Pakistan Journal of Criminology
Vol. 16, No. 03, July—September 2024 (97-114)

Problems of Investigation of Crimes in the Field of Information Technology

Ruslan Jilkishiyev[1] &Yernar Begaliyev[2]

Abstract

The purpose of the study is to analyse the main problems that law enforcement agencies and information technology security specialists face when investigating cybercrime. In particular, the research work is also aimed at identifying the main shortcomings in the process of investigating crimes in the relevant area, analysing the legal acts governing these legal relations, and elucidating foreign experience in further improving the investigation of cybercrime. The methods that were used to write the work are as follows: legal hermeneutics, comparative, statistical, method of analysis, synthesis. The main results of the study were: clarification of the concept of "information technology", as well as the categories involved in this concept, in particular, information legal relations, cybercrimes; analysis of the legislation regulating relations in the information sphere and the main shortcomings of the relevant legislation of Kazakhstan, possible improvements in regulatory legal acts.

Keywords: Cybercrime; Cybersecurity; Computer Crimes; Cyberspace; Rights and Freedoms.

Introduction

Given the rapid development of digital technologies, participants in information legal relations are more likely to encounter cybercrime, which creates a serious threat to the security of information, private data, financial resources. It should be noted that the main objectives of the research work were to study the state of cybercrime both in Kazakhstan and in the world, assess the effectiveness of legislation regulating the relevant area, as well as study the possibilities of improving cooperation between government and international organizations to ensure the safety of users on the Internet.

A.B. Omarova and Sh.B. Malikova (2018) explored the problems of protecting personal information and security in the information sphere. It has been established that with wider access to Internet resources, new specific forms of

[1]Doctoral Student, Department of Criminal Procedure and Criminalistics, M. Esbolatov Almaty Academy of the Ministry of Internal Affairs of the Republic of Kazakhstan, Almaty, Republic of Kazakhstan.Kazakhstan. ruslan.ji121@gmail.com
[2]Professor, Department of Special Legal Disciplines, Law Enforcement Academy under the Prosecutor General's Office of the Republic of Kazakhstan, Kosshy, Republic of Kazakhstan, Kazakhstan. ye_begaliyev2@outlook.com

offences arise that are not covered by the criminal legislation of the Republic of Kazakhstan. The authors conclude that now an important step in the fight against crime aimed at violating information security is the development of a universal and detailed conceptual apparatus in criminal legislation relating to the information sphere, along with additional explanations and clarifications that such terms need. Concepts must be formed based on an understanding of the technical characteristics of new information processing tools and the essence of the information itself stored on computer media, contained in information systems or transmitted through information and communication networks as a new category of criminal law (Beisbekova et al., 2019). Insufficiently precise expression of a particular concept in criminal law can lead to different interpretations and erroneous application of the rule of law.

For example, K. Aratulu (2019) pointed out that, at the international level, there are several main approaches to the classification of crimes occurring in the field of information relations, among them, in particular, crimes related to the circulation of information, crimes related to computer networks, with access to personal data, spread of viruses, computer fraud. In turn, A. Shukan et al. (2020) noted the main problems existing in the field of investigation of cybercrimes in the Republic of Kazakhstan, such that the country does not have special bodies specializing in the investigation of offences arising in the field of information relations. The authors indicate that the investigation of this category of crimes is carried out by persons who are qualified in solving general crimes. Law enforcement agencies are not adequately trained to increase their understanding of the specifics of cybercrime. The authors also cite as an example global experience in eliminating these problems, in particular, it is indicated that in the United States of America a retraining program was developed and launched to increase awareness of cybercrime and its counteraction. Today, a pilot project called CyberPol is underway in the cities of Almaty and Astana. CyberPol is a department that deals exclusively with crimes related to computer crimes. It includes 5 investigators, 5 detectives and 1 crime analyst (Safargalieva, 2023).

Authors, such as T.S. Temiraliev and E.A. Omarov (2019), consider issues related to the problems of legal and organizational support for the fight against cybercrime. These problems, according to the authors, are associated with the lack of special knowledge of the subject of the crime among authorized persons, which significantly complicates the investigation process. It is proposed to create a separate specialized service within each pre-trial investigation body, which will be authorized to investigate and combat crimes related to information technology. Employees of this service are required to complete an education course in information technology.

B.H. Aidosova (2021) noted that phishing attacks and the use of botnets were among the most common types of cybercrime in the Republic of Kazakhstan. The problems that the author highlights in this area are related to the lack of sufficient awareness of the dangers of cybercrime, the lack of technical equipment for monitoring information security and reliable means of protection. The study also provides examples of attacks on user data, the main reasons for which are the use of licensed software, the use of weak passwords, connecting to free unfamiliar networks, transferring personal data to third parties. The author pointed to positive changes on the way to the development of cybersecurity, in particular, the adoption of the Cybersecurity Concept, according to which a number of legal acts have been developed and adopted to improve the regulation of the relevant area, as well as the relevant institutions, information security coordinating centres created, the like. As the author points out, in the global cybersecurity rating, the Republic of Kazakhstan took 40th place, as opposed to the previous 82nd.

