Л.Н. Гумилев атындағы Еуразия ұлттық университетінің ХАБАРШЫСЫ.
ISSN: 2616-6844. eISSN: 2663-1318

ҚҰҚЫҚ СЕРИЯСЫ/ LAW SERIES/ СЕРИЯ ПРАВО

Қылмыстық құқық. Қылмыстық процесс / Criminal law. Criminal process / Уголовное право. Уголовный процесс

IRSTI 01.07.01 https://doi.org/10.32523/2616-6844-2026-154-1-205-217
Scientific article

Problems of Legal Regulation of Cyber Violations in Kazakhstan and Ways to Eliminate Them

A.B. Mukhamedzhan[1], A.S. Ibrayeva[2], S.E. Assanova*[3]

[1,2,3]Al-Farabi Kazakh National University, Almaty, Kazakhstan

(E-mail: [1]akmow.009@gmail.com, [2]ibraeva_tgp@mail.ru, [3]saida.assanova2020@gmail.com)

Abstract. This article explores the challenges of ensuring cybersecurity and regulating cybercrime in Kazakhstan in the context of international best practices. The leading goal of the study is to identify weaknesses in national cybersecurity legislation and propose ways to enhance threat prevention by examining the experiences of the United States, the European Union, and China. The research underlines that the rising number of cybercrimes and their cross-border nature highlight the urgent need for coordinated and comprehensive legal responses. Effective legal regulation of cybersecurity is a critical factor for protecting national information security, defending citizens' rights, and ensuring the sustainable development of the digital economy. The study analyzes significant regulatory frameworks such as the GDPR, CFAA, CLOUD Act, and China's Cybersecurity Law, focusing on their content and implementation mechanisms. Methodologically, the research applies comparative legal and regulatory analysis. It reveals key issues, including weak coordination between state and private entities and insufficient incident response mechanisms. The article presents specific recommendations, including establishing a unified coordinating body and strengthening international cooperation. The study's findings propose a valuable contribution to improving Kazakhstan's cybersecurity legal framework.

Keywords: cyber violations, cybersecurity, legal regulation, Kazakhstan, European Union, China, USA, cyberattacks, international experience, information security.

Introduction

The period of rapid development of information technologies has led to significant changes in all spheres. At the same time, this process has generated one of the most complex and pressing problems of the present day – cyber offences.

A cyber offence is any violation of law committed through the use of computer systems, networks, and data. It may be criminal (for example, cybercrime) or administrative, and it may manifest as incidents that compromise information security.

Received: 19.02.2025. Accepted: 18.03.2026. Available online: 30.03.2026

***[3]the corresponding author**

Cybersecurity is the practice of protecting users, their information systems, networks, and software from digital attacks. The unlawful acquisition of users' personal data and its use for other purposes may constitute the primary objective of cyber offences.

In this regard, especially for public institutions and large private entities, the legal regulation of cyber offences and their remediation for the purposes of safe operation in cyberspace are among the strategically important tasks for both Kazakhstan and other countries.

To date, there is no single statutory definition of the term "cybersecurity". For example, in Russia, the term "information security" is more frequently used than the concept of "cybersecurity"; however, the common task is to ensure information security and the stable operation of systems [1].

At the same time, it is known that countries such as Spain (Supreme Council, 2019), Lithuania (Ministry of National Defence, 2018), the United States (the White House, 2018), Australia (Government of Australia, 2016), France (French Republic, 2015), and Singapore (Cyber Security Agency of Singapore, 2016) use the term "cybersecurity" in their national strategies.

Although the Internet offers children opportunities for learning, it can also be a dangerous and harmful resource. In the article by Adejoke T. et al., strategies and programs for ensuring children's safety in cyberspace are discussed, as well as informing and supporting parents and guardians in protecting children in cyberspace.

It is indicated that in the United Kingdom, Canada, Norway, France, Singapore, Spain, and the United States, there are no specialized services or initiatives aimed directly at protecting children on the Internet. Estonia's violence prevention strategy (2015–2020) aims to ensure the safe use of mass media by children and adolescents and to improve their understanding of Internet dangers. In Australia, the Office of the eSafety Commissioner for children has been established to protect children from cyberbullying and provide information on the safe use of the Internet.

Despite the implementation of initiatives and programs, cybersecurity strategies in many countries must still account for the specific risks associated with adolescents' use of the Internet and develop appropriate measures to address them [2].

Given the annual increase in cyber offences, effective legal regulation is necessary to prevent, detect, and deter cybercrimes. The purpose of this article is to identify the main problems of the legal regulation of cyber offences in the Republic of Kazakhstan and to propose measures for addressing them, based on the experience of various countries.

To achieve this purpose, the legal norms of the Republic of Kazakhstan are considered and analyzed, the practice of their application is examined, and a comparative legal analysis of international experience is conducted.

The legal regulation of cyber offences comprises a set of measures adopted by the state to counter unlawful actions committed in computer systems and on the Internet. It should be noted that legal regulation is carried out not only by imposing liability on offenders, but also by preventing offences, improving the legal literacy of managers and specialists, implementing a system of technical standards, and clarifying the powers of authorized bodies.

