https://doi.org/10.31489/2026L1/6-19
UDC 340.341
Received: 22.10.2025 | Accepted: 11.12.2025 | Published online: 30.03.2026

L.K. Amandykova[1], G.K. Kulsharbekova[2*]

[1]*Astana International University, Astana, Kazakhstan;*
[2] *Astana Representative Office of the Distance Learning Center of the Karaganda University of Kazpotrebsoyuz, Astana, Kazakhstan*
(E-mail: kg-k@mail.ru, monamie2000@mail.ru)
ORCID ID: https://orcid.org/0000-0001-5341-1776
ORCID ID: https://orcid.org/0009-0004-3340-8798

The legal content of Kazakhstan's cybersecurity in international and national context

The aim of this study is to analyze the implementation of international cybersecurity standards in the Republic of Kazakhstan. The country actively cooperates with the United Nations and other international organizations, applying strategic approaches and regulatory mechanisms to strengthen the stability of its cyberspace. Threats such as cyberterrorism, cyber espionage, and interference in national processes are increasing, which requires intensified international cooperation. In this context, the role of the United Nations in coordinating efforts to develop universal principles and norms of state behavior in cyberspace is growing, as reflected in the adoption of new resolutions and the expanded mandate of the Open-ended Working Group on Cybersecurity. The study employs structural, logical, and dialectical methods to examine Kazakhstan's cybersecurity legislation. Additionally, international acts, scientific publications, and materials from international organizations were analyzed to establish a theoretical foundation. The results indicate that Kazakhstan's international commitments, particularly within the UN framework, play a key role in shaping its national cybersecurity policy. Active participation in international initiatives, adaptation of national legislation, and implementation of strategic programs contribute to strengthening the country's cybersecurity and integrating it into the global digital space. The incorporation of international legal norms into national legislation remains a crucial element of this process.

Keywords: cybersecurity, cyber threats, international cyber regulation, international law, UN, Kazakhstan's cyber shield, Digital Kazakhstan, Information technology, soft law, artificial intelligence.

Introduction

The increasing dependence of society on digital technologies has heightened the relevance of this topic, as it gives rise to new threats in cyberspace. In today's evolving global society, cyberspace is becoming increasingly important for economic growth, national security, and social stability. Cyberspace threats are becoming increasingly complex and diverse, necessitating coordinated efforts by the international community. Since the internet transcends borders, cyberthreats can impact multiple countries and regions, which, in turn, requires the development of effective mechanisms for international cooperation in cybersecurity and the establishment of universal regulatory standards.

Protecting personal data is becoming an important component of security in the digital age. Personal data is becoming a valuable asset and is often targeted by criminals, both for financial gain and to discredit individuals and destabilize society as a whole. Therefore, legal regulation of the collection, storage, and use of

* Corresponding author's e-mail: *kg-k@mail.ru*

personal data is becoming increasingly important, aimed at protecting privacy and preventing cybercrimes such as identity theft, identity fraud, and attacks on critical infrastructure.

The relevance of this research topic is heightened by recent global trends. In 2022–2024, many states, including the Republic of Kazakhstan, faced large-scale cyberattacks targeting public and private entities. Threats of cyberterrorism, cyberespionage, and interference in national processes through cyberspace are growing, requiring more active international cooperation.

An additional factor complicating the legal regulation of cybersecurity is the rapid development of artificial intelligence, the Internet of Things, and automated systems, which is leading to the emergence of new threats and the transformation of existing risks. In response, states are increasingly entering into bilateral and multilateral agreements aimed at strengthening cooperation in the cyber sphere, highlighting the need for a thorough study of the international legal framework for cybersecurity, particularly in the context of intensifying global technological competition.

Recognizing the scale of cyber threats, countries are developing national cybersecurity strategies and adopting laws aimed at preventing, detecting, and combating cyber threats, as well as protecting critical infrastructure and ensuring citizens' rights in the digital space.

All of the above circumstances highlight the importance of systematic scientific analysis and improvement of legal norms in the field of cybersecurity to effectively protect the interests of the state, business, and society in the context of digitalization.

The purpose of this scientific article is to study the legal content of Kazakhstan's cybersecurity in an international and national context.

Objectives:

- to study the existing international legal norms governing the field of cybersecurity;
- to analyze Kazakhstan's participation in international agreements and UN initiatives on this topic;
- to consider the mechanisms of cooperation between Kazakhstan and other countries with international organizations in the field of information security.

The purpose of the research article is to determine theoretical and legal foundations of Kazakh cybersecurity in the international and national context.

A review of the development of this issue shows that it has received little attention from domestic researchers. Kazakh researchers have not conducted a comprehensive fundamental study of this topic. A fragmentary analysis is provided on: cybercrime issues: the experience of international cooperation (Satbayeva, A.M., Alimbetova, A.R., Beisenbayeva, M.T.); legal issues in combating cybercrime: the experience of the Republic of Kazakhstan (Baimagambetova, Z.M.); international law and its response to modern security threats arising from the development of weapons and technologies (Ibragimov, Zh.I., Asanova, T.S.).

This study is based on the work of scholars such as Assaf A., Satbaeva A.M., Sidorova T.Y., and Tikk E., who specialize in international law, human rights, and global security issues, including aspects of cyberspace. These authors paid particular attention to the development of the international legal regime in cybersecurity and the role of international organizations, particularly the UN, in ensuring digital stability. Their research provided the methodological and conceptual basis for analyzing the Republic of Kazakhstan's participation in international initiatives aimed at countering cyber threats.

In Russian legal science, fundamental analyses of cybersecurity and international law have been conducted by researchers such as Yakovleva, A.V., Korostelev, D.A., and Danelian, A.A.

However, comprehensive scientific research in the Republic of Kazakhstan remains incomplete. The development of the digital economy is accompanied by increasing dependence on information technology, which leads to the emergence of new vulnerabilities and requires additional measures to protect cyberspace. The Republic of Kazakhstan, implementing its digital transformation policy within the framework of the Digital Kazakhstan program, is faced with the need to constantly update its cybersecurity legislation and actively participate in international initiatives and agreements, which is the basis for considering this topic.

The authors believe the findings of this study are useful for students majoring in law. The results of the study can be used in developing a state cybersecurity strategy, shaping Kazakhstan's foreign policy approaches, and drafting international agreements. They can also serve as a basis for educational and analytical materials in the fields of international law and ICT security.

Methods and materials

The study was conducted on the basis of an analysis of the theoretical and legal foundations of Kazakhstan's cybersecurity at the international and national levels. The information security doctrine has long been enriched by the results of applying methods such as comparative legal and institutional regulatory analysis, the result of which will make it possible to identify and highlight all the relationships, that is, all the differences and similarities between the terms being compared, we will determine the importance of the established relationships, as well as the content of such relationships, as a result. It is not only the scientific and educational block of research that is being replenished by studying international experience, However, additional scientific and legal tools are being formed to ensure the optimization of domestic legislation on the application of norms regulating cybersecurity in Kazakhstan. Peer-reviewed publications: This is an important element, as publications in peer-reviewed journals provide scientific assessment and analysis. Works focusing on comparative legal analysis or institutional aspects of cybersecurity are particularly important. The main sources for this study included regulatory legal acts of the Republic of Kazakhstan, monographs, dissertations, educational materials, and information from the United Nations. These sources were analyzed and served as the theoretical foundation for the article.

