https://doi.org/10.31489/2025L1/87-97 Received: 25 November 2024 | Accepted: 27 December 2024

UDC 343.136

N.M. Apsimet[1*], A.Zh. Muratova[2]

[1]*Al Farabi Kazakh National University, Almaty, Kazakhstan;*
[2]*L.N. Gumilyov Eurasian National University, Astana, Kazakhstan*
(E-mail: Apsimet.nurdaulet@gmail.com, muratova_azh@enu.kz)

[1]*ORCID ID: https://orcid.org/0000-0002-5127-5579*
[2]*ORCID ID: https://orcid.org/0000-0002-0159-9671*
[2]*Scopus Author ID: 58650612800*

On the possibility of using the provisions of the Budapest Convention on cybercrime in the investigation of crimes in the field of online fraud

The article explores the potential of applying the provisions of the Budapest Convention on Cybercrime to improve the effectiveness of online fraud investigations in Kazakhstan. The main purpose of the work is to analyze the possibilities of the Convention in combating the growing threat of this type of crime, especially given their cross-border nature. The authors apply a comprehensive methodological approach, including an analysis of documents, a comparative study of legislation and an analysis of the practice of its application in other countries. The study revealed inconsistencies between the national legislation of Kazakhstan and the provisions of the Convention. The main issues relate to the definition of cybercrimes, digital evidence collection procedures, and international cooperation. Based on successful cases of the Convention's application in other countries, recommendations are proposed for improving legislation and law enforcement practice in Kazakhstan. In particular, the authors emphasize the need to adapt national legislation to the standards of the Convention, create specialized units to combat cybercrime, introduce digital platforms for data analysis and enhance international cooperation. This will increase the effectiveness of countering online fraud and strengthen Kazakhstan's position in the global fight against cybercrime.

Keywords: cybercrime, online fraud, Budapest Convention, international cooperation, digital evidence, legislation of Kazakhstan, law enforcement practice.

Introduction

The rapid development of information and communication technologies benefits modern society, but at the same time generates new, technologically more complex risks and threats. In recent years, there has been a rapid increase in cybercrime, especially in the field of online fraud.

According to Resolution No. 281 of the Board of the National Bank of the Republic of Kazakhstan dated October 29, 2018 On Approval of the Cybersecurity Strategy of the Financial Sector of the Republic of Kazakhstan for 2018–2022 [1], cybercrime is defined as a type of crime involving legally punishable acts committed using information technology in cyberspace.

According to Cybersecurity Ventures, it is expected that by 2026, the annual global damage from cybercrime will exceed 20 trillion US dollars [2]. This forecast highlights the scale of the problem and the need to strengthen measures to counter such threats. In recent years, there has been a significant increase in cybercrime in Kazakhstan, especially in the field of online fraud. According to the Committee on Legal Statistics and Special Accounts of the Prosecutor General's Office of the Republic of Kazakhstan, the number of registered cases of online fraud has increased more than 40 times over the past few years: from just over 500 cases in 2018 to 21.8 thousand in 2023 [3].

In the first half of 2024, 9,936 cases of online fraud were registered, which is 4.1 % more than in the same period of 2023 [4]. Fraud related to online purchases on marketplaces and bulletin boards is especially common: about 24 % of all cases [5]. The damage from such crimes is also increasing. In 2023, the amount of damage amounted to 17.5 billion tenge [6], and in the first seven months of 2024, the damage reached 7.1 billion tenge, of which only 11 % were reimbursed. Despite the efforts of law enforcement agencies, most cases of online fraud remain unsolved. In 2022, about 70 % of criminal cases for such crimes were suspended due to the failure to identify the perpetrators [7].

* Corresponding author's e-mail: *Apsimet.nurdaulet@gmail.com*

According to the rating of the Global Cybersecurity Index 2024 (GCI) [8] on the cybersecurity of countries based on 83 indicators in 5 key areas: legislation, technical equipment, organization, capacity development and international cooperation, Kazakhstan fell into the Tier 2 category — "Advancing", next to countries such as China, Austria, Canada and Azerbaijan. The report involved 194 countries. For comparison, in the previous ranking (2020/2021), based on the old methodology, Kazakhstan ranked 31st. Although the rate of development of the information society in Kazakhstan is quite high and the country has been ranking higher in the international rankings, the rise of cybercrime is also increasing and therefore there is the need to improve on the cybersecurity measures and finding better ways of fighting online fraud. This is particularly important given the need to learn more about international practices related to these issues and to ensure that the provisions of the Budapest Convention on Cybercrime are fully integrated into the investigation and prevention of such crimes.

Cybercrime has become transnational with the increase in the rate of digitalization and globalization and thus requires an appropriate response from individual states. There are several problems regarding the scope of domestic mechanisms and their misalignment with international standards that limit national legal frameworks including those of Kazakhstan from combating these threats. Cybercrime is an emerging challenge that Kazakhstan is grappling with; however, some progress has been made, for instance, in 2008 the country ratified the UN Convention against Transnational Organized Crime [9]. But the challenges in dealing with the cross-border nature of cybercriminal activity are evident given the increasing number of online fraud cases that require quick action and cooperation with other countries.

A key international framework for dealing with cybercrime is the Budapest Convention on Cybercrime of 2001 [10]. The convention was adopted with the aim of harmonizing national legislation, enhancing the means of cybercrime investigation, and improving cooperation between international organizations. It offers state parties guidance on measures to fight cybercrime, and prompts them to consider amending their substantive and procedural criminal laws. This includes establishing liability for cybercrime-related offenses and defining the methods by which criminal investigations and prosecutions should be carried out. It also has recommendations for States parties on mutual assistance and is a mutual legal assistance treaty (i.e., an agreement on cooperation in investigation and prosecution of some and/or all offences defined as such in the national laws of both parties) for countries that do not have such a treaty with the country which seeks our assistance.

