IRSTI
11.15.89
20.01.07

https://doi.org/10.52536/2788-5860.2026.90.2.006

Dameli Nyssankuatova [1], ***Gulzhan Khussainova*** [2], ***Nurgul Ismatullayeva*** [3], ***Botakoz Nuralina*** [4]

[1] *International Educational Corporation, KNP university named after Abay, doctoral student, faculty of the institute of history and law, e-mail: dameli-1983@mail.ru*

[2] *Aktobe Regional University named after K.Zhubanov, Department of Socio-Political Disciplines e-mail: kuluv@mail.ru (Aktobe, Kazakhstan)*

[3] *KNP university named after Abay, doctoral student, faculty of the institute of history and law, e-mail: nurgulismatullaeva42@gmail.com (Almaty, Kazakhstan)*

[4] *International Educational Corporation, Assosiate Professor e-mail: botanur@mail.ru (Almaty, Kazakhstan)*

PROTECTING HUMANITARIAN VALUES IN THE DIGITAL MEDIA SPACE

Abstract. In the context of global instability, information and digital technologies have emerged as strategically significant resources for Kazakhstan, exerting a strong influence on economic growth and the strengthening of national security. Their importance extends to all areas of public life, including the media sphere. However, insufficient information security creates serious risks – from data leaks to the erosion of humanitarian values in society.

In the digital era, as the media landscape continues to transform under the influence of advancing technologies, safeguarding humanitarian values has become an increasingly urgent priority. This paper analyzes cybersecurity challenges within Kazakhstan's media sector, highlighting the role of digital platforms in facilitating the spread of cyber threats, as well as their capacity to be used for political and social manipulation. It also considers the influence of civil society and social media on shaping the information environment.

The authors stress the importance of implementing a comprehensive approach to cybersecurity in the media sphere, encompassing technological measures (such as firewalls, artificial intelligence systems, and continuous monitoring), the development of effective legal regulations, professional training for personnel, and clearly defined incident response procedures.

The article offers approaches for developing national strategies to counter digital threats and ensure media resilience while preserving humanitarian values.

Keywords: *information security, media, cyber threats, humanitarian values, digital technologies, Kazakhstan, cybersecurity, mass media.*

Дәмели Нысанкуатова, Гулжан Хусаинова, Нұргүл Исматуллаева, Ботакөз Нұралина

ЦИФРЛЫҚ МЕДИА КЕҢІСТІГІНДЕ ГУМАНИТАРЛЫҚ ҚҰНДЫЛЫҚТАРДЫ ҚОРҒАУ

Аңдатпа. Қазіргі жаһандық сын-тегеуріндер жағдайында ақпарат пен цифрлық технологиялар Қазақстан үшін экономикалық өсуді қамтамасыз ететін және ұлттық қауіпсіздікті нығайтатын негізгі стратегиялық ресурстардың біріне айналып отыр. Аталған ресурстар қоғамдық өмірдің барлық бағыттарында, соның ішінде медиа кеңістікте де айрықша маңызға ие. Дегенмен ақпараттық қауіпсіздік деңгейінің жеткіліксіз болуы құпия деректердің таралуы мен қоғамдағы гуманитарлық құндылықтардың әлсіреуіне әкелетін елеулі қатерлерді туындатады.

Цифрландыру дәуірінде медиа технологиялардың қарқынды дамуы мен өзгеруі жағдайында гуманитарлық құндылықтарды сақтау мәселесі өзекті сипатқа ие болуда. Бұл мақалада Қазақстанның медиа саласындағы киберқауіпсіздік мәселелері талданып, цифрлық платформалардың киберқауіптерді таратудағы рөлі, сондай-ақ олардың саяси және әлеуметтік ықпал ету құралы ретінде қолданылу мүмкіндіктері қарастырылады. Сонымен қатар азаматтық қоғам мен әлеуметтік желілердің ақпараттық кеңістікке әсері сараланады.