Results

Cybersecurity, as a key area of international cooperation, remains the subject of intense academic, political, legal, and diplomatic debate. The increasing frequency of cross-border cyber threats, the impossibility of effectively addressing them within the sovereignty of a single state, and the destructive potential of cyberattacks necessitate the search for sustainable international mechanisms. This necessitates a comprehensive understanding of the legal framework for cybersecurity as a cross-cutting category of international law.

For the Republic of Kazakhstan, as a state located at the intersection of geopolitical and technoeconomic zones of influence, it is especially important not only to follow international trends but also to develop its own legal identity in the digital sphere. This requires a careful study of the conceptual approaches of leading researchers, identifying patterns and contradictions, and adapting the findings to the country's national interests and international obligations.

Assaf A.'s article "Violation of State Sovereignty in Cyberspace: An Analysis Through the Prism of the UN Charter" (2024) examines a key conflict of contemporary international law: the applicability of traditional norms enshrined in the UN Charter to state actions in the cyber environment. The author analyzes Articles 2(4) (prohibition on the use of force) and 51 (the right to self-defense), as well as their interpretations in the context of cyberattacks and cyberespionage [1]. Assaf emphasizes that sovereignty in the digital age acquires not only a territorial but also an infrastructural dimension, encompassing communication networks, information resources, and even data. The problem lies in the lack of consensus on which cyber actions constitute a violation of sovereignty: cyberespionage, election interference, attacks on critical infrastructure?

This area is critically important for Kazakhstan, as the country is developing as a digital hub in Central Asia and increasingly participating in cross-border digital interactions. Given Kazakhstan's neutral position in global politics, Assaf's emphasis on the universalism of the UN Charter can serve as the basis for developing the country's legal position within the OEWG [1].

Emphasis is placed on the multilateral nature of UN efforts in the field of information security [2]. He examines in detail the evolution of the Group of Governmental Experts (GGE) and the Open-Ended Working Group (OEWG) as two key formats for developing international norms. Sidorova emphasizes in his work that, despite the absence of legally binding documents, it is these mechanisms that lay down the principles of responsible behavior in cyberspace. Particular attention is paid to the concept of "soft law", through which the UN shapes global approaches without violating the principles of sovereignty. Sidorova also points out that effective international cybersecurity is impossible without trust between states, transparency of intentions, and the voluntary exchange of strategies [2].

For Kazakhstan, Sidorova T.Y.'s work is particularly valuable, as it demonstrates a model of participation in the global legal architecture without the imposition of binding obligations. This approach aligns with Kazakhstan's foreign policy commitment to multilateralism, diplomatic flexibility, and engagement in international platforms as a bridge between East and West [2].

A strategic approach to international law focuses on institutional adaptation [3]. According to the author, international legal institutions must evolve in line with digital threats, including the creation of new working groups, digital ombudsmen, transnational cybercrime tribunals, and response institutions. He be-

lieves that the UN institutional framework needs modernization, including a review of the decision-making mechanism, expansion of the mandates of the ITU and UNODC, and the development of hybrid platforms between states and private companies. He also raises questions about the effectiveness of norm-building initiatives and the importance of engaging states in the Global South [3].

Discussion

Analysis of scientific approaches to international legal regulation of cybersecurity

Kazakhstan, as a country with growing influence in Central Asia, could use these ideas to advance its regional cybersecurity initiative. This involves establishing a UN-supported Central Asian cyber coordination center, where Kazakhstan would act as a mediator between international organizations and local states [3; 35].

Emphasizing gaps and the legal aspect of international regulation, the author argues that the lack of clear definitions of cyber aggression, digital sovereignty, and the military use of Information and Communication Technology leads to arbitrary interpretation and politicization of the law. He raises the issue of the impossibility of effective enforcement, even with the political will—particularly in matters of cyber espionage or cyber sabotage, which states often find difficult to prove or present in a legally acceptable form.

This approach is particularly relevant for Kazakhstan, as the country must consider the risks of digital attacks that are difficult to classify but can have devastating consequences for the economy or public order. Danel'yan's work highlights the need for not only legal but also technical mechanisms to verify cyber incidents. In this regard, Kazakhstan could propose participation in UN pilot programs on digital attribution.

It is emphasized that in order to effectively combat cross-border crime, it is necessary to strengthen information exchange and procedural compatibility with foreign jurisdictions. The paper shows that Kazakhstan is ready not only to adopt international experience, but also to share its own as an example of a "legal bridge" between different legal systems. This strengthens the validity of Kazakhstan's participation in global discussions at the UN and expands its diplomatic influence in the field of digital regulation [4; 113].

In June 2024, a meeting of the Committee of the Convention on Cybercrime was held in Strasbourg. Kazakhstan began to establish cooperation with the Council of Europe on combating cybercrime and was invited to join. European Treaty Series–No. 185 Convention on Cybercrime, Budapest, 23.XI.2001. This Convention will be implemented to complement applicable multilateral or bilateral treaties or arrangements European Convention on 1957 (ETS No. 24), on Mutual Legal Assistance in Criminal Matters of 1959 (ETS No. 30), and additional Protocol to it of 1978 (ETS No. 99) [5].

Authors Ibragimov Zh.I. and Asanova T.S. examine the impact of new military and technological developments, including cyber weapons, on international security. They emphasize that international law has lagged behind the pace of technological progress, and existing treaties (the Geneva Conventions, the UN Charter) do not provide sufficient responses to cyber threats. The legal vacuum in matters of cyber conflicts and attribution of responsibility is particularly acute. For Kazakhstan, which seeks to strengthen the nonproliferation regime and prevent the militarization of cyberspace, such ideas provide a basis for diplomatic initiatives at the UN aimed at developing international agreements banning cyber weapons [6; 184].

Zabikh S. has an applied focus and offers a systematic review of foreign models of legal regulation of information security, including practices of the USA, EU, China, and Russia. Particular attention is paid to the possibility of adapting these approaches to Kazakhstan's conditions. The author proposes a hybrid model that combines elements of legal control (in the spirit of the EU) and technical autonomy (in the spirit of China). Zabikh concludes that the regionalization of international norms, taking into account the specifics of CIS countries, is advisable. For Kazakhstan, this is of interest as a conceptual basis for developing a national strategy based on international experience and the principle of multi-level integration [7; 72].

There are significant differences in approaches to the legal regulation of cybersecurity in Russia and other countries. Particular emphasis is placed on institutional models, the role of the state in ensuring information security, and the balance between the public and private sectors [8]. He notes that Western models emphasize public-private partnerships and soft law, while Russia and a number of other countries focus on state control. The importance of this author's work for Kazakhstan lies in the need to determine its own regulatory model: whether to strengthen state control or pursue deregulation. Yakovleva, A.V. also offers an assessment of the potential for unifying technical standards, which is important for Kazakhstan in its dialogue with the ITU and the UN [8; 112].

Lim V.B. focuses on the evolution of information security in the Republic of Kazakhstan. He provides a detailed analysis of strategic documents (the State Program "Digital Kazakhstan", the information security

strategy, and the Law "On Personal Data") and their compliance with international standards. Lim emphasizes that Kazakhstan is moving toward harmonization with global standards, including through cooperation with international organizations. The work is useful as an empirical basis illustrating Kazakhstan's progress in the area of digital regulation. It also points to the importance of expanding Kazakhstan's participation in international initiatives on certification and cross-border data protection [9].

Korostelev, D.A. reviews the UN's activities, focusing on the GGE and OEWG documents. She emphasizes the strategic challenges facing the organization: the lack of a universal understanding of threats, differences between countries in the West and the Global South, and gaps in law enforcement. In her article, Korostelev, D.A. concludes that the UN needs to rethink its regulatory instruments—a transition from norm-building to enforcement. For Kazakhstan, this work is of interest as a justification for participation in UN mechanisms not only as an observer but also as a mediator and initiator of new initiatives [10; 590].