Kazakhstan is not a party to the Budapest Convention on Cybercrime yet, which limits its ability to integrate into global mechanisms to combat cybercrime. However, in April 2023, Kazakhstan received an invitation to join this convention, which indicates recognition of the country's efforts in the field of cybersecurity [11].

The limitations of national legislation are reflected in the lack of unified approaches and standards in the definition of cybercrime, collection and exchange of digital evidence. This hinders the creation of effective mechanisms for cooperation with international partners. An analysis of existing problems shows that the harmonization of national legislation with international standards, including the provisions of the Budapest Convention, can increase the effectiveness of countering online fraud and other types of cybercrime.

The rapid development of digital technologies has a significant impact on the socio-economic sphere of Kazakhstan. At the same time, the growth of cyber threats, including online fraud, is becoming a serious challenge to national security and law enforcement. The problem is complicated by the cross-border nature of cybercrimes, which requires coordinated action by law enforcement agencies at the international level [12; 71]. In this situation, the provisions of the Budapest Convention are an important resource, as they ensure the unification of standards and form the basis for international cooperation.

For Kazakhstan, which is not a party to the Budapest Convention, the issue of harmonization of national legislation with international standards remains one of the key tasks in the field of countering cybercrime. Accession to the Convention could not only strengthen national efforts to investigate and prosecute cybercriminals, but also help build trust between Kazakhstan and its international partners. The application of the Convention's provisions, such as joint investigations and the rapid exchange of information, opens up new opportunities for effective solutions to the problem of online fraud.

In the context of increasing digital transformation and economic globalization, the importance of the Budapest Convention as an international legal instrument continues to grow. Its potential to strengthen the rule of law in cyberspace makes this document particularly relevant for countries such as Kazakhstan that seek to develop their approaches to cybersecurity and countering online crimes.

The purpose of this article is to analyze the possibilities of applying the provisions of the Budapest Convention on Cybercrime to improve the effectiveness of online fraud investigations in Kazakhstan.

Methods and materials

This study uses a comprehensive methodological approach, including an analysis of documents, a comparative analysis of legislation and an analysis of the practice of applying the provisions of the Budapest Convention. The analysis of the documents included the study of the text of the Budapest Convention, the legislation of the Republic of Kazakhstan in the field of combating cybercrime, as well as analytical materials and reports of international organizations. A comparative analysis of the legislation was aimed at identifying the compliance of the national legislation of Kazakhstan with the main provisions of the Budapest Convention. The analysis of the practice of applying the Convention was based on a study of publicly available materials, including judicial practice and reports from law enforcement agencies in different countries. This methodological approach made it possible to conduct a comprehensive analysis of the possibilities of applying the provisions of the Budapest Convention in Kazakhstan and formulate recommendations for improving national legislation and practice in countering online fraud.

Results

The Budapest Convention on Cybercrime is a key international instrument aimed at combating cyber threats. Its provisions create a universal legal framework for the criminal prosecution of cybercrimes, including crimes related to fraud in the digital environment [13; 306]. In the context of online fraud investigations, articles dealing with both direct violations and supporting procedures related to obtaining and processing digital evidence are of particular importance.

Article 7 of the Convention defines computer fraud as the intentional insertion, modification, deletion or suppression of computer data in order to cause property damage by deception. The introduction of this rule creates the basis for the criminal prosecution of fraudulent activities related to data manipulation in electronic systems. For Kazakhstan, the relevance of this article is particularly high, given the growing number of cases of unauthorized interference in payment systems and e-commerce platforms. From January to August 2022, 11.7 thousand cases of Internet fraud were detected in Kazakhstan, and 7 billion tenge worth of damage was caused [14]. The inclusion of this provision in the national legislation of the Republic of Kazakhstan would contribute to more effective prosecution of online fraud, which is often cross-border in nature.

The provisions of article 8 focus on the creation and use of fake computer data in order to mislead other users or systems. This aspect is also closely related to crimes aimed at stealing funds or personal information. In Kazakhstan, where efforts to digitalize the economy are accompanied by an increase in cyber threats, the application of this article can support the process of investigating crimes related to the use of forged electronic documents, especially in the financial sector. Due to the presence of a large set of national and international payment systems in the market of the Republic of Kazakhstan, there are a number of risks when working in cyberspace [1].

One of the central rules of the Convention for the investigation of online fraud is article 14, which regulates access to digital evidence. This article focuses on the need to harmonize legal procedures between countries to ensure effective access to electronic data, which is critical for investigating crimes committed in a cross-border format. For Kazakhstan, active participation in international initiatives to combat cybercrime underscores the importance of developing robust internal mechanisms. These mechanisms are crucial for ensuring compliance with the Convention's provisions, particularly through strengthened cooperation with foreign Internet service providers.

Chapter III of the Budapest Convention holds particular significance for Kazakhstan due to the increasing necessity of cross-border data exchange in online fraud investigations. The articles on mutual legal assistance, such as Article 27, set up a legal procedure for accelerating the acquisition of data related to criminal activities occurring via the Internet from platforms outside the jurisdiction of the country. Incorporating these procedures into the legal system of Kazakhstan could not only improve the effectiveness of investigations but also strengthen international cooperation — a significant factor, given the globalization of cyber threats.

A defining characteristic of online fraud is that it is inherently transnational in its nature and facilitated by the global reach of the Internet [15; 70]. In this regard, the provisions of the Budapest Convention on cross-border cooperation are pivotal. They equip member states with tools to address crimes that cross national boundaries effectively. Central to these efforts are information exchange mechanisms, streamlined co-

operation among law enforcement agencies and improved access to digital evidence, all of which are critical for effective international collaboration.

The enforcement of the Budapest Convention provisions is a significant step in enhancing Kazakhstan's capabilities in the fight against cybercrime. Such measures as improving legal bases and creating favorable conditions for cooperation with international organizations directly contribute to the fight against online fraud and other cybercrimes. Thus, the integration of Kazakhstan's domestic efforts with the global standards is in line with the country's efforts to develop effective responses to the challenges of the digital sphere.