Thus, it should be noted that the issue of cybercrimes in scientific doctrine is developed and is constantly being researched (Vilks et al., 2022), however, it is also advisable to point out that little attention is paid to foreign experience as the basis for improving the relevant area, as well as the incompleteness of practical cases and statistical information that directly relates to the security of users on the Internet. The investigation of such crimes requires an in-depth understanding of the technologies, methods, and features of the procedure according to which the perpetrators can be brought to justice, which is why the purpose of the study is to analyse the main obstacles to the investigation of offences arising in the field of information relations and to develop recommendations and practical solutions to improve the relevant process.

Materials and Methods

Scientific research was carried out by using a number of methods of scientific knowledge. The method of legal hermeneutics should also be singled out, with the help of which such concepts as cybercrime, cybercrime, information technology, information society were interpreted. The method will also allow to explore the main legislation, projects, and concepts that regulate the field of information technology and influence the process of investigating crimes committed in the relevant field; the interpretation of relevant concepts in other countries was studied. The historical and legal method made it possible to study the process of development of criminology, taking into account the scientific and technical process, computer technology and informatization of society. The method was also useful in determining the impact of information technology on the investigation of crimes related to cyberspace and the security of network user

data. It is also necessary to single out the method of analysis, which made it possible to reveal the main problematic features of the object under study, as well as to establish causal relationships and highlight key aspects that hinder the effective investigation of crimes related to information technology. It is worth noting that the synthesis method was used to develop new concepts, models, and approaches based on analysis, which can help solve the problems associated with the process of investigating offences in the field of information relations.

The comparative legal method made it possible to characterize the experience and similar methods of regulating the cybersecurity industry in the Republic of Kazakhstan and the United States of America, as well as in Israel, Singapore, Estonia, and Japan. Also, this method made it possible to highlight and reveal the positive aspects of foreign experience regarding the creation of a safe cyberspace in the country, the effective investigation of cybercrimes and methods for preventing cyberattacks, which should be taken into account when reforming the relevant sphere in the territory of the Republic of Kazakhstan. Together with the comparative method, the statistical method was also used to highlight basic data related to the number of cybercrimes committed on the territory of Kazakhstan, in accordance with the country's criminal legislation.

It is important to point out that in the analysis of theoretical works and current legislation relating to the protection of the rights and legitimate interests of citizens in the field of information relations and its application, a formal-logical approach was used to highlight the existing contradictions in regulations and scientific approaches to research in the field of informatization and computer science. technologies. This, in turn, made it possible to propose changes in the field of cybercrime investigation in order to improve the protective mechanism for the privacy of individuals, as well as their data on the Internet. Such a scientific method as modelling made it possible to form the future vision and type of the institute for combating cybercrime on the territory of Kazakhstan and highlight the necessary steps based on foreign experience and analysis of the theoretical works of other scientists who have studied similar issues. Based on the results obtained, conclusions about the problems of investigating crimes in the field of information technology are formulated and recommendations for solving them and further prospects for the development of the sector are indicated.

Results and Discussion

The concept and specific features of cybercrime

The information society reflects the current stage of development of society, where information and information technologies play a key role in the production, exchange, transmission, and consumption of information. This society, where

information becomes a valuable resource and determines economic, social and cultural activities, is also characterized by widespread access to information, the growth of communication technologies and public engagement in the digital sphere. The main feature of the information society is information relations that arise as a result of the exchange of information between subjects of society. They include the transfer, processing, storage and use of information in various fields of activity. An important component of both the information society and information relations are information technologies, which refer to the means, methods, and technologies that are used to collect, process, store, transmit and use information. Information technology also includes hardware and software, network communications, databases, Internet technologies, cloud computing and other tools (Adanbekova et al., 2022).

In Law of the Republic of Kazakhstan No. 418-V "On informatization" (2015) states that "information and communication technologies are a set of methods for working with electronic information resources and methods of information interaction carried out using a hardware-software complex and a telecommunications network". For example, in the United States, information technology covers a wide range of information, including computers, mobile devices, Internet networks and software. In European countries, information technology includes aspects such as cybersecurity, electronic identification and digital signature (Arnone, 2021). In Israel, information technology is of great importance in the high-tech and start-up sectors. The country is a centre of innovation and research in cybersecurity, artificial intelligence, biomedicine and other information technology-related fields (Deora and Chudasama, 2021).