In his work, Danelian, A.A. emphasizes that cyberspace is a new sphere of international interaction that requires the creation of specific norms and institutions. He proposes three levels of regulation: universal (at the UN level), regional (EU, CSTO, SCO), and national. The author emphasizes that the lack of uniform definitions and standards slows the legal development of cyberspace and creates legal pluralism. For Kazakhstan, this study is valuable as an argument in favor of aligning national legislation with global and regional norms. Participation in the development of such norms, especially within the OEWG, is strategically important, so as not to be a passive object of legal regulation, but to become a subject of its formation [11; 263].

Authors Satbaeva A.M., Alimbetova A.R., and Beisenbaeva M.T. analyze international instruments to combat cybercrime, including the Budapest Convention, and emphasize the importance of bilateral and multilateral cooperation. Particular attention is paid to the role of INTERPOL, UNODC, and regional initiatives such as the digital units of the CSTO and SCO. The work is useful in demonstrating how Kazakhstan can effectively utilize existing platforms to deepen legal and operational cooperation. The authors also raise the issue of a shortage of specialists and technology, which requires state support and may become a subject of foreign policy cooperation.

The book focuses on issues of digital sovereignty, control over internet infrastructure (in particular, DNS and IP addressing), and participation in the governance of global digital resources. The author critically evaluates the dominance of Western platforms and raises the issue of "information inequality" between states. For Kazakhstan, this is important in the context of formulating a position on internet regulation. Krylov D.N., P'yankova A.A, proposes viewing the internet as a "global public good" requiring an international regulatory regime under the auspices of the UN. This paves the way for Kazakhstan to propose its own initiative to democratize internet governance.

Verhelst, E. Vauters, Y., examines the mechanisms for the formation and application of international treaties, particularly in a context where the cyber environment is evolving faster than jurisprudence. She identifies soft law, UN resolutions, and technical regulations as elements of a flexible regulatory environment [14; 141]. The author emphasizes that, in the face of political disagreements, the UN is increasingly using declarations, norms of conduct, and advisory documents rather than binding agreements. For Kazakhstan, this represents a window of opportunity: it is through the process of soft norm-building that the country can influence the formation of rules without possessing superpower status.

Analyzing the relationship between public international law, EU law, and private international law in regulating global cyberspace, she emphasizes the blurred boundaries between the public and private sectors and the growing influence of non-state actors—tech companies. Kazakhstan, as a country where digitalization is gaining momentum, could take at Yakovleva proposals into account when developing national legislation, taking into account cross-border jurisdiction, the protection of personal data, and the digital rights of citizens, while remaining within the framework of the UN Charter and global norms.

She systematizes approaches to cyber regulation in Russia and abroad, emphasizing the normative differences between "control" (Russia, China) and "liberal" (USA, EU) models [12]. Her study also provides an overview of the development of the legal framework: from the general principles of international law to specialized laws and strategies. She points out that effective cybersecurity is impossible without taking into account the transnational nature of threats and, therefore, requires interaction between the national and international levels. Yakovleva proposes the concept of a "legal compromise"—a system of flexible, but practice-based international obligations that can be adapted to the local context. For Kazakhstan, this work provides a theoretical basis for constructing a "balanced model" that combines elements of sovereign control with active participation in international mechanisms (including the OEWG at the UN) [12].

Moynihan C. views international law as a system aimed at ensuring predictability, responsibility, and mutual trust in cyberspace [13]. The author advocates for the development of universal principles of responsible behavior, including: prohibiting malicious cyber operations against critical infrastructure, respecting digital sovereignty, and cooperating on attribution issues. She points out that international law should take into account the behavior of both states and non-state actors, including transnational IT companies. This implies the need for hybrid governance models and a stronger role for the UN in regulating not only conflicts but also everyday interactions in the cyber environment [13].

For Kazakhstan, these ideas are relevant in the context of its participation in the OEWG and global normative initiatives. Kazakhstan can offer a model of cooperative regulation that accepts responsibility for actions within the national territory, but without restricting cross-border digital trade [14].

Tikk E. and Kerttunen M. analyze the evolution of the mandates of the UN Group of Governmental Experts (GGE) and its impact on the formation of norms for responsible state behavior in cyberspace. They examine the development of soft law instruments, such as the GGE reports of 2013, 2015, and 2021, which enshrine the fundamental principles of respect for sovereignty, non-interference, confidence-building measures, and transparency [14].

The authors criticize the GGE for its closed nature and propose a shift to more inclusive mechanisms—such as the OEWG, where all states can participate equally. They also emphasize the importance of aligning GGE norms with national security strategies. For Kazakhstan, this confirms the importance of participating not only as an observer in the GGE but also as an active participant in the OEWG, where it can advance its own initiatives tailored to the needs of developing countries [14].

Theoretical Framework: Universality and Adaptability of International Law

The scholarly literature on international cyberlaw demonstrates two opposing, yet largely complementary, approaches. The first, presented by Assaf and Kittichaisaree, insists on the applicability of traditional international law—primarily the UN Charter and international humanitarian law—to actions in cyberspace. According to their approach, the universal principles of sovereignty, the prohibition of the use of force, the principle of non-intervention, and the right to self-defense remain applicable in the digital environment. Furthermore, the authors believe that abandoning these norms in cyberspace would lead to the destruction of the foundations of the international legal order [1, 15].

Researchers such as Danel'yan A.A. and Verhelst, E. and Wouters, Y. take the opposite position. They argue that the digital space creates unique challenges that cannot be effectively regulated within existing legal models. In this context, soft law—a system of international political and legal documents, declarations, resolutions, and codes of conduct that, although not binding, shape the legal practices of states—is becoming a key instrument of legal evolution [4].

Kazakhstan, striving for a balance between global integration and the protection of national sovereignty, would do well to adopt a middle ground. On the one hand, it is important to recognize the applicability of fundamental norms of international law, while on the other hand, it is important to actively participate in their development and adaptation through OEWG mechanisms and participation in lawmaking within the UN [1].

Soft Law vs. Hard Law: The Dilemma of Efficiency and Legal Evolution

One of the most pressing issues is the choice between soft and hard forms of legal regulation. Researchers Tikk and Kerttunen, as well as Moynihan, emphasize the importance of "soft law", formed through resolutions, declarations, and framework commitments within the framework of the GGE and OEWG. These norms are becoming an important tool for developing agreed standards of state behavior in the digital environment and can serve as a basis for subsequent consolidation in legally binding treaties [13, 14].

In such a situation, Kazakhstan may put forward an initiative to create a hybrid international platform that combines elements of strict regulation (for example, at the conventional level) with voluntary mechanisms for monitoring, evaluation and exchange of practices.

Sovereignty in Cyberspace: Conceptual Transformations

The concept of digital sovereignty is central to the analysis of international regulation. Chernenko and Yakovleva interpret it as the state's right to fully regulate digital infrastructure, including control over data, traffic, and access infrastructure. This approach strengthens state power, but simultaneously draws criticism from proponents of an open internet and net neutrality.

In contrast, Tikk and Moynihan propose a concept of network pluralism, in which state jurisdiction is limited by international obligations and regulation is carried out with the participation of multilateral actors, ranging from intergovernmental organizations to private corporations [13, 14].