Article 23 of the Convention is a cornerstone in facilitating international cooperation in cybercrime investigations. This provision has paved way to a comprehensive legal framework for coordinated actions, information exchange and mutual assistance between states. Adopting these measures as Kazakhstan presents a significant opportunity to enhance the country's interactions with foreign partners and thus to have more effective and timely responses to cybercrime. The simplified and structured approach of Article 23 makes transnational investigations easier and brings domestic practices in line with internationally recognized legal norms. Therefore, the mechanisms provided for in the Convention are incorporated into the legal system of Kazakhstan, which enhances the country's capacity to fight the complexities of modern cyber threats through partnership.

Another important provision is Article 25 which controls the availability of data stored outside of the national jurisdictions. In this regulation, law enforcement agencies are allowed to request and use basic information like Internet traffic logs and user account details from foreign service providers. Since most digital crimes occur on platforms based abroad, this article is crucial to enhance the efficiency of investigations. Likewise, Article 27 defines and simplifies the measures regarding mutual legal assistance requests for obtaining evidence, searching and seizing data in the context of international cooperation. To implement this article for Kazakhstan, legislative changes are needed and the creation of specific structures to manage international collaboration is necessary.

Furthermore, the 24/7 rapid response network described in Article 35 presents new possibilities for accelerating the exchange of information in cases of online fraud. In this regard, for Kazakhstan, which is strategically located at the intersection of global transportation and digital networks, this initiative greatly enhances the nation's capacity to fight transnational threats. Nevertheless, to achieve the best results, several issues must be solved, including: limited technical resources; compatibility with international procedural standards; and modernization of the technological infrastructure. To overcome these challenges, further actions are clearly required. These include the development of specialized training programs, the enhancement of the logistical capacity of law enforcement agencies and the enhancement of cooperation with international partners.

Ensuring cross-border cooperation on the basis of the provisions of the Convention is becoming an important tool in the fight against online fraud. The combination of legal, organizational and technological tools is the basis for creating mutual confidence between the countries and creation of a global system for fighting cyber threats.

The implementation of the provisions of Budapest Convention into the laws of Kazakhstan is an important step towards enhancing the efficiency of the fight against cybercrime. The Convention provides for measures such as criminalization of major types of cybercrime, simplification of access to digital evidence and the development of international cooperation. An analysis of the current legislation of the Republic of Kazakhstan shows the need for further improvement of certain norms in order to comply with international standards, which will become the basis for strengthening law enforcement practices and increasing the level of national cybersecurity.

Kazakhstan's criminal legislation establishes liability for a range of cybercrime-related offenses, including provisions of the Criminal Code of the Republic of Kazakhstan (CC RK) [16], specifically Article 190 ("Fraud") and Article 205 ("Unauthorized Interference with the Operation of an Information System") [16]. The lack of clear differentiation between traditional and cyber fraud creates legal and practical challenges in the qualification and investigation of crimes. This, in turn, leads to difficulties in preparing the evidence base necessary for successful criminal prosecution. However, the specifics of the Convention suggest a more detailed approach to the definition of cybercrimes, such as computer fraud (article 7 of the Convention) and data forgery (article 8). At this stage, there are no separate rules in the Criminal Code of the Republic of Kazakhstan concerning fraudulent manipulation of data in digital systems, which creates a legal gap in the investigation of a number of crimes committed exclusively using information and communication technologies.

Although the Criminal Procedure Code of the Republic of Kazakhstan [17] contains provisions regulating the collection and processing of evidence, their adaptation to the requirements of the digital age remains limited. One of the key requirements of the Budapest Convention is the availability of procedures for the prompt collection, preservation and provision of digital evidence (Articles 14–21). In Kazakhstan, legislation partially regulates this process through the norms of the Criminal Procedure Code of the Republic of Kazakhstan (CPC RK) concerning the seizure of electronic media and obtaining information from Internet service providers. However, there are no clearly established mechanisms in the existing legal framework, e.g., mandatory temporary storage of data by Internet service providers and specific practices of cooperation with foreign service providers. This essentially hampers the capability of law enforcement agencies to secure crucial evidence in many cases, including those that are cross border crimes.

In the fight against cybercrime Kazakhstan is actively developing cooperation with international organizations and partner countries. The standards for mutual legal assistance and operational data exchange are articles 23–35 of the Budapest Convention. At the present time the national legislation of Kazakhstan provides a legal basis for international cooperation that includes the execution of requests for legal assistance and joint investigations. However, there is one of the problems — there are no sufficiently well-defined procedures for direct communication with foreign ISP's, and there are no clear rules for requesting foreign countries within the 24/7 network or for interacting with foreign jurisdictions during joint investigative activities. It can also lead to some delays in the course of investigation and can reduce the effectiveness of the investigation.

A review of the laws of Kazakhstan shows that the country has made significant efforts to meet the standards set by the Budapest Convention; however, there are some issues that require further attention. Major problems are: 1. Not enough detail on offences of cyber fraud; 2. Low capabilities of the law enforcement agencies in preserving and acquiring digital evidence; 3. No standards for effective cooperation with foreign countries [18; 57].

To close these gaps, it is advised to modify the Criminal Code of the Republic of Kazakhstan to incorporate provisions covering cybercrimes, for instance computer fraud and data forgery. Further, modifying the Criminal Procedure Code (CPC) to provide for the storage and handling of digital evidence is also important. Also, establishing a dedicated structure for international cooperation via the 24/7 network would add weight to Kazakhstan's fight against cross border online fraud.

The practical use of the Budapest Convention is based on the fact that it facilitates international cooperation and sets standards for legal mechanisms to fight cybercrime including cyber fraud. Studying the cases where its provisions were used to investigate such crimes is a great way to understand their applicability and effectiveness in cross border operations.