In general, the development of information technology has gone a long way through the emergence of the first computers, the development of electronics and the first electronic computers that were used for calculations and data processing. In the 1960s, the creation of computer networks began, which later became the Internet. This global networking space facilitated the exchange of information and communication between users from all over the world. With the advent of personal computers in the 1970s and 1980s, information technology became more accessible to the public. New software products and technologies have appeared, such as graphical interfaces, Internet mail and browsers (Sviatun et al., 2021).

Although the interpretation of information technologies may differ depending on the country in which these technologies are developed and operated, an important part of all definitions is the affinity for user security associated with information technologies. Thus, it is expedient to characterize the security threat – cybercrime. Cybercrime refers to crimes committed using information technology and networks. These are illegal actions aimed at illegally obtaining, using,

modifying or destroying information, as well as damaging computer systems, networks and electronic devices. With the spread of computer technology in the 1970s, the first cybercrimes appeared, these were mainly acts of intrusion into computer systems, theft of data and the spread of viruses (Chandra and Snowe, 2020). Depending on technological and social changes, cybercrime has also evolved. New types of attacks have emerged, such as phishing, cyber blackmail, identity theft, account hacking. Over time, cybercrime has become more organized and has taken on the dimensions of international crime (Metelskyi & Kravchuk, 2023).

If analysing the Criminal Code of the Republic of Kazakhstan (1997), it is advisable to describe the following examples of crimes in the field of informatization: illegal access to information, to an information system or a telecommunications network, illegal destruction or alteration of information, disruption of an information system or telecommunications networks, misappropriation of information, coercion to transfer information, creation, use, or distribution of malicious computer programs and software products, illegal distribution of electronic information resources with restricted access, provision of services for hosting Internet resources for illegal purposes, illegal change of the identification code of a mobile communication subscriber device, subscriber identification device, as well as the creation, use, distribution of applications for changing the identification code of the subscriber device (Shah and Chudasama, 2021).

Information technology and cybercrimes have a variety of reasons, including economic ones, where criminals seek financial gain by stealing money, personal information or financial data, using fraud or blackmail to enrich themselves, and cybercriminals may also attempt to gain unauthorized access to confidential information such as commercial and industrial secrets, state secrets or personal data for political, personal or other reasons (Pawar et al., 2021). Cybercriminals can purposefully target specific websites, systems, or networks with the intent to cause harm, disrupt functionality, or simply make efforts to break security. Another motive may be social orientation or activism, so that individuals may direct their attacks at organizations or individuals that do not correspond to their ideological or political views, or human rights standards.

In addition to these reasons, there are some other factors that contribute to the commission of crimes in the field of information technology, in particular, the presence of technical vulnerabilities in information systems, software products or networks can lead to the commission of cybercrimes (Luknar, 2020). The Internet provides an opportunity to commit crimes with a high degree of anonymity and remoteness through the use of secure proxy servers, virtual private networks

(VPN) to hide one's data and location (Cristea, 2020). The spread and accessibility of information technology also creates opportunities for illegal actions, while the lack of knowledge on cybersecurity, low level of digital education can put people in a vulnerable position and threaten the loss of private data. It is important to note that information technology and cybercrimes are constantly evolving and adapting to new technologies and defences. Advancement in cybersecurity and increased awareness of cybersecurity practices are key to preventing such crimes and maintaining the privacy and security of users.

Investigation of crimes in the field of information technology: statistics, problematic aspects

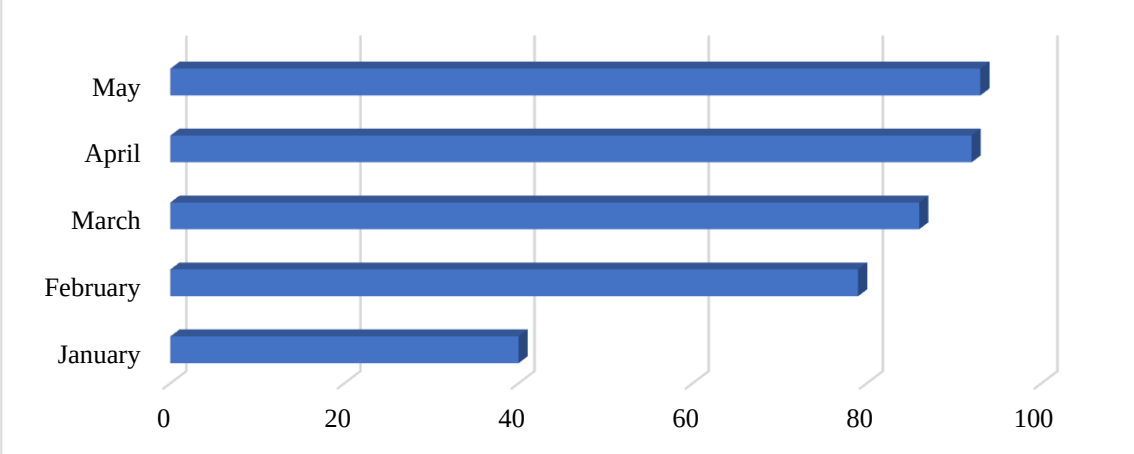
In the Republic of Kazakhstan, the investigation of crimes in the information sphere is carried out in accordance with the criminal law (Shah and Chudasama, 2021). However, at the same time, it is important to highlight the significant problems that arise in the process of conducting an investigation, for example, a lack of qualifications and technical knowledge in the relevant field, because the investigation of cybercrime requires high expertise in the field of information technology and cybersecurity. The low number of qualified specialists and the lack of specialized units in law enforcement agencies can complicate the investigation of this type of crime. Also, important is the lack of sufficient financial, technical and human resources, which can complicate the effective investigation of cybercrime. Insufficient access to specialized hardware, software, and hardware can limit the ability of law enforcement agencies to detect and document cybercrime. Difficulties are also due to the complexity of international cooperation and the lack of development of diplomatic relations with other countries, but this institution plays an important role in ensuring the security and safety of users' private data. The technical complexity of the investigation lies in the inability of law enforcement agencies to identify and identify the offender, this problem is associated with a low amount of financial resources (Li and Liu,2021).