Of particular importance are the works of Lim, Zabikh, Satbayeva, and other Kazakhstani researchers, who focus on institutional, educational, and legal transformation within the country [5, 7, 9, 12]. They emphasize the need to adapt foreign experience to Kazakhstani realities, in particular, borrowing principles from EU and Russian models, but adapting them to national goals.

Given Kazakhstan's transit position between East and West, the country can offer a unique concept of "digital transit"—a model that combines compatibility with international standards, openness to cooperation, and the development of local legal and technical solutions [7, 9]. Developing digital diplomacy and establishing a national position on international cyber regulation are also becoming important tasks [12].

An analysis of scientific approaches reveals a broad spectrum of opinions, from normative universalism to pragmatic regionalism. Kazakhstan, located at the epicenter of these processes, has the potential to become an active participant and even initiator of key international processes in the field of digital regulation [1, 5, 9]. A scientific understanding of these approaches allows for the development of a balanced foreign policy strategy in the field of cybersecurity, incorporating elements of soft and hard law, protecting sovereignty, and openness to international cooperation.

The interim conclusion is that Kazakhstan should actively participate in international lawmaking, promoting its own initiatives based on the principles of accountability, transparency, legal certainty, and regional balance [1, 2, 3]. This will not only protect the country's digital interests but also contribute to the global architecture of sustainable and equitable regulation of cyberspace.

International initiatives and their impact on Kazakhstan's cyber policy: Kazakhstan is actively involved in international cybersecurity efforts. In 2024, the UN General Assembly adopted the Convention on Cybercrime, the first international criminal justice treaty in more than 20 years aimed at strengthening global cooperation in combating cyber threats. Kazakhstan supported this initiative, demonstrating its commitment to comply with international cybersecurity standards, which resulted in the signing of the Decree of the President of the Republic of Kazakhstan dated October 24, 2025 No. 1067 "UN Convention against Cybercrime; strengthening international cooperation in combating certain crimes committed using information and communication systems and in the exchange of evidence in electronic form related to serious crimes" [16].

Furthermore, in 2024, Kazakhstan ratified an agreement with the UN to organize the Asia-Pacific Ministerial Conference on Digital Inclusion and Transformation. This agreement provides for the establishment of a UN Digital Solutions Center for Sustainable Development in Central Asia in Almaty, strengthening regional cooperation and the exchange of best practices in digitalization [17].

National strategies and programs in the context of international commitments: In response to international challenges and obligations, Kazakhstan has developed and is implementing a number of national strategies and programs. One of the key ones is the "Kazakhstan Cyber Shield" cybersecurity concept, approved in 2017. It aims to ensure the protection of electronic information resources, information systems, and telecommunications networks from external and internal threats.

The "Digital Kazakhstan" State Program is also being implemented, which includes measures to establish information security operations centers, incident response services, and research laboratories. The program provides institutional support, including legislative amendments and the definition of cybersecurity standards in line with international requirements and best practices.

Improving Kazakhstan's international ranking and recognition of its efforts: Through the active implementation of national programs and participation in international initiatives, Kazakhstan has significantly improved its position in global cybersecurity rankings 2024. In September, the UN report for 2024 was published, in which Kazakhstan scored 94.04 points out of 100 possible in the second group (advanced level 2) according to the Global Cybersecurity Index. In 2024, the country ranked third in the Tier 2 ranking of the UN International Telecommunication Union, demonstrating a high level of cybersecurity development. Key initiatives contributing to this achievement include the launch of the Malicious Code Research Center, the expansion of the CyberShield-2 program, and the implementation of the Stop Credit function on EGOV [18].

Regional cooperation and integration into international structures: Kazakhstan actively participates in regional and international organizations, such as the Collective Security Treaty Organization (CSTO), the Shanghai Cooperation Organization (SCO), and the Commonwealth of Independent States (CIS). In 2019, the country ratified the Agreement on Cooperation between CSTO Member States in the Field of Information Security, strengthening collective efforts to counter cyber threats.

Furthermore, Kazakhstan advocates for increased cooperation between the CSTO and international organizations such as the UN, CIS, and SCO, which facilitates the exchange of experience and information, as well as the use of partners' potential to counter cyber threats.

The Impact of International Obligations on Domestic Cyber Policy: International commitments, particularly within the UN, play a key role in the formation and development of the domestic cyber policy of the Republic of Kazakhstan. Active participation in international initiatives, the adaptation of national legislation, and the implementation of strategic programs contribute to strengthening the country's cybersecurity and its integration into the global digital space. An important element of this process is the implementation of international law into national legislation. In accordance with the Constitution of the Republic of Kazakhstan (Article 4), international treaties ratified by the Republic of Kazakhstan take precedence over its laws, which create a legal mechanism for the direct incorporation of international norms [19].

Similarly, the provisions of UN resolutions on international information security are reflected in national strategies, such as the "Kazakhstan Cyber Shield" [20]. We see that Kazakhstan is implementing both in the form of incorporation (incorporation of norms of international treaties into the national system) and through transformation-adaptation of international norms through the adoption of national legal acts.

Concepts used in cybersecurity law

The International Organization for Standardization's International Standard "Information Technology—Security Techniques—Guidelines for Cybersecurity" contains the terms "cybersecurity", "cybercrime", "cyberspace",

Cybersecurity ISO/IEC 27002:2022 "Code of practice for information security controls" [21].

Cybersecurity is "the preservation of the confidentiality, integrity, and availability of information in cyberspace".

Cybercrime is "criminal activity in which cyberspace services or applications are the instrumentality or target of the crime or in which cyberspace itself is the source, instrumentality, target, or location of the crime".

Cyberspace is "a complex environment that results from the interaction of people, software, and services on the Internet through connected technological devices and networks, and that does not exist in physical form".

Cybersecurity is "the state of being protected from physical, social, spiritual, financial, political, emotional, professional, psychological, educational, or other negative consequences resulting from failures, damage, errors, incidents, accidents, and other events in cyberspace considered undesirable" [21].

The Republic of Kazakhstan, as a member state of the International Telecommunication Union (ITU), is subject to ITU-T Recommendation X.1208 (01/2014), "X Series: Data networks, open systems interconnection and security—Security of cyberspace: Cybersecurity". This recommendation defines the terms "cyber environment" and "cybersecurity". The cyber environment "includes users, networks, devices, all software, processes, stored or transit information, applications, services, and systems that may be directly or indirectly connected to networks" [22].

Cybersecurity is "a set of tools, strategies, security principles, security safeguards, guidelines, risk management approaches, actions, training, practical experience, insurance, and technologies that can be used to protect the cyber environment, organizational, and user resources" [22].

Organizational and user resources include connected computing devices, personnel, infrastructure, applications, services, telecommunications systems, and all information transmitted and/or stored in the cyber environment. Cybersecurity consists of an attempt to achieve and maintain security properties in organizational or user resources against relevant security threats in the cyber environment.

Common security tasks include the following: accessibility; integrity, which may include authenticity and non-repudiation; confidentiality.

The Council of Europe Convention on Cybercrime of November 23, 2001, classifies cybercrime as: 1) crimes against the confidentiality, integrity and availability of computer data and systems (illegal access, unauthorized interception, impact on data, impact on the functioning of a system, unlawful use of devices); 2) crimes related to the use of computer equipment (forgery using computer technology, fraud using computer technology); 3) crimes related to data content (crimes related to child pornography); 4) crimes related to the infringement of copyright and related rights [5].

To implement its cybersecurity program, in 2017 Kazakhstan adopted the Cybersecurity Concept (also known as the "Kazakhstan Cyber Shield" or "KS"). This document is an integral component of state policy and defines its key areas of focus in protecting electronic information resources, information systems, and telecommunications networks, as well as ensuring the secure use of information technology.