In Kazakhstan, the legal regulation of cyber offences is carried out through the Criminal Code, the Code on Administrative Offences, the Laws "On Informatization", "On Communications", "On Personal Data and Their Protection", and other regulatory legal acts. However, these documents do not fully cover all types of cyber offences, as a result of which there arises a need for a comprehensive review of legislation, bringing it into conformity with international standards,

as well as increasing the level of specialization of law-enforcement agencies in order to enhance the effectiveness of legal regulation in this sphere.

Methodology

This scientific work examines the legal regulation of cyber offences in the Republic of Kazakhstan and the ways of preventing them. Improving Kazakhstan's cybersecurity regulatory framework based on international experience enables effective management of cyber offences and their prevention.

During the research, legislative acts of the Republic of Kazakhstan relating to cybersecurity were analyzed, including the "Cyber Shield of Kazakhstan" Concept, as well as the legislation of the People's Republic of China and the European Union in this field. The methodological basis of the work consisted of comparative legal analysis, system analysis, and analysis of regulatory legal acts.

Results and Discussion

The main difficulties currently associated with cyber offences include the ability of malefactors to commit several unlawful actions simultaneously, as well as the complexity of establishing their location. Taking these difficulties into account, our country is adopting strategic measures to prevent and counter them.

In particular, pursuant to the "Kazakhstan-2050" Strategy and the Address of the Head of State, "The Third Modernization of Kazakhstan: Global Competitiveness", in June 2017, the "Cyber Shield of Kazakhstan" Concept (hereinafter referred to as the "Concept") was developed. It defines the legal and organizational foundations for ensuring cybersecurity. The Concept is aimed at protecting state-significant information, information held by other organizations and institutions, and ensuring security in the use of information and communication technologies.

The document covers key issues, including cybersecurity, international experience, goals and objectives, expected results and implementation timeframes, core principles and approaches, and a list of regulatory legal acts that facilitate the implementation of the Concept.

The primary goal of the Concept is to ensure sustainable development of the country by increasing the protection of information systems and infrastructure from internal and external cyberattacks. The Concept envisages implementation in two stages. At the first stage (2017–2018), it provides advanced training of specialists in information security and the creation of mechanisms for cooperation to develop domestic IT solutions. These efforts should form the basis for expanding the participation of Kazakhstani IT companies in ensuring information security at the second stage (2019–2022). By 2022, under the second stage, Kazakhstan was planning to bring the Global Cybersecurity Index (GCI) score to 0.600.

In Kazakhstan, the number of mobile network users increased threefold from 2010 to 2016. This emphasizes the importance of Internet access, especially in cases of restricted availability or service disruptions. The triggers contributing to the spread of cyber violations in the country include a low level of legal literacy in information security, occurring often violations of technical standards and information regulations, employee errors, and damaging activities by foreign intelligence services and international cybercriminal structures. Therefore, there is a need to review the legislation and introduce the necessary additions.

Among domestic regulatory acts, first and foremost, Articles 205–207 of the Criminal Code of the Republic of Kazakhstan should be noted, which provide for liability for cybercrimes (for example, unlawful access to information systems, unlawful acquisition of information, etc.). The Laws "On Informatization" (2015) and "On National Security" (2012) also fix norms for protecting information security and cyberspace. However, these laws do not contain a clear classification of cyber offences and are insufficiently adapted to modern types of cyber threats.

In accordance with the cybersecurity Concept, models of public administration and legal regulation have been developed in certain countries, in which information security is considered alongside cybersecurity issues. For example, in Norway, the information security strategy presupposes heightened requirements for users in the operation of services and devices. Information system security in Estonia is governed by legal frameworks.

France underscores the need to counter incidents that compromise the availability, integrity, and confidentiality of information systems, concentrating on technical protection measures, fighting cybercrime, and establishing a cyber shield.

Germany's strategy aims to ensure the security of critical information systems, prevent cyberattacks, support legal prosecution of cybercriminals, and prevent technological failures. It includes national and international measures to safeguard the integrity of information systems.

Thus, each country has developed its own unique system to prevent cybercrimes, with differing strategies and mechanisms.

The cybersecurity Concept states that this sphere is based on several important principles. First, cybersecurity is an important component of national security and is aimed at safeguarding the legal interests of the government, society, and private entities. Second, cybersecurity policy should be consistent, centralized, and systemically managed.

Third, ensuring cybersecurity is a shared responsibility of the government, the private sector, and citizens. All parties bear responsibility for adhering to security requirements within the scope of their operations. Fourth, particular attention should be given to preventive measures, threat prevention, and risk management systems, which enable timely responses to potential risks.

The next principle is the use of contemporary and advanced technologies. An efficient response to cyberattacks requires the use of intelligent systems and artificial intelligence. The sixth principle is the development and creation of human resources and the formation of a culture of knowledge, both of which contribute to the long-term growth of the cybersecurity sphere.

