UDC 343.9:004.056.5
DOI: 10.32518/sals1.2025.179

Соціально-правові студії. 2025. Т. 8, № 1
Social & Legal Studios. 2025. Vol. 8, No. 1

Countering cyber attacks in the Republic of Kazakhstan: Interdisciplinary issues and legal frameworks in the context of social security and economic stability

Nurgul Kubanova*
Doctoral Student
Almaty Academy of the Ministry of Internal Affairs
of the Republic of Kazakhstan named after Makan Yesbulatov
050060, 29 Utepov Str., Almaty, Republic of Kazakhstan
https://orcid.org/0009-0006-1141-1165

Indira Nessipbayeva
PhD in Law
International Taraz University named after Sh. Murtaza
080000, 69B Zheltoksan Str., Taraz, Republic of Kazakhstan
https://orcid.org/0009-0007-9657-0313

Soledad Dyussebaliyeva
PhD in Law, Associate Professor
Atyrau University named after Halel Dosmukhamedov
060011, 1 Studenchesky Ave., Atyrau, Republic of Kazakhstan
https://orcid.org/0009-0001-4548-7946

Halibiyati Halibati
Doctoral Student
Al-Farabi Kazakh National University
050040, 71 Al-Farabi Ave., Almaty, Republic of Kazakhstan
https://orcid.org/0009-0000-4664-7844

Serikhan Adilgazy
PhD in Law, Professor
Narxoz University
050035, 55 Zhandosov Str., Almaty, Republic of Kazakhstan
https://orcid.org/0000-0001-8625-4172

Abstract. The study aimed to develop theoretical and methodological foundations and practical recommendations for improving the system of countering cyberattacks, covering legal, technical and organisational mechanisms for ensuring cybersecurity. The study was based on a comprehensive interdisciplinary approach using systemic analysis, formal legal, comparative legal and descriptive statistics methods. The statistics analysis for 2020-2024 revealed a rapid increase in the number and complexity of cyberattacks. In 2024, 4,507 cases of malware were recorded, more than doubling year-on-year. The study confirmed that the small and medium-sized business segment was the most vulnerable: in the banking sector alone, in the second half of 2024, losses from cyberattacks totalled Kazakhstani tenge 1.5 billion, with 35% of attacks using social engineering techniques. An analysis of the structure of cyberattacks showed that 62% of the total number of cyberattacks were directed at the public sector, of which 28% targeted critical infrastructure. The study determined that about 70% of successful interventions are related to the human factor – insufficient staff qualifications

Suggested Citation **Article's History**: Received: 13.09.2024 Revised: 15.02.2025 Accepted: 26.03.2025

Kubanova, N., Nessipbayeva, I., Dyussebaliyeva, S., Halibati, H., & Adilgazy, S. (2024). Countering cyber attacks in the Republic of Kazakhstan: Interdisciplinary issues and legal frameworks in the context of social security and economic stability. *Social & Legal Studios*, 8(1), 179-194. doi: 10.32518/sals1.2025.179.

*Corresponding author

and system configuration errors. Significant gaps in Kazakhstan's cyber defence system are identified: lack of effective interagency coordination mechanisms, insufficient regulation of public-private partnerships, and inefficiency of the existing legal framework for regulating the liability of critical infrastructure operators. The author substantiated the need to create a single cyber defence coordination centre that will combine the efforts of the state monitoring system KZ-CERT and the industry system FinCERT and proposes economic mechanisms to stimulate investment in cyber security through a system of tax incentives and grant programmes. The peculiarities of the cybercrime investigation process were analysed, including the procedures for video recording of equipment seizure and the specifics of procedural registration of evidence. According to the General Prosecutor's Office of the Republic of Kazakhstan, in 2023, 476 criminal cases of cybercrime were brought to court, of which 312 resulted in guilty verdicts. The research findings formed a comprehensive understanding of the relationship between the legal, technical, and socio-economic aspects of cybersecurity and proved the need for systematic interaction between all stakeholders in countering cyber threats

Keywords: information systems; digital evidence; malware; critical infrastructure; public-private partnerships

Introduction

In the context of rapid digitalisation and growing cyber threats, the issue of countering cyberattacks in the Republic of Kazakhstan is becoming particularly relevant. Information security challenges require a comprehensive interdisciplinary approach and improved legal protection mechanisms. Ensuring cybersecurity is becoming a critical factor in maintaining social stability and economic development of the country, especially in the context of growing cross-border cybercrime and increasing geopolitical tensions. The need to develop effective strategies to counter cyberattacks is driven by their potential impact on Kazakhstan's critical infrastructure, financial sector and national security, as well as the growing complexity and sophistication of cybercriminals' methods. In the context of the global digital transformation, it is of particular importance to create a reliable system of protection against cyberattacks that considers technological, socio-economic and legal aspects of security.

A comprehensive analysis of the scientific literature demonstrates the diversity of approaches to solving cybersecurity problems in Kazakhstan. The study by A.M. Satbayeva *et al.* (2024) on international cooperation in combating cybercrime underlined the need to harmonise national legislation with international standards and expand cooperation between states under the auspices of the United Nations. The authors analysed in detail the activities of the "K" Department of the Ministry of Internal Affairs and the 2023 Cyberpol Strike Task Force pilot project, noting their key role in combating a wide range of cybercrime. The researchers emphasised the importance of establishing international cybercrime units that would have the right to transfer traffic data, extradite and provide assistance.

Developing the technological aspect of the problem, M. Bolatbek *et al.* (2024) presented an innovative system for analysing the illegal use of Internet resources in university networks by developing network real-time network activity monitoring and creating a specialised dictionary of extremist terms in Kazakh. Their research successfully integrated advanced machine learning models to classify network traffic and proposed an experimental architecture for connecting educational organisations to enhance cybersecurity. K. Bishmanov *et al.* (2024) have significantly contributed to the development of technical aspects of countering cyberterrorism by developing a comprehensive plan that includes innovative approaches to tracking network traffic and analysing data transmission using Python code. Their structural scheme for systemising the process of countering cyberattacks covers the entire cycle from identifying potential threats to evaluating the effectiveness of the measures taken. K. Azanbay (2024) conducted an in-depth analysis of the introduction of innovative technologies to ensure information security, combining a systematic analysis of Kazakhstan's legislation with empirical modelling of the key principles of technological innovation. The author proposed such innovations as integrated circuits, virtual client protection, big data analytics, and advanced cloud security, emphasising their advantages over traditional systems in terms of resource efficiency and scalability.

The social aspect of the problem is explored in depth by M. Jekebayeva *et al.* (2023), who focused on studying youth cybersecurity issues and developing recommendations for creating a safe digital environment. Based on a large-scale survey, they identified critical gaps in youth awareness of cyber threats and proposed comprehensive educational programmes on the basics of safe internet use and personal data protection. The researchers stressed the importance of developing cooperation between government agencies, the private sector and educational institutions to create an effective system of protection against cyber threats.

A comprehensive legal analysis of the issue was presented by several researchers. S. Shaisultanov *et al.* (2024) and K. Zhakenov *et al.* (2024) conducted a comprehensive analysis of the legal aspects of combating cybercrime using formal logical and systemic-structural analysis methods. The authors examined in detail the regulatory framework of Kazakhstan and the European Union (EU) countries in the field of combating Internet fraud, studied the activities of authorised entities in the field of crime prevention, and analysed international experience in this area. R. Jilkishiyev and Y. Begaliyev (2024) conducted an in-depth analysis of the problems faced by law enforcement agencies and information security professionals in investigating cybercrime. They identified critical problematic aspects, including the low level of technical support, insufficient funding for the industry, and the lack of a dedicated law enforcement agency to investigate cybercrime.

A. Pollini *et al.* (2022) conducted a detailed analysis of the effectiveness of cybersecurity measures by addressing them in the context of the human factor in healthcare organisations. Their study determined that security measures are often implemented in the form of complex procedures that do not sufficiently support the daily work of employees. The researchers emphasised the importance of a holistic approach to cybersecurity that addresses individual, organisational and technological factors. They developed recommendations for improving cybersecurity systems by leveraging the human factor and implementing non-technical

countermeasures, such as user awareness programmes. A. Saraswat and G. Tiwari (2025) conducted a systematic analysis of cybersecurity issues in the energy sector, focusing on legal mechanisms for protecting critical energy infrastructure. The study determined that the energy sector accounted for 10.7% of reported cyberattacks in 2022, including notable incidents affecting renewable energy facilities. The study highlighted the importance of international cooperation and legal mechanisms in countering cyber threats, examining the application of various provisions of the UN Charter to cyberattacks.

S. Zabikh (2020) conducted a fundamental study of the problems of information security and methods of identifying threats in the information sphere. The author emphasised the importance of protecting the rights and interests of citizens, society and the state in the information space from real and potential threats. The researcher analysed the international experience of legal regulation of information security and the possibilities of its application in the Republic of Kazakhstan, emphasising the growing influence of modern information systems on politics, economy and the spiritual and ideological sphere of society. An analysis of the scientific literature shows significant progress in the study of various aspects of countering cyberattacks in Kazakhstan, including technological solutions, legal mechanisms, social aspects and international cooperation. At the same time, the issues of creating a unified system for countering cyber threats, improving the legislative framework in line with international standards, and developing domestic technological infrastructure remain unresolved.

The study aimed to provide theoretical and methodological substantiation and develop scientific and practical recommendations for improving the system of countering cyberattacks in the Republic of Kazakhstan based on a comprehensive interdisciplinary analysis of legal, technical and organisational mechanisms for ensuring cybersecurity in the context of socio-economic stability. The objectives of the study were:

1) to analyse the current state of legal regulation of countering cyberattacks in the Republic of Kazakhstan, to identify the main gaps in the legislation and to propose ways to improve it, addressing international standards and best practices of other countries.

2) to study the peculiarities of qualifying and investigating cyberattacks, including forensic characteristics, methods of collecting digital evidence and specifics of procedural design, to increase the effectiveness of law enforcement activities in the field of combating cybercrime.

3) to develop comprehensive recommendations for improving the system of countering cyberattacks based on an interdisciplinary approach, including measures to develop public-private partnerships, stimulate investment in cybersecurity and increase the level of digital literacy of the population.

Materials and methods

The empirical basis of the study was formed by a wide range of legal acts, statistics and analytical materials. The key source of statistical information was the data of the National Computer Emergency Response Team, which covers the period of 2020-2024 and contains detailed information on the number and types of cyber incidents (KZ-CERT, n.d.). Separately, the data of the Financial Security Department KZ-FinCERT on incidents in the banking sector, statistics of the General Prosecutor's Office of the Republic of Kazakhstan on cybercrime investigations, and materials of the National Security Committee on countering cyberterrorism were analysed (Incident overview for…, 2024; Only 5% of…, 2023). This data was processed using statistical methods to identify trends and patterns in the dynamics of cyber threats.

