагаются адаптивные подходы к обеспечению информационной безопасности: использование технических средств, обучение персонала, протоколы реагирования и усиление нормативного регулирования. Подчёркивается необходимость устойчивой правовой базы для защиты национальных информационных ресурсов в условиях цифровизации.

Ключевые слова: *информация; безопасность; политика; глобализация; сми; кибербезопасность; регулирование; информационные технологии; цифровые технологии.*

Introduction.

In an age when information is predominant and the influence of the media is enormous, the protection of the social infosphere is becoming an important imperative. Realizing the importance of ensuring its national security in the digital age, the Republic of Kazakhstan has taken measures aimed at strengthening the integrity of its information space.

According to the Decree of the Government of the Republic of Kazakhstan on the Concept of Cybersecurity ("Cybersecurity Kazakhstan") dated June 30, 2017 No. 407, the strategy outlines key approaches to the development of a cybersecurity system that provides effective protection of electronic data resources, information systems and telecommunications networks of financial market entities. Compliance with this strategy makes it possible to respond promptly to both current and developing cyber threats, thereby contributing to the achievement of the goals set out in the Concept [1].

Currently, Kazakhstan is in the 31st place in Global Cybersecurity Index (GCI) being ahead of such countries as China, Denmark, Croatia, Slovakia, Israel and Switzerland [2]. According to statistics provided by the Ministry of Information and Public Development of the Republic of Kazakhstan, in 2023 the number of cyber attacks directed against state resources of Kazakhstan and objects of strategically important infrastructure of the country reached 83 million. These attacks were mainly carried out from the CIS and European countries, with the main impact coming from the public sector, which accounted for 62% of the total number of attacks [3]. This alarming trend highlights the vulnerability of government agencies and large industrial organizations to cyber threats, which requires immediate and reliable cybersecurity measures. Also, in addition to government data, there are significant threats to the information security of citizens.

Recognizing these problems, this study aims to understand the intricacies of Kazakhstan's information security system, evaluate existing regulatory measures and identify areas for improvement. The study, devoted to a thorough analysis of legislative provisions and their consequences, is designed to provide an idea of how to effectively confront the changing challenges of the digital era while protecting the interests and values of the country.

The cornerstone of Kazakhstan's defense strategy is based on several fundamental principles set out in the law, which impose specific responsibilities on government agencies. These include preventing the information isolation of key government bodies such as the President, Parliament, Government and national security forces to ensure the continuity and coherence of national decision-making processes. In addition, efforts are aimed at combating the deliberate dissemination of false information that endangers national security, as

well as at eliminating mechanisms that contribute to covert information influence on government decisions [4]. In addition, the legislation imposes restrictions on the distribution of certain content through printed materials and foreign media, recognizing their potential threat to national security. To strengthen these measures, restrictions on media ownership and control by foreign organizations will be introduced, which will serve as protection against external manipulation in the media sector of Kazakhstan.

However, while these rules apply to traditional channels of information dissemination, they may not take into account new platforms, leaving potential loopholes for propaganda. Moreover, data protection is closely linked to the social infosphere, which requires a careful approach. The provisions aimed at limiting information dependence and countering external influence emphasize the multifaceted nature of the problems that arise. However, ambiguity of interpretation makes it difficult to develop effective mitigation strategies.

It is noteworthy that the legislative framework prioritizes the protection of national interests, covering tasks ranging from strengthening social harmony and political stability to fostering Kazakhstani patriotism and unity. Special attention is paid to the preservation and enhancement of social values, educational and scientific potential, the protection of constitutional order, as well as the promotion of a positive international image of Kazakhstan [5]. Given the growth of cyber threats, the authors of the study advocate a comprehensive analysis and improvement of Kazakhstan's cybersecurity infrastructure. Focusing on technological progress, the Government emphasizes the importance of modern information technologies and the development of domestic industry to effectively counter emerging digital threats.

In addition, the study examines the transformative impact of social media on political behavior in Kazakhstan. While social media platforms provide unprecedented access to information and opportunities for self-expression, they also increase risks such as misinformation and manipulation. By exploring the relationship between civil society and political discourse on these platforms, the study aims to identify strategies for reducing risks and using social media to positively engage civil society.

In addition, the study provides an assessment of the regulatory framework governing information security in Kazakhstan, indicating its strengths and weaknesses. Assessing the effectiveness of current measures and identifying areas for improvement, the study aims to substantiate future policy decisions and increase the sustainability of Kazakhstan's information infrastructure.