In this document, cybersecurity is understood as the state of protection of information in electronic form and the environment for its processing, storage, and transmission (electronic information resources, infor-

mation systems, and information and communication infrastructure) from external and internal threats, that is, information security in the field of informatization.

The Cybersecurity Concept "CC" notes that the classical model of information security is based on three components that ensure the security of information: confidentiality, integrity, and availability. At the same time, due to the development of communication facilities (network technologies) and the possibility of remote use of the network, authenticity and non-repudiation stand out. In Chapter 2 of this law (terms and definitions), along with such concepts as cyberspace, cybersecurity and cybercrime, another definition is given—ensuring cybersecurity, which means maintaining confidentiality, integrity and accessibility of information, but nothing is said about reliability and non-repudiation [8; 113].

In addition, the document enshrines such concepts as threats to information security, lists the most common threats and defines actions related to computer attacks, presents measures to protect information or electronic information resources and systems, and introduces the definitions of "authentication" (establishing authenticity) and "identification" [8; 115].

Key terms and concepts, such as cybersecurity, cyberspace, and cybercrime, are defined in international ISO standards and ITU recommendations, which ensures their universality and common understanding at the global level.

At the same time, the national Cyber Shield Concept of Kazakhstan does not merely replicate these definitions, but adapts them to the realities of digital sovereignty and the country's institutional capacities. It also introduces additional parameters—authenticity and non-repudiation—and links them to the stages of law enforcement practice and the development of domestic IT companies. This integration allows Kazakhstan to operate within the strict norms of hard law (application of the UN Charter and IHL norms) while simultaneously utilizing flexible soft law instruments (OEWG, GGE), creating a platform for "cooperative sovereignty" and "digital transit" in the Central Asian region. As a result, the national strategic model combines the universality of international law and the adaptability of local mechanisms, serving as a reliable foundation for the formation of a responsible, transparent, and effective legal position for Kazakhstan in the global cyberregulation arena.

The relationship between regulatory acts of the Republic of Kazakhstan in the field of cybersecurity

The development of the Republic of Kazakhstan's cybersecurity regulatory framework is based on a clear hierarchy of documents, with each subsequent act clarifying, developing, and concretizing the provisions of its predecessors. This creates an end-to-end system of legal regulation for protecting the country's digital space, ensuring the consistent development of cybersecurity at the strategic, regulatory, and applied levels.

The Law of the Republic of Kazakhstan "On National Security" laid the foundation for all subsequent legal acts in the field of cybersecurity. For the first time, national legislation clearly recognized information security as an independent component of national security. The law defined the main threats in cyberspace, established the responsibility of government agencies for ensuring information security, and created a framework for the development of specialized regulations in this area. At this stage, significant emphasis was placed on the need to create a system for protecting critical information infrastructure (CII) and international cooperation to counter cross-border cyber threats [20].

The "Kazakhstan Cyber Shield" concept developed and further elaborated on the provisions of the National Security Law, applying them to the rapidly changing digital reality. The concept proposed a strategic action plan for ensuring the state's cybersecurity, identifying the main threats, risks, areas, and mechanisms for protecting cyberspace. It established the need to create centralized cybersecurity management bodies (such as KZ-CERT), introduced the concept of categorizing critical information infrastructure facilities, and outlined measures to improve citizens' digital literacy. The concept supplemented the provisions of the National Security Law with an emphasis on the current challenges of the digital age and set guidelines for the regulatory specification of these tasks [20].

The Unified Requirements for Information and Communication Technologies and Information Security were the next step in the development of legislation, designed to specify the mechanisms for implementing the objectives set forth in the Concept. While the Concept defines the strategic goals of protecting critical information infrastructure, the Requirements establish practical requirements for critical information infrastructure entities: the procedure for categorizing objects, the mandatory certification and monitoring measures, and requirements for technical and organizational security measures. Thus, the Requirements transform strategic guidelines into specific obligations for government agencies, businesses, and other critical infrastructure operators [20].

Thus, the following relationship is established between these documents:

The Law "On National Security" sets the basis, introducing the concept of information security as an element of national security;

The "Kazakhstan Cyber Shield" concept develops and specifies the provisions of the law in relation to cyber threats, defining strategic directions;

The rules for ensuring cybersecurity of critical information infrastructure facilities implement the provisions of the Concept at the level of practical mandatory protective measures;

The Digital Kazakhstan program ensures the systemic integration of cybersecurity issues into the digitalization process, focusing on human capital, infrastructure, and regulatory support.

This structure of legal regulation reflects a general trend in international law: a combination of basic principles for protecting the information space with detailed measures and the broad involvement of civil society in digital transformation processes.

This interconnected structure of documents demonstrates that Kazakhstan is building its national cybersecurity system in line with international practice, adhering to the principles of comprehensiveness, consistency, and multi-layered approaches recommended by the UN, OSCE, and other international organizations.

Thus, key terms and concepts such as "cybersecurity", "cyberspace", "cybercrime", and "cybersecurity" are enshrined in international ISO standards and ITU recommendations, ensuring their universality and mutual understanding globally. At the same time, the national "Kazakhstan Cyber Shield" concept not only replicates these definitions but adapts them to the realities of digital sovereignty and the country's institutional capabilities, introducing additional parameters—authenticity and applicability—and linking them to the stages of law enforcement practice and the development of domestic IT.

This integration allows Kazakhstan to operate within the strict norms of hard law (the application of the UN Charter and IHL) while simultaneously utilizing flexible soft law instruments (OEWG, GGE), creating a platform for "cooperative sovereignty" and "digital transit" in the Central Asian region. As a result, the national strategic model combines the universality of international law with the adaptability of local mechanisms, serving as a reliable foundation for the development of a responsible, transparent, and effective legal position for Kazakhstan in the global cyberregulation arena.

It should be noted that international obligations, particularly within the UN, have a significant impact on the development of Kazakhstan's domestic cyber policy. Adapting international norms and standards helps strengthen national cybersecurity, increase the effectiveness of the fight against cybercrime, and improve the country's position in international rankings. Kazakhstan continues to actively integrate into the global digital space, demonstrating its commitment to international standards and aspirations for leadership in cybersecurity.

Conclusion

This study aimed to analyze the international legal framework for cybersecurity and the specifics of the Republic of Kazakhstan's participation in relevant United Nations initiatives. Key international legal documents were examined, including UN resolutions, reports of the Group of Governmental Experts (GGE), materials of the Open-Ended Working Group (OEWG), and International Telecommunication Union (ITU) standards.

Kazakhstan's participation in international platforms is analyzed, and its practical steps to implement global approaches to cybersecurity are reflected.

Firstly, international commitments, particularly within the UN, have played a significant role in structuring the Republic of Kazakhstan's domestic cyber policy. The implementation of soft law standards enshrined within the OEWG and GGE occurs both through the direct adaptation of norms into national legislation and through the development of practical mechanisms (CERT centers, response strategies, critical information infrastructure classification, etc.).

Secondly, Kazakhstan is demonstrating positive dynamics in international rankings (for example, the ITU Global Cybersecurity Index), confirming the effectiveness of its domestic policies. However, it is important to note that the ranking reflects not only regulatory frameworks but also the actual functioning of technical structures, international participation, and the level of human resources—factors that require continuous strengthening.