Among the regulatory sources, the author analyses the provisions of the Resolution of the Government of the Republic of Kazakhstan No. 407 "On Approval of the Concept of Cybersecurity" ("Cyber Shield of Kazakhstan") (2017), the Criminal Procedure Code of the Republic of Kazakhstan (2014) and the Penal Code of the Republic of Kazakhstan (2014), and the Law of the Republic of Kazakhstan No. 418-V "On Informatization" (2015). In the international legal aspect, the Convention on Cybercrime (2001), and materials of the European Police College on the standards of training for cybercrime investigators were analysed (CEPOL Knowledge Centres, n.d.). An important source of information was official reports and press releases of government agencies, including Report on the implementation of the Strategic Plan of the Ministry of Digital Development, Innovations and Aerospace Industry of the Republic of Kazakhstan for 2020-2024 (2021), press releases of the Ministry of Internal Affairs and the National Bank of Kazakhstan (Turlybek, 2023, 2024; New types of fraud..., 2024; Anti-Fraud Center…, 2025). To study the international context, reports and analytical materials by Cybersecurity Ventures on global losses from cybercrime, a study by the International Monetary Fund on the impact of cyberattacks on financial stability, analytical data by Datami Newsroom (2024) on the role of the human factor in cybersecurity breaches, and materials by PortSwigger on vulnerability bounty programmes were used. Additionally, the materials of leading international organisations in the field of cybersecurity were analysed, in particular, INTERPOL (2022) and Organization for Security and Co-operation (OSCE) reports, which contain important information on international cooperation in combating cybercrime (Leyden, 2023; Calif, 2023; International Monetary Fund & Monetary and Capital Markets Department, 2024; Concluding event of…, 2024).

The theoretical and methodological basis of the study is a comprehensive interdisciplinary approach to analysing the problems of countering cyberattacks in the Republic of Kazakhstan, based on the concept of the socio-legal and economic dimensions of cybersecurity. This conceptual framework, developed by A. Dimitriadis *et al.* (2020), E. Karafili *et al.* (2020), and A.Y. Ofori and D. Akoto (2020), was used to analyse cyberattacks as a complex threat to the social stability and economic development of the state, which requires a multidimensional analysis of legal, social and economic aspects. The research methodology is based on a combination of general scientific and special legal methods. A comprehensive study of the legal framework and institutional mechanisms for countering cyberattacks was conducted using the systemic analysis method, which was used to identify systemic shortcomings in regulation and propose ways to eliminate them. The statistical method was used to analyse the dynamics and structure of cyber incidents, which identified the main trends in the development of cyber threats and assessed the effectiveness of countermeasures.

The formal legal method was used for a detailed analysis of the provisions of Kazakhstan's national legislation, which made it possible to identify the specifics of legal regulation of countering cyberattacks and gaps in regulatory support.

The comparative legal method was used to compare Kazakhstan's experience with international practices of combating cybercrime, especially in the context of implementing the provisions of international treaties. The modelling method was used to develop recommendations for improving the cybersecurity system. Quantitative methods were key to processing and analysing data on the dynamics of cyber incidents in 2020-2024, which was used to identify the main trends in the development of cyber threats.

The research was conducted in three stages, which ensured consistency and completeness of the analysis. The first stage involved a theoretical analysis of the problem of countering cyberattacks, systematisation of the regulatory framework and definition of the conceptual framework of the study. The second stage examined the peculiarities of qualifying and investigating cyberattacks, developed a classification of digital evidence, and analysed the specifics of its collection and evaluation. In the third stage, a comprehensive analysis of interdisciplinary issues and the legal framework for countering cyberattacks in the context of ensuring social security and economic stability was carried out, which allowed the author to formulate systematic conclusions and practical recommendations for improving the mechanisms for countering cyber threats. Additionally, the method of expert assessments was applied by conducting interviews with cybersecurity and law enforcement experts to validate the results and recommendations.

Results

Theoretical aspects of countering cyber attacks. Cyberattacks are one of the most complex and multifaceted threats of our time, as they affect not only the information systems of individual companies, government agencies and infrastructure facilities but also the stability of socio-economic processes in the country. The Resolution of the Government of the Republic of Kazakhstan No. 407 (2017) defines a computer attack as a targeted attempt to implement a threat of unauthorised influence on or access to information, an electronic resource, an information system using software or hardware (or interconnection protocols). This document emphasises the importance of protecting the national information and communication infrastructure from various cyber threats, including unauthorised actions aimed at violating the confidentiality, integrity and availability of information systems.

In the context of the Republic of Kazakhstan, the issue of countering cyberattacks has become of strategic importance after several legislative and policy documents came into force, among which the Law of the Republic of Kazakhstan No. 418-V (2015) is central. This law stipulated a legal basis for regulating social relations arising in the field of creation and use of electronic information resources, systems and networks, and defined the competence of authorised state bodies in the field of cybersecurity. However, the practice has demonstrated that legislative consolidation of basic provisions alone is not enough to effectively counter the rapid evolution of attack methods. The technologies used by criminals are often ahead of the capabilities of law enforcement agencies, which necessitates a comprehensive analysis of cyber threats from the standpoint of criminal law, forensics, socio-economic impact and international legal cooperation.

From the legal and scientific perspective, one of the most important aspects of countering cyberattacks is to clearly define their classification and characteristics. A common type of cyberattack is distributed denial of service (DDoS) attacks, in which attackers overload a server or network with multiple requests, forcing the target system to temporarily or completely stop working (Metelskyi & Kravchuk, 2023). This type of impact is particularly dangerous when targeting government portals or financial institutions, as it can disrupt their operations and cause significant economic damage. In 2024, 105 incidents related to DDoS attacks were registered, which continues the trend of annual decline in the number of such attacks in 2020-2024 (Incident overview for…, 2024). Despite the effectiveness of measures to counter DDoS attacks, cybercriminals are actively developing other methods of unauthorised interference. Phishing poses a particular danger, as its dynamics demonstrate a heterogeneous nature – periods of significant growth are followed by periods of decline, which may indicate that attackers are adapting to the protective mechanisms being implemented.

Phishing is the fraudulent acquisition of confidential data (passwords, logins, bank card details) by sending emails or creating fake web pages that look like legitimate resources. According to statistics, 3,947 cases of phishing were detected on the Internet (KZ-CERT, n.d.). Phishing is often underestimated, but it causes direct financial losses and affects a significant segment of ordinary users, thus undermining trust in digital services and e-government. In addition, the category of cyberattacks includes the spread of malware, which accounts for a significant portion of all incidents (4,507 cases in 2024), and unauthorised intrusions into corporate or government networks aimed at stealing information, espionage or extortion.

Statistics confirm the heterogeneity of cybersecurity trends. DDoS attacks are demonstrating a downward trend, while other types of cyberattacks are characterised by increasing complexity. As shown by the dynamics of cyber incidents in 2020-2024 (Fig. 1), DDoS attacks recorded in 2024 demonstrate not only a high level of technical organisation but also the use of distributed infrastructures, such as botnets, which make it difficult to identify the initiators and effectively counteract them. Similarly, many phishing incidents, which cause both financial and reputational losses, indicate systemic vulnerabilities in the architecture of digital platforms and imperfect user authentication mechanisms, which creates the preconditions for successful social engineering attacks.

The Ministry of Internal Affairs of the Republic of Kazakhstan is actively countering cyberattacks, recognising the growing threat posed by international criminal groups. In 2024, the Department for Combating Cybercrime was established, highlighting the need to improve organisational structures and defence strategies (Turlybek, 2024). In addition, the holding of international conferences, such as "Cybercrime in the CIS: Current Trends and Directions of Counteraction", demonstrates the significant attention to the issue of international cooperation in combating transnational threats. This, in turn, requires strengthening mechanisms for information exchange, coordination between states, and the development of technical means of monitoring and protection. In particular, the high level of malware incidents confirms the need to improve technical solutions and strengthen legal and organisational response mechanisms.

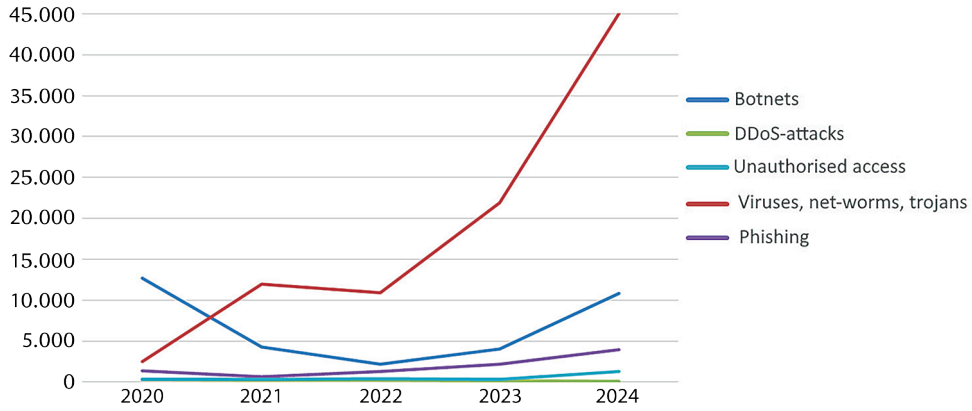

Figure 1. Dynamics of cyber incidents in Kazakhstan (2020-2024)
Source: compiled by the authors based on KZ-CERT (n.d.)

The analysis of graphical data on the dynamics of cyber incidents in the Republic of Kazakhstan over the past 5 years indicates the existence of complex transformation processes in the field of cybersecurity, which require appropriate regulatory and legal response and improvement of counteraction mechanisms. A trend towards the qualitative evolution of cyberattack methods is notable, which is confirmed by changes in their structure and intensity. In particular, the cyclical nature of botnet activity indicates that attackers are constantly adapting to the security measures implemented, which necessitates regular updates of regulatory requirements for critical infrastructure operators to monitor network traffic.

The relative stabilisation of the number of DDoS attacks (from 290 cases in 2020 to 105 cases in 2024, with a gradual annual decrease of 8-12%) may indicate the effectiveness of the implemented legislative protection mechanisms and relevant technical solutions, however, the simultaneous increase in phishing incidents (with an average annual growth rate of 30% in 2020-2022 and further acceleration to 74% in 2023 and 83% in 2024) demonstrates a shift in the focus of cybercriminals towards social engineering, which requires strengthening legal regulation in the field of personal data protection and improving mechanisms for identifying users of digital services. The exponential increase in malware-related incidents points to the need to develop and implement new legal instruments to counter the automated spread of cyber threats, including mechanisms for international cooperation and information exchange on new types of malwares.