Through a comprehensive study of these interrelated factors, this study aims to offer a holistic understanding of the complex interaction between media, politics and information security in Kazakhstan. By shedding light on the challenges and opportunities inherent in this dynamic landscape, the study aims to contribute to ongoing efforts to protect national interests and promote the good faith participation of civil society in the digital age.

Materials and methods

The research methodology used in this article is aimed at conducting a comprehensive study of the significant impact of mass media on information security in Kazakhstan, as well as at developing effective solutions to mitigate this problem. Combining qualitative and quantitative data obtained from both foreign and Kazakhstani scientists, this approach aims to combine theoretical foundations with empirical data from various sources, thereby offering a detailed understanding of how media channels increase the risk of cyber attacks in the country.

It is extremely important to emphasize the qualitative aspect of the methodology, which involves a comprehensive study of various media platforms, including the Internet, social networks and television content, to identify potential ways of information attacks in Kazakhstan. This involves a thorough study of the use of social media to obtain confidential information and an analysis of the strategies adopted by developed countries to raise awareness about data protection. Moreover, along with content analysis, the methodology includes an analysis of the best global practices of developed countries in regulating this problem. This analysis, aimed at identifying relevant and effective measures to combat information threats in the field of mass media, aims to analyze the approaches used by developed countries to protect their information ecosystems. The methodology is based on a holistic understanding of information threats in Kazakhstan, combining careful analysis with practical conclusions from the best international practices.

In addition, the inclusion of quantitative data is of paramount importance in this context, since the article combines various statistical data obtained from official sources. This quantitative aspect covers statistical data, legal norms and other relevant information.

Results and discussion

The Information Security Committee within the Ministry, established by the decree of the Government of the Republic of Kazakhstan dated November 15, 2016, is directly responsible for information security. In addition to the implementation of a unified state policy in the field of information security and international cooperation within its competence and the implementation of similar tasks and functions, the Committee is responsible for monitoring and certifying compliance with the information security of the e-government platform (egov.kz) and websites of government agencies. Given the number and quality of attacks carried out for these purposes over the past few years, experts expect significant results in the work of the Ministry and the Committee, which, in addition to reducing the number of attacks, should also minimize losses from them – in terms of leaks of authoritative, financial, temporary and confidential data [6].

As a result of the analysis of existing regulatory and legal documents on information security, it was revealed that the first concept of information security in Kazakhstan was adopted in 2006. This concept is based on a number of normative legal acts – the Constitution of the Republic of Kazakhstan, the

laws "On National Security of the Republic of Kazakhstan", "On electronic Document management and electronic digital signature", "On Informatization", as well as the concept of information security of the CIS member states in the military sphere [7]. In 2011, a second concept was adopted, in which the list was supplemented by the laws "On Technical Regulation" (2004), "On Mass Media", "On Communications" (2004) (Rader and Vigel, 2013). At the same time, the provisions of the agreement between the governments of the SCO member states on cooperation in the field of international information security (2010) and the Concept of Cooperation of the CIS member states in the field of information security (2008) were used [8].

It should be noted that from the point of view of the regulatory framework, a new concept has not been developed. The list of laws was expanded due to the fact that it could be included in the 2006 version, all of them, with the exception of the law on mass media, have not changed much. This indicates a very slow reaction of legislation to changes in the information sphere that occur every year. At the same time, it is clear that the main focus is on the technical side of data protection. It is assumed that officials pay very little attention to the socio-political aspects of information security. Basically, foreign policy threats (national security laws, secrets, the fight against terrorism) or the media sphere are taken into account. This suggests that the concept assumes an integrated approach [9].

In 2006, E. K. Aliyarov, in addition to a number of weak regulatory measures and threats, noted the shortage of specialists in the information field and the system of their retraining and advanced training, the unsatisfactory state of the information infrastructure, as well as the emergence of information inequality. Aliyarov E. K. noting the important role of the media in ensuring information security, warns about the threat of their monopolization (media) and the wide possibilities of manipulating public consciousness, outlined in this work [10]. Later, we can say that the list of threats has expanded, their danger and relevance have increased. There are significant positive changes, in particular, in the field of e–government and overcoming the "internal" information inequality - it is obvious that various segments of the population have greater access to new information and communication technologies and are actively mastering them.