Авторлар медиа саласында киберқауіпсіздікті қамтамасыз етудің кешенді тәсілін енгізудің маңыздылығын атап көрсетеді. Бұл тәсіл техникалық құралдарды (брандмауэрлер, жасанды интеллектке негізделген жүйелер, мониторинг), құқықтық реттеуді жетілдіруді, мамандарды даярлауды және тиімді әрекет ету тетіктерін қамтиды. Мақалада сонымен бірге цифрлық қатерлер жағдайында медианың тұрақтылығын арттыруға және гуманитарлық құндылықтарды қорғауға бағытталған ұлттық стратегияларды қалыптастыру жолдары ұсынылады.

Түйін сөздер: *ақпараттық қауіпсіздік, медиа, киберқауіптер, гуманитарлық құндылықтар, цифрлық технологиялар, Қазақстан, киберқауіпсіздік, бұқаралық ақпарат құралдары.*

Дамели Нысанкуатова, Гулжан Хусаинова, Нургуль Исматуллаева, Ботакоз Нұралина

ЗАЩИТА ГУМАНИТАРНЫХ ЦЕННОСТЕЙ В ЦИФРОВОМ МЕДИА-ПРОСТРАНСТВЕ

Аннотация. В условиях современных глобальных вызовов информация и цифровые технологии всё более утверждаются в качестве одного из важнейших стратегических ресурсов Казахстана, оказывая определяющее влияние на развитие экономики и обеспечение национальной безопасности. Эти ресурсы играют значимую роль во всех сферах общественной жизни, включая медиапространство. Вместе с тем недостаточный уровень информационной защищённости приводит к возникновению серьёзных угроз – от утечек данных до ослабления гуманитарных ценностей в обществе.

В эпоху цифровизации, когда медиа активно изменяются под воздействием технологического прогресса, задача сохранения гуманитарных ориентиров приобретает особую актуальность. В статье анализируются вопросы кибербезопасности в медийной сфере Казахстана, в том числе влияние цифровых платформ

на распространение киберугроз и их использование в целях политического и социального воздействия. Особое внимание уделяется значению гражданского общества, социальных сетей и информационной среды в формировании общественного мнения и степени уязвимости гуманитарных ценностей.

Авторы акцентируют внимание на необходимости внедрения комплексного подхода к обеспечению кибербезопасности в сфере средств массовой информации, включающего как технические решения (например, брандмауэры, системы искусственного интеллекта и мониторинга), так и совершенствование нормативно-правовой базы, подготовку специалистов и разработку эффективных протоколов реагирования. В работе также рассматриваются направления формирования национальных стратегий, ориентированных на укрепление устойчивости медиасреды и защиту гуманитарных ценностей в условиях нарастающих цифровых рисков.

Ключевые слова: *информационная безопасность, медиа, киберугрозы, гуманитарные ценности, цифровые технологии, Казахстан, кибербезопасность, СМИ.*

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 [1].

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 [2].

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 [3]. 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 [4]. 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, focused on an in-

depth examination of legal frameworks and their implications, aims to illustrate effective approaches to addressing the evolving challenges of the digital age while safeguarding national interests and core values.

Kazakhstan's defense strategy is grounded in a set of key principles enshrined in legislation, which assign clearly defined responsibilities to state institutions.

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 [5]. Additionally, the legislation sets limits on the dissemination of certain content through print media and foreign outlets, recognizing their potential risk to national security. To reinforce these safeguards, new restrictions on foreign ownership and control of media will be implemented, aimed at protecting Kazakhstan's media sector from external influence and manipulation.

However, while these rules apply to traditional channels of information dissemination, they may not take into account new platforms, leaving potential loopholes for propaganda. Furthermore, safeguarding data is closely intertwined with the social information environment, necessitating a careful and measured approach. Regulations aimed at reducing information dependency and countering external interference highlight the complexity and multifaceted nature of the challenges involved. However, ambiguity of interpretation makes it difficult to develop effective mitigation strategies.