The identified trends in the development of cyber threats require a review of criminal legislation on the qualification of cybercrime and increased liability for their commission, which raises the issue of creating specialised units to investigate high-tech crimes and develop appropriate forensic techniques. An analysis of international practice shows significant differences in approaches to punishment for cybercrime. In the United States, according to the Computer Fraud and Abuse Act (1986), the sanctions for cyberattacks include imprisonment for up to 10 years (up to 20 years for repeat offences) in cases of obtaining nationally important information (a)(1), causing damage to a computer system by intentional malicious interference (a)(5)(A), and in cases of intentional access for fraud (a)(4) – up to 5 years (up to 10 years for repeat offences). In the European Union, the punishment for cybercrime is established following the Directive of the European Parliament and of the Council No. 2013/40/EU "On Attacks Against Information Systems and Replacing Council Framework Decision 2005/222/JHA" (2013), which obliges Member States to ensure effective, proportionate and dissuasive criminal sanctions. According to Article 9 of this Directive, the minimum penalty for such crimes should be at least two years in prison (in cases that are not minor), and for the malicious use of tools intended to commit cybercrime – up to three years in prison. The most serious cases, including attacks on critical infrastructure, crimes causing serious damage, or actions as part of an organised criminal group, should be punishable by imprisonment for at least five years. At the same time, in Kazakhstan, according to Article 205 of the Penal Code of the Republic of Kazakhstan (2014), unlawful access to information systems entails much milder sanctions, including fines, correctional labour or arrest for up to 50 days, and only in cases of serious consequences, imprisonment for up to two years is possible. This imbalance in the approaches to the qualification and sanctions for cybercrime demonstrates the need to harmonise Kazakhstan's criminal legislation with international standards, which will help strengthen digital security, increase the effectiveness of preventive measures and expand mechanisms for international cooperation in the field of cybersecurity. Improving sanctions, especially concerning attacks on critical infrastructure, as well as developing public-private partnerships and introducing modern digital security measures are key elements in ensuring effective countering cybercrime in the face of modern threats (Kassymzhanova *et al.*, 2022).

The theoretical framework for the study of cyberattacks, therefore, has an interdisciplinary basis, covering criminological and criminal law analysis of offenders' behaviour, technical aspects of information security, as well as socio-economic and political-legal consequences of attacks. On the one hand, a cyberattack can undermine the stability of entire industries, such as the energy, healthcare or telecommunications sectors. On the other hand, it poses large-scale social risks: the leakage of personal data and confidential information reduces the level of trust in digital services and creates concerns among the population that e-government and commercial services are not sufficiently protected (Mazur & Flogaitis, 2023). Finally, cyberattacks are directly related to national security and the observance of citizens' rights and freedoms, as they concern the protection of personal and state secrets, information sovereignty and economic stability.

In this context, the legal regulation of the powers of state bodies, the formation of specialised cybersecurity units and the development of comprehensive state programmes, such as the Resolution of the Government of the Republic of Kazakhstan No. 407 (2017), aimed at developing the domestic information security infrastructure, professional development of specialists, as well as international cooperation, are of high priority. The legal assessment of cyberattacks is based on the analysis of the relevant provisions of the Penal Code of the Republic of Kazakhstan (2014), which establishes criminal liability for unauthorised access to computer information, creation, use and distribution of malicious software, as well as for violation of the rules for the operation of automated information systems. However, even with the relevant articles of the Criminal Code of the Republic of Kazakhstan, the problem of evidence and lack of technical capabilities of law enforcement agencies remains relevant, which creates the need for special training and close cooperation with IT experts (UNODC and partners…, n.d.).

Therefore, the theoretical aspects of countering cyberattack in the Republic of Kazakhstan are primarily related to the formation of a comprehensive understanding of the nature of these crimes, their forms and methods of commission, as well as the analysis of how legislation, science and practice respond to the new challenges of the digital age. Given the rapid change in technology and the international nature of cyberattacks, national laws should incorporate the provisions of international agreements and be guided by the best practices of other countries that have developed their cyber defence models. Legal regulation should not be limited to repressive measures – effective deterrence of cybercrime requires a preventive, educational, scientific and technical approach that allows the system of countering cyberattacks to be timely adapted to evolving methods and means of their implementation. Without such an interdisciplinary framework and constant monitoring of new forms of threats, it is impossible to guarantee an adequate level of social security and economic stability in the country, especially since cyberattacks are increasingly becoming a tool not only for criminals but also for politically motivated actions. As the experience of international cooperation within INTERPOL (2022) and the OSCE shows, a comprehensive approach based on clear regulation in national legislation, effective interagency coordination and the involvement of international partners is the most effective way to prevent cyberattacks and minimise their negative consequences (Concluding event of…, 2024). INTERPOL coordinates global operations against organised cybercrime, combining the efforts of law enforcement agencies and the private sector to identify and neutralise cyber threats. The OSCE, for its part, implements regional projects to build capacity in the fight against cybercrime, promoting international cooperation and the exchange of best practices among participating States. For Kazakhstan, the project "Capacity Building on Combating Cybercrime in Central Asia" (n.d.), covering five Central Asian states and aiming to develop a domestic cybercrime counteraction system, is notable. The project implements a comprehensive training programme for law enforcement officials on cybercrime investigation methods, procedures for handling digital evidence, and the use of modern technologies in law enforcement. The practical implementation of the project involves regular training and seminars for representatives of law enforcement agencies in Kazakhstan to improve their cybersecurity skills. The effectiveness of this approach is confirmed by the successful holding of specialised training on digital forensics in May 2022 with the participation of experts from Kazakhstan, Kyrgyzstan and Uzbekistan, which created additional opportunities for the exchange of experience and the establishment of professional contacts between law enforcement agencies in the region (OSCE trains Central…, 2022). Thus, the successful counteraction to cyberattacks in Kazakhstan requires a multifaceted strategy that integrates national legislative improvements, international cooperation, and continuous professional training, ensuring the country's resilience against evolving cyber threats.

Peculiarities of qualification and investigation of cyber attacks. Criminal law regulation of countering cyberattacks in the Republic of Kazakhstan is based on the provisions of the Penal Code of the Republic of Kazakhstan (2014), which defines objective and subjective signs of crimes related to the disruption of information systems and electronic networks. According to the analysis of the text of the Penal Code of the Republic of Kazakhstan, the most relevant articles in this context are the provisions on unauthorised access to information resources, creation and distribution of malicious software and disruption of the normal functioning of computer systems. At the same time, the legislator provides for punishment proportionate to the scale of damage or danger posed by such interference to economic, social and national security.

To qualify a particular act, it is necessary to address the object of the attack (confidentiality, integrity or availability of information), the method and consequences of the attack, as well as the presence of direct or indirect intent. For example, a DDoS attack that blocks the operation of a government portal may fall under "Unlawful interference with the operation of an information system", while the theft of a confidential database using special software qualifies as "Unauthorised access to an information system" or "Creation, use or distribution of malicious computer programs" (Penal Code of the Republic of Kazakhstan, 2014). It is necessary to distinguish between situations where a person intentionally causes harm or seeks to gain mercenary benefit from cases of unintentional actions, as well as to address the degree of preparation of the crime, its group nature or cross-border aspect.

In qualifying cyberattacks, the subjective side of the act and the motives of the offender should be emphasised. In law enforcement practice, it is necessary to recognise the difference between intentional actions aimed at causing damage and cases where interference with information systems occurs without criminal intent. This is of fundamental importance for the correct qualification of the act and the distinction between criminal offences and administrative or disciplinary violations. The proper differentiation of sanctions and consideration of the actual harm or threat posed by such acts is crucial to ensure effective criminal law policy and proportionality of punishment concerning cyberattacks, which have recently become increasingly complex.

The forensic characterisation of cyberattacks is based on a set of methods used by attackers and the typical traces they leave in the digital environment. According to the data on the specifics of collecting and evaluating digital evidence (Table 1), attacks are increasingly being carried out with the help of special vulnerability search tools (exploit kits), botnets and artificial intelligence (AI) programs, which allow

automating the intrusion process. DDoS attacks, phishing, watering hole attacks (injecting malicious code into visited websites), and malware that can be embedded in files or distributed via USB drives or infected emails are noteworthy. To hide tracks, criminals commonly use VPN services, the Tor network, fake IP addresses and traffic encryption methods, making it difficult to identify specific perpetrators. In such circumstances, the investigation requires high-quality digital forensics, which includes analysing log files, and network traffic, recovering deleted and encrypted data, and capturing and examining metadata. Hardware and software tools for cloning hard drives, collecting RAM images, and hashing seized media are becoming increasingly important. If these procedures and techniques are not followed, the results of the examinations may be declared inadmissible, making it impossible to fully prove the offender's guilt in court. Law enforcement agencies insist on the need to carefully comply with the standards of authenticity of electronic evidence, by recording checksums and maintaining detailed procedural documentation.

Table 1. Specifics of collecting and evaluating digital evidence in the investigation of various types of cyberattacks

Type of cyber attack	Key digital evidence	Specifics of the collection	Difficulties in proving	Expertise requirements
Computer viruses, network worms, trojans	Malware samples, memory dumps, antivirus logs	The need to quickly identify new software samples	Virus polymorphism and encryption	Reverse engineering and analysis of malware behaviour
Botnet attacks	IP addresses, C2 server data, botnet controller logs	Monitor the distributed network of infected devices	The difficulty of de-anonymising botnet operators	Technical analysis of botnet command traffic
Phishing attacks	Email logs, DNS records, HTML code of fake pages	Quick response due to the short lifespan of phishing sites	Proving intent when using fake accounts	Linguistic expertise in emails, technical analysis of domains
Unauthorised access	Access logs, authorisation logs, exploit traces	Real-time recording of unauthorised access attempts	Use of anonymous or temporary accounts	Access system forensics and event log analysis
DDoS attacks	Traffic logs, NetFlow data, server logs	Rapid analysis of large volumes of network traffic	Attacks can be disguised as normal traffic	Analyse network traffic, correlate events in real-time
Attacks on banking systems	Transaction logs, SWIFT records, monitoring system data	Synchronise data from different banking systems	Differences in time stamps due to different time zones	Financial, economic computer and technical expertise
Insider data leaks	Access logs, copy history, network traffic	Preserving the integrity of file metadata to identify the culprit	Difficulty in distinguishing between business and non-business use	Expertise in data storage media following the organisation's security policies

Source: compiled by the authors based on A. Dimitriadis *et al.* (2020), E. Karafili *et al.* (2020), A.Y. Ofori and D. Akoto (2020)

The systematisation of the procedural features of handling digital evidence presented in Table 1 reflects the multidimensional nature of forensic support for the investigation of cybercrime and highlights the need to develop specialised forensic techniques. Establishing the relationship between the technological specifics of unlawful acts and the relevant procedural mechanisms for ensuring the admissibility of evidence is of fundamental importance, which has a direct impact on the effectiveness of pre-trial investigation and court proceedings in this category. The practical significance of such systematisation is confirmed by successful investigations, particularly the case of the Apple engineer in 2022, where digital forensics revealed the unauthorised copying of confidential files of a self-driving car project (ERMProtect Staff, n.d.). The importance of an integrated approach to collecting and analysing digital evidence is demonstrated by the 4 million USD Miami cryptocurrency fraud case in 2022, where a combination of analysing forged documents and tracking cryptocurrency movements led to the successful disclosure of the crime. Additional evidence of the effectiveness of a systematic approach is the Waifu hacker case of 2025, where the use of a set of digital forensics methods, including the analysis of IP addresses and darknet activity, uncovered large-scale interference with the systems of 165 companies (How digital forensics…, 2025). Such examples highlight the need for continuous improvement of digital evidence collection and analysis techniques correlates with the evolution of cyber threats and technological advances.