Additionally, there must be open and trust-based cooperation between public entities and citizens. And finally, but no less importantly, international cooperation. Since cyber threats do not recognize state borders, common international standards and international partnerships are necessary [3].

It should be noted that, according to the latest edition of the Global Cybersecurity Index (GCI) for 2024, prepared by the International Telecommunication Union (ITU), Kazakhstan was assigned to Tier 2 alongside countries such as Canada, China, and Russia, with an overall score of 85-95. This tier indicates a high degree of the state's commitment to ensuring cybersecurity through coordinated and government-led actions covering the development, assessment, and implementation of widely recognized cybersecurity mechanisms across a number of key areas.

Nevertheless, despite the progress achieved and the good results, the problems in the legal regulation of cyber offences remain relevant. That is, despite a high position in the GCI, the quality and effectiveness of legislative mechanisms to counter cybercrime do not always match

that level. In this regard, there is a need to conduct a comprehensive legal examination of existing acts and to implement new approaches, including bringing national legislation into conformity with international standards [4].

Among Kazakhstani researchers studying cybersecurity issues, such legal scholars as Imangaliyev N.K. and Temirzhanova L.A. may be noted. According to their research, one reason for the widespread prevalence of cybercrime on the Internet may be the limited knowledge of IT specialists and organizational managers regarding information protection legislation. For example, in some organizations, employees are not trained in cybersecurity, leading to unauthorized access to confidential data [5].

In the countries of the European Union, in response to the growth of cyberattacks (in 2022-2023, approximately 2,580 cybercrimes were registered), various legal, organizational, and technical measures are being adopted at the national and international levels. According to the latest data, cyber offences span sectors including banking, media, energy, healthcare, and industry – all of which have been victims of cybercrime. The consequences of such offences may include crisis situations, financial losses, production suspensions, a decrease in consumer numbers, loss of trust, costs of business recovery, and possible legal liability. This underscores the cross-sectoral nature of the digital space and the vulnerability of any organization to cyber threats.

In addition, cybercrimes adversely affect individual rights and freedoms. For example, cyberattacks may lead to breaches of the confidentiality of citizens' personal data. Subsequently, stolen data may be used for extortion, fraud, and other criminal purposes. In European Union legislation, such cases are treated as a violation of citizens' fundamental rights to the protection of personal data (Article 16 of the Treaty on the Functioning of the European Union and Articles 7 and 8 of the Charter of Fundamental Rights of the European Union (CFR)).

In such situations, organizations are obliged to report annually on their cybersecurity policy and the precautionary measures taken. Such reports must include not only financial indicators but also data on the company's ability to withstand cyber threats. Transparent and reliable provision of information to interested parties (investors, partners, public authorities) about current and potential risks contributes to maintaining the organization's reputation and resilience [6].

In Kazakhstan, a culture of open and accurate reporting on cybersecurity issues is only beginning to form. In our view, based on international experience, it is necessary to specify legal requirements in the field of cybersecurity and to fix at the legislative level the obligation of organizations to provide such reports, as is done in EU countries. In addition, the articles of the Criminal Code and the Code on Administrative Offences relating to cyber offences should be clear and comprehensible. At present, the legislation contains general articles such as "unlawful access to an information system" and "destruction or distortion of information"; they are insufficient for the legal assessment of new and more complex types of cyberattacks.

During the current year, important structural changes were introduced to the European Union Cybersecurity Act to strengthen the overall cybersecurity policy. According to the changes, the significance of the European Union Agency for Cybersecurity (ENISA) was increased; it was granted permanent powers, additional resources, and new tasks. In accordance with the changes, ENISA plays a key role in shaping and supporting the European cybersecurity certification framework. These measures become the primary instruments for combating cyber threats, preventing cyberattacks, and recovering from incidents.

In addition, ENISA was granted powers to enhance cooperation in responding to cybersecurity incidents within the European Union and to coordinate actions in the event of cross-border cyberattacks.

In January 2025, a targeted amendment will be introduced to the European Union Cybersecurity Act, and in April 2025, public consultations will be held to revise the Act. This will make it possible to evaluate the effectiveness of legislation and propose ways to improve it [7].

The legislative experience of European Union countries in cybersecurity may serve as an important example for Kazakhstan. The existence of a cybersecurity agency analogous to ENISA, mandatory reporting by private organizations, and a system of mandatory legal liability should be integrated into our country's legislative system. Based on this, when improving legislation in the field of cybersecurity, Kazakhstan should use the following steps:

1. Introduction of a clear classification of cybercrimes, adding specific and comprehensible articles for new types of cyberattacks;

2. Introduction of mandatory annual reporting by organizations on cybersecurity issues, which will increase the level of transparency and trust.

3. Strengthening coordinating and supervisory structures, considering European experience;

4. Conducting a legal examination to identify and eliminate deficiencies in existing legislation.

Thus, Kazakhstan will be able to assume a leading role in ensuring cybersecurity at both the national and international levels.