Also, in the Republic of Kazakhstan there is no special body for investigating crimes in the information system, which can negatively affect all stages of the investigation in the following ways: investigating crimes in the information sphere requires a deep understanding of technology, software, networks, and cybersecurity (Chawki, 2021). The absence of a specialized body may mean that law enforcement agencies do not have the necessary knowledge and skills to effectively investigate and prosecute cybercriminals. Also, the lack of a single body leads to the fact that the investigation of this type of crime, due to the complexity and lack of technical capabilities, may be less of a priority for general law enforcement agencies. It is important to note that a specialized body

may have access to software, a range of technical resources, technical and qualified expertise. However, in the absence of a separate unit with specific competence, it reduces the effectiveness of traditional law enforcement agencies.

In general, the absence of a special body for investigating crimes in the information sphere can lead to insufficient response to cybercrime, limited resources and expertise, as well as low priority of the investigation. The fact that the problem of investigating crimes in the field of information exists is indicated by statistics (Figure 1).

Figure 1: Number of registered offences in the field of informatization, January-May 2023



Statistics show that the number of crimes in the region continues to grow every month. It should also be noted that the number of registered offences may differ significantly from the actual cases of offences committed in the field of information technology, due to the problems identified above, namely: the lack of a special investigative body, technical, financial support. The attention also should be paid to the statistics of the State Technical Service, which indicate that for the period from January to July 2023, 2396 were recorded – botnets, 8476 – computer viruses, trojans, 76 – DoS/DDoS attacks, 258 – unauthorized access, 379 – phishing and about 800 cases of other types of misconduct in the field of information technology.

The reasons for the growth of cybercrime are not only the development of information technology, but also, for example, the period of the COVID-19 pandemic, which led to a massive transition of companies to a remote work format. Companies not ready for a drastic change in the way they work often store confidential or personal information of users on insufficiently protected media.

During the coronacrisis, the exchange of information has increased significantly, which has led to higher risks for all areas of business. Rising prices for licensed software, network equipment, servers also led to the fact that companies attract fewer funds to the cybersecurity sector, which, accordingly, creates higher risks of cyberattacks on unprotected storage media (Chudyk & Vivchar, 2023). It is worth pointing out that cybercrime is currently gaining organized proportions due to the competent planning of information attacks, the involvement of more people and the necessary equipment, so the protection of personal data and important data of companies in both the private and public sectors becomes an urgent issue.

To combat cyberattacks and cybercrime in the Republic of Kazakhstan, the corresponding Draft was approved concept for the Development of the Digital Ecosystem for 2022-2027 ("Cybershield-2") (2022). Thus, the document proposed the creation of separate centres in the areas of protection of critical sectors, in particular, financial, fuel, educational and medical, oil and gas, transport, agricultural and defence. For example, in the field of banking services, a corresponding centre began to operate, authorized to collect and analyse information about problems in the field of information security in the relevant sector; this centre is designed to warn the banking system about possible cyberattacks and vulnerabilities in information security. The mentioned project mostly focuses on large companies; with regard to medium and small enterprises, which also suffer from cyberattacks, it is noted that the main reason for attacks on these businesses is the owners' ignorance of the consequences of careless information protection. Therefore, the authors of the project proposed to increase the level of information education and increase funding for companies developing storage media protection systems. Given this project, the most common and relevant cyber threats remain phishing attacks and DDoS attacks that exclude the operation of the enterprise and the processing of requests (Tvaronavičienė et al., 2020).