It is important to note that the legal framework places a strong emphasis on safeguarding national interests, addressing objectives such as enhancing social cohesion and political stability, as well as promoting patriotism and unity among the people of Kazakhstan. 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 [6]. In light of the growing cyber threats, the study's authors stress the importance of a thorough assessment and strengthening of Kazakhstan's cybersecurity infrastructure. Emphasizing technological advancement, the government highlights the critical role of modern information technologies and the development of domestic industry in effectively countering emerging digital challenges.

In the theoretical section of the study, it is necessary to further elaborate on the concept of "humanitarian values" within the context of the digital media environment. In contemporary academic discourse, this concept can be interpreted as a set of universal and socially significant norms and principles aimed at ensuring human rights and freedoms, preserving cultural diversity, promoting social justice, and fostering critical thinking in the digital sphere.

It should be emphasized that the transformation of the media environment under the influence of digital technologies significantly affects both the content and mechanisms of implementation of humanitarian values. The algorithmization of information flows, the dominance of platform-based ecosystems, and the

transnational nature of information dissemination create new challenges, including the spread of misinformation, manipulative practices, and the intensification of digital inequality. These factors may undermine fundamental values such as information reliability, public trust, and the responsibility of communication actors.

Materials and Methods

The qualitative component of the study is based on an in-depth content analysis of various media platforms, including television channels, online news portals, and social media such as Instagram, Facebook, and Telegram.

The selection of media sources was guided by the following criteria: (1) audience reach and influence within Kazakhstan's information space; (2) frequency and relevance of content publication; (3) presence of politically and socially significant topics; and (4) representation of different types of media (state-owned, private, and independent). This ensured a balanced and representative sample of the national media landscape.

The content analysis employed a mixed-method approach, combining both qualitative and quantitative techniques. These included:

– thematic coding (disinformation, cyber propaganda, information attacks, PSYOP);

– sentiment analysis (positive, negative, neutral);

– identification of narrative strategies and manipulative techniques;

– frequency analysis of key topics and messages.

2.1 Qualitative Approach

Particular attention was paid to the mechanisms through which disinformation, cyber propaganda, and psychological operations (PSYOP) are disseminated within Kazakhstan's digital space, including cases of political manipulation, public destabilization, and information leakage.

The interpretation of quantitative data on cyber threats was conducted using comparative and longitudinal analysis methods. Specifically, the study applied: (1) time-series analysis to identify trends in cyberattack frequency; (2) cross-sectoral comparison (government agencies, critical infrastructure, private sector); and (3) correlation analysis between the level of digitalization and vulnerability to cyber threats. This approach made it possible to identify not only current risks but also their evolution over time.

The study also considers the legislative responses of these countries, including frameworks for media accountability, content regulation, and digital literacy education, assessing their potential applicability within the Kazakhstani context.

This comparative legal analysis supports the development of adaptive models to be potentially integrated into Kazakhstan's legal system for the purpose of enhancing resilience against cyber threats.

2.2 Quantitative Approach

The comparative analysis covers countries such as Finland, South Korea, the United Kingdom, Canada, and Japan, which are recognized for their advanced

practices in media literacy and information security. The study goes beyond descriptive comparison by emphasizing the adaptability of these models to Kazakhstan's context. For instance:

– Finland's media literacy model can be integrated into national education systems;

– South Korea's cybersecurity practices are applicable to critical infrastructure protection;

– regulatory frameworks from the United Kingdom and Canada may inform media policy reforms;

– Japan's approaches to information risk management are relevant for enhancing digital resilience.

The quantitative component relies on data from official governmental and international sources, including the Ministry of Information and Public Development of Kazakhstan and reports from the International Telecommunication Union, particularly the Global Cybersecurity Index. Additional data from national cybersecurity centers are also incorporated.