Third, the adaptation of international norms to Kazakhstani jurisdiction occurs with a lag of two to three years. Between 2017 and 2023, there was a tendency to reduce this lag through targeted reforms, but certain

barriers remain: difficulties with interagency coordination, a shortage of qualified ICT lawyers, and problems synchronizing technical and legal standards.

Based on the above, the following recommendations are formulated:

Continue active participation in the UN OEWG, putting forward proposals reflecting the interests of developing digital economies, including technical assistance mechanisms, human resource exchange and data sovereignty standards.

Develop the initiative to create a Central Asian Cyber Coordination Center, coordinating interaction between the states of the region, international organizations and the private sector.

Accelerate internal harmonization of terminology and procedures, based on ITU standards and UN recommendations, including the mandatory inclusion of soft law documents in curricula and regulations.

Promote the implementation of digital diplomacy into the structure of the Ministry of Foreign Affairs and expand the powers of digital attachés at diplomatic missions in the UN, EU, ASEAN and other countries.

Thus, this work represents both a theoretical contribution to the development of international cyberlaw and a practical resource for improving the state policy of the Republic of Kazakhstan in the context of global digital transformation. The findings and recommendations can be used as a basis for further research, the preparation of strategic documents, and the development of a constructive foreign policy position for the country in the international arena.

References

1 Ассаф А. Нарушение государственного суверенитета в «киберпространстве»: взгляд через призму Устава ООН / А. Ассаф // Журнал ВШЭ по международному праву. HSE University Journal of International Law. — 2024. — 1(3). — С. 4–20. https://doi.org/10.17323/jil.2023.18848

2 Сидорова Т.Ю. Международная информационная безопасность: правовые аспекты и деятельность ООН [Электронный ресурс] / Т.Ю. Сидорова // Сибирский юридический вестник. — 2020. — № 3 (90). — С. 103–108. — Режим доступа mezhdunarodnaya-informatsionnaya-bezopasnost-pravovye-aspekty-i-deyatelnost-oon (1).pdf

3 Горелик И.Б. Возможные направления развития международно-правовых институтов в области обеспечения глобальной кибербезопасности [Электронный ресурс] / И.Б. Горелик // Международное право. — №2. — 2023. — Режим доступа https:/nbpublish.com/library_read_article.php?id=40618. DOI: 10.25136/2644 5514.2023.2.40618 EDN: UZESRS

4 Данельян А.А. Киберпространство и международное право [Электронный ресурс] / А.А. Данельян // Международный правовой курьер. — Режим доступа https://inter-legal.ru/kiberprostranstvo-i-mezhdunarodnoe-pravo?ysclid=mi2pjp9ql3599785180

5 Convention on Cybercrime (ETS No. 185). — [Electronic resource]. — Access mode: https://www.coe.int/en/web/conventions/full-list?module=treaty-detail&treatynum=185

6 Ibragimov Zh.I. International law and its response to modern security threats that stem from developments in weaponry and technology / Zh.I. Ibragimov, T.S. Assanova // Bulletin of L.N. Gumilyov Eurasian National University Law Series. — 2023. — 143(2). — P. 182–190. https://doi.org/10.32523/2616-6844-2023-143-2-182-190

7 Zabikh S.A. International Experience of Legal Support of Information Security and the Possibilities for its Application in the Republic of Kazakhstan / S.A. Zabikh // PP 3 '20 International Experience of Legal Support of Information Security. — 2020. — P. 71–85. DOI: 10.14746/pp.2020.25.3.6

8 Яковлева А.В. Кибербезопасность и ее правовое регулирование (зарубежный и российский опыт) [Электронный ресурс] / А.В. Яковлева // Информационное право. — 2021. — № 4. — С. 70–81. — Режим доступа https://cyberleninka.ru/article/n/kiberbezopasnost-i-ee-pravovoe-regulirovanie-zarubezhnyy-i-rossiyskiy-opyt. DOI: 10.33693/2223-0092-2021-11-4-70-81

9 Лим В.Б. Развитие информационной безопасности в Казахстане [Электронный ресурс] / В.Б. Лим // Наука, техника и образование. — 2020. — № 11(75). — Режим доступа https://cyberleninka.ru/article/n/razvitie-informatsionnoy-bezopasnosti-v-kazahstane

10 Коростелев Д.А. Ответ ООН на киберугрозы в современных международных отношениях [Электронный ресурс] / Д.А. Коростелев // Международные отношения и диалог культур. — 2020. — № 2. — С. 587–590. — Режим доступа https://elar.urfu.ru/bitstream/10995/95664/1/978-5-7996-3164-2_2020_186.pdf

11 Данельян А.А. Международно-правовое регулирование киберпространства [Электронный ресурс] / А.А. Данельян // Образование и право. — 2020. — № 1. — С. 261–269. — Режим доступа https://cyberleninka.ru/article/n/mezhdunarodno-pravovoe-regulirovanie-kiberprostranstva. DOI 10.24411/2076-1503-2020-10140

12 Информационная безопасность Казахстана оказалась вне закона [Электронный ресурс] // Kursiv Media. — 2019. — Режим доступа: https://kz.kursiv.media/2019-07- 25/informacionnaya-bezopasnost-kazakhstana-okazalas-vne-zakona/

13 Moynihan C. The Vital Role of International Law in the Framework for Responsible State Behaviour in Cyberspace [Electronic resource] / C. Moynihan // Research Gate. — 2020. — Access mode:

https://www.researchgate.net/publication/346561548_The_vital_role_of_international_law_in_the_framework_for_responsible_state_behaviour_in_cyberspace

14 Tikk E. What are we talking about when we talk about international cybersecurity? [Electronic resource] / E. Tikk, M. Kerttunen // Routledge handbook of international cybersecurity. — 2020. — Access mode: https://researchportal.helsinki.fi/en/publications/what-do-we-talk-about-when-we-talk-about-international-cybersecur/

15 Kittichaisaree K. Application of International Humanitarian Law and the Law of Armed Conflict in Cyberspace [Electronic resource] / K. Kittichaisare // Central Asian Journal of Social Sciences and Humanities. — 2017. — P. 201–231. — Access mode: https://www.researchgate.net/publication/314156045_Application_of_the_Law_of_Armed_Conflict_Including_International_Humanitarian_Law_In_Cyberspace

16 О подписании Конвенции Организации Объединенных Наций против киберпреступности; укрепление международного сотрудничества в борьбе с определенными преступлениями, совершаемыми с использованием информационно-коммуникационных систем, и в обмене доказательствами в электронной форме, относящимися к серьезным преступлениям. Указ Президента Республики Казахстан от 24 октября 2025 года № 1067. — [Электронный ресурс]. — 2025. — Режим доступа https://adilet.zan.kz/rus/docs/U2500001067

17 О ратификации Соглашения между Правительством Республики Казахстан и Организацией Объединенных Наций об организации Азиатско-Тихоокеанской министерской конференции по цифровой инклюзии и трансформации Закон Республики Казахстан от 15 июля 2024 года № 124-VIII ЗРК. — [Электронный ресурс]. — Режим доступа: https://https://adilet.zan.kz/rus/docs/Z2400000124

18 International Telecommunication Union. Global Cybersecurity Index 2024: Country Results — Kazakhstan. — [Electronic resource]. — Access mode: https://www.itu.int/epublications/publication/global-cybersecurity-index-2024

19 Конституция Республики Казахстан от 30 августа 1995 г. (с изм. и доп. на 2023 г.). — [Электронный ресурс]. — Электронный портал нормативных правовых актов РК. — Режим доступа: https://adilet.zan.kz/rus/docs/K950001000_

20 Постановление Правительства Республики Казахстан от 30 июня 2017 г. № 407 «Об утверждении Концепции кибербезопасности («Киберщит Казахстан»). — [Электронный ресурс]. — Режим доступа: https://online.zakon.kz/rus/docs/1706Ffhvgj

21 ISO/IEC 27002:2022 Information security, cybersecurity and privacy protection — Information security controls [Electronic resource]. — 2022. — Access mode: https://www.iso.org/standard/75652.html/

22 Серия x: сети передачи данных, взаимосвязь открытых систем и безопасность x.1208 (01/2014). Безопасность киберпространства — Кибербезопасность. Показатель риска в области кибербезопасности для укрепления доверия и безопасности при использовании электросвязи/информационно-коммуникационных технологий. — [Электронный ресурс]. — 2014. — Режим доступа: https://www.itu.int/ITU-T/recommendations/rec.aspx?rec=11950&lang=ru. T-REC-X.1208-201401-I!!PDF-R.pdf.