The identification of key difficulties in proving each type of cyberattack creates a methodological basis for improving investigative tactics and developing relevant forensic recommendations and justifies the need to legislate a special procedure for handling electronic evidence. In Kazakhstan, the investigation of cybercrime is regulated by the Criminal Procedure Code of the Republic of Kazakhstan (2014). Pre-trial investigations are conducted by the internal affairs bodies, the National Security Committee and other competent authorities. The process includes several key investigative actions, including inspection of the scene, seizure of electronic media, traffic analysis, recovery of deleted data, expert research and other forensic measures. Proof of the authenticity of digital evidence and compliance with procedural rules are important. Since 2018, Kazakhstan has implemented the Electronic Criminal Proceedings system, which automates the investigation and trial processes, through the maintenance of case files in digital format. At the same time, special attention is paid to the issues of authorised access to confidential information, which is regulated by the provisions of the Criminal Procedure Code. Cybercrime investigations may also involve international cooperation when it comes to crimes that go beyond national jurisdiction. Kazakhstan is actively working to improve its legislative framework on

digital evidence and methods of investigating cybercrime, in the context of harmonisation with international standards.

The requirements for expert research, systematised by type of cyberattack, demonstrate the need to develop an interdisciplinary approach to the development of expert methodologies and training of relevant specialists, which should be reflected in departmental regulations and methodological recommendations. An important aspect is to define the specifics of digital evidence collection, which indicates the need to develop specialised software and hardware systems for recording and investigating traces of cybercrime, as well as the expediency of introducing unified standards for working with electronic evidence at the international level (Kobets, 2023). The collection of digital evidence in Kazakhstan is conducted based on the national legislation regulating the procedure for handling electronic evidence, its collection, storage and use in court. In 2023, a law was passed that prohibits the collection and processing of paper copies of identity documents, except in certain cases, which are aimed at strengthening the protection of personal data (Tokayev signs law…, 2023). In contrast to Kazakhstan, the European Union and the United States have more detailed standards and guidelines for the collection and processing of digital evidence. The EU has the General Data Protection Regulation, which establishes strict rules for the processing of personal data and provides measures to ensure its security. In the United States, the Association of Chiefs of Police has developed recommendations that emphasise the need to use forensically sound methods when collecting and analysing digital data (Sobirov, 2023). Thus, approaches to the collection of digital evidence in Kazakhstan, the EU and the US differ in the degree of detail and strictness of regulations, which indicates the need to develop unified international standards in this area.

Pre-trial investigations in the Republic of Kazakhstan are conducted based on the provisions of the Criminal Procedure Code of the Republic of Kazakhstan (2014) the provisions on inspection of the scene, seizure and search of computer equipment, computer and technical expertise and ensuring the preservation of confidential information. The seizure of hardware and electronic media is conducted following the general provisions of the Criminal Procedure Code of the Republic of Kazakhstan on evidence and investigative actions. The appointment of examinations covering the recovery of deleted files, detection of malware and determination of the exact time of the cyberattack is regulated by the rules on conducting forensic examinations.

Documentation of the seizure of digital media and their analysis is a substantial part of the investigation process (Nurbatyrova *et al.*, 2024). According to Article 221 of the Criminal Procedure Code of the Republic of Kazakhstan (2014), all items seized during investigative actions are subject to a thorough examination, after which they may be recognised as material evidence and attached to the case file. The legislation provides for the use of photo and video recording in the process of seizing digital equipment, which allows for avoiding doubts about the integrity of evidence. The seizure procedure involves recording the device's identification data, including serial numbers and hash amounts of the seized media, which guarantees their integrity and authenticity. According to Article 126 of the Criminal Procedure Code of the Republic of Kazakhstan, special scientific and technical means are used to collect digital evidence, including forensic software for analysing hard drives, mobile devices and server logs. The algorithm of digital evidence seizure includes several mandatory steps:

1. Preliminary inspection of devices and creation of digital copies without changing the contents of the media.
2. Verification of data integrity using hashing.
3. Documentation of the seizure process with an indication of time, place and persons involved in the procedure.
4. Further examination to analyse the contents of the device.

The seized equipment must be packed, sealed and transferred to a specially designated storage facility controlled by the pre-trial investigation authorities. When investigating cross-border cybercrime, the competent authorities of Kazakhstan actively cooperate with international organisations, such as INTERPOL (2022), and OSCE, and exchange information through international legal assistance mechanisms (Concluding event of…, 2024). This makes it possible to detect attackers' IP addresses, identify botnet control servers, and identify sources of attacks located outside Kazakhstan. At the same time, such investigations are complicated by differences in national legislation and personal data protection issues, which require careful adherence to international standards of evidence.

Prevention of cybercrime within the framework of the Resolution of the Government of the Republic of Kazakhstan No. 407 (2017) concept involves not only improving criminal procedure and operational and investigative measures but also developing partnerships between the public and private sectors. Through cooperation with telecom operators and software developers, law enforcement agencies can quickly detect abnormal traffic patterns, and new types of malware and block attacks at the initial stage. A significant contribution to prevention is made by cyber-attack response centres (CERTs), which monitor network activity, issue technical recommendations and coordinate actions to neutralise large-scale attacks (KZ-CERT, n.d.). CERT conducts regular training to raise awareness of the dangers of phishing, social engineering and unauthorised intrusions among civil servants, corporate users and public sector representatives. For example, the Defence Information Systems Agency (DISA) offers an interactive course, Phishing and Social Engineering: Virtual Communication Awareness Training DS-IA103.06 (n.d.), which explains different types of social engineering attacks, including phishing, spear phishing, whaling, smishing, and vishing (Department of Defence..., n.d.). Additionally, the Centre for Security Development (CDSE) offers a similar course that teaches users how to recognise the signs of social engineering attempts and offers recommendations on how to avoid such attacks and their consequences (Defence Counterintelligence..., n.d.).

Statistics from KZ-CERT (n.d.) show a significant increase in the number of detected cyber incidents: in 2024, the number of cases of computer viruses, network worms and trojans more than doubled compared to 2023 (from 21,940 to 45,027 cases), which underscores the importance of strengthening interagency cooperation and improving automated intrusion detection systems. Statistical analysis of the effectiveness of pre-trial investigations of cybercrime provides important data for assessing the effectiveness of the law enforcement system in combating this type of crime. In Kazakhstan, only a small proportion of criminal cases related to cybercrime go to trial. According to the Committee for

Legal Statistics and Special Accounts of the General Prosecutor's Office of the Republic of Kazakhstan, in 2022, out of 142 criminal cases in progress, only 8 were brought to court, which is about 5.6%. In the first half of 2023, out of 106 pending cases, only 3 were sent to court, i.e., 2.8%. The main reasons for the termination of investigations are the expiry of the statute of limitations, insufficient evidence or the absence of suspects. In addition, in 2022, the number of losses from cybercrime was 58 million tenge, of which 27.6 million was the state's loss and 30.4 million was the loss to individuals. However, only the funds stolen from the state budget were recovered (Only 5% of…, 2023). In the future, an important task remains to develop a comprehensive early warning system and integrate existing security programmes into a single platform. Currently, Kazakhstan has a National Computer Emergency Response Team (KZ-CERT, n.d.) that detects and responds to incidents in the public sector and among users of national information systems and the Internet segment. In the financial sector, there is the Centre for Information Exchange and Analysis of Cyber Threats (KZ-FinCERT, n.d.), which operates under the auspices of the Agency for Regulation and Development of the Financial Market of the Republic of Kazakhstan and specialises in protecting the national financial institutions.

An analysis of the reasons for the low effectiveness of cybercrime investigations also points to the need to study the institutional factors that affect the effectiveness of the law enforcement system. According to official data, in 2023, about 1,500 corruption offences were registered, involving more than 1,100 people, including 158 managers of various levels (Zhumagali, 2024). Such indicators demonstrate the systemic nature of corruption in government agencies, which directly affects the objectivity of the investigation and consideration of criminal cases of cybercrime. To counteract this phenomenon, the Anti-Corruption Agency has developed a draft law "On Testing for Professional Integrity", which aims to identify corruption risks in the behaviour of law enforcement officers and to form an anti-corruption culture in their environment (A way to…, 2024). However, despite the measures taken, corruption in pre-trial investigation bodies continues to lead to procedural violations and delays in the investigation, which negatively affects the quality and effectiveness of criminal proceedings in cybercrime cases.

It is also necessary to expand the professional training of investigators, prosecutors and judges in the field of IT crime. In line with the strategic approach of the European Union Agency for the Training of Law Enforcement Officers (CEPOL), such specialists should regularly undergo advanced training by participating in international training programmes and exchanging experience. As part of cooperation with CEPOL, joint training and seminars are organised, where specialists from Kazakhstan learn the best practices of investigating cybercrime from their European colleagues (CEPOL Knowledge Centres, n.d.). An important element is also the development of the procedural framework. In Kazakhstan, procedural actions concerning cybercrime are regulated by special provisions of the Criminal Procedure Code of the Republic of Kazakhstan (2014), which establish the procedure for collecting and recording digital evidence, conducting computer-technical examinations and applying special investigative actions in the digital environment. This multidimensional approach is crucial for ensuring social security and economic stability in the digital age when cyberattacks are increasingly becoming a tool not only for criminals but also for politically motivated actions.