Importantly, the study includes multi-year statistical dynamics, enhancing its analytical depth. The analysis covers:

– the number and frequency of cyberattacks targeting government institutions and critical infrastructure over time;

– statistics on digital media consumption across demographic groups;

– the prevalence of disinformation campaigns;

– the number of legal cases related to cybercrime and media law violations.

This integrated methodological approach enables a more comprehensive understanding of the interplay between media, political processes, and information security in Kazakhstan.

2.3 Methodological Rationale

By combining qualitative and quantitative approaches, this study provides a comprehensive perspective on the challenges of safeguarding humanitarian values within a digital environment characterized by rapid technological advancement and geopolitical uncertainty. The methodological design ensures academic rigor, practical relevance, and applicability, particularly for policymakers, cybersecurity experts, and media regulatory authorities.

The methods employed also reflect the interdisciplinary nature of the issue, drawing on insights from political science, media studies, international law, and cybersecurity. This integrated framework facilitates the development of actionable recommendations aimed at strengthening Kazakhstan's ability to protect its informational sovereignty and preserve core humanitarian values within the digital media landscape.

Results and Discussion

In the context of protecting humanitarian values in the digital media sphere, maintaining the stability and security of the information environment represents a critical strategic priority for Kazakhstan. A pivotal role in this process is played by the Information Security Committee under the Ministry of Digital Development,

Innovations, and Aerospace Industry, established by the Government of the Republic of Kazakhstan on November 15, 2016. The Committee is responsible for implementing a unified national policy on information security, coordinating intergovernmental cooperation, and ensuring that digital platforms–including the e-Government portal (egov.kz) and official state websites–comply with established cybersecurity standards.

Given the increasing number and complexity of cyberattacks in recent years, experts forecast that the work of this Committee will be instrumental not only in reducing the number of attacks but also in minimizing their impact–particularly regarding data leaks of a political, economic, and social nature [10].

An analysis of Kazakhstan's regulatory framework shows that the first national information security concept was adopted in 2006. This document was based on a number of legal instruments, including the Constitution of the Republic of Kazakhstan, and laws such as On National Security, On Electronic Document Management and Electronic Digital Signature, On Informatization, and the CIS Concept of Information Security in the Military Sphere [11]. In 2011, an updated concept was introduced, broadening the legal framework with new legislation, including the laws "On Technical Regulation," "On Mass Media," and "On Communications," many of which were aligned with international legal standards.

However, despite these advancements, the regulatory system remains predominantly technocratic and reactive, with limited adaptability to the rapidly evolving threats within the digital information environment. Significantly, the majority of legal reforms have concentrated on technical safeguards and external risks, such as terrorism and espionage, while insufficiently addressing the socio-political aspects of information security, including public trust, media influence, and civic engagement [12].

Significant concerns were already raised in 2006 by Kazakhstani researcher E.K. Aliyarov, who emphasized structural weaknesses in the information system. These include the lack of qualified cybersecurity personnel, limited professional development infrastructure, poor state of information networks, and the emergence of informational inequality–all of which pose serious threats to national cohesion. Aliyarov also warned of the monopolization of the media, a factor that facilitates the manipulation of public consciousness and undermines democratic processes.

While notable advancements have been achieved–particularly in the expansion of e-government services and broader public access to digital technologies–significant gaps remain. Mere access to digital platforms does not inherently ensure the development of critical thinking skills, media literacy, or the capacity for civic resilience against digital propaganda, disinformation, and covert political manipulation.

The contemporary information security challenges confronting Kazakhstan can be broadly categorized into internal and external threats, as outlined in the following analysis.