The development of the cybersecurity strategy in the People's Republic of China began even before the entry into force of the Cybersecurity Law, with the publication of an opinion prepared by three state bodies in August 2016. This opinion emphasized the strategic role of standards in bringing China into the ranks of "cyber powers" and in becoming the main instrument for implementing the Cybersecurity Law.

Then, in November 2017, China's National People's Congress adopted the Standardization Law (through the revision of the 1988 law), which consolidated state policy on modernizing the standardization system in line with the pace of development of China's industry and technologies.

China's national standards are applied not only through laws and regulations but also as regulatory instruments. Although they are not mandatory, companies may be required to undergo certification or pass compliance inspections against these standards. Thus, standards are used to verify companies' compliance with legislative requirements [8].

According to China's Cybersecurity Law, when creating or using network services, it is necessary to comply with approved standards and norms, including technical and organizational measures to ensure the security, confidentiality, and availability of information. Also, to enhance cybersecurity, organizations operating in the Internet sphere are recommended to develop ethical standards and internal rules. China places particular emphasis on protecting citizens' rights to the free use of the Internet within the law, preventing cybercrimes, limiting the dissemination of destructive and illegal content online, and protecting minors.

Ensuring cybersecurity is viewed in China as a primary step toward protecting national security and citizens' rights. Article 1 of China's Cybersecurity Law clearly indicates that the law's main purposes are the protection of cybersecurity, the development of the information society, and the strengthening of digital sovereignty, and Article 4 obliges the creation and continuous improvement of a cybersecurity strategy. Article 17 establishes requirements for enterprises and institutions regarding certification, testing, risk assessment, and the provision

of other security services. Thus, the Law is aimed at ensuring the stable functioning of the cybersecurity infrastructure.

Article 20 of the Law requires enterprises, universities, vocational schools, and other educational institutions to support training programs for cybersecurity specialists. The state stimulates the training of qualified specialists and the development of professional links among them.

Article 28 of the Cybersecurity Law of the People's Republic of China obliges network operators to provide technical support and assistance to public security and national security authorities for the purposes of ensuring national security and investigating criminal acts. This means that online activities are subject to strict state control, and in the event of threats to information security, the private sector is obliged to intervene. Thus, China strengthens state control and responsibility in combating cybercrime and maintaining stability in the information space [9].

Thus, China holds a special place in international cybersecurity. Cybersecurity in China is regulated by a system of legislative acts and standards. These standards are widely applied in practice by companies and organizations as normative and assessment instruments. Thus, the combination of legislation and standardization may serve as an effective instrument of governance in cybersecurity.

In addition, in China, special attention is given to enhancing human capacity through education, training, and preparation of qualified specialists. The formation of professional personnel in the field of cybersecurity is one of the strategic tasks aimed at strengthening the state's information independence.

In sum, China's approach to cybersecurity is an example of a comprehensive, centralized, and future-oriented policy. This approach may serve as an important reference point for Kazakhstan, especially when harmonizing the legal framework with international standards.

In China, the term "information security" is used, whereas in the United States, the concept "cybersecurity" is applied. The United States supports the development of a framework for the governance and use of cyberspace and digital technologies in collaboration with its allies, partners, and stakeholders around the world. This enables economic prosperity and stronger security, including the fight against cybercrime.

The United States expects that the responsible and effective use of digital technologies and interconnected networks will provide citizens with opportunities and open new ways to address global challenges. An open, harmonious, safe, and reliable Internet network is the primary instrument for achieving these goals.

However, autocratic states and other actors use cyber and digital tools to threaten international peace and stability, cause harm, exert malicious influence, and obstruct the implementation of human rights. Therefore, an innovative international policy in the field of cyberspace and digital technologies, based on respect for human rights, constitutes the foundation for the strategic, security, economic, and foreign policy interests of the United States.

In its National Security Strategy, published in October 2022, the United States identified a "free, open, secure, and prosperous world" as the basis for implementing cybersecurity and the digital economy [10].

U.S. regulatory legal acts on cybersecurity are aimed at active information protection, risk management, and timely notification of threats. By complying with such legislative requirements, organizations can prepare in advance for potential threats and demonstrate their cybersecurity responsibility.

The Cybersecurity and Information Sharing Act (CISA), adopted in 2018, allows private entities to share information on cyber threats with the government. This strategy improves

cooperation across sectors, develops guidelines to protect vital infrastructure from cyber threats, and also helps prevent and lessen the consequences of cyberattacks.

The implementation of security measures based on the U.S. National Institute of Standards and Technology (NIST) Cybersecurity Framework+ and annual reporting by accountable parties on the work completed are mandated by the Federal Information Security Modernization Act (FISMA).

The Computer Fraud and Abuse Act (CFAA), enacted in 1986, is one of the main legal tools to combat cybercrime in the United States. According to this law, unauthorized access to personal data is treated as a crime, which enables litigation in cybercrime cases. In addition, the injured party may bring a civil lawsuit to recover damages.

In addition, the Clarifying Lawful Overseas Use of Data Act (CLOUD Act), adopted in 2018, expands the capabilities of U.S. law-enforcement agencies to obtain information from servers located abroad. This law plays an important role in the collection of data necessary for criminal investigations and also strengthens protection against cybercrime in the United States. It also demonstrates the United States' aspiration to expand international control over information.