Л.К. Амандықова, Г.Қ. Құлшарбекова

Халықаралық және ұлттық контекстегі Қазақстан киберқауіпсіздігінің құқықтық мазмұны

Мақаланың мақсаты — киберкеңістіктің тұрақтылығын нығайту мақсатында Біріккен Ұлттар Ұйымымен және басқа да халықаралық ұйымдармен белсенді түрде өзара әрекеттесетін, әртүрлі стратегиялық тәсілдер мен реттеуші механизмдерді қолданатын Қазақстан Республикасында тиімді халықаралық киберқауіпсіздік стандарттарын енгізуді талдау. Кибертерроризм, кибертыңшылық және киберкеңістік арқылы ұлттық процестерге араласу қаупінің өсуі байқалады, бұл неғұрлым белсенді халықаралық ынтымақтастықты талап етеді. Осыған байланысты киберкеңістіктегі мемлекеттердің тәртібінің әмбебап қағидаттары мен нормаларын әзірлеу жөніндегі күш-жігерді үйлестірудегі БҰҰ-ның рөлі артып келеді, бұл жаңа қарарлардың қабылдануы және Киберқауіпсіздік жөніндегі ашық топтың мандатының кеңеюімен дәлелденеді. Әдістер ретінде киберқауіпсіздік саласындағы қазақстандық заңнаманың нормаларын зерделеу үшін құрылымдық, логикалық және диалектикалық әдістер пайдаланылды. Тұжырымдардың теориялық негізін әзірлеу үшін халықаралық актілердің нормалары, ғылыми еңбектер, халықаралық ұйымдардың материалдары да зерттелді. Нәтижесінде халықаралық міндеттемелер, әсіресе БҰҰ шеңберінде, Қазақстанның ішкі киберсаясатының қалыптасуы мен дамуында маңызды рөл атқаратынын көрсетеді. Халықаралық бастамаларға белсенді қатысу, ұлттық заңнаманы бейімдеу және стратегиялық бағдарламаларды іске асыру елдің киберқауіпсіздігін нығайтуға және оның жаһандық цифрлық кеңістікке интеграциялануына ықпал етеді. Бұл процестің маңызды элементі халықаралық құқық нормаларын ұлттық заңнамаға енгізу.

Кілт сөздер: киберқауіпсіздік, киберқауіптер, халықаралық киберреттеу, халықаралық құқық, БҰҰ, Қазақстанның кибер қалқаны, Цифрлық Қазақстан, ақпараттық технологиялар, жұмсақ құқық, жасанды интеллект.

Л.К. Амандыкова, Г.К. Кульшарбекова

Правовое содержание кибербезопасности Казахстана в международном и национальном контексте

Целью исследования является анализ внедрения эффективных международных стандартов кибербезопасности в Республике Казахстан, при этом государство стремится к укреплению устойчивости своего киберпространства, активно взаимодействует с Организацией Объединённых Наций и иными международными организациями, использует различные стратегические подходы и механизмы регулирования. Отмечается рост угроз кибертерроризма, кибершпионажа и вмешательства в национальные процессы через киберпространство, что требует более активного международного сотрудничества. На этом фоне усиливается роль ООН в координации усилий по разработке универсальных принципов и норм поведения государств в киберпространстве, что проявляется в принятии новых резолюций и расширении мандата Группы открытого состава по вопросам кибербезопасности. В качестве методов использованы структурный, логический и диалектический методы для изучения норм казахстанского законодательства в области кибербезопасности. Для составления теоретической основы также были изучены нормы международных актов, научные труды, материалы международных организаций. Результатами выступили международные обязательства, особенно в рамках ООН, которые играют ключевую роль в формировании и развитии внутренней киберполитики Республики Казахстан. Активное участие в международных инициативах, адаптация национального законодательства и реализация стратегических программ способствуют укреплению кибербезопасности страны и её интеграции в глобальное цифровое пространство. Важным элементом этого процесса является имплементация норм международного права в национальное законодательство.

Ключевые слова: кибербезопасность, киберугрозы, международное киберрегулирование, международное право, ООН, киберщит Казахстана, Цифровой Казахстан, информационные технологии, мягкое право, искусственный интеллект.

References

1 Assaf, A. (2024). Narushenie gosudarstvennogo suvereniteta v «kiberprostranstve»: vzgliad cherez prizmu Ustava OON [Violation of state sovereignty in cyberspace: an analysis through the prism of the UN charter]. *Zhurnal Vysshei Shkoly Ekonomiki po mezhdunarodnomu pravu — Journal of the Higher School of Economics (HSE) on International Law, 1*(3), 4–20. https://doi.org/10.17323/jil.2023.18848 [in Russian].

2 Sidorova, T.Y. (2020). Mezhdunarodnaia informatsionnaia bezopasnost: pravovye aspekty i deiatelnost OON [International information security: legal aspects and UN activities]. *Sibirskii Yuridicheskii vestnik — Siberian Legal Bulletin,* 3(90), 103–108. Retrieved from https://cyberleninka.ru/article/n/mezhdunarodnaya-informatsionnaya- bezopasnost-pravovye-aspekty-i-deyatelnost-oon [in Russian].

3 Gorelik, I.B. (2023). Vozmozhnye napravleniia razvitiia mezhdunarodno-pravovykh institutov v oblasti obespecheniia globalnoi kiberbezopasnosti [Possible directions for the development of international legal institutions in the field of global cybersecurity]. *Mezhdunarodnoe pravo — International Law*, 2. Retrieved from https://cyberleninka.ru/article/n/vozmozhnye-napravleniya-razvitiya-mezhdunarodno-pravovyh-institutov-v-oblasti-obespecheniya-globalnoy- kiberbezopasnosti [in Russian].

4 Danel'yan, A.A. (2023). Kiberprostranstvo i mezhdunarodnoe pravo [Cyberspace and international law]. *Mezhdunarodnyi pravovoi kurer — International legal courier.* Retrieved from https://inter-legal.ru/kiberprostranstvo-i-mezhdunarodnoe-pravo?ysclid=mi2pjp9ql3599785180 [in Russian].