Table 1. Internal and External Information Security Threats in Kazakhstan

Internal Threats	External Threats
Outdated legal and technical mechanisms for personal data protection	Deployment of information warfare capabilities by major geopolitical actors
Ineffective cybersecurity systems in public institutions	Cyberattacks conducted by terrorist organizations
Shortage of qualified cybersecurity professionals	Dissemination of radical propaganda through ICT networks by extremist groups
Low level of legal awareness and digital literacy among the population	Use of ransomware and AI-generated deepfake technologies
Violations of citizens' digital rights and privacy	Attacks on critical infrastructure and cloud-based information systems
Insufficient interagency coordination in cyber incident response	Distribution of malware through dark web cybercrime marketplaces
Financial losses and declining public trust in digital platforms and services	Espionage, disinformation, and manipulation through foreign media channels

The data presented in Table 1 indicate that mass media function simultaneously as both a vector of risk and a mechanism of mitigation within the information environment. On one side, media channels facilitate the spread of disinformation, enable cyberpropaganda, and support social engineering operations. Conversely, they act as instruments for cybersecurity awareness, public education campaigns, and the promotion of responsible digital behavior.

Within this framework, safeguarding humanitarian values in the digital domain depends on the accountable and transparent engagement of media actors. Effective collaboration among government institutions, civil society, and the private sector–including media organizations–is essential for cultivating a resilient information culture that not only ensures technical security but also strengthens public trust, upholds freedom of expression, and supports democratic governance.

The expanding deployment of Artificial Intelligence (AI), encompassing machine learning and natural language processing, introduces both significant opportunities and potential hazards. As highlighted in the 2024 report by the State Technical Service of the Republic of Kazakhstan, AI can enhance defensive capabilities by enabling real-time threat detection and proactive response mechanisms.

However, it also enables more sophisticated deepfake technologies, automated misinformation, and targeted manipulation of social narratives, which complicates regulatory response.

Although the advancement of domestic cybersecurity technologies is promoted, several experts contend that Kazakhstan's priority should not be the wholesale replacement of foreign solutions. Instead, emphasis should be placed on cultivating a skilled workforce capable of auditing, monitoring, and securing critical information systems effectively.To evaluate international best practices,

Table 2. Presents a comparative overview of cybersecurity systems in developed countries:

International Experience in Cybersecurity Governance	
Country	**Key Characteristics**
Japan	National Cybersecurity Strategy (2013); oversight by NISC; emphasis on adaptability and global relevance
United Kingdom	Global leader; dual strategy of public disclosure and intelligence use of vulnerabilities; strong regulatory body
Canada	National Cybersecurity Strategy (2010); multi-level collaboration; strong public awareness focus
Finland	National Cybersecurity Center; focus on resilience and secure access to public infrastructure .
South Korea	Multi-agency system including KISA and police cyber units; emphasis on resilience to APTs and cyberterrorism.

This comparative insight suggests that Kazakhstan could benefit from establishing similarly coordinated institutional frameworks, comprehensive national strategies, and inclusive approaches that actively involve media stakeholders in cybersecurity governance.

While Kazakhstan has achieved measurable progress–particularly in international cooperation and initiatives aimed at raising digital awareness–substantial gaps remain. Efforts must continue to align technical security measures with governance principles that uphold human dignity, freedom of expression, and public trust in the digital media sphere.

Conclusion

The findings of this study indicate that ensuring cybersecurity in Kazakhstan amid digital transformation extends beyond technical defenses; it constitutes a foundational prerequisite for safeguarding humanitarian values, democratic institutions, and civic confidence. An assessment of regulatory frameworks, institutional capacity, and international experience has highlighted structural vulnerabilities as well as opportunities for advancement.

It is clear that the resilience of Kazakhstan's cybersecurity ecosystem is closely linked to economic development, digital literacy, and the capacity to harmonize national policies with international standards. However, current strategies largely prioritize foreign threats and infrastructure protection, leaving socio-political dimensions–such as media accountability, public awareness, and information equity–insufficiently addressed.

To effectively preserve humanitarian values within the digital media landscape, Kazakhstan must adopt a multi-dimensional strategy that combines technological innovation, institutional reform, and a human-centered information policy. Drawing on international best practices, the following strategic measures are recommended:

- Development of a comprehensive national cybersecurity model that includes not only infrastructure defense but also protection of informational and ethical standards in media.