It is worth noting that "Cybershield-2" (Government of the Republic…, 2022), although it significantly improves the cyber defence system on the territory of the Republic of Kazakhstan, the legal field remains unresolved, namely the process of investigating offences that were nevertheless committed in the field of information technology and which could not be prevented. The project does not provide for the creation of a separate special unit authorized to investigate this type of crime. The question of a possible increase in funding for existing law enforcement agencies to improve technical capabilities in this area, as well as additional qualifications of employees, also remains open.

Foreign experience in the field of cybercrime investigation: borrowing positive aspects

Attention should be paid to the experience of Estonia, which has a strong level of cyber defence associated with the constant development of information technology and the need to protect the private data of users, as well as large companies. A special Cyber Center has been established in Estonia, the performance standards of which are approved by NATO. An important role is also played by the creation of special legislative initiatives that define the powers of state bodies, coordination between law enforcement departments and provide for regular training sessions. Another condition for the success of the country's cybersecurity is the allocation of a significant amount of the budget to the relevant area, as well as an understanding of the need to establish a secure use of the network. So, as universities provide for the teaching of a cybersecurity course, so in institutions of secondary education; there are mandatory courses for young citizens in cyber training, as well as a developed area of training – military cybersecurity. This creates the basis for successful prevention of cyberattacks, as well as effective and timely response of responsible law enforcement agencies to committed offences through the provision of technical and financial activities. It is worth mentioning an important area of cooperation with representatives of other countries within the framework of international legal assistance in order to ensure the possibility of ensuring the safety of users in any circumstances (Tvaronavičienė et al., 2020).

It is advisable to single out the experience of the United States of America, based on the provisions of the Cybersecurity Strategy. This strategy indicates that the priority is to protect the state and data from attacks by hackers and other states, with special attention to Iran, North Korea and the Russian Federation. The need for staffing state and law enforcement agencies with specialists with the necessary special knowledge and experience in interacting with information technology was also noted (Hatcher et al., 2020). An interesting indication is that the United States of America has the right to demand compensation for the consequences of cyberattacks from their perpetrators. The successful implementation of the Strategy is evidenced, in particular, by the exposure and conviction of those responsible for the creation of the criminal group Infraud, where stolen personal data was traded using cards, bank accounts.

It is also interesting to explore the cyber defence of Singapore, the development of which extends in several directions: the development of a solid information infrastructure, the strengthening of the protection of the information space of the state, as well as the improvement of diplomatic relations in the field of international legal assistance for the effective investigation of cybercrime

(Marwan et al., 2022). It is important in the country's cybersecurity system to ensure the functioning of specialized institutions of specialized companies represented by the Cybersecurity Agency, Cyber Command. As in other countries surveyed, Singapore places a strong emphasis on the educational and scientific component of cyber defence through the establishment of research centres, schools of computer technology, as well as private institutions that advise on security in the digital space and build a cybersecurity strategy for companies, small, medium and large businesses (Bartlett, 2023).

Israel's cyber defence system also deserves attention, as it consists of a number of global cyber companies, start-ups, the necessary education and training in the military and law enforcement agencies, and support for public and private initiatives to improve cybersecurity in the country. Considering that the country is often subjected to cyberattacks on various sectors, in particular critical infrastructure, at the beginning, special intelligence agencies were created to monitor cyberattacks and repel them (Somogyi & Nagy, 2022). Currently, cybersecurity is coordinated by the government and is being developed through large investments in the field, in particular through the educational level and opportunities to profile cybersecurity at the level of secondary and higher education, as well as the creation of research centres to analyse the nature of cyberattacks to further prevent a repeated threat (Sikos, 2021).

Regarding the procedural aspect of the investigation of the crimes under study, attention should be paid to the experience of Japan, where control is introduced over persons or criminal groups already held accountable for attacks on public and private information resources, and in case of monitoring suspicious activity on the part of such persons, take preventive actions, in particular, preventive talks, counter-cyberattacks (Bartlett, 2023). Thus, based on the analysis of the experience of different countries in implementing reforms to improve cybersecurity, the following aspects can be identified that should be taken into account by the Republic of Kazakhstan:

- a high-quality plan for the development of cyber defence and security of the country;
- the highest level of investment in the sphere of cyberspace, highlighting such an area as a priority;
- introduction of an educational campaign on information literacy at all levels: school, university;
- conducting training to improve the skills of law enforcement officials in the field of cybersecurity in order to provide institutions with competent specialists;

- the creation of separate units or specialized institutions authorized to investigate crimes related to information technology;
- creation of research centres to ensure the prevention of a repeat cyberattack. improving international cooperation and adopting foreign experience.