The Convention is a major international treaty that establishes Joint Investigation Teams (JITs) as a central means of combating transnational crime. These teams are very useful in the collection of digital evidence like servers that have been used in fraudulent activities. The institutional support and operational coordination that the Convention provides really does improve the efficiency of the investigation. For example, Article 16 of the Budapest Convention, the data preservation provision, was very useful in a fraud case involving fake social media accounts. The cooperation with the platform providers located in the United States assisted Kazakhstan's law enforcement authorities in collecting the proof of the crime, although the perpetrators sought to erase it from the digital domain. This effort resulted in the identification and prosecution of people behind the scheme [19].

These examples reflect the central role of the Budapest Convention in cybercrime investigation especially in an international context. In this regard, Kazakhstan's experience with the effective application of the Convention stresses the need to enhance the cooperation with international partners. Important actions are: enhancing the mechanisms for mutual legal assistance, increasing cooperation through the 24/7 network, and promoting the adoption of data retention measures in the national laws. Moreover, the experience with the application of the Convention's provisions in practice underlines the necessity of the specialized professional training for law enforcement personnel. Such training should focus on the proper application of international instruments in the fight against cybercrime.

In the end, successful case studies prove that compliance with the standards of the Convention does improve the efficiency of the fight against cybercrime. This not only safeguards the rights and interests of citizens and organizations in the digital realm but also enhances the position of Kazakhstan in the global battle against cybercrime.

Discussion

Over the past two decades, the Budapest Convention has been the principal international instrument for combating cybercrime. It has been widely ratified and implemented by a number of states and has been found to be practical and effective in combating online fraud and other cyber-crimes. Studying the international experience allows identifying the critical aspects of successful implementation and, therefore, serves as a reference point for assessing Kazakhstan's practices against the global standards.

Views on the Budapest Convention are quite divergent. Some countries have pointed out that it has no enough tools for cooperation and for that reason support the need to develop a new framework; but other countries especially the EU and OECD members have explained that the Convention is a good framework for collaboration globally. They argued that it promotes international cooperation and was signed by a geographically diverse group of countries [20; 219].

Member states of the European Union are a good example of the effective implementation of the measures through the harmonization of the laws and the establishment of the common standards. For instance, Germany, one of the earliest signers of the Convention, incorporated the provisions on computer fraud (Article 7) of the Convention into its Criminal Code (Strafgesetzbuch, StGB). Another significant success is the existence of dedicated structures including the Cybercrime Investigation Division of the Federal Criminal Police Office (Bundeskriminalamt, BKA) [21]. This division guarantees proper functioning of the 24/7 network and has a strong cooperation with international partners. The integration of technical and legal measures by Germany is a good practice that Kazakhstan should follow especially in setting up of specialized agencies.

Estonia, a country famed for its digital prowess, is a good example of how digitalization can support legal frameworks. After the Convention was ratified, Estonia introduced automated monitoring systems and network traffic analysis tools that are vital for detecting and preventing online fraud. The country's international cooperation is evident in cases such as the November 2022 arrest of two nationals involved in cryptocurrency fraud amounting to $575 million. This is because the investigation was done in partnership with the United States, which shows the efficiency of collaboration within the legal frameworks [22].

Many of the Budapest Convention's provisions have been adaptively learned by Kazakhstan, but this is in comparison to much lower standards than the best international practices. Kazakhstan does not have a specialized agency fighting cybercrime, which restricts the efficiency and speed of investigations, unlike Germany. Additionally, its relation with the 24/7 cybercrime network is not yet compatible with the EU standards.

This approach of Estonia shows how the integration of technical solutions can improve the existing systems of digital law enforcement. Cyber-crime prevention and investigation has been enhanced greatly through these advancements in technologies. Such technologies are still in the process of being adopted in Kazakhstan, and this demands substantial financial resources and complete training. Moreover, the success of Estonia in the cooperation with foreign partners in the course of international investigations is also due to the existence of strong collaboration with the foreign partners. Kazakhstan has started similar cooperation; however, such cooperation has to be institutionalized to ensure that it is sustained in the future.

The United States, also a signatory of the Budapest Convention, serves as a valuable benchmark for comparing Kazakhstan, as it has integrated the Convention's provisions and bilateral legal assistance agreements into its domestic law. The main focus of the U.S. strategy is the effective application of instruments analogue to the 24/7 network and active implication in the international cooperation in the fight against fraud. By contrast, Kazakhstan has limited participation in bilateral agreements and uses the Convention at a general level. To this end, Kazakhstan should expedite the negotiation of agreements with major international partners including China, the EU and the United States, especially for the data sharing with large internet service providers (ISPs).

Global practices reflect that the effective implementation of the Budapest Convention requires an integrated approach to legislative reforms, institutional development, and technological innovation. The experiences of Germany, Estonia and the United States are varied strategies that can inform Kazakhstan's efforts. To achieve similar results, Kazakhstan must prioritize the following measures within its national framework:

- The establishment of a specialized agency to combat cybercrime;
- The creation and use of digital platforms for data monitoring and analysis;
- The enhancement of international cooperation by the negotiation and conclusion of bilateral treaties.

These strategies, if adopted, would allow Kazakhstan to better align with international standards and thus better position itself to meet the multifaceted challenges of cybercrime.

A comparison shows that based on the successful practices available, Kazakhstan has the potential to adopt the provisions of the Budapest Convention and even improve its capabilities in the fight against cybercrime, including online fraud. Nevertheless, integrating international norms such as the Budapest Convention into national legislation entails inherent challenges. These are rooted in variations in legal systems, levels of digitalization, and preparedness for international cooperation. Paring down to the root issues identified in comparing national legislation with the Convention's requirements offers a chance to plug those gaps by adopting the best of international practices.

One major problem is that there is no uniform definition of cybercrime. For instance, the Budapest Convention specifically spells out computer data fraud in Article 7 and computer forgery in Article 8, giving clear legal definitions. By contrast, the Kazakhstani laws classify such offences within more general categories like fraud (Criminal Code Article 190) or forgery (Criminal Code Article 385). This lack of distinction for digital crimes creates legal ambiguities as to what constitutes a crime and what does not, and thus what can be investigated.