- Enhance the mandate and operational capacity of the National Cybersecurity Coordination Center to oversee threat assessment, strategic planning, and rapid response to emerging cyber risks across all sectors, including critical infrastructure and media platforms.
- Develop and institutionalize mechanisms for the proactive identification, reporting, and public disclosure of vulnerabilities in information systems, thereby promoting transparency and reinforcing societal trust in digital governance.
- Implement obligatory, periodic security audits and stress tests for essential digital infrastructure, with priority given to government services, e-government portals, and mass media outlets, to ensure resilience against cyberattacks.
- Introduce comprehensive legal frameworks and nationwide educational initiatives aimed at improving media literacy, fostering critical thinking, and increasing public awareness of cyber threats and disinformation campaigns.
- Promote structured public-private partnerships and active collaboration with civil society organizations, particularly in areas related to media content regulation, counter-disinformation strategies, and the establishment of responsible digital practices.
- Establish and enforce national standards for the ethical use of Artificial Intelligence, focusing on algorithmic transparency, content moderation, and mitigation of manipulative technologies, including deepfakes, automated propaganda, and AI-driven behavioral targeting.

These initiatives should be reinforced through sustained public engagement, adherence to freedom of expression, and the preservation of the cultural and moral foundations of Kazakhstani society within the digital environment. Conclusion: Cybersecurity in Kazakhstan must transcend its traditional perception as the responsibility of technical experts and regulatory bodies. It should be conceptualized as a comprehensive, nation-wide strategy aimed at safeguarding the sovereignty, integrity, and ethical framework of the country's digital space. Only through an integrated approach–combining media accountability, technological innovation, and active civic participation–can Kazakhstan cultivate a secure, resilient, and socially responsible digital ecosystem capable of supporting democratic governance, protecting humanitarian values, and ensuring a safe online environment for future generations.

REFERENCES:

1. Postanovlenie Pravitelstva Respubliki Kazakhstan ot 30 iyunya 2017 g. № 407 «O Kontseptsii kiberbezopasnosti (Cybersecurity Kazakhstan)» [Resolution of the Government of the Republic of Kazakhstan dated June 30, 2017 No. 407 "On the Cybersecurity Concept (Cybersecurity Kazakhstan)"] // Official Internet Resource of Legal Information. Available at: https://articlekz.com/en/article/33295 (Accessed: 15 June 2026).
2. International Telecommunication Union (ITU). Global Cybersecurity Index 2024. 5th ed. Geneva: ITU, 2024. Available at: https://www.itu.int/pub/D-HDB-GCI.01-2024 (Accessed: 15 June 2026).