5 Convention on Cybercrime (ETS No. 185). *coe.int.* Retrieved from https://www.coe.int/en/web/conventions/full-list?module=treaty-detail&treatynum=185

6 Ibragimov, Zh.I., & Asanova, T.S. (2023). International law and its response to modern security threats that stem from developments in weaponry and technology. *Bulletin of L.N. Gumilyov Eurasian National University. Law Series, 143*(2), 182–190. https://doi.org/10.32523/2616-6844-2023-143-2-182-190

7 Zabikh, S.A. (2020). International Experience of Legal Support of Information Security and the Possibilities for its Application in the Republic of Kazakhstan. *PP 3 '20 International Experience of Legal Support of Information Security,* 71–85. DOI: 10.14746/pp.2020.25.3.6

8 Yakovleva, A.V. (2021). Kiberbezopasnost i ee pravovoe regulirovanie (zarubezhnyi i rossiiskii opyt) [Cybersecurity and its legal regulation (foreign and Russian experience)]. *Informatsionnoe pravo — Information Law*, 4, 70–81. Retrieved from https://cyberleninka.ru/article/n/kiberbezopasnost-i-ee-pravovoe-regulirovanie-zarubezhnyy-i-rossiyskiy-opyt DOI: 10.33693/2223-0092-2021-11-4-70-81 [in Russian].

9 Lim, V.B. (2020). Razvitie informatsionnoi bezopasnosti v Kazakhstane [Development of information security in Kazakhstan]. *Nauka, tekhnika i obrazovanie — Science, technology and education,* 11(75). Retrieved from https://cyberleninka.ru/article/n/razvitie-informatsionnoy-bezopasnosti-v-kazahstane [in Russian].

10 Korostelev, D.A. (2020). Otvet OON na kiberugrozy v sovremennykh mezhdunarodnykh otnosheniiakh [The UN's response to cyber threats in modern international relations]. *Mezhdunarodnye otnosheniia i dialog kultur — International Relations and Intercultural Dialogue,* 2, 587–590. Retrieved from https://elar.urfu.ru/bitstream/10995/95664/1/978-5-7996-3164-2_2020_186.pdf [in Russian].

11 Danelian, A.A. (2020). Mezhdunarodno-pravovoe regulirovanie kiberprostranstva [International legal regulation of cyberspace]. *Obrazovanie i pravo — Education and law,* 1, 261–269. Retrieved from https://cyberleninka.ru/article/n/mezhdunarodno-pravovoe-regulirovanie-kiberprostranstva. DOI 10.24411/2076-1503-2020-10140 [in Russian].

12 (2019). Informatsionnaia bezopasnost Kazakhstana okazalas vne zakona [Kazakhstan's information security has been outlawed]. *Kursiv Media. kz.kursiv.media*. Retrieved from https://kz.kursiv.media/2019-07-25/informacionnaya-bezopasnost-kazakhstana-okazalas-vne-zakona/ [in Russian].

13 Moynihan, C. (2020). The Vital Role of International Law in the Framework for Responsible State Behaviour in Cyberspace. *Research Gate. researchgate.net*. Retrieved from https://www.researchgate.net/publication/346561548_The_vital_role_of_international_law_in_the_framework_for_responsible_state_behaviour_in_cyberspace

14 Tikk, E., & Kerttunen, M. (2020). What are we talking about when we talk about international cybersecurity? *Routledge handbook of international cybersecurity*. Retrieved from https://unidir.org/publication/role-un-gge-advancing-international-norms-responsible-state-behaviour-cyberspace

15 Kittichaisaree, K. (2023). Application of International Humanitarian Law and the Law of Armed Conflict in Cyberspace. *Central Asian Journal of Social Sciences and Humanities,* 201–231. Retrieved from https://cajssh.centralasianstudies.org/index.php/CAJSSH/article/view/1109

16 (2025). O podpisanii Konventsii Organizatsii Obedinennykh Natsii protiv kiberprestupnosti; ukreplenie mezhdunarodnogo sotrudnichestva v borbe s opredelennymi prestupleniiami, sovershaemymi s ispolzovaniem informatsionno-kommunikatsionnykh sistem, i v obmene dokazatelstvami v elektronnoi forme, otnosiashchimisia k sereznym prestupleniiam. Ukaz Prezidenta Respubliki Kazakhstan ot 24 oktiabria 2025 goda № 1067 [On the signing of the United Nations Convention against Cybercrime; strengthening international cooperation in combating certain crimes committed using information and communication systems and in the exchange of electronic evidence related to serious crimes. Decree of the President of the Republic of Kazakhstan dated October 24, 2025 No. 1067.]. *adilet.zan.kz*. Retrieved from https://adilet.zan.kz/rus/docs/U2500001067 [in Russian].

17 (2024). O ratifikatsii Soglasheniia mezhdu Pravitelstvom Respubliki Kazakhstan i Organizatsiei Obedinennykh Natsii ob organizatsii Aziatsko-Tikhookeanskoi ministerskoi konferentsii po tsifrovoi inkliuzii i transformatsii Zakon Respubliki Kazakhstan ot 15 iiulia 2024 goda [On the Ratification of the Agreement between the Government of the Republic of Kazakhstan and the United Nations on the Organization of the Asia-Pacific Ministerial Conference on Digital Inclusion and Transformation, the Law of the Republic of Kazakhstan dated July 15, 2024]. *adilet.zan.kz.* Retrieved from https://adilet.zan.kz/rus/docs/Z2400000124 [in Russian].

18 International Telecommunication Union. Global Cybersecurity Index 2024: Country Results — Kazakhstan. *www.itu.int.* Retrieved from https://www.itu.int/en/ITU-D/Cybersecurity/Pages/global-cybersecurity-index.aspx

19 (2023). Konstitutsia Respubliki Kazakhstan ot 30 avgusta 1995 g. (s izmeneniiami i dopolneniiami na 2023 g.) [Constitution of the Republic of Kazakhstan dated August 30, 1995 (as amended)]. *adilet.zan.kz*. Retrieved from https://adilet.zan.kz/rus/docs/K950001000_ [in Russian].

20 (2017). Postanovlenie Pravitelstva Respubliki Kazakhstan ot 30 iiunia 2017 g. № 407 «Ob utverzhdenii Kontseptsii kiberbezopasnosti («Kibershchit Kazakhstan») [Resolution of the Government of the Republic of Kazakhstan dated June 30, 2017 On Approval of the Cybersecurity Concept ("Cybershield Kazakhstan")]. *online.zakon.kz.* Retrieved from https://online.zakon.kz/rus/docs/1706Ffhvgj [in Russian].

21 ISO/IEC 27002:2022 Information security, cybersecurity and privacy protection — Information security controls. *iso.org*. Retrieved from https://www.iso.org/standard/75652.html/ [in Russian].

22 (2014). Seriia x: seti peredachi dannykh, vzaimosviaz otkrytykh sistem i bezopasnost x.1208 (01/2014). Bezopasnost kiberprostranstva — Kiberbezopasnost. Pokazatel riska v oblasti kiberbezopasnosti dlia ukrepleniia doveriia i bezopasnosti pri ispolzovanii elektrosviazi/informatsionno-kommunikatsionnykh tekhnologii [x series: data transmission networks, interconnection of open systems and security x.1208 (01/2014). Cyberspace Security — Cybersecurity. A cybersecurity indicator of risk to enhance confidence and security in the use of telecommunication/information and communication technologies]. *itu.int.* Retrieved from https://www.itu.int/ITU-T/recommendations/rec.aspx?rec=11950&lang=ru [in Russian].

Information about the authors

Amandykova Leila Koshkenovna — Candidate of Law, Associate Professor, Higher School of Law, Astana International University; Astana, Kazakhstan; e-mail:monamie2000@mail.ru

Kulsharbekova Gulmira Kozybaevna — Master of Law, Senior Lecturer, Astana Representative Office of the Distance Learning Center of the Karaganda University of Kazpotrebsoyuz, Astana, Kazakhstan; e-mail:kg-k@mail.ru