Interdisciplinary issues and legal framework in the context of social security and economic stability. Cyberattacks have become so widespread and diverse that their impact extends far beyond the purely criminal law sphere to include the economic, social and even political dimensions. From the perspective of economic stability, the consequences of successful cyberattacks are particularly noticeable in the financial, energy and telecommunications sectors, which form the basis of the modern digital economy. According to a study, in 2023, more than 223 million cyberattack attempts were recorded in Kazakhstan, most of which originated from foreign hackers. The main targets were local executive bodies, government agencies, the quasi-public sector, telecommunications operators, and private companies. According to a report by Cybersecurity Ventures, global annual losses from cybercrime in 2023 amounted to USD 8 trillion and were projected to grow to USD 10.5 trillion in 2025 (Calif, 2023). This growth is driven by the active implementation of the Internet of Things, the development of cloud technologies and the digitalisation of business processes.

In the context of the Republic of Kazakhstan, financial losses can be particularly significant for small and medium-sized businesses that do not always have a sufficient level of cyber defence. According to the report of the National Bank of the Republic of Kazakhstan, in the first half of 2024, a significant increase in cases of fraud aimed at Internet banking was recorded (New types of fraud…, 2024). According to the Committee for Legal Statistics and Special Accounts of the General Prosecutor's Office of the Republic of Kazakhstan, in January-July 2024, the number of established losses from Internet fraud amounted to KZT 7.1 billion, of which KZT 6.8 billion was incurred by individuals and KZT 304.1 million by legal entities (Damage from internet…, n.d.). In addition, the Anti-Fraud Centre of the National Bank registered 17,802 incidents in six months of operation, which resulted in the timely blocking of approximately KZT 1.5 billion. Of this amount, KZT 1.1 billion was blocked by the sending bank, and KZT 343.4 million by the receiving bank. Voluntarily, KZT 88.9 million was returned to the victims (Anti-Fraud Center…, 2025). In the energy sector, 49.1% of computers in automated control systems were attacked by malware in 2023, which is higher than the global average of 39% (Where is the rise…, 2023). In addition, Kazakhtelecom recorded a massive DDoS attack on several information resources from abroad, which caused significant disruptions in their operation (Kazakhtelecom announced DDoS…, 2022). Such incidents had not only economic but also social consequences, as power outages directly affected the welfare of the population and caused public discontent.

In turn, the social aspect of cyberattacks is directly related to public trust in public and private digital platforms. In the event of a successful intrusion into databases containing the personal or financial information of citizens, there is a risk of a large-scale leak of confidential information. According to the State Technical Service of Kazakhstan, in 2023, more than 223 million cyberattack attempts were recorded from abroad, with 62% of them targeting the public sector (Over 223 million…, 2024). According to the survey, the financial losses of Kazakhstani companies as a result of cyberattacks were distributed as follows: 42% of organisations reported losses of less than 800 thousand tenges, 10% of

companies suffered losses from 800 thousand to 2.4 million tenges, and 5% of enterprises faced losses exceeding 8 million tenges (Ishekenova, 2023). With the development of electronic services, cybersecurity and personal data protection issues are becoming increasingly relevant.

Global trends indicate an increase in the number of cyberattacks and data breaches worldwide. For example, in 2023, several high-profile data breaches were reported, highlighting the importance of strengthening security measures (Cybersecurity predictions for…, 2023). Kazakhstan has also seen an increase in cyberattacks on independent media, which is causing concern in society and reducing trust in government institutions. In 2023, Adil Soz recorded 56 cases of cyberattacks on media outlets and journalists, which is significantly higher than the previous year. The affected publications include KazTAG and Nege.kz, Kursiv.Media and inbusiness.kz. These attacks led to the temporary unavailability of the websites and slowed down their work. In response, the Committee to Protect Journalists (CPJ) called on the Kazakh authorities to conduct a thorough investigation and bring those responsible to justice (CPJ urges Kazakh..., 2024). In this regard, governments and organisations in various countries, including Kazakhstan, prioritise the protection of personal data and increasing public trust in electronic public services.

The lack of information on specific incidents in Kazakhstan may indicate the effectiveness of security measures or a lack of transparency in reporting such incidents. The level of transparency often correlates with a country's democracy. According to the Democracy Index, which assesses the state of democracy in 165 countries in five categories: electoral process and pluralism, government functioning, political participation, political culture and civil liberties, Kazakhstan has a score of 3.08, which places it among authoritarian regimes (Our World in Data, 2023). Cyberattacks are often accompanied by the spread of disinformation or malicious fakes, which can exacerbate social tensions and provoke mass unrest, especially when attackers pursue political or ideological goals. According to a report by the International Monetary Fund & Monetary and Capital Markets Department (2024), such actions can destabilise society and undermine trust in state institutions.

Given the critical impact of cyberattacks on the economy and social stability, legal regulation of cybersecurity in Kazakhstan is of great importance. There are gaps in law enforcement practice due to the lack of detailed rules on the liability of critical facilities operators for inadequate cyber security, as well as an insufficient mechanism for monitoring and auditing their activities. The legal framework includes the Law of the Republic of Kazakhstan No. 418-V (2015), which sets out basic requirements for operators and liability for violations in this area. Regulation of the European Parliament and of the Council No. 2016/679 "On the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)" (2016) introduced the obligation of owners of critical information and communications infrastructure to create domestic operational information security centres or engage relevant services, ensuring their interaction with the National Coordination Centre. The procedure for mandatory monitoring and auditing of these facilities is regulated by the Order of the Minister of Digital Development, Innovation and Aerospace Industry of the Republic of Kazakhstan No. 175/HK "On Determining the Amount of Payment for Services of State Registration of Civil Status Acts" (2023). However, there are gaps in law enforcement practice due to the lack of detailed regulations on the liability of critical facilities operators for inadequate cyber security, as well as an insufficient mechanism for monitoring and auditing their activities. In particular, the Report on the implementation of the Strategic Plan of the Ministry of Digital Development, Innovations and Aerospace Industry of the Republic of Kazakhstan for 2020-2024 (2021) notes the need to improve the system of control over information security by critical infrastructure operators. In addition, in the context of public-private partnerships, which should be one of the priority areas, there are no specific legal requirements for the mandatory exchange of information on vulnerabilities and cyberattacks between private businesses and law enforcement agencies. International practice shows that without clear requirements for reporting cyber incidents and without adequate guarantees of confidentiality of information, companies are reluctant to disclose attacks to avoid reputational losses, which generally complicates the response to threats.

Given the interdisciplinary nature of the problem, the state seeks to harmonise national legislation with international standards, with the provisions of the Convention on Cybercrime (2001) and other multilateral agreements that simplify the procedures for extradition of cybercriminals, joint investigation of complex attacks and exchange of electronic evidence. However, further improvement of the legal framework requires the development of new specialised regulations aimed at detailing the rules of operation of a single cyber defence coordination centre. Such a centre could unite the efforts of relevant ministries (Ministry of Internal Affairs (MoIA)), National Security Committee (NSC), Ministry of Digital Development, Innovation and Aerospace Industry (MinDigit), Ministry of Defence (MoD)) and response centres (CERT), and establish a transparent procedure for information exchange and rapid decision-making in crises.

It is advisable to introduce economic incentives for critical systems operators to invest in cybersecurity, for example, through tax breaks or grant programmes for equipment upgrades. Similar mechanisms are successfully operating in the UK, Germany, and France, where the private sector is involved in the protection of critical infrastructure through a system of public-private partnerships and economic incentives, as well as in the US, which has a developed system of partnerships between federal agencies and private companies in the field of cybersecurity (Llazo *et al.*, 2024). In particular, the U.S. Department of Homeland Security (DHS) has established the Critical Infrastructure Partnership Advisory Council (CIPAC) (n.d.) to facilitate interaction between government agencies and representatives of the critical infrastructure owner and operator community. This partnership aims to improve the security and resilience of the country's critical infrastructure through effective information sharing and coordinated efforts.

In addition to improving legislation, the issue of training and retraining deserves special attention. About 70% of successful large-scale attacks in Ukraine, Russia and other CIS countries were caused by the human factor: insufficient staff qualifications, system configuration errors, and lack of regular software updates (Vuković & Štefanac, 2023). According to a study by Datami Newsroom (2024), human factors and

system failures account for 52% of data security breaches. Therefore, the development of curricula in universities and colleges, practical training and professional certifications should be a priority for government policy.

Equally important is public outreach to ensure that ordinary users understand the risks of phishing, account hacking and other types of fraud and follow basic digital hygiene principles. Without awareness of the general dangers associated with cyberattacks, even the most advanced legislation will remain ineffective. In addition, global practice shows that one of the most effective ways to encourage businesses to openly report vulnerabilities is to introduce so-called "bug bounty" programmes that reward researchers and cybersecurity experts for identifying and reporting system flaws. For instance, in 2023, several new programmes were launched, such as those by ATG and Bybit, which offer rewards of up to 4,000 USD and 20,000 USD, respectively, for vulnerabilities discovered (Leyden, 2023). At the legislative level, it is advisable to establish a secure legal status for white hat hackers who act in good faith to avoid confusion with criminal prosecution. In Germany, it is planned to decriminalise the activities of ethical hackers, which will reduce legal risks for cybersecurity researchers (Naprys, 2024).

Summing up the above arguments, it should be emphasised that effective counteraction to cyberattacks requires the integration of economic, social and legal instruments. The losses for business and the state can be catastrophic, and the social consequences can be even more profound if an attack undermines trust in state institutions or creates conditions for social instability. The current legislation, including the Law of the Republic of Kazakhstan No. 418-V (2015), the Resolution of the Government of the Republic of Kazakhstan No. 407 (2017) and relevant bylaws forms the basic framework for the protection of digital infrastructure, but the pace of technological development requires further adaptation of these norms.

Gaps in the regulation of critical facilities, insufficient motivation of the private sector to transparently report incidents, and a shortage of highly qualified specialists remain key challenges that require comprehensive measures by the state. Over the past two years, the demand for such specialists in the republic has doubled, but the supply has not kept pace with the growing needs. Depending on experience and company, the salary offered can reach KZT 1.5 million. Despite this, there is a substantial shortage of personnel in this area (Cybersecurity threats to Kazakhstan, 2024). The development of centralised mechanisms for interagency cooperation, legislative support for public-private partnerships, active involvement of the expert community in the development of security standards and audits and raising the public's awareness of digital risks can become effective components of a system designed to ensure an adequate level of social security and economic stability. As a result, the Republic of Kazakhstan will have the opportunity to create a sustainable digital ecosystem where cyber threats are minimised, and society and businesses benefit from the safe and reliable use of modern technologies.