Procedural inconsistencies only compound these challenges as well. Articles 16 and 17 of the Budapest Convention set forth the means of preserving and making available digital data, but Kazakhstan's procedural codes are not fully compliant with these provisions. For example, there are no rules governing the obligations of Internet service providers to store temporarily traffic data, as is the case in several European countries, and hence there is a risk of missing crucial evidence which can compromise international legal assistance.

Another major difficulty is limited national capacity to interface with foreign jurisdictions. Article 27 of the Budapest Convention sets up standardized procedures for mutual legal assistance but their practical implementation is problematic. The problem with data requested from providers in countries that are not Convention countries is that they are particularly difficult to obtain, more bilateral agreements are required to solve this problem. These procedural inefficiencies are then coupled with slow bureaucratic processes and the absence of harmonized protocols.

Germany and France are examples of countries that have overcome these challenges. Germany has also improved its legislation to fill the gaps in the cybercrime definitions and has enacted particular provisions for computer fraud and data manipulation which have improved the investigation processes. Compliance with Article 16 of the Convention has inspired regulations of providers' data retention for a certain period of time which enhances the cooperation international. Just like France, Kazakhstan needs to establish a similar body like the Interagency Centre for Combating Cybercrime that handles all the mutual legal assistance requests and cuts down on the time taken to respond. These institutional frameworks can be a good reference for Kazakhstan to create a more effective mechanism of sharing information with its international partners.

In order to fulfil the provisions of Article 19 of the Budapest Convention which deals with the access to the stored data, Kazakhstan has taken some measures. The Law of the Republic of Kazakhstan "On Access to Information" of November 16, 2015, No. 401-V provides a legal basis for accessing non-restricted information [23]. However, the progress can only be sustained with regulatory changes and the development of dedicated institutions to facilitate cross-border cooperation. These efforts are in line with the objectives of the Concept of Digital Transformation. In the fight against cybercrime and in order to fulfil the international obligations, Kazakhstan has to further develop its legal system and institutional arrangements. The implementation of the Budapest Convention and other international standards will increase the country's cyber security and build partnership globally.

Conclusions

The Budapest Convention on Cyber Crime is a primary international legal instrument that addresses cyber threats and includes provisions for online fraud. They cover almost all issues, from the legalization of norms to digital evidence collection and promotion of cooperation. The relevance of the Convention for Kazakhstan can be illustrated by the growing cybercrime rates. Because online fraud is borderless and cannot always be addressed through national measures, standard setting becomes of vital importance. Therefore, it is crucial to leverage the full potential of its mechanisms by aligning Kazakhstan's national legislation with the Convention's provisions. This would help improve the effectiveness of information exchange, the rate of access to digital evidence, and the unity of legal processes. One of the most significant provisions is Article

35, which mandates the creation of a round-the-clock rapid response network, which could be a useful strategy to improve international law enforcement cooperation.

Implementing the changes required by the Budapest Convention will not only strengthen the domestic legal system of Kazakhstan but will also lead to the development of better cooperation with the international partners. Thus, with the help of the Convention as a reference point for matching the national legal standards to the international standards, Kazakhstan can significantly contribute to the formation of a sustainable digital ecosystem. This way, the country will be better prepared to fight cybercrime and at the same time enhance its position in the international community as a country that can be trusted in the fight against cyber threats.

The importance of this research is in the fact that it offers the ways to enhance the effectiveness of online fraud investigations with the help of the enhanced approaches. The main measures are the creation of dedicated cybercrime structures, the creation of new and improved digital tools for data analysis, and the enhancement of international cooperation through the conclusion of bilateral treaties and the simplification of the MLA system. If these measures are to be implemented, it will enhance Kazakhstan's institutional arrangements and, therefore, support the sustainable development of the digital ecosystem.

The scientific contribution of this study is evident in its comprehensive analysis of how international legal frameworks are employed to combat transnational cybercrime. Through the use of case studies, the research shows the practical application of the Convention's provisions and offers practical recommendations for improving legal and investigative practices. These findings can be used as a starting point for future research, especially regarding the experiences of non-ratifying countries and the implications of technological change for strategies designed to prevent cybercrime.

Thus, aligning the Kazakh legislation with the Budapest Convention is a significant progression that will help the country to improve its capacity in fighting online fraud and advance its role in the cybercrime fight globally. The proposed solutions are a good starting point for developing a comprehensive approach to the various issues posed by the modern digital environment and creating the basis for a secure and sustainable cybersecurity system.

References

1 Постановление Правления Национального Банка Республики Казахстан от 29 октября 2018 года № 281 Об утверждении Стратегии кибербезопасности финансового сектора Республики Казахстан на 2018-2022 годы. — [Электронный ресурс]. — Режим доступа: https://online.zakon.kz/Document/? doc_id=34451945

2 Cybersecurity Ventures, ожидается, что к 2026 году ежегодный глобальный ущерб от киберпреступлений превысит 20 триллионов долларов США. — [Электронный ресурс]. — Режим доступа: https://www.websiterating.com/ru/blog/research/cybersecurity-statistics-facts/

3 Казахстанцы лишились почти $15 000 из-за интернет-мошенничества — аналитика — [Электронный ресурс]. — Режим доступа: https://ru.sputnik.kz/20240826/kazakhstantsy-lishilis-pochti-15-000-iz-za-internet-moshennichestva—analitika-46589230.html

4 Какой вид онлайн-мошенничества наиболее распространен в Казахстане? — [Электронный ресурс]. — Режим доступа: https://orda.kz/kakoj-vid-onlajn-moshennichestva-naibolee-rasprostranen-v-kazahstane-388940/

5 Интернет-мошенничество: как и где чаще всего обманывают граждан. — [Электронный ресурс]. — Режим доступа: https://www.zakon.kz/finansy/6441298-internetmoshennichestvo-kak-i-gde-chashche-vsego-obmanyvayut-grazhdan.html