Below is the main list of internal and external threats, according to which the state of information security in Kazakhstan is assessed:

Table 1. External and internal risks to information security

Internal risks	External risks
- Inadequate legal, organizational and technical framework for the protection of personal data of citizens [11]. - Inefficient functioning of information security systems. - Lack of qualified specialists in the information and communication sector [12]. - Limited level of general legal and information literacy, including skills for	- The deployment of information troops by large countries poses a threat to information security and stability [15]. - There is a risk of using computer attacks by terrorist organizations as a tactic, which creates significant security threats. - Extremist and terrorist groups actively use information and communication networks for propaganda purposes, contributing to

the safe use of cyberspace in a society [13].- Violation of the legitimate rights and interests of individuals, organizations and the state in the field of information. - Lack of coordination and cooperation between government agencies, private sector enterprises and civil society organizations in addressing cybersecurity issues. - The emergence of new cyber threats and attack directions that require constant adaptation and improvement of cybersecurity measures. - Potential economic consequences as a result of data leakage, cyber attacks and loss of consumer confidence in digital services and platforms [14].	radicalization and recruitment Sophisticated cybercrime networks involved in ransomware attacks. - Exploiting vulnerabilities in Internet of Things (IoT) devices and cloud infrastructure, leading to massive disruptions and compromise of confidential information. - The proliferation of malicious software and hacking tools in underground cybercrime markets, which makes possible cyber attacks by non-State actors [16].

If we compare the conclusions from Table 1 with the mass media, it becomes obvious that they play a crucial role in both enhancing and reducing information security risks. On the one hand, the media can amplify external threats by spreading disinformation, promoting cyber propaganda, and facilitating social engineering attacks. On the other hand, the media can serve as a platform for cybersecurity education, information campaigns and dissemination of best practices for protecting personal data and combating cyber threats [17].

Cooperation between government agencies, private sector organizations, civil society organizations and the media is needed to address these issues. The media can play a key role in raising awareness of cybersecurity risks, promoting responsible online behavior, and exposing disinformation. In addition, media organizations should prioritize cybersecurity measures to protect their own networks and platforms from cyber attacks and data leaks. Ultimately, effective reduction of information security risks in the digital age requires a multifaceted approach combining media literacy, regulatory reforms and international cooperation.

Article 9 emphasizes the paramount importance of ensuring information security for individuals, society and the State in accordance with government regulation and policy. Therefore, according to the State Technical Service of the Republic of Kazakhstan, as the development of Artificial Intelligence (hereinafter-AI) accelerates in 2024, the integration of AI and machine learning into information security provides many advantages, expanding human capabilities, analyzing vast amounts of data and adapting to changing threats. However, there are concerns about potential AI-driven attacks, including sophisticated social engineering deepfake (English deepfake from deep learning "deep learning" + fake "fake") and automated malware. However, artificial intelligence can help identify and mitigate risks through real-time anomaly detection and intelligent security incident response mechanisms [18]. Mass media and social networks can

use artificial intelligence to moderate content, identify fake news and improve user safety.

However, there is another opinion that Kazakhstan cannot and should not replace advanced innovative technologies with domestic developments. Instead, the focus should be shifted to training specialists capable of auditing installed systems and ensuring their safety [19].

During the analysis of foreign literature in search of innovative and effective measures to combat the lack of information security, the following was revealed:

Table 2. The experience of developed countries in the formation of a cybersecurity system

Country	Characteristics of the cybersecurity system
Japan	Japan's Cybersecurity Strategy, adopted by the Information Security Policy Council on June 10, 2013, aims to transform Japanese cyberspace into a globally significant, sustainable and adaptable sphere, with the aim of positioning the country as a leader in cybersecurity. Cybersecurity oversight is the responsibility of the National Information Security Center (IS), which is responsible for developing government standards, providing recommendations based on cybersecurity assessments, and promoting cybersecurity initiatives [20].
The United Kingdom	The UK tops the global cybersecurity index. It uses two approaches to address vulnerabilities in cyberspace: firstly, by publicly disclosing vulnerabilities for the benefit of technology users around the world and, secondly, by storing information about vulnerabilities for intelligence purposes to curb malicious activity in the UK. In addition, the UK's National Cyber Security Center, established in the UK, is recognized as highly effective and ranks fifth in the world [21].
Canada	Canada's National Cybersecurity Strategy, launched in 2010, aims to prevent threats from foreign government agencies, criminals and terrorists. The strategy is based on three key principles: protecting the systems of the federal government, cooperating with lower-level government agencies and the private sector to protect cyber systems outside federal jurisdiction, and improving the online security of Canadians through a combination of public awareness campaigns and law enforcement capacity building [22].
Finland	In 2013, Finland adopted a cybersecurity strategy, followed by the establishment of a National Cybersecurity Center in 2014. The mission of the center is to protect cyberspace, ensure secure user access to both general and specialized communication networks, as well as to counter cyber threats [23].
South Korea	In South Korea, cyberspace protection efforts are focused on implementing network access encryption, building an intrusion prevention System (IPS), increasing resilience to advanced persistent threats (APT), and strengthening Internet security. There are three key cybersecurity institutions in the country: the National Cybersecurity Center, the Korea Internet Security Agency (KISA) and the Cyberterrorism Response Center at the National Police Department. In addition, South Korea has established a specialized school for conducting cyber warfare and training security specialists [24].