Analysis of the reasoning of researchers and scientists in the field of cybercrime

L.F. Sikos (2021) explored the role of artificial intelligence in forensics and noted that digital forensics involves the collection, analysis, and preservation of electronic evidence to investigate cybercrimes such as hacking, data breaches and online fraud, and that it is in this area that artificial intelligence can significantly increase the efficiency of the investigation process by analysing large volumes of data. The author also pointed out that the ontology of AI-driven digital forensics can cover various aspects, such as network logs, file system data, social media posts, forensic methods and tools, as well as legal and regulatory frameworks (Shevchuk, 2020). Artificial intelligence algorithms can be used to detect patterns and anomalies in network traffic, identify malware, and predict potential attack vectors. Additionally, machine learning techniques can help in identifying suspects and predicting future cyber threats. The results of the author do not coincide with the results of this work, however, they are interesting for the analysis and addition of the topic. It is also important to note that although artificial intelligence offers significant advantages in the field of digital forensics, human judgment still plays a decisive role, because it is the investigators who must interpret and verify the results provided by artificial intelligence systems, as well as take into account legal and ethical considerations when using artificial intelligence in cybercrime investigation.

S. Rani et al. (2021) explored the concept of Internet security in the light of existing cyber threats. So, the main problems can be unauthorized access, low level of data confidentiality, device vulnerability in software, DDoS attacks. To prevent and avoid these problems, the authors suggest the implementation of strong authentication mechanisms, such as multifactor authentication, regular software updates, the implementation of encryption for sensitive data, the implementation of intrusion detection systems, and continuous monitoring of network traffic, which can help identify suspicious activity and promptly regular security assessments and penetration testing of Internet devices and systems, detect vulnerabilities and make sure that appropriate security measures are taken, it is also important to increase user awareness of the risks of the Internet (Holt et al., 2022). The authors' results partially coincide with the results of this work, in

particular in terms of minimizing the risks of private data being taken over by others, however, research conducted by S. Rani et al. (2021) are quite important for understanding how to protect the user and reduce the burden on investigative authorities due to the prevention of cyberattacks and offences in the field of information technology. T.J. Holt et al. (2022) clarified the essence of cybercrime and determined that it refers to criminal activities carried out using computers, networks, or the Internet. It also covers a wide range of illegal activities, including hacking, data breaches, online fraud, identity theft, malware distribution, and cyber espionage. The authors noted that the investigation of cybercrime has its own specific features, in particular, in the methods of conducting an investigation due to the need for special equipment, software, the availability of digital evidence. Important in this process is cooperation and assistance at all levels in order to fully investigate the crime committed and bring the perpetrators to justice.

J. Bandler and A. Merzon (2020) have a study that resembles the above-mentioned one, where it is noted that the investigation of information crimes requires a number of tools and technologies, in particular specialized software, equipment, as well as a database of cybercrime for their further analysis and research. The authors note the importance of preventing such types of crime due to a sufficient level of digital education and the necessary institutions that would constantly monitor the state of security of sensitive data. The results of the authors coincide with the results of this work, but it should be added that cooperation is an important link in the investigation of cybercrime not only at the level of law enforcement agencies at the national level, but also at the international level, in cases where cyberattacks are committed against one state by a citizen of another.

A.O. Adesina et al. (2022) investigated cybercrime among youth and youth. Such crimes often involve hacking to gain unauthorized access to computer systems, networks or online accounts. This may involve the use of password cracking or social engineering techniques to bypass security measures and gain control of targeted systems. Youths can also use phishing techniques to trick people into revealing sensitive information such as usernames, passwords, or credit card information. They may create fake websites, send deceptive emails, engage in online fraud, engage in cyberbullying or online harassment that includes certain threats of action if the individual does not provide access to personal data or confidential information. The authors identify several main reasons why young people may decide to take these actions: the influence of peers plays a significant role in shaping the behaviour of young people. In some cases, youths may engage in cybercrimes to gain recognition or a certain status, financial gain may be the driving force behind cybercrimes committed by youths. They may engage in activities such as credit card fraud, identity theft, or online scams to obtain money

or valuable goods. Emotional and psychological factors may also play a role, but the most important factors are lack of awareness and digital literacy. Most young people have grown up in the digital age with widespread access to technology, however, they lack adequate education on responsible digital behaviour. The authors' results partially coincide with the results of this work, however, it should be noted that it is the educational component of cybersecurity that turns out to be the key to conscious use of the Internet without the risks of cyberattacks and cybercrime. Due to the fact that digital education currently does not exist in Kazakhstan, it is advisable to introduce the first steps to ensure that citizens and minors understand the responsibility of using certain means of communication on the network. In turn, such an educational policy will lead to a reduced level of cybercrime and, accordingly, the burden on law enforcement agencies.

It should also be noted that the successful investigation of cybercrime requires an integrated approach through the creation of an effective legislative framework, as well as special units for the investigation of offences related to information technology, the introduction of reporting mechanisms on existing cybercrime for their further investigation, the creation of special laboratories for digital forensics on the basis of experience Japan to prevent the same cyberattacks from happening again. Strengthening cooperation and international legal assistance to improve the exchange of experience in the field of cybersecurity. Regular assessment, monitoring, and adaptation of the cybercrime investigation model are critical to addressing the changing nature of cyber threats. Ongoing collaboration and knowledge sharing among stakeholders is key to building an effective and sustainable cybercrime investigation system in Kazakhstan.