Discussion

The results of the study on countering cyberattacks in the Republic of Kazakhstan reveal critical trends and systemic problems in the field of cybersecurity, which are important both for understanding the current situation and for developing effective mechanisms to counter cyber threats. The recorded increase in the number of malware incidents by 105% in 2024 (from 21,940 to 45,027 cases) is fully consistent with the findings of Y. Li and Q. Liu (2021), who identified an exponential increase in cyber threats and their direct impact on the national security of states. However, unlike their study, which focused mainly on the technological aspects of cybersecurity, the analysis revealed the critical importance of the human factor and the need for an integrated approach to ensuring the protection of information systems. This is supported by statistics that show that about 70% of successful attacks are due to insufficient staff qualifications and system configuration errors.

The fact that 62% of cyberattacks are directed at the public sector is consistent with the findings of M. Lehto (2022), who identified critical infrastructure as a priority target of cyberattacks. Particularly important is the observation that physical infrastructure can be damaged by penetrating digital control systems, which is supported by documented cases of successful attacks on the energy sector in Kazakhstan. According to the data, in 2022, the share of attacks on the energy sector increased from 28% to 32% (Galushko, 2022). At the same time, in contrast to M. Lehto (2022) optimistic forecasts about the possibility of rapidly improving security systems, the study revealed significant institutional and technological limitations that impede a rapid response to new types of threats. This observation is reinforced by the findings of A. Djenna *et al.* (2021), who emphasises the need for in-depth mapping of cyber threats before implementing protective measures.

The analysis of the financial consequences of cyberattacks, the recorded losses of the banking sector in the amount of KZT 1.5 billion in the second half of 2024, is of particular importance in the context of the study by J. Hiller *et al.* (2024). Their proposal for the introduction of a federal tax credit in the United States to stimulate investment in cybersecurity is noteworthy, but the study's findings indicate the need for a more differentiated approach in Kazakhstan, especially to support small and medium-sized businesses. This thesis is supported by the data on disproportionately high losses in this sector and the limited capacity of small businesses to implement comprehensive security systems.

A particularly important aspect of the study is the analysis of the role of the human factor in the cybersecurity system. The high percentage of successful attacks related to the human factor confirms the findings of E. Kadena and M. Gupi (2021) on the critical importance of behavioural aspects in cybersecurity. However, in contrast to their focus on psychological factors, this study demonstrates the need for a comprehensive approach that includes both behavioural and technical aspects of staff training. This observation is complemented by the findings of A. Kuek and S. Hakkennes (2020), who found that approximately one-fifth of employee's experience anxiety when working with information systems. In contrast to their recommendation for general digital literacy training, the study's findings highlight the need for specialised cybersecurity training programmes tailored to specific professional contexts.

The results of the study on the growing complexity of cyberattacks and the use of AI are confirmed by S. Lysenko *et al.* (2024) and I. Naseer (2024), who emphasise the critical role of AI in modern cyber defence systems. However, while their studies demonstrate optimistic forecasts

for the rapid adoption of AI defence systems, the analysis reveals significant limitations and challenges in the context of Kazakhstan, especially in the public sector. These limitations are not only related to technological capabilities but also to institutional and regulatory barriers. S. Zeadally *et al.* (2020) also emphasise the need to develop new AI methods to counter cyber threats, but their conclusions on the possibility of rapid adaptation of traditional security systems do not find confirmation in Kazakhstan, where the process of introducing new technologies faces several organisational and resource constraints.

The gaps in the public-private partnership system identified in the study are largely in line with the observations of Y.E. Tabrez (2020), and T. Walshe and A. Simpson (2020), who emphasise the importance of innovative mechanisms for technological development. However, their proposals for a system of prizes and grants appear to be insufficient in the context of the identified systemic problems in protecting Kazakhstan's critical infrastructure. The results of the study highlight the need for a deeper institutional transformation and the creation of effective mechanisms for coordination between the public and private sectors. This is supported by documented cases where the lack of proper coordination led to delays in responding to cyber incidents and increased the scale of damage.

The social consequences of cyberattacks are particularly noteworthy, correlating with the findings of R. Shandler and M.A. Gomez (2023). Their observation that fear has a greater impact on reducing trust in government institutions than anger is confirmed in the analysis of public reaction to large-scale cyberattacks in Kazakhstan. In particular, the results of the study show that after cybersecurity incidents, citizens demonstrate an increased level of caution in using state electronic services and express doubts about the ability of state authorities to protect their data. However, in contrast to the findings of R. Shandler and M.A. Gomez (2023) regarding the long-term persistence of negative social consequences, our study demonstrates that public trust can be restored through transparent communication and effective incident response.

A significant aspect of the study is the analysis of the use of AI technologies in cyberattacks. M.M. Yamin *et al.* (2021) warn of the growing threat of "armed AI", and this is confirmed by the detected cases of automated systems being used to conduct attacks. However, in contrast to their predictions of a rapid development of this trend, the study shows a more gradual introduction of AI in cyberattacks in the region, which may be due to technological and resource limitations of local cybercriminal groups.

The issue of digital literacy, studied in the context of cybersecurity, is theoretically substantiated by D. Cetindamar *et al.* (2021), who analysed digital literacy as a fundamental prerequisite for the effective use of technology. In contrast to their general approach to digital literacy, the current study determined that the problem of insufficient technical skills is a critical factor in Kazakhstan's cybersecurity, as evidenced by the high percentage of successful attacks related to human error and system configuration errors.

Conclusions by K. Mitsarakis (2023) on the growing influence of geopolitical factors on cybersecurity are fully confirmed by the results of the study, which demonstrate a significant increase in the number of politically motivated cyberattacks on Kazakhstan's critical infrastructure. However, in contrast to its optimistic assessment of the effectiveness of international mechanisms for countering cyber threats, the study found limited effectiveness of such mechanisms in the regional context, which points to the need to develop more adapted approaches to international cooperation.

Following S. Zeadally *et al.* (2020), the study results not only confirm global trends in cybersecurity but also identify specific features and challenges that are characteristic of Kazakhstan and the region. This creates the basis for developing more effective mechanisms to counter cyber threats, addressing the local context, available resources and institutional constraints. Particularly, the relationship between technological, organisational and human factors in ensuring cybersecurity, which requires a comprehensive approach to the development and implementation of protective mechanisms.

Conclusions

The results of the study demonstrate the rapid growth of technological complexity and the systemic nature of cyber threats in the Republic of Kazakhstan. In 2024, the number of malware-related incidents increased by 105% compared to the previous period, reaching 4,507 cases. Targeted attacks on critical infrastructure and the public sector pose a particular danger, as evidenced by the State Technical Service's statistics: more than 223 million cyberattack attempts from abroad in 2023, of which 62% were aimed at government agencies. Financial losses demonstrate the significant negative impact of cyberattacks on economic stability: in the banking sector alone, losses of KZT 1.5 billion were recorded in the second half of 2024, with the small and medium-sized business segment being the most vulnerable.

Significant gaps in the cyber defence system have been identified, including the lack of clear mechanisms for interagency coordination and insufficient regulation of public-private partnerships in the field of cybersecurity. The analysis of law enforcement practice has shown that the existing legal framework does not fully meet the current challenges, especially in terms of regulating the liability of critical infrastructure operators and mechanisms for prompt response to cyber incidents. The study determined that the lack of unified security standards and audit procedures significantly complicates the process of assessing the vulnerabilities of information systems. The human factor remains an important factor in the success of cyberattacks approximately 70% of successful interventions are due to insufficient staff qualifications and system configuration errors. DDoS and phishing attacks pose a particular danger, as they can not only paralyse critical facilities but also undermine public confidence in digital services.

The study established the need to create a single cyber defence coordination centre that would combine the efforts of relevant ministries, law enforcement agencies and cyber incident response centres. The study proposed a model of such a centre with a clear division of powers and mechanisms for rapid response to incidents. The effectiveness of economic mechanisms to stimulate investment in cybersecurity through a system of tax incentives and grant programmes is proven. The positive impact of "bug bounty" programmes on identifying vulnerabilities in information systems is revealed, which is confirmed by the international experience of leading technology companies.

Promising areas for further research include studying the impact of AI technologies on the evolution of cyberattack methods, developing a methodology for assessing the

effectiveness of public-private partnership mechanisms in the field of cybersecurity, and researching the legal and technical aspects of international cooperation in combating cross-border cybercrime, especially in the context of crypto-currencies and decentralised financial systems.

Acknowledgements

None.

Conflict of interest

None.

References

[1] A way to combat corruption in law enforcement agencies in Kazakhstan has been found. (2024). Retrieved from https://www.zakon.kz/sobytiia/6450017-nayden-sposob-borby-s-korruptsiey-v-pravookhranitelnykh-organakh-kazakhstana.html.

[2] Anti-Fraud Center results: Suspicious transactions worth over 1.4 billion tenge blocked. (2025). Retrieved from https://nationalbank.kz/kz/news/informacionnye-soobshcheniya/17388.

[3] Azanbay, K. (2024). Innovative technologies as a factor of information security of the Republic of Kazakhstan. *Information Systems Engineering,* 29(2), 523-532. doi: 10.18280/isi.290213.

[4] Bishmanov, K., Muratzhan, Z., Dilbarkhanova, Z., & Lyutsik, V. (2024). Analysis of modern types of cyberterrorism and methods of countering them. *IDP Internet Journal Law and Politics*, 41. doi: 10.7238/idp.v0i41.428542.

[5] Bolatbek, M., Baispay, G., Mussiraliyeva, S., & Usmanova, A. (2024). A framework for detection and mitigation of cyber criminal activities using university networks in Kazakhstan. *Radioelectronic and Computer Systems*, 2, 186-202. doi: 10.32620/reks.2024.2.15.

[6] Calif, S. (2023). *2023 Cybersecurity Almanac: 100 facts, figures, predictions, and statistics*. Retrieved from https://cybersecurityventures.com/cybersecurity-almanac-2023/.

[7] Capacity building on Combating Cybercrime in Central Asia. (n.d.). Retrieved from https://www.osce.org/project/capacity-building-on-combating-cybercrime-in-central-asia.

[8] CEPOL Knowledge Centres. (n.d.). Retrieved from https://cepol.europa.eu/training-education/cepol-knowledge-centres.

[9] Cetindamar, D., Abedin, B., & Shirahada, K. (2021). The role of employees in digital transformation: A preliminary study on how employees' digital literacy impacts use of digital technologies. *IEEE Transactions on Engineering Management*, 71, 7837-7848. doi: 10.1109/tem.2021.3087724.

[10] Computer Fraud and Abuse Act of 1986. (1986, October). Retrieved from https://www.congress.gov/99/statute/STATUTE-100/STATUTE-100-Pg1213.pdf.