3. Informatsiya o kiberbezopasnosti v sfere informatizatsii [Information on Cybersecurity in the Field of Informatization] // eGov Kazakhstan. Available at: https://egov.kz/cms/en/cyberspace (Accessed: 15 June 2026).
4. Pravila sertifikatsii informatsionnoi sistemy, platformy «Elektronnoe pravitelstvo» i internet-resursa gosudarstvennogo organa na sootvetstvie trebovaniyam informatsionnoi bezopasnosti. Postanovlenie Pravitelstva Respubliki Kazakhstan ot 23 maya 2016 g. № 298 [Rules for Certification of Information Systems, the E-Government Platform and Government Internet Resources for Compliance with Information Security Requirements. Resolution of the Government of the Republic of Kazakhstan dated May 23, 2016 No. 298] // Zakon Uchet. Available at: https://zakon.uchet.kz/eng/docs/P1600000298 (Accessed: 15 June 2026).
5. Ukaz o sozdanii Ministerstva oborony i aerokosmicheskoi promyshlennosti Respubliki Kazakhstan ot 6 oktyabrya 2016 g. [Decree on the Establishment of the Ministry of Defense and Aerospace Industry of the Republic of Kazakhstan dated October 6, 2016] // Official Website of the President of the Republic of Kazakhstan. Available at: https://www.akorda.kz/en/legal_acts/decrees/on-formation-of-defense-and-aerospace-industry-ministry-of-kazakhstan-1 (Accessed: 15 June 2026).
6. Regulatory Framework for the Formation of Information Culture of Modern Kazakhstan Youth // ArticleKZ. Available at: https://articlekz.com/en/article/33295 (Accessed: 15 June 2026).
7. Nurmagambetov A.I. et al. Kontseptsiya informatsionnoi bezopasnosti Kazakhstana (pervaya versiya) [Concept of Information Security of Kazakhstan (First Version)]. Almaty, 2006.
8. Bogdanov S.V. Strategic Communications: Conceptual Approaches and Models for Public Administration // Public Administration. Electronic Bulletin. 2017. No. 61. Available at: http://e-journal.spa.msu.ru/vestnik/item_895 (Accessed: 17 March 2024).
9. Topa I., Karyda M. From Theory to Practice: Guidelines for Enhancing Information Security Management // Information and Computer Security. 2019. Vol. 27, No. 3. Pp. 326–342. DOI: 10.1108/ICS-09-2018-0108.
10. Aliyarov E.K. Informatsionnaya politika Respubliki Kazakhstan v usloviyakh globalizatsii [Information Policy of the Republic of Kazakhstan in the Context of Globalization]. Almaty: Kazakh University, 2006. P. 36.
11. Schmitt M.N. Cyberspace and International Law: The Penumbral Mist of Uncertainty // Harvard Law Review Forum. 2013. Vol. 126. No. 5. Pp. 176–180.
12. Kshetri N. The Quest to Cyber Superiority: Cybersecurity Regulations, Frameworks, and Strategies of Major Economies. Cham, Switzerland: Springer, 2016.
13. Yarovenko H. Evaluating the Threat to National Information Security // Problems and Perspectives in Management. 2020. Vol. 18. No. 3. Pp. 195–210. DOI: 10.21511/ppm.18(3).2020.17.
14. Kuznetsov A., Smirnov O., Gorbacheva L., Babenko V. Hiding Data in Images Using a Pseudo-Random Sequence // CEUR Workshop Proceedings. 2020. Vol. 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. No. 4. Pp. 257–264.
16. Christine D. et al. Beyond Supply and Demand: Addressing the Multidimensional Workforce Gaps in Cybersecurity // World Economic Forum. 21 October 2022. Available at: https://www.weforum.org/agenda/2022/10/cybersecurity-workforce-gapsinclusive-approach-jobs/ (Accessed: 15 June 2026).
17. Zhang J., Kim Y. Digital Government and Wicked Problems: Solution or Problem? // Information Polity. 2016. Vol. 21. Pp. 215–221. DOI: 10.3233/IP-160395. Available at: https://content.iospress.com/download/information-polity/ip395?id=information-polity%2Fip395 (Accessed: 24 March 2024).
18. Kak razvivaetsya kiberbezopasnost Kazakhstana [How Cybersecurity is Developing in Kazakhstan] // Strategy-2050. 28 October 2019. Available at: https://strategy2050.kz/ru/news/kak-razvivaetsya-kiberbezopasnost-kazakhstana (Accessed: 25 March 2024).
19. Ugolovnyi kodeks Respubliki Kazakhstan ot 3 iyulya 2014 g. № 226-V [Criminal Code of the Republic of Kazakhstan dated July 3, 2014 No. 226-V] (as amended and supplemented).
20. Zavhorodnii A., Ohiienko M., Biletska Y., Bondarenko S., Duiunova T., Bodenchuk L. Digitization of Agribusiness in the Development of Foreign Economic Relations of the Region // Journal of Information Technology Management. 2021. Special Issue. Pp. 123–141. DOI: 10.22059/JITM.2021.82613.