The United States also pays particular attention to strengthening international cooperation. In 2024, the "Global Cyber Alliance Initiative" (Global Cyber Alliance) was established as a joint effort by the United States, European Union countries, the United Kingdom, Australia, and Canada to combat cyber threats [11]. Within this partnership, information exchange, the creation of a coordinated system for counteracting cyberattacks, and the implementation of preventive measures are planned. The United States also continues to organize joint training, simulations, and operations to increase preparedness to counter cyberattacks.

However, despite all efforts, unresolved cybersecurity problems remain. These include insufficient coordination between public and private institutions, as well as weak rapid-response mechanisms to cyberattacks, which continue to create significant difficulties [12].

Thus, the United States' cybersecurity and regulatory activities play an important role in protecting citizens' rights and enhancing the country's significance in the global digital space. The responsible and effective use of digital technologies and network infrastructure enables the United States not only to provide new opportunities to its citizens but also to contribute to addressing pressing international problems.

The U.S. cybersecurity regulatory framework (e.g., CISA, FISMA, CFAA, CLOUD Act) provides a comprehensive set of measures to prevent cyber threats, ensure timely responses, and define legal liability. These laws ensure the coordination of actions of public and private entities and contribute to strengthening national cybersecurity [13, 14].

Additionally, the United States places strong emphasis on international cooperation and cyberattack prevention. However, as previously mentioned, in combating cyber threats, there are structural problems such as weak coordination between public and private entities and slow reactions to cyberattacks. Therefore, to further improve the United States' cybersecurity strategy, it is necessary not only to comply with legal requirements but also to implement systemic strategies that can be applied in practice.

Conclusion

In this regard, based on foreign experience, adopting a comprehensive cybersecurity law, strengthening personnel training, increasing citizens' legal culture, and strengthening international cooperation in Kazakhstan are important and urgent steps. These measures will

enable the establishment of effective legal mechanisms to counter cyber offences and ensure security and stability in the information society.

Even though the cybersecurity sphere in Kazakhstan has been actively developing in recent years, unresolved legal issues remain. First, the regulatory framework in this sphere is not yet fully developed, and rapid-response mechanisms to cyber incidents are insufficiently developed. In addition, there is weak coordination between public and private organizations, and there is no reliable specialized platform for the operative exchange of information about cyber threats.

By comparison, in countries such as the United States, the EU, China, and other developed states, cybersecurity is regarded as a priority area of national security. In these countries, alongside clear legislation, operate effective institutional structures, international alliances, and information-sharing systems. In China, for example, a strict, centralized control system governs cybersecurity, with information security prioritized. The European Union emphasizes the protection of personal data, safeguards citizens' rights through regulatory acts, and strives to prevent cyber threats.

Relying on foreign experience, we consider it appropriate to implement the following changes in the sphere of prevention and legal regulation of cyber offences in Kazakhstan:

· First, it is necessary to clarify the legislative framework relating to cybersecurity. In particular, norms are needed to clearly regulate the types of cyber offences, the measures of liability, and the classification of offences by severity.

· Second, it is proposed to establish a national coordination center analogous to the CISA agency in the United States, which would ensure the exchange of information about cyber threats and prompt responses to them. This will strengthen the interaction between public and private structures.

· Third, it is necessary to increase the significance of international cooperation. Kazakhstan, by participating in global cybersecurity alliances and partner organizations, will gain access to technical, legal, and organizational expertise. In this regard, the Global Cyber Alliance partnership, which includes the United States and EU countries, may serve as a model for emulation.

By implementing these steps, Kazakhstan will be able to establish effective legal mechanisms to counter cyber threats, strengthen digital sovereignty, and secure a significant position in international cybersecurity.

Contribution of the authors

A.B. Mukhamedzhan – developed the overall concept of the study and defined the main scientific problem concerning the legal regulation of cyber violations in Kazakhstan. He formulated the research objectives, coordinated the structure of the article, and contributed to the development of the main conclusions and recommendations.

A.S. Ibrayeva – conducted a comprehensive analysis of the national legislation of the Republic of Kazakhstan in the field of cybersecurity and digital law. She examined existing legal gaps, enforcement challenges, and institutional mechanisms for combating cyber violations. She prepared the core analytical sections of the article, including the "Results and Discussion" related to legislative shortcomings and proposed legal reforms.

S.E. Assanova – was responsible for the preparation of the introductory and methodological sections of the study. She analyzed international legal practices and comparative approaches to regulating cyber offenses, contributed to the formulation of research methods, and participated in drafting the final version of the manuscript, ensuring its academic coherence and clarity.

Gratitude, conflict of interest

This research has been/was/is funded by the Committee of Science of the Ministry of Science and Higher Education of the Republic of Kazakhstan **(Grant No. BR27101389** The introduction of artificial intelligence tools into the legislative process of the Republic of Kazakhstan to optimize and improve the efficiency and transparency of legislation).