France	In 2009, the French Network and Information Security Agency (ANSSI) was established in France as part of the Prime Minister's Office to protect information systems, reflecting a shift towards prioritizing cybersecurity in defense and national security policy [25].

A review of organizational measures to ensure cybersecurity in leading countries shows that they are implementing effective cybersecurity protocols. These countries have developed their own strategies, defense policies, and national security frameworks. In addition, they have created new agencies, national centers and special teams to promptly eliminate computer-related incidents.

Despite the continued vulnerability of Kazakhstan's information space, notable successes have been achieved in various fields. These include increased international cooperation, efforts to modernize State-owned media, and raising public awareness. However, despite the optimistic forecast provided by initiatives such as "Cyber Shield of Kazakhstan", the task of protecting the country's information space and ensuring its future, including the well-being of youth and the sovereignty of the state, requires more attention and allocation of resources.

Conclusion

In this study, we examined the general state of Kazakhstan regarding cybersecurity regulation measures in the context of digitalization with an emphasis on the media sphere. It emphasizes that a country's ability to withstand cyber threats is closely linked to the means at its disposal. The data obtained indicate that the general state of Kazakhstan's cybersecurity system correlates with the level of its economic development, which indicates the direct impact of development on information security.

The key components for strengthening legal and institutional support for cybersecurity in Kazakhstan, based on the best practices of developed countries, are:

- Creation of an organizational and technical model of cyber defense.
- Planning and implementation of the measures outlined in the Cybersecurity Strategy, coordinated by the National Cybersecurity Coordination Center.
- Implementation of coordinated mechanisms for vulnerability detection and information disclosure in information and communication systems.
- Creation of mechanisms for timely detection of cyber threats and response to them.
- Implementation of a national program to identify vulnerabilities in information and communication systems.
- Regular security checks of critical infrastructure facilities.

By taking these measures, Kazakhstan will be able to strengthen its position in the field of cybersecurity, reduce risks and ensure the sustainability of its digital infrastructure in the face of developing cyber threats.

REFERENCES:

1. The legal information system of normative legal acts of the Republic of Kazakhstan, Adilet database About the approval of the Concept of cybersecurity ("cyber Shield of Kazakhstan") the Resolution of the Government of the Republic of Kazakhstan of June 30, 2017 № 407, Available at: http://adilet.zan.kz/rus/docs/P1700000407 [Accessed 20 March 2024].
2. Global Cybersecurity Index Ranking, 2023, Available at: https://www3.weforum.org/docs/WEF_Global_Security_Outlook_Report_2023.pdf, [Accessed 25 March 2024].
3. Official website of RSE "State technical service" of the national security Committee of the Republic of Kazakhstan, General information, Available at: http://sts.kz/ru/organization [Accessed 15 April 2024].
4. The State Program "Information Kazakhstan 2020": approved By Decree of the President of the Republic of Kazakhstan dated January 8, 2013, No. 464. Available at: https://adilet.zan.kz/rus/docs/U1300000464 [Accessed 17 April 2024].
5. Bruggemann M. Information policy and public sphere: EU communications and the promises of dialogue and transparency // Javnost-The Public. European Institute for Communication & Culture (EURICOM). -2010. - Vol.17, Iss. 1. - 7 p.
6. Nussipova A.U. Modern conditions of information security in the Republic of Kazakhstan // Bulletin of the Kazakh Leading Academy of Architecture and Civil Engineering, series "Social and Political Sciences", 2019, December No. 4 (74), RK, Almaty, P. 352-364
7. Bershadskaya L., Chugunov A., Dzhusupova Z. Understanding E-Government Development Barriers in CIS Countries and Exploring Mechanisms for Regional Cooperation // Technology-Enabled Innovation for Democracy, Government and Governance. Springer Edition. – 2013. – P. 87–101.
8. Bogdanov S.V. Strategic communications: conceptual approaches and models for public administration // Public administration. Electronic bulletin. - 2017. - № 61. Available at: http://e-journal.spa.msu.ru/vestnik/ item_895. [Accessed 17 March 2024].
9. Topa, I., & Karyda, M. (2019). From theory to practice: guidelines for enhancing information security management. Information and Computer Security, 27(3), 326-342. Available at: https://doi.org/10.1108/ICS09-2018-0108, [Accessed 17 March 2024].
10. Aliyarov E. K., Information Policy of the Republic of Kazakhstan in the conditions of globalization – Almaty: Kazakh university, 2006. - P. 36.
11. Schmitt, Michael N. 2013. "Cyberspace and International Law: The Penumbral Mist of Uncertainty." Harvard Law Review Forum 126 (5): 176–80.
12. Kshetri, Nir. 2016. The Quest to Cyber Superiority: Cybersecurity Regulations, Frameworks, and Strategies of Major Economies. Cham, Switzerland: Springer.
13. Yarovenko, H. (2020). Evaluating the threat to national information security. Problems and Perspectives in Management, 18(3), 195-210. https://doi.org/10.21511/ppm.18(3).2020.17.
14. Kuznetsov, A., Smirnov, O., Gorbacheva, L., Babenko, V. (2020). Hiding data in images using a pseudo-random sequence. CEUR Workshop Proceedings, 2608, pp. 646-660.
15. McClure C.R., Jaeger P.T. Government information policy research: Importance, approaches, and realities // Library & Information Science Research. - 2008. - Vol. 30, № 4. - P. 257-264.
16. Christine, D., et al, "Beyond Supply and Demand: Addressing the Multidimensional Workforce Gaps in Cybersecurity", World Economic Forum, 21 October 2022: https://www.weforum.org/agenda/2022/10/cybersecurity-workforce-gapsinclusive-approach-jobs/.
17. Jing Zhanga, and Yushim Kimb, Digital government and wicked problems: Solution or problem?, Information Polity 21 (2016) 215–221 215 DOI 10.3233/IP-160395 IOS Press, Special Issue Editorial, pp. 215-221 Available at: https://content.iospress.com/download/information-polity/ip395?id=information-polity%2Fip395 [Accessed 24 March 2024]
18. How is cybersecurity developing in Kazakhstan, "Strategy", 28 October 2019, https://strategy2050.kz/ ru/news/kak-razvivaetsya-kiberbezopasnost-kazakhstana [Accessed 25 March 2024]
19. The Criminal Code of the Republic of Kazakhstan dated July 3, 2014 No. 226-V (as amended and supplemented as of January 11, 2020).
20. Zavhorodnii, A., Ohiienko, M., Biletska, Y., Bondarenko, S., Duiunova, T. & Bodenchuk, L. (2021). Digitization of agribusiness in the development of foreign economic relations of the region. Journal of Information Technology Management, Special Issue, 123-141. doi: 10.22059/JITM.2021.82613
21. Mitrofanova E.A., Bulkina N.V. (2016), Formation and development of a system for stimulating the labor activity of personnel in the information technology industry: theory and practice: monograph, State University of Management Publ. House, Moscow, Russia
22. Afonin A. I. (2006), Legal support for countering spam, Publishing House of Moscow State Technical University, N.E. Bauman, 128 p.

23. World Economic Forum, "Global Cybersecurity Outlook 2022", January 2022: https://www3.weforum.org/docs/WEF_ Global_Cybersecurity_Outlook_2022.pdf. [Accessed 28 March 2024].
24. Pipikaite, A., Holla-Maini, A., Ware, B. and Dickinson, M., "Will the Battle for Space Happen on the Ground?", World Economic Forum, 25 May 2022: https://www.weforum.org/agenda/2022/05/increased-cybersecurity-for-spacebased-services/ [Accessed 20 March 2024].
25. Sehl Melloulia, Luis F. Luna-Reyesb and Jing Zhang, Smart government, citizen participation and open data, Information Polity 19 (2014) 1–4 1 DOI 10.3233/IP-140334 IOS Press, pp. 1-4, Available at: https://pdfs.semanticscholar.org/e2c5/8b04ebcb0c8e5a4d9f2627bb2d9e103b1183.pdf [Accessed 20 March 2024].