6 Число киберпреступлений в Казахстане за 5 лет выросло почти в три раза. — [Электронный ресурс]. — Режим доступа: https://inbusiness.kz/ru/last/chislo-kiberprestuplenij-v-kazahstane-za-5-let-vyroslo-pochti-v-tri-raza

7 7 из 10 интернет-мошенников в Казахстане остаются безнаказанными. — [Электронный ресурс]. — Режим доступа: https://prosud.kz/news/7-iz-10-internet-moshennikov-v-kazahstane-ostayutsya-neizvestnymi-i-beznakazannymi/

8 Global Cybersecurity Index 2024. 5th Edition. — [Электронный ресурс]. — Режим доступа: https://www.itu.int/en/ITU-D/Cybersecurity/Documents/GCIv5/2401416_1b_Global-Cybersecurity-Index-E.pdf

9 О ратификации Конвенции Организации Объединенных Наций против транснациональной организованной преступности. Закон Республики Казахстан от 4 июня 2008 года N 40-IV. — [Электронный ресурс]. — Режим доступа: https://adilet.zan.kz/rus/docs/Z080000040_

10 Convention on Cybercrime. Budapest, 23.XI.2001. — [Электронный ресурс]. — Режим доступа: https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent? documentId=0900001680081561

11 Сотрудничество Республики Казахстан с Советом Европы. — [Электронный ресурс]. — Режим доступа: https://www.gov.kz/memleket/entities/mfa/press/article/details/487

12 Яковлева А.В. Кибербезопасность и ее правовое регулирование (зарубежный и российский опыт) / А.В. Яковлева // Социально-политические науки. — 2021. — Т. 11. — № 4. — С. 70-81.

13 Шестак В.А. Будапештская конвенция как основополагающий механизм противодействия киберпреступности: новации и перспективы международно-правового регулирования / В.А. Шестак, А.С. Чеботарь // Образование и право. — 2023. — № 8. — С. 305–310. doi:10.24412/2076-1503-2023-8-305-310

14 Кибермошенничество в Казахстане: факты, тенденции и анализ. — [Электронный ресурс]. — Режим доступа: https://er10.kz/read/analitika/kibermoshennichestvo-v-kazahstane-fakty-tendencii-i-analiz /

15 Маслова Ж.Н. Мошенничество в трансграничной электронной коммерции / Ж.Н. Маслова // Ученые записки Санкт-Петербургского имени В.Б. Бобкова филиала Российской таможенной академии. — 2020. — № 3 (75). — С. 70–72.

16 Уголовный кодекс Республики Казахстан. Кодекс Республики Казахстан от 3 июля 2014 года № 226-V ЗРК. — [Электронный ресурс]. — Режим доступа: https://adilet.zan.kz/rus/docs/K1400000226

17 Уголовно-процессуальный кодекс Республики Казахстан. Кодекс Республики Казахстан от 4 июля 2014 года № 231-V ЗРК. — [Электронный ресурс]. — Режим доступа: https://adilet.zan.kz/rus/docs/K1400000231

18 Сабиров К.К. Некоторые вопросы законодательного укрепления кибербезопасности в Республике Казахстан / К.К. Сабиров, Ф.Р. Ахмеджанов // Вопросы кибербезопасности. — 2017. — № 3 (21). — С. 55–62.

19 Филиппов С. Совместные следственные группы как эффективный инструмент противодействия трансграничной преступности / С. Филиппов // Национальный юридический журнал: Теория и практика. — 2018. — Т. 1. — № 4. — С. 133–137.

20 Сатбаева А.М. Проблемы противодействия киберпреступности: опыт международного сотрудничества / А.М. Сатбаева, А.Р. Алимбетова, М.Т. Бейсенбаева // Вестник Института законодательства и правовой информации Республики Казахстан. — 2024. — № 3(78). — С. 211–221. doi: 10.52026/2788-5291-2024-78-3-211

21 BKA. Internet Crime/Cybercrime. — [Electronic resource]. — Access mode: https://www.bka.de/EN/OurTasks/AreasOfCrime/Cybercrime/internetCrime.html

22 Two Estonian Citizens Arrested in $575 Million Cryptocurrency Fraud and Money Laundering Scheme. — [Electronic resource]. — Access mode: https://ee.usembassy.gov/2022-11-21/

23 Закон Республики Казахстан от 16 ноября 2015 года № 401-V «О доступе к информации» (с изменениями и дополнениями по состоянию на 20.08.2024 г.). — [Электронный ресурс]. — Режим доступа: https://adilet.zan.kz/rus/docs/Z1500000401

Н.М. Әпсімет, А.Ж. Муратова

Онлайн алаяқтық қылмыстарын тергеуде Будапешт киберқылмыс жөніндегі конвенциясының ережелерін қолдану мүмкіндігі туралы

Мақалада Қазақстандағы онлайн алаяқтықты тергеудің тиімділігін арттыру үшін киберқылмыс туралы Будапешт конвенциясының ережелерін қолдану әлеуеті зерттелген. Жұмыстың негізгі мақсаты — осы қылмыс түрінің өсіп келе жатқан қауіп-қатеріне қарсы күресте, әсіресе оның трансшекаралық сипатын ескере отырып, Конвенцияның мүмкіндіктерін талдау. Авторлар құжаттарды талдауды (Конвенция мәтіні, Қазақстан Республикасының заңнамасы, талдау материалдары), заңнаманы салыстырмалы зерттеуді (Қазақстан нормаларының Конвенция ережелеріне сәйкестігін анықтау) және оның басқа елдерде қолданылу тәжірибесін сараптауды қамтитын кешенді әдістемелік тәсілді қолданған. Зерттеу барысында Қазақстанның ұлттық заңнамасы мен Конвенция ережелерінің арасындағы сәйкессіздіктер анықталды. Негізгі мәселелер киберқылмыстарды анықтау, цифрлық дәлелдерді жинау рәсімдері және халықаралық ынтымақтастыққа қатысты. Басқа елдерде Конвенция ережелерін табысты қолдану жағдайларын негізге ала отырып, авторлар Қазақстанда заңнама мен құқық қолдану тәжірибесін жетілдіруге арналған ұсыныстар әзірледі. Атап айтқанда, ұлттық заңнаманы Конвенция стандарттарына бейімдеу қажеттігін, киберқылмыспен күресуге арналған мамандандырылған бөлімшелер құруды, деректерді талдау үшін цифрлық платформаларды енгізуді және халықаралық ынтымақтастықты жандандыруды ұсынады. Бұл онлайн алаяқтыққа қарсы күрестің тиімділігін арттыруға және Қазақстанның жаһандық киберқылмыспен күрестегі орнын нығайтуға мүмкіндік береді.