References

1. Яковлева А.В. (2021) Кибербезопасность и ее правовое регулирование (зарубежный и российский опыт). Социально-политические науки. Т. 11. № 4. С. 79. DOI: 10.33693/2223-0092-2021-11-4-70-81.

2. Odebade, A.T. and Benkhelifa, E. (2023) A Comparative Study of National Cyber Security Strategies of ten nations. [Preprint] arXiv. Available at: https://arxiv.org/abs/2303.13938 (Accessed: 14 April 2025).

3. Постановление Правительства Республики Казахстан от 30 июня 2017 года № 407 «Об утверждении Концепции кибербезопасности ("Киберщит Казахстана")». https://adilet.zan.kz/rus/docs/P1700000407.

4. Cybersecurity Index 2024: 5th Edition. Geneva: ITU Telecommunication Development Bureau. doi: https://www.itu.int/hub/publication/d-hdb-gci-01-2024/

5. Имангалиев Н.К., Темиржанова Л.А. (2022) "Актуальные проблемы выявления и раскрытия уголовных правонарушений, совершаемых в сети Интернет", Вестник ЕНУ им. Л.Н. Гумилева. Серия Право 1(138), стр 125.

6. Boggini, C. (2024). Reporting cybersecurity to stakeholders: A review of CSRD and the EU cyber legal framework. Computer Law and Security Review, 53, Article 105987. Available at: https://doi.org/10.1016/j.clsr.2024.105987 (Accessed: 16 April 2025)

7. The EU Cybersecurity Act (2025) Digital Strategy. Available at: https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-act (Accessed: 16 April 2025).

8. Sacks, S. and Li, M.K., 2018. How Chinese Cybersecurity Standards Impact Doing Business in China. [online] CSIS. Available at: https://www.csis.org/analysis/how-chinese-cybersecurity-standards-impact-doing-business-china (Accessed 14 Apr. 2025).

9. Creemers, R., Webster, G. and Triolo, P., 2018. Translation: Cybersecurity Law of the People's Republic of China (Effective June 1, 2017). DigiChina, Stanford University. [online] 29 June. Available at: https://digichina.stanford.edu/work/translation-cybersecurity-law-of-the-peoples-republic-of-china-effective-june-1-2017/ (Accessed 14 Apr. 2025).

10. U.S. Department of State, 2024. The United States International Cyberspace and Digital Policy Strategy: Towards an Innovative, Secure, and Rights-Respecting Digital Future. [pdf] Washington, D.C.: U.S. Department of State. Available at: https://www.state.gov/wp-content/uploads/2024/07/United-States-International-Cyberspace-and-Digital-Strategy-FINAL-2024-05-15_508v03-Section-508-Accessible-7.18.2024.pdf (Accessed 19 Apr. 2025).

11. NRI Secure, 2024. A Guide to U.S. Cybersecurity Laws and Compliance. [online] NRI Secure Blog, 5 December. Available at: https://www.nri-secure.com/blog/us-cybersecurity-laws-compliance (Accessed 19 Apr. 2025).

12. А Амангельдиева А. М. Байсултанова К. Ш., 2024. Әлем елдеріндегі киберқауіпсіздік пен интернетті басқару тәжірибесін салыстырмалы саралау. In The World of Science and Education, [online] (2024). Available at: https://cyberleninka.ru/article/n/lem-elderindegi-kiber-auipsizdik-pen-internetti-bas-aru-t-zhiribesin-salystyrmaly-saralau (Accessed 19 Apr. 2025).

13. Apsimet, N.M., Smanova, A.B. and Utegenova, G.A., 2024. The role of the Internet in the evolution of fraud: a historical aspect. Bulletin of L.N. Gumilyov Eurasian National University. Law Series, No. 1(146), pp. 247–257. https://doi.org/10.32523/2616-6844-2024-146-1-247-257

14. Bisaliev, M.S. and Shakirov, K.N., 2023. Digital traces as a factor of security of personal data circulation on the Internet. Bulletin of L.N. Gumilyov Eurasian National University. Law Series, No. 1(142), pp. 81–98. https://doi.org/10.32523/2616-6844-2023-142-1-81-98

А.Б. Мұхамеджан[1], А.С. Ибраева[2], С.Э. Асанова*[3]
[1,2,3]Әл-Фараби атындағы Қазақ Ұлттық университеті, Алматы, Қазақстан
(E-mail: [1]akmow.009@gmail.com, [2]ibraeva_tgp@mail.ru, [3]saida.assanova2020@gmail.com)

Қазақстандағы кибербұзушылықты құқықтық реттеу мәселелері және оларды жою жолдары