[11] Concluding event of the OSCE regional project on combating cybercrime in Central Asia. (2024). Retrieved from https://www.osce.org/secretariat/570738.

[12] Convention on Cybercrime. (2001, November). Retrieved from https://rm.coe.int/1680081561.

[13] CPJ urges Kazakh authorities to investigate cyberattacks on media. (2024). Retrieved from https://cpj.org/2024/02/cpj-urges-kazakh-authorities-to-investigate-cyberattacks-on-media/.

[14] Criminal Procedure Code of the Republic of Kazakhstan. (2014, July). Retrieved from https://adilet.zan.kz/eng/docs/K1400000231.

[15] Critical Infrastructure Partnership Advisory Council (CIPAC). (n.d.). Retrieved from https://www.cisa.gov/resources-tools/groups/critical-infrastructure-partnership-advisory-council-cipac.

[16] Cybersecurity predictions for 2024. (2023). Retrieved from https://corewin.ua/news-ru/cybersecurity-forecasts-2024/.

[17] Cybersecurity threats to Kazakhstan. (2024). Retrieved from https://e-cis.info/news/566/115478/.

[18] Damage from internet fraud cases in Kazakhstan has grown to 7 billion tenge. (n.d.). Retrieved from https://finprom.kz/ru/article/usherb-ot-sluchaev-internet-moshennichestva-v-kazahstane-vyros-do-7-milliardov-tenge.

[19] Datami Newsroom. (2024). *What is threat analysis in cybersecurity?* Retrieved from https://datami.ee/blog/shho-take-analiz-zagroz-v-kiberbezpetsi/.

[20] Dimitriadis, A., Ivezic, N., Kulvatunyou, B., & Mavridis, I. (2020). D4I – digital forensics framework for reviewing and investigating cyber attacks. *Array*, 5, article number 100015. doi: 10.1016/j.array.2019.100015.

[21] Directive of the European Parliament and of the Council No. 2013/40/EU "On Attacks Against Information Systems and Replacing Council Framework Decision 2005/222/JHA". (2013, August). Retrieved from https://eur-lex.europa.eu/eli/dir/2013/40/oj.

[22] Djenna, A., Harous, S., & Saidouni, D.E. (2021). Internet of things meet Internet of threats: New concern cyber security issues of critical cyber infrastructure. *Applied Sciences*, 11(10), article number 4580. doi: 10.3390/app11104580.

[23] ERMProtect Staff. (n.d.). *5 notable digital and crypto forensics investigations of 2022*. Retrieved from https://ermprotect.com/blog/5-notable-digital-and-crypto-forensics-investigations-of-2022/.

[24] Galushko, M. (2022). *Industrial sectors were subject to the largest number of cyber attacks in Kazakhstan*. Retrieved from https://inbusiness.kz/ru/news/naibolshemu-kolichestvu-kiberatak-v-kazahstane-podverglis-promyshlennye-sektora.

[25] Hiller, J., Kisska-Schulze, K., & Shackelford, S. (2024). Cybersecurity carrots and sticks. *American Business Law Journal*, 61(1), 5-29. doi: 10.1111/ablj.12238.

[26] How digital forensics solved famous cybercrime cases? Real-life cases solved using digital evidence. (2025). Retrieved from https://www.webasha.com/blog/how-digital-forensics-solved-famous-cybercrime-cases-real-life-cases-solved-using-digital-evidence.

[27] Incident overview for Q1 2024. (2024). Retrieved from https://cert.gov.kz/news/11/2641.

[28] International Monetary Fund, & Monetary and Capital Markets Department. (2024). Cyber risk: A growing concern for macrofinancial stability. In *Global financial stability report: The last mile: Financial vulnerabilities and risks* (pp. 53-76).Washington: International Monetary Fund.

[29] INTERPOL. (2022). *Financial and cybercrimes top global police concerns, says new INTERPOL report*. Retrieved from https://www.interpol.int/News-and-Events/News/2022/Financial-and-cybercrimes-top-global-police-concerns-says-new-INTERPOL-report.
[30] Ishekenova, B. (2023). *Kazakhstani companies lose millions due to hacker attacks*. Retrieved from https://lsm.kz/kazahstanskie-kompanii-teryayut-milliony-iz-za-hakerskih-atak.
[31] Jekebayeva, M., Iztaeva, V., Anassova, K., & Manapbayev, N. (2023). Cybersecurity: Importance for Kazakhstan and international experiences. *Bulletin of Ablai Khan KazUIRandWL Series "International Relations and Regional Studies"*, 54(4). doi: 10.48371/ismo.2023.54.4.005.
[32] Jilkishiyev, R., & Begaliyev, Y. (2024). Problems of investigation of crimes in the field of information technology. *Pakistan Journal of Criminology*, 16(3), 97-114. doi: 10.62271/pjc.16.3.97.114.
[33] Kadena, E., & Gupi, M. (2021). Human factors in cybersecurity. *Security Science Journal*, 2(2), 51-64. doi: 10.62271/pjc.16.3.97.114.
[34] Karafili, E., Wang, L., & Lupu, E.C. (2020). An Argumentation-Based Reasoner to assist digital investigation and attribution of cyber-attacks. *Forensic Science International Digital Investigation*, 32, article number 300925. doi: 10.1016/j.fsidi.2020.300925.
[35] Kassymzhanova, A.A., Usseinova, G.R., Baimakhanova, D.M., Ibrayeva, A.S., & Ibrayev, N.S. (2022). Legal framework for external security of the Republic of Kazakhstan. *International Journal of Electronic Security and Digital Forensics*, 14(2), 209-222. doi: 10.1504/IJESDF.2022.121180.
[36] Kazakhtelecom announced DDoS attacks from abroad on Kazakhstan's information resources. (2022). Retrieved from https://zonakz.net/2022/09/26/kazaxtelekom-zayavil-o-ddos-atakax-iz-za-rubezha-na-informresursy-kazaxstana/.
[37] Kobets, M. (2023). Extraction of information from a cellular phone (mobile communication device) during investigative (search) actions. *Scientific Journal of the National Academy of Internal Affairs*, 28(2), 52-60. doi: 10.56215/naia-herald/2.2023.52.
[38] Kuek, A., & Hakkennes, S. (2020). Healthcare staff digital literacy levels and their attitudes towards information systems. *Health Informatics Journal*, 26(1), 592-612. doi: 10.1177/1460458219839613.
[39] KZ-CERT. (n.d). *Incidents statistics*. Retrieved from https://cert.gov.kz/press_club/infographics.
[40] KZ-CERT. National computer emergency response team. (n.d.). Retrieved from https://cert.gov.kz/.
[41] KZ-FinCERT. team information. (n.d.). Retrieved from https://www.first.org/members/teams/kz-fincert.
[42] Law of the Republic of Kazakhstan No. 418-V "On Informatization". (2015, November). Retrieved from https://adilet.zan.kz/eng/docs/Z1500000418.
[43] Lehto, M. (2022). Cyber-attacks against critical infrastructure. In M. Lehto & P. Neittaanmäki (Eds.), *Cyber security: Critical infrastructure protection* (pp. 3-42). Cham: Springer. doi: 10.1007/978-3-030-91293-2_1.
[44] Leyden, J. (2023). *Bug Bounty Radar // The latest bug bounty programs for March 2023*. Retrieved from https://portswigger.net/daily-swig/bug-bounty-radar-the-latest-bug-bounty-programs-for-march-2023.
[45] Li, Y., & Liu, Q. (2021). A comprehensive review study of cyber-attacks and cyber security; Emerging trends and recent developments. *Energy Reports*, 7, 8176-8186. doi: 10.1016/j.egyr.2021.08.126.
[46] Llazo, E., Ryspaeva, A., Kubiczek, J., Mehdiyev, V., & Ketners, K. (2024). Trends and prospects of financial system development in the context of digitalization. *Theoretical and Practical Research in the Economic Fields*, 15(4), 783-797. doi: 10.14505/tpref.v15.4(32).01.
[47] Lysenko, S., Bobro, N., Korsunova, K., Vasylchyshyn, O., & Tatarchenko, Y. (2024). The role of artificial intelligence in cybersecurity: Automation of protection and detection of threats. *Economic Affairs,* 69, 43-51. doi: 10.46852/0424-2513.1.2024.6.
[48] Mazur, T., & Flogaitis, S. (2023). Electronic parliament as a factor of sustainable development: History and prospects. *Law Journal of the National Academy of Internal Affairs*, 13(2), 19-29. doi: 10.56215/naia-chasopis/2.2023.19.
[49] Metelskyi, I., & Kravchuk, M. (2023). Features of cybercrime and its prevalence in Ukraine. *Law, Policy and Security*, 1(1), 18-25.
[50] Mitsarakis, K. (2023). *Contemporary cyber threats to critical infrastructures: Management and counter-measures*. Thessaloniki: International Hellenic University.
[51] Naprys, E. (2024). *Germany plans to decriminalize whitehat hacking*. Retrieved from https://cybernews.com/security/germany-plans-to-decriminalize-whitehat-hacking/.
[52] Naseer, I. (2024). The role of artificial intelligence in detecting and preventing cyber and phishing attacks. *European Journal of Engineering Science and Technology*, 11(9), 82-86.
[53] New types of fraud have emerged in Kazakhstan. (2024). Retrieved from https://dknews.kz/ru/finansy/348558-v-kazahstane-poyavilis-novye-vidy-moshennichestva.
[54] Nurbatyrova, R., Japarov, B., Apakhayev, N., Abdulaziz, B., & Khushkeldiyeva, S. (2024). Digital transformation of archives in the context of the introduction of an electronic document management system in Kazakhstan. *Preservation, Digital Technology and Culture*, 53(3), 147-155. doi: 10.1515/pdtc-2024-0017.
[55] Ofori, A.Y., & Akoto, D. (2020). Digital forensics investigation jurisprudence: Issues of admissibility of digital evidence. *HSOA Journal of Forensic, Legal & Investigative Sciences*, 6, article number 045. doi: 10.24966/FLIS-733X/100045.
[56] Only 5% of cybercrime cases reach court in Kazakhstan. (2023). Retrieved from https://surl.gd/mqento.
[57] Order of the Minister of Digital Development, Innovation and Aerospace Industry of the Republic of Kazakhstan No. 175/HK "On Determining the Amount of Payment for Services of State Registration of Civil Status Acts". (2023, June). Retrieved from https://adilet.zan.kz/rus/docs/V2300032755.
[58] OSCE trains Central Asian law enforcement experts to combat cybercrime through open source digital forensics. (2022). Retrieved from https://www.osce.org/secretariat/518697.
[59] Our World in Data. (2023). *Democracy index*. Retrieved from https://ourworldindata.org/grapher/democracy-index-eiu#research-and-writing.