Кілт сөздер: киберқылмыс, онлайн алаяқтық, Будапешт конвенциясы, халықаралық ынтымақтастық, цифрлық дәлелдер, Қазақстанның заңнамасы, құқық қолдану тәжірибесі.

Н.М. Апсимет, А.Ж. Муратова

О возможности применения положений Будапештской конвенции о киберпреступности при расследовании преступлений в сфере онлайн-мошенничества

В статье рассматривается потенциал применения положений Будапештской конвенции о киберпреступности для повышения эффективности расследований в сфере онлайн-мошенничества в Казахстане. Основной целью работы является анализ возможностей конвенции в борьбе с растущей угрозой этого вида преступлений, особенно учитывая их трансграничный характер. Авторы применяют комплексный подход, включающий анализ документов (текста конвенции, законодательства Республики Казахстан, аналитических материалов), сравнительное изучение прав человека на предмет соответствия законодательства Казахстана положениям конвенции и анализ практики её применения в других странах. В ходе исследования выявлены несоответствия между национальным законодательством Казахстана и положениями конвенции. Основные проблемы касаются определения киберпреступлений, процедур сбора цифровых доказательств и международного сотрудничества. На основе успешных кейсов применения конвенции в других странах, предложены рекомендации по совершенствованию законодательства и правоприменительной практики в Казахстане. В частности, авторы подчеркивают необходимость адаптации национального законодательства к положениям Конвенции, создания специализированных подразделений по борьбе с киберпреступностью, внедрения цифровых платформ для анализа данных и активизации международного сотрудничества. Это позволит повысить эффективность противодействия онлайн-мошенничеству и укрепить позиции Казахстана в глобальной борьбе с киберпреступностью.

Ключевые слова: киберпреступность, онлайн-мошенничество, Будапештская конвенция, международное сотрудничество, цифровые доказательства, законодательство Казахстана, правоприменительная практика.

References

1 Postanovlenie Pravleniia Natsionalnogo Banka Respubliki Kazakhstan ot 29 oktiabria 2018 goda № 281 Ob utverzhdenii Strategii kiberbezopasnosti finansovogo sektora Respubliki Kazakhstan na 2018–2022 gody [Resolution of the Board of the National Bank of the Republic of Kazakhstan No. 281 on Approval of the Cybersecurity Strategy for the Financial Sector of the Republic of Kazakhstan for 2018–2022]. (2018, 29 Okober). *online.zakon.kz.* Retrieved from https://online.zakon.kz/Document/?doc_id=34451945 [in Russian].

2 Cybersecurity Ventures. Ozhidaetsia, shto k 2026 godu ezhegodnyi globalnyi ushcherb ot kiberprestuplenii prevysit 20 trillionov dollarov SShA [Cybersecurity Ventures: Global annual damage from cybercrime is expected to exceed $20 trillion by 2026]. *www.websiterating.com.* Retrieved from https://www.websiterating.com/ru/blog/research/cybersecurity-statistics-facts/ [in Russian].

3 Kazakhstantsy lishilis pochti 15 000$ iz-za internet-moshennichestva [Kazakh citizens lost nearly $15,000 due to online fraud]. *sputnik.kz.* Retrieved from https://ru.sputnik.kz/20240826/kazakhstantsy-lishilis-pochti-15-000-iz-za-internet-moshennichestva—analitika-46589230.html [in Russian].

4 Kakoi vid onlain-moshennichestva naibolee rasprostranen v Kazakhstane? [What type of online fraud is most common in Kazakhstan?]. *orda.kz.* Retrieved from https://orda.kz/kakoj-vid-onlajn-moshennichestva-naibolee-rasprostranen-v-kazahstane-388940/ [in Russian].

5 Internet-moshennichestvo: kak i gde chashche vsego obmanyvaiut grazhdan [Internet fraud: where and how citizens are most often deceived]. *www.zakon.kz*. Retrieved from https://www.zakon.kz/finansy/6441298-internetmoshennichestvo-kak-i-gde-chashche-vsego-obmanyvayut-grazhdan.html [in Russian].

6 Chislo kiberprestuplenii v Kazakhstane za 5 let vyroslo pochti v tri raza [The number of cybercrimes in Kazakhstan has almost tripled in 5 years]. *inbusiness.kz.* Retrieved from https://inbusiness.kz/ru/last/chislo-kiberprestuplenij-v-kazahstane-za-5-let-vyroslo-pochti-v-tri-raza [in Russian].

7 7 iz 10 internet-moshennikov v Kazakhstane ostanutsa beznakazannymi [7 out of 10 online fraudsters in Kazakhstan go unpunished]. *prosud.kz.* Retrieved from https://prosud.kz/news/7-iz-10-internet-moshennikov-v-kazahstane-ostayutsya-neizvestnymi-i-beznakazannymi/ [in Russian].

8 Global Cybersecurity Index 2024. (5th ed.). *www.itu.int.* Retrieved from https://www.itu.int/en/ITU-D/Cybersecurity/Documents/GCIv5/2401416_1b_Global-Cybersecurity-Index-E.pdf

9 O ratifikatsii Konventsii Organizatsii Obedinennykh Natsii protiv transnatsionalnoi organizovannoi prestupnosti [On the ratification of the United Nations Convention against Transnational Organized Crime]. *adilet.zan.kz.* Retrieved from https://adilet.zan.kz/rus/docs/Z080000040_ [in Russian].