Аңдатпа. Бұл мақалада Қазақстандағы киберқауіпсіздікті қамтамасыз ету және кибербұзушылықтарды құқықтық реттеу мәселелері халықаралық тәжірибе аясында қарастырылады. Зерттеудің негізгі мақсаты – киберқауіпсіздік саласындағы ұлттық заңнаманың әлсіз тұстарын анықтау, сондай-ақ АҚШ, Еуропалық Одақ және Қытай елдерінің тәжірибесіне сүйене отырып, киберқауіптердің алдын алу бойынша жетілдіру жолдарын ұсыну болып табылады. Зерттеуде соңғы кезде киберқылмыстардың көбеюі мен олардың трансшекаралық сипат алуы қазіргі таңда кешенді және үйлестірілген құқықтық әрекеттердің қажеттілігін көрсететіні атап өтілді. Киберқауіпсіздіктітиімдіқұқықтықреттеуұлттықақпараттыққауіпсіздіктісақтау,азаматтардың құқықтарын қорғау және цифрлық экономиканың орнықты дамуын қамтамасыз ету үшін маңызды фактор болып табылады. Ғылыми мақалада GDPR, CFAA, CLOUD Act және Қытайдың «Киберқауіпсіздік туралы» заңы сияқты ірі нормативтік актілер қарастырылып, олардың мазмұны мен қолдану ерекшеліктері сипатталған. Зерттеу әдістемесі ретінде салыстырмалы-құқықтық және нормативтік талдау әдістері қолданылды. Зерттеу нәтижесінде мемлекеттік және жеке мекемелер арасындағы үйлестірудің жеткіліксіздігі, кибероқиғаларға жедел әрекет ету тетіктерінің әлсіздігі сияқты өзекті мәселелер анықталды. Бұған қатысты ұсыныстар қатарында бірыңғай үйлестіру органын құру, халықаралық ынтымақтастықты арттыру секілді нақты қадамдар берілді. Бұл зерттеу Қазақстандағы киберқауіпсіздік саласындағы құқықтық жүйені жетілдіруге айтарлықтай үлес қосады.

Түйін сөздер: кибербұзушылық, киберқауіпсіздік, құқықтық реттеу, Қазақстан, Еуропалық Одақ, Қытай, АҚШ, кибершабуыл, халықаралық тәжірибе, ақпараттық қауіпсіздік.

А.Б. Мұхамеджан[1], А.С. Ибраева[2], С.Э. Асанова*[3]
[1,2,3]Казахский национальный университет имени аль-Фараби, Алматы, Казахстан
(E-mail: [1]akmow.009@gmail.com, [2]ibraeva_tgp@mail.ru, [3]saida.assanova2020@gmail.com)

Проблемы правового регулирования кибернарушений в Казахстане и пути их устранения

Аннотация. В статье рассматриваются проблемы обеспечения кибербезопасности и правового регулирования кибернарушений в Казахстане с учетом международного опыта. Основная цель исследования – выявление слабых сторон национального законодательства в сфере кибербезопасности, а также выработка предложений по совершенствованию механизмов предупреждения киберугроз на основе анализа опыта США, Европейского союза и Китая. В работе отмечается, что рост количества киберпреступлений и их трансграничный характер требуют скоординированных комплексных правовых действий. Эффективное правовое регулирование кибербезопасности является важным условием обеспечения национальной информационной безопасности, защиты прав граждан и устойчивого развития цифровой экономики. В статье

рассматриваются ключевые нормативные акты, такие как GDPR, CFAA, CLOUD Act и Закон КНР «О кибербезопасности», с акцентом на особенности их применения. Методология исследования включает сравнительно-правовой и нормативный анализ. В результате выявлены актуальные проблемы, такие как недостаточная координация между государственными и частными структурами, а также слабые механизмы реагирования на инциденты. В качестве рекомендаций предлагается создание единого координирующего органа и активизация международного сотрудничества. Результаты исследования вносят вклад в развитие правовой системы кибербезопасности Казахстана.

Ключевые слова: кибернарушения, кибербезопасность, правовое регулирование, Казахстан, Европейский союз, Китай, США, кибератаки, международный опыт, информационная безопасность.

References

1. Yakovleva A.V. (2021) Kiberbezopasnost' i ee pravovoe regulirovanie (zarubezhnyj i rossijskij opyt). Social'no-politicheskie nauki. T. 11. № 4. S. 79. DOI: 10.33693/2223-0092-2021-11-4-70-81.

2. Odebade, A.T. and Benkhelifa, E. (2023) A Comparative Study of National Cyber Security Strategies of ten nations. [Preprint] arXiv. Available at: https://arxiv.org/abs/2303.13938 (Accessed: 14 April 2025).

3. Postanovlenie Pravitel'stva Respubliki Kazahstan ot 30 iyunya 2017 goda № 407 «Ob utverzhdenii Koncepcii kiberbezopasnosti ("Kibershchit Kazahstana")». https://adilet.zan.kz/rus/docs/P1700000407.

4. Cybersecurity Index 2024: 5th Edition. Geneva: ITU Telecommunication Development Bureau. doi: https://www.itu.int/hub/publication/d-hdb-gci-01-2024/

5. Imangaliev N.K., Temirzhanova L.A. (2022) "Aktual'nye problemy vyyavleniya i raskrytiya ugolovnyh pravonarushenij, sovershaemyh v seti Internet", Vestnik ENU im. L.N. Gumileva. Seriya Pravo 1(138), str 125.

6. Boggini, C. (2024). Reporting cybersecurity to stakeholders: A review of CSRD and the EU cyber legal framework. Computer Law and Security Review, 53, Article 105987. Available at: https://doi.org/10.1016/j.clsr.2024.105987 (Accessed: 16 April 2025).

7. The EU Cybersecurity Act (2025) Digital Strategy. Available at: https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-act (Accessed: 16 April 2025).

8. Sacks, S. and Li, M.K., 2018. How Chinese Cybersecurity Standards Impact Doing Business in China. [online] CSIS. Available at: https://www.csis.org/analysis/how-chinese-cybersecurity-standards-impact-doing-business-china (Accessed 14 Apr. 2025).

9. Creemers, R., Webster, G. and Triolo, P., 2018. Translation: Cybersecurity Law of the People's Republic of China (Effective June 1, 2017). DigiChina, Stanford University. [online] 29 June. Available at: https://digichina.stanford.edu/work/translation-cybersecurity-law-of-the-peoples-republic-of-china-effective-june-1-2017/ (Accessed 14 Apr. 2025).

10. U.S. Department of State, 2024. The United States International Cyberspace and Digital Policy Strategy: Towards an Innovative, Secure, and Rights-Respecting Digital Future. [pdf] Washington, D.C.: U.S. Department of State. Available at: https://www.state.gov/wp-content/uploads/2024/07/United-States-International-Cyberspace-and-Digital-Strategy-FINAL-2024-05-15_508v03-Section-508-Accessible-7.18.2024.pdf (Accessed 19 Apr. 2025).

11. NRI Secure, 2024. A Guide to U.S. Cybersecurity Laws and Compliance. [online] NRI Secure Blog, 5 December. Available at: https://www.nri-secure.com/blog/us-cybersecurity-laws-compliance (Accessed 19 Apr. 2025).

12. A Amangel'dieva A. M. Bajsultanova K. SH., 2024. Alem elderindegi kiberkauipsizdik pen internetti baskaru tazhiribesin salystyrmaly saralau. In The World of Science and Education, (online) (2024). Available at: https://cyberleninka.ru/article/n/lem-elderindegi-kiber-auipsizdik-pen-internetti-bas-aru-t-zhiribesin-salystyrmaly-saralau (Accessed 19 Apr. 2025).

13. Apsimet, N.M., Smanova, A.B. and Utegenova, G.A., 2024. The role of the Internet in the evolution of fraud: a historical aspect. Bulletin of L.N. Gumilyov Eurasian National University. Law Series, No. 1(146), pp. 247–257. https://doi.org/10.32523/2616-6844-2024-146-1-247-257.

14. Bisaliev, M.S. and Shakirov, K.N., 2023. Digital traces as a factor of security of personal data circulation on the Internet. Bulletin of L.N. Gumilyov Eurasian National University. Law Series, No. 1(142), pp. 81–98. https://doi.org/10.32523/2616-6844-2023-142-1-81-98.

Information about the authors:

Mukhamedzhan A.B. **–** 3rd-year doctoral student of the Faculty of Law, Al-Farabi Kazakh National University, 050040, 71 Al-Farabi Ave., Almaty, Ka-zakhstan.

Ibrayeva A.S. **–** Doctor of Law, Professor, Al-Farabi Kazakh National University, 050040, 71 Al-Farabi Ave., Almaty, Kazakhstan.

Assanova S.E. **–** corresponding author, PhD, Deputy Dean of the Faculty of Law for Academic, Methodological and Educational Work, Al-Farabi Kazakh National University, 050040, 71 Al-Farabi Ave., Almaty, Kazakhstan.

Мұхамеджан А.Б. **–** докторант, заң факультеті, әл-Фараби атындағы Қазақ ұлттық университеті, 050040, әл-Фараби даңғылы 71, Алматы, Қазақстан.

Ибраева А.С. – заң ғылымдарының докторы, профессор, әл-Фараби атындағы Қазақ ұлттық университеті, 050040, әл-Фараби даңғылы 71, Алма-ты, Қазақстан.

Асанова С.Э. **–** хат-хабар авторы, PhD, әл-Фараби атындағы Қазақ ұлттық университеті заң факультеті деканының оқу, әдістемелік және тәрбие жұмысы жөніндегі орынбасары, 050040, әл-Фараби даңғылы 71, Алматы, Қазақстан.

Мухамеджан А.Б. **–** докторант 3 курса юридического факультета, Ка-захский национальный университет имени аль-Фараби, 050040, пр. Аль-Фараби 71, Алматы, Казахстан.

Ибраева А.С. **–** доктор юридических наук, профессор, Казахский национальный университет имени аль-Фараби, 050040, пр. Аль-Фараби 71, Алматы, Казахстан.

Асанова С.Э. **–** автор для корреспонденции, PhD, заместитель декана юридического факультета по учебной, методической и воспитательной рабо-те, Казахский национальный университет имени аль-Фараби, 050040, пр. Аль-Фараби 71, Алматы, Казахстан.