Conclusions

Thus, the study made it possible to gain a deeper understanding of aspects related to the investigation of cybercrime in the Republic of Kazakhstan. In particular, the paper highlights the features of the concepts of cybercrime, information technology, the information society and how these categories are interconnected. It was found that with the development of computer networks and technological progress, the risks of cyberattacks and other types of crimes in the field of information technology have increased, which threaten the smooth functioning of critical infrastructure institutions, as well as hinder the guarantee of rights and freedoms of security on the Internet. The study also contains an analysis of the main legal acts regulating the relevant area, in particular, criminal law, as well as special specialized laws. Considerable attention is paid to the concept of the Republic of Kazakhstan Cybershield-2, which is designed to improve the area under study and counteract the threats that arise in the modern era of the digital

society. Statistics are also given that indicate the existence of problems in the field of cybersecurity in Kazakhstan, as well as those problematic aspects that affect the investigation process are characterized. Such aspects are the low level of technical support, insufficient funding of the sphere, the absence of a special law enforcement body that would be authorized to investigate cybercrimes, because the absence of such a body creates a lack of a fair balance between crimes related to informatization and other traditional crimes, as well as an insufficient level of qualification and competence of investigators. Attention is also paid to the considerations of other scientists regarding the relevant issue, as in this study, in the works of the authors, significant attention is paid to the problems of cybersecurity and effective investigation, which consist in insufficient resource and financial support.

Foreign experience was illustrated using the example of the USA, Israel, Japan, Estonia, and Singapore in regulating cybersecurity. It has been determined that the main steps towards improving the reliability of the country's cyber defence are a proper educational campaign at all levels, increasing investment in the field, constant monitoring and research of cybercrime to prevent repeated cyberattacks, improving cooperation between departments and between countries in the exchange of experience and improving government private cooperation, in particular to create more of the necessary institutions and centres providing a range of consulting services regarding the adequacy of the level of cyber protection in companies, the strength of passwords, equipment, risk assessment software and the provision of recommendations. In the future, it is advisable to explore the following topics: the role of artificial intelligence in the process of investigating cybercrimes, digital evidence: search methods and research features, the role of cryptocurrency in the field of cybercrime, the importance of cyber intelligence for the security of the country's information infrastructure, countering cyberattacks on the country's critical infrastructure.

References

Adanbekova, Z.N., Omarova, A.B., Yermukhametova, S.R., Khudaiberdina, G.A. & Tynybekov, S.T. (2022). Features of the conclusion of a civil transaction on the internet. *International Journal of Electronic Security and Digital Forensics, 14*(1), 19-36.

Adesina, A.O., Ajagbe, S.A., Afolabi, O.S., Adeniji, O.D. & Ajimobi, O.I. (2022). Investigating data mining trend in cybercrime among youths. In: *Pervasive Computing and Social Networking: Proceedings of ICPCSN 2022* (pp. 725-741). Singapore: Springer.

Aidosova, B.H. (2021). Cyber security in Kazakhstan: Status and problems. In: *Collection of Scientific Papers of the 3rd International Scientific and Practical Conference "Strategy for Forming the Ecosystem of the Digital Economy"* (pp. 12-15). Kursk: Southwestern State University.

Aratulu, K. (2019). Crimes in the field of computer information in the Republic of Kazakhstan and foreign countries. *Journal of Actual Problems of Jurisprudence*, *56*(4), 105-109.

Arnone, R. (2021). Hackers cybercrime – Computer security: Ethical hacking: Learn the attack for better defense. *ARIS2-Advanced Research on Information Systems Security*, *1*(1), 50-61.

Bandler, J. & Merzon, A. (2020). *Cybercrime investigations: A comprehensive resource for everyone*. Boca Raton: CRC Press.

Bartlett, B. (2023). Why do states engage in cybersecurity capacity-building assistance? Evidence from Japan. *The Pacific Review*. https://doi.org/10.1080/09512748.2023.2183242

Beisbekova, G.K., Konussova, V.T., Ismagulov, K.E., Saktaganova, I.S. & Mukasheva, A.A. (2019). Problems of concretization of legal norms in Kazakhstan. *Journal of Advanced Research in Law and Economics, 10*(1), 52-57.

Chandra, A. & Snowe, M.J. (2020). A taxonomy of cybercrime: Theory and design. *International Journal of Accounting Information Systems*, *38*, 100467.

Chawki, M. (2021). Cybercrime in the context of COVID-19. In: *Intelligent computing: Proceedings of the 2021 Computing Conference, Volume 3* (pp. 986-1002). Cham: Springer.