[60] Over 223 million cyberattack attempts by foreign hackers on Kazakhstan in 2023. (2024). Retrieved from https://www.kt.kz/rus/society/bolee_223_mln_popytok_kiberatak_soversheno_ot_zarubezhnyh_1377959819.html.
[61] Penal Code of the Republic of Kazakhstan. (2014, July). Retrieved from https://adilet.zan.kz/eng/docs/K1400000226.
[62] Phishing and social engineering: Virtual communication awareness training DS-IA103.06. (n.d.). Retrieved from https://www.cdse.edu/Training/eLearning/DS-IA103/.
[63] Pollini, A., Callari, T.C., Tedeschi, A., Ruscio, D., Save, L., Chiarugi, F., & Guerri, D. (2022). Leveraging human factors in cybersecurity: An integrated methodological approach. *Cognition Technology & Work*, 24, 371-390. doi: 10.1007/s10111-021-00683-y.
[64] Regulation of the European Parliament and of the Council No. 2016/679 "On the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation)". (2016, April). Retrieved from https://eur-lex.europa.eu/eli/reg/2016/679/oj/eng.
[65] Report on the implementation of the Strategic Plan of the Ministry of Digital Development, Innovations and Aerospace Industry of the Republic of Kazakhstan for 2020-2024. (2021). Retrieved from https://www.gov.kz/memleket/entities/mdai/documents/details/130694?lang=kk.
[66] Resolution of the Government of the Republic of Kazakhstan No. 407 "On Approval of the Concept of Cybersecurity" ("Cyber Shield of Kazakhstan"). (2017, June). Retrieved from https://adilet.zan.kz/rus/docs/P1700000407.
[67] Saraswat, A., & Tiwari, G. (2025). United Nations and beyond: Legal strategies for defending critical energy infrastructure against cyber attacks. In M. Chawki & A. Abraham (Eds.), *Cybercrime unveiled: Technologies for analysing legal complexity. Studies in computational intelligence* (pp. 291-307). Cham: Springer. doi: 10.1007/978-3-031-80557-8_13.
[68] Satbayeva, A.M., Alimbetova, A.R., & Beissenbayeva, M.T. (2024). Cybercrime challenges: Experience of international cooperation. *Bulletin of Institute of Legislation and Legal Information of the Republic of Kazakhstan*, 3(78), 211-221. doi: 10.52026/2788-5291_2024_78_3_211.
[69] Shaisultanov, S., Akimzhanov, T., Abdrakhmanov, B., Bazarlinova, A., & Bazarlinova, A. (2024). Combating internet fraud through operative-search measures. *Law, State & Telecommunications Review*, 16(2), 257-275. doi: 10.26512/lstr.v16i2.50740.
[70] Shandler, R., & Gomez, M.A. (2023). The hidden threat of cyber-attacks – undermining public confidence in government. *Journal of Information Technology & Politics*, 20(4), 359-374. doi: 10.1080/19331681.2022.2112796.
[71] Sobirov, S. (2023). Comparative legal analysis of the regulation of electronic evidence in criminal proceedings: The experience of the USA, EU, and CIS countries. *Society and Innovations*, 4(5), 96-117.
[72] Tabrez, Y.E. (2020). National cybersecurity innovation. *West Virginia Law Review*, 123(2), 483-546.
[73] Tokayev signs law banning collection of copies of identity documents. (2023). Retrieved from https://atpress.kz/ru/news/v-kazakhstane/tokaev-podpisal-zakon-zapreshchayushchij-sbor-kopij-dokumentov-udostoveryayushchikh-lichnost.
[74] Turlybek, S. (2023). *International cyber conference held at Almaty Academy of the Ministry of Internal Affairs*. Retrieved from https://polisia.kz/ru/mezhdunarodnaya-kiberkonferentsiya-provedena-v-almatinskoj-akademii-mvd/.
[75] Turlybek, S. (2024). *The Ministry of Internal Affairs has created a department to combat cybercrime*. Retrieved from https://polisia.kz/ru/v-mvd-sozdan-departament-po-protivodejstviyu-kiberprestupnosti/.
[76] UNODC and partners conducted a regional seminar "Specific Features of the Investigation of Criminal Cases on Cybercrime: International Cooperation, Experience, Trends, Tactics and Problems" in Kazakhstan. (n.d.). Retrieved from https://www.unodc.org/roca/en/NEWS/Archive/unodc-and-partners-conducted-a-regional-seminar-specific-features-of-the-investigation-of-criminal-cases-on-cybercrime_-international-cooperation--experience--trends--tactics-and-problems-in-kazakhstan.html.
[77] Vuković, M., & Štefanac, T. (2023). Digital cultural heritage, cybersecurity, and the human factor. *Preservation, Digital Technology & Culture*, 52(4), 129-141. doi: 10.1515/pdtc-2023-0040.
[78] Walshe, T., & Simpson, A. (2020). An empirical study of bug bounty programs. In X. Luo, W. Shang, X. Sun & T. Zhang (Eds.), *Proceedings of the 2020 IEEE 2nd international workshop on intelligent bug fixing (IBF)* (pp. 35-44). London: Institute of Electrical and Electronics Engineers. doi: 10.1109/IBF50092.2020.9034828.
[79] Where is the rise of cyber attacks observed in Kazakhstan? (2023). Retrieved from https://bluescreen.kz/gdie-nabliudaietsia-rost-kibieratak-v-kazakhstanie/.
[80] Yamin, M.M., Ullah, M., Ullah, H., & Katt, B. (2021). Weaponized AI for cyber attacks. *Journal of Information Security and Applications*, 57, article number 102722. doi: 10.1016/j.jisa.2020.102722.
[81] Zabikh, S. (2020). International experience of legal support of information security and the possibilities for its application in the Republic of Kazakhstan. *Political Science Review*, 3, 71-85. doi: 10.14746/pp.2020.25.3.6.
[82] Zeadally, S., Adi, E., Baig, Z., & Khan, I.A. (2020). Harnessing artificial intelligence capabilities to improve cybersecurity. *IEEE Access*, 8, 23817-23837. doi: 10.1109/access.2020.2968045.
[83] Zhakenov, K., Kultemirova, L. & Ibraeva, A. (2024). Comparative analysis of the activities of authorities to ensure the prevention of offenses in the Republic of Kazakhstan and other world countries. *Security Journal*, 37, 1430-1446. doi: 10.1057/s41284-024-00425-5.
[84] Zhumagali, A. (2024). *158 executives punished for corruption since the beginning of the year in Kazakhstan*. Retrieved from https://ulysmedia.kz/news/22683-158-rukovoditelei-nakazali-za-korruptsiiu-s-nachala-goda-v-kazakhstane/.

Протидія кібератакам в Республіці Казахстан: міждисциплінарні питання та правові рамки в контексті соціальної безпеки та економічної стабільності

Нургуль Кубанова

Аспірант
Алматинська академія Міністерства внутрішніх справ Республіки Казахстан імені Макана Єсбулатова
050060, вул. Утепова, 29, м. Алмати, Республіка Казахстан
https://orcid.org/0009-0006-1141-1165

Індіра Несіпбаєва

Кандидат юридичних наук
Міжнародний Таразський університет імені Ш. Муртази
080000, вул. Желтоксан, 69Б, м. Тараз, Республіка Казахстан
https://orcid.org/0009-0007-9657-0313

Соледад Дюсебалієва

Кандидат юридичних наук, доцент
Атирауський університет імені Галеля Досмухамедова
060011, проспект Студентський, 1, м. Атирау, Республіка Казахстан
https://orcid.org/0009-0001-4548-7946

Халібіяті Халібіяті

Аспірант
Казахський національний університет імені аль-Фарабі
050040, проспект Аль-Фарабі, 71, м. Алмати, Республіка Казахстан
https://orcid.org/0009-0000-4664-7844

Серіхан Аділгази

Доктор юридичних наук, професор
Університет Нарксоз
050035, вул. Жандосова, 55, м. Алмати, Республіка Казахстан
https://orcid.org/0000-0001-8625-4172

Анотація. Метою дослідження була розробка теоретико-методологічних засад та практичних рекомендацій щодо вдосконалення системи протидії кібератакам, які охоплюють правові, технічні та організаційні механізми забезпечення кібербезпеки. Дослідження ґрунтувалося на комплексному міждисциплінарному підході з використанням методів системного аналізу, формально-юридичного, порівняльно-правового та описової статистики. Аналіз статистичних даних за 2020-2024 роки виявив стрімке зростання кількості та складності кібератак. У 2024 році було зафіксовано 4,507 випадків використання шкідливого програмного забезпечення, що більш ніж удвічі більше, ніж у попередньому році. Дослідження підтвердило, що найбільш вразливим виявився сегмент малого та середнього бізнесу: лише в банківському секторі у другій половині 2024 року збитки від кібератак склали 1,5 мільярда тенге, причому 35% атак було здійснено з використанням методів соціальної інженерії. Аналіз структури кібератак показав, що 62% від загальної кількості кібератак були спрямовані на державний сектор, з яких 28% – на об'єкти критичної інфраструктури. Дослідження визначило, що близько 70% успішних втручань пов'язані з людським фактором – недостатньою кваліфікацією персоналу та помилками в конфігурації системи. Виявлено суттєві прогалини в системі кіберзахисту Казахстану: відсутність ефективних механізмів міжвідомчої координації, недостатнє регулювання державно-приватного партнерства та неефективність існуючої нормативно-правової бази щодо регулювання відповідальності операторів критичної інфраструктури. Обґрунтовано необхідність створення єдиного координаційного центру кіберзахисту, який об'єднає зусилля державної системи моніторингу KZ-CERT і галузевої системи FinCERT, а також запропоновано економічні механізми стимулювання інвестицій у кібербезпеку через систему податкових пільг і грантові програми. Проаналізовано особливості процесу розслідування кіберзлочинів, зокрема процедури відеофіксації вилучення обладнання та специфіку процесуального оформлення доказів. За даними Генеральної прокуратури Республіки Казахстан, у 2023 році до суду було направлено 476 кримінальних справ про кіберзлочини, з яких 312 закінчилися обвинувальними вироками. Результатами дослідження стало комплексне розуміння взаємозв'язку між правовими, технічними та соціально-економічними аспектами кібербезпеки та довели необхідність системної взаємодії всіх зацікавлених сторін у протидії кіберзагрозам

Ключові слова: інформаційні системи; цифрові докази; шкідливе програмне забезпечення; критична інфраструктура; державно-приватне партнерство