ANNOTATION

Topic: Criminal offenses in the field of informatization and communication (criminal law and criminological aspects)

The purpose of the study is a comprehensive analysis of the composition, historical aspects, problems of law enforcement practice of criminal offenses in the field of informatization and communication, as well as the development of proposals for improving legislation and improving the effectiveness of the fight against criminal offenses.

To achieve this goal, the following tasks are defined in the work:

1.study of historical aspects of liability for criminal offenses in the field of informatization and communication.

2.to reveal the current formation of the concept of criminal offenses in the field of informatization and communication and to conduct a theoretical analysis of them.

3.analysis of the regulatory legal framework governing liability for criminal offenses in the field of informatization and communication and identification of its shortcomings.

4.providing a criminological description of criminal offenses in the field of informatization and communication.

5.to conduct a comparative analysis of foreign experience in combating criminal offenses in the field of informatization and communication.

6.development and justification of proposals for improving legislation and measures to prevent criminal offenses in the field of informatization and communication.

Object of study: public relations in the field of informatization and criminal offenses in the field of communication.

Subject of the study: criminal law and criminological aspects of offenses in the field of informatization and communication.

Research methods. The methodology for studying criminal offenses in the field of informatization and communication is based on an integrated approach that combines historical-legal, logical, statistical, comparative-legal, theoretical and empirical methods of analysis. One of the main methods is the analysis of regulatory documentation, which allows you to study the current legislation regulating the field of Information Technology and communications. This method involves a detailed study of the Criminal Code, special laws, by-laws, as well as an analysis of judicial practice and decisions made. The purpose of the analysis is to identify legal gaps, contradictions and assess the effectiveness of regulatory legal acts in the fight against cybercrime. The use of statistical data of law enforcement agencies and research institutes makes it possible to assess the scale of the problem, identify the most common types of criminal offenses and evaluate the effectiveness of measures taken to prevent and disclose them. In addition, a comparative analysis of international experience plays an important role in the study of effective practices and methods of regulating and combating cybercrime in different countries. This method allows

you to identify successful strategies that can be adapted and applied in the context of other jurisdictions, thereby contributing to the improvement of international cooperation in the fight against criminal offenses in the field of informatization and communication.

Theoretical and methodological foundations of the study. The study of the theoretical and methodological foundations of criminal offenses in the field of informatization and communication includes an analysis of the concept, classification and criminal legal aspects of these criminal offenses, taking into account their historical development and international cooperation. In the criminological aspect, it allows us to understand the causes and conditions that contribute to cybercrime and develop effective preventive measures. The research methodology is based on the integrated use of theoretical and empirical methods that provide a comprehensive analysis of the problem and contribute to the development of proposals for improving legislation and increasing the effectiveness of the fight against criminal offenses in the field of informatization and communication.

Scientific novelty of the study. The scientific novelty of this study lies in the formulation and development of new scientific principles related to the analysis and differentiation of criminal offenses in the field of informatization and communication. In the course of the work, the main aspects that determine the signs and mechanisms for committing such criminal offenses were identified and systematized, which made it possible to update theoretical approaches in criminal law and criminology. The study contributes to the development of the theoretical foundations of legal science through a detailed analysis of the impact of information and technological progress on changing the nature and structure of criminal offenses, as well as substantiating the need to adapt the legal system to new tasks.

Theoretical and practical significance of the study.

The theoretical significance of the study lies in the enrichment and expansion of already existing knowledge about cybercrime, as well as in the development of methodological approaches to the study and fight against criminal offenses in the field of informatization and communication. The study proposes a new classification of cybercrimes, which will contribute to a more accurate understanding of their nature and, as a result, more effective law enforcement. The work also expands the boundaries of criminological theory and introduces aspects related to the digitalization of society and information security.

Practical significance of the study. The practical value of the dissertation is associated with the development and presentation of specific proposals to improve the legislation and the practice of its application in the fight against criminal offenses in the field of informatization and communication. In the course of the study, ways to strengthen the regulatory framework aimed at eliminating existing gaps in legislation and improving the mechanisms of interdepartmental and international cooperation of criminal offenses in the field of informatization and communication are proposed. In addition, in the course of the work, proposals were formulated to

improve the efficiency of the activities of internal affairs bodies through the introduction of modern technologies and investigative methods, as well as to train and improve the skills of employees in accordance with the requirements of the digital age.

Theoretical and practical significance of the study.

The theoretical significance of the study lies in the enrichment and expansion of already existing knowledge about cybercrime, as well as in the development of methodological approaches to the study and fight against criminal offenses in the field of informatization and communication. The study proposes a new classification of cybercrimes, which will contribute to a more accurate understanding of their nature and, as a result, more effective law enforcement. The work also expands the boundaries of criminological theory and introduces aspects related to the digitalization of society and information security.

Practical significance of the study. The practical value of the dissertation is associated with the development and presentation of specific proposals to improve the legislation and the practice of its application in the fight against criminal offenses in the field of informatization and communication. In the course of the study, ways to strengthen the regulatory framework aimed at eliminating existing gaps in legislation and improving the mechanisms of interdepartmental and international cooperation of criminal offenses in the field of informatization and communication are proposed. In addition, in the course of the work, proposals were formulated to improve the efficiency of the activities of internal affairs bodies through the introduction of modern technologies and investigative methods, as well as to train and improve the skills of employees in accordance with the requirements of the digital age.

The main conclusions proposed by the defense:

1.Taking into account the implementation of the concept of legal policy of the Republic of Kazakhstan until 2030 and the concept of cybersecurity, the author was given an author's definition of a criminal offense of a theoretical nature in the field of informatization and communication.

In the context of the rapid development of innovative digital technologies, offenders are using new approaches to committing criminal offenses, as well as additional criminal risks arise for many areas of public life, including freedom of entrepreneurial activity, in such conditions a full-fledged informatization and definition of a criminal offense in the field of communication is necessary.

Criminal offenses in the field of informatization and communications are «criminal offenses carried out through the illegal use of information systems, databases and networks of telecommunications, computer communications, with the aim of accessing, modifying or destroying personal and state data».

2.In the course of differentiation of criminal offenses in the field of informatization and communication, shortcomings in the conceptual apparatus were identified. In order to eliminate shortcomings in this direction, we propose to introduce the

following concepts. Paragraph 3-41 of Article 1 of the Criminal Code of the Republic of Kazakhstan should be introduced and supplemented with the following concepts: «Cybercrime», «computer communications», «cybersecurity». «Cybercrime» - is the act of illegal possession and use of information technologies, computer systems, confidential information, personal data in cyberspace. «Computer communication is the process of using various network technologies, such as the Internet, local area (LAN) and wireless networks, to send and receive data between computers», «cybersecurity - measures and processes designed to protect computer systems, networks and data from unauthorized access, attacks and threats». In the course of studying criminal offenses in the field of informatization and communication, there is a need to clearly and timely identify by definition the main signs of socially dangerous actions and omissions, as well as potentially or actually arising serious and especially serious consequences. Such definitions make it possible to classify criminal offenses, improve law enforcement practice and apply effective law enforcement measures against such actions. In this context, the timely detection and accurate description of criminal offenses plays an important role, as it contributes to the correct behavior of law enforcement agencies and ensuring information security.

At the same time, it is proposed to amend paragraph 38 of Article 3 of the Criminal Code of the Republic of Kazakhstan with articles 205, 206, 208 of the Criminal Code of the Republic of Kazakhstan