Chudyk, N. & Vivchar, O. (2023). Strategy of strengthening the economic security of enterprises of network structures: Pragmatics and key vectors of development. *Law, Policy and Security, 1*(1), 55-67.

Criminal Code of the Republic of Kazakhstan. (1997). https://adilet.zan.kz/eng/docs/K970000167_

Cristea, L.M. (2020). Current security threats in the national and international context. *Journal of Accounting and Management Information Systems*, *19*(2), 351-378.

Deora, R.S. & Chudasama, D. (2021). Brief study of cybercrime on an internet. *Journal of Communication Engineering & Systems*, *11*(1), 1-6.

Government of the Republic of Kazakhstan. (2022). Draft Concept for the Development of the Digital Ecosystem for 2022-2027 ("Cybershield-2"). https://online.zakon.kz/Document/?doc_id=31786606

Hatcher, W., Meares, W.L. & Heslen, J. (2020). The cybersecurity of municipalities in the United States: An exploratory survey of policies and practices. *Journal of Cyber Policy*, *5*(2), 302-325.

Holt, T.J., Bossler, A.M. & Seigfried-Spellar, K.C. (2022). *Cybercrime and digital forensics: An introduction*. London: Routledge.

Law of the Republic of Kazakhstan No. 418-V "On informatization". (2015). https://adilet.zan.kz/eng/docs/Z1500000418

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.

Luknar, I.M. (2020). Cybercrime-emerging issue. *Archibald Reiss Days*, *10*, 621-628.

Marwan, A., Jiow, H.J. & Monteiro, K. (2022). Cybersecurity regulation and governance during the pandemic time in Indonesia and Singapore. *International Journal of Global Community*, *V*(1), 13-32.

Metelskyi, I. & Kravchuk, M. (2023). Features of cybercrime and its prevalence in Ukraine. *Law, Policy and Security, 1*(1), 18-25.

Omarova, A.B. & Malikova, Sh.B. (2018). To the concept of the identity of the offender of crimes in the field of computer information. *Journal of Actual Problems of Jurisprudence*, *79*(3), 292-297.

Pawar, S.C., Mente, R.S. & Chendage, B.D. (2021). Cyber crime, cyber space and effects of cyber crime. *International Journal of Scientific Research in Computer Science, Engineering and Information Technology*, *7*(1), 210-214.

Rani, S., Kataria, A., Sharma, V., Ghosh, S., Karar, V., Lee, K. & Choi, Ch. (2021). Threats and corrective measures for IoT security with observance of cybercrime: A survey. *Wireless Communications and Mobile Computing*, *2021*, 5579148.

Safargalieva, M. (2023). *Cyberpol started its work in the WKO.* https://www.inform.kz/ru/kiberpol-nachal-svoyu-rabotu-v-zko_a4094755

Shah, A. & Chudasama, D. (2021). Investigating various approaches and ways to detect cybercrime. *Journal of Network Security, 9*(2), 12-20.

Shevchuk, V.M. (2020). Methodological problems of the conceptual framework development for innovation studies in forensic science. *Journal of the National Academy of Legal Sciences of Ukraine, 27*(2), 170-183.

Shukan, A., Yusupova, T.K. & Rakhimbaeva, M.V. (2020). Criminalistic problems on fighting crime in the sphere of information technologies in RK. In: *Collection of Scientific Articles on the Results of the International Scientific and Practical Conference "Innovative Clustering of Science*

and Practice in the Context of Digitalization" (pp. 177-179). St. Petersburg: St. Petersburg State University of Economics.

Sikos, L.F. (2021). AI in digital forensics: Ontology engineering for cybercrime investigations. *WIREs Forensic Science*, *3*(3), e1394.

Somogyi, T. & Nagy, R. (2022). Some impacts of global warming on critical infrastructure protection - heat waves and the European financial sector. *Insights into Regional Development, 4*(4), 11-20.

Sviatun, O.V., Goncharuk, O.V., Chernysh, R., Kuzmenko, O. & Kozych, I.V. (2021). Combating cybercrime: Economic and legal aspects. *WSEAS Transactions on Business and Economics*, *18*, 751-762.

Temiraliev, T.S. & Omarov, E.A. (2019). Problems of combating crimes committed with the use of information systems and ways to solve them. *Bulletin of the Institute of Legislation and Legal Information of the Republic of Kazakhstan*, *1*(55), 93-99.

Tvaronavičienė, M., Plėta, T., Della Casa, S. & Latvys, J. (2020). Cyber security management of critical energy infrastructure in national cybersecurity strategies: Cases of USA, UK, France, Estonia and Lithuania. *Insights into Regional Development*, *2*(4), 802-813.

Vilks, A., Kipane, A., Kudeikina, I., Palkova, K. & Grasis, J. (2022). Criminological Aspects of Current Cyber Security. *Revista de Direito, Estado e Telecomunicacoes, 14*(2), 94-108.