10 Convention on Cybercrime. Budapest, 23.XI.2001. *www.itu.int* Retrieved from https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent? documentId=0900001680081561.

11 Sotrudnichestvo Respubliki Kazakhstan s Sovetom Evropy [Cooperation of the Republic of Kazakhstan with the Council of Europe]. *www.gov.kz.* Retrieved from https://www.gov.kz/memleket/entities/mfa/press/article/details/487 [in Russian].

12 Yakovleva, A.V. (2021). Kiberbezopasnost i ee pravovoe regulirovanie (zarubezhnyi i rossiiskii opyt) [Cybersecurity and its legal regulation (foreign and Russian experience)]. *Sotsialno-politicheskie nauki — Social and Political Sciences, 11*(4), 70–81 [in Russian].

13 Shestak, V.A. & Chebotar, A.S. (2023). Budapeshtskaia konventsiia kak osnovopolagaiushchii mekhanizm protivodeistviia kiberprestupnosti: novatsii i perspektivy mezhdunarodno-pravovogo regulirovaniia [The Budapest Convention as a fundamental mechanism for combating cybercrime: innovations and prospects for international legal regulation]. *Obrazovanie i pravo — Education and Law*, 8, 305-310. doi:10.24412/2076-1503-2023-8-305-310 [in Russian].

14 Kibermoshennichestvo v Kazakhstane: fakty, tendentsii i analiz [Cyberfraud in Kazakhstan: facts, trends, and analysis]. *er10.kz.* Retrieved from https://er10.kz/read/analitika/kibermoshennichestvo-v-kazahstane-fakty-tendencii-i-analiz/ [in Russian].

15 Maslova, Zh.N. (2020). Moshennichestvo v transgranichnoi elektronnoi kommertsii [Fraud in cross-border e-commerce]. *Uchenye zapiski Sankt-Peterburgskogo imeni V.B. Bobkova filiala Rossiiskoi tamozhennoi akademii — Scientific notes of the Saint Petersburg V.B. Bobkov Branch of the Russian Customs Academy,* 3(75), 70–72 [in Russian].

16 Ugolovnyi kodeks Respubliki Kazakhstan. Kodeks Respubliki Kazakhstan ot 3 iiulia 2014 goda № 226-V ZRK [Criminal Code of the Republic of Kazakhstan. Code of the Republic of Kazakhstan No. 226-V dated July 3, 2014]. (2014, 3 July). *adilet.zan.kz.* Retrieved from https://adilet.zan.kz/rus/docs/K1400000226 [in Russian].

17 Ugolovno-protsessualnyi kodeks Respubliki Kazakhstan. Kodeks Respubliki Kazakhstan ot 4 iiulia 2014 goda № 231-V ZRK [Criminal Procedure Code of the Republic of Kazakhstan. Code of the Republic of Kazakhstan No. 231-V dated July 4, 2014]. (2014, 4 July). *adilet.zan.kz.* Retrieved from https://adilet.zan.kz/rus/docs/K1400000231 [in Russian].

18 Sabirov, K.K. & Akhmedzhanov, F.R. (2017). Nekotorye voprosy zakonodatelnogo ukrepleniia kiberbezopasnosti v Respublike Kazakhstan [Some issues of legislative strengthening of cybersecurity in the Republic of Kazakhstan]. *Voprosy kiberbezopasnosti — Cybersecurity Issues,* 3(21), 55–62 [in Russian].

19 Filippov, S. (2018). Sovmestnye sledstvennye gruppy kak effektivnyi instrument protivodeistviia transgranichnoi prestupnosti [Joint investigative teams as an effective tool for combating transnational crime]. *Natsionalnyi yuridicheskii zhurnal: Teoriia i praktika — National Legal Journal: Theory and Practice, 1*(4), 133–137 [in Russian].

20 Satbayeva, A.M., Alimbetova, A.R., & Beysenbayeva, M.T. (2024). Problemy protivodeistviia kiberprestupnosti: opyt mezhdunarodnogo sotrudnichestva [Problems of combating cybercrime: experience of international cooperation]. *Vestnik Instituta zakonodatelstva i pravovoi informatsii Respubliki Kazakhstan — Bulletin of the Institute of Legislation and Legal Information of the Republic of Kazakhstan,* 3(78), 211–221. doi:10.52026/2788-5291-2024-78-3-211 [in Russian].

21 BKA. Internet Crime/Cybercrime. *bka.de.* Retrieved from https://www.bka.de/EN/OurTasks/AreasOfCrime/Cybercrime/internetCrime.html.

22 Two Estonian Citizens Arrested in $575 Million Cryptocurrency Fraud and Money Laundering Scheme. *usembassy.gov.* Retrieved from https://ee.usembassy.gov/ru/2022-11-21/

23 Zakon Respubliki Kazakhstan ot 16 noiabria 2015 goda № 401-V «O dostupe k informatsii» (s izmeneniiami i dopolneniiami po sostoianiiu na 20.08.2024 g.) [Law of the Republic of Kazakhstan No. 401-V "On Access to Information" (as amended and supplemented as of August 20, 2024)]. (2015, 16 November). *adilet.zan.kz.* Retrieved from https://adilet.zan.kz/rus/docs/Z1500000401 [in Russian].

Information about the authors

Apsimet Nurdaulet Mukhamediyaruly — Master of Legal Sciences, Doctoral student of the Faculty of Law, Al Farabi Kazakh National University, Almaty, Kazakhstan, e-mail: Apsimet.nurdaulet@gmail.com;

Muratova Alua Zhaslankyzy — PhD, Head of the Department of Criminal Law Disciplines of the Faculty of Law, L.N. Gumilyov Eurasian National University, Astana, Kazakhstan, e-mail: muratova_azh@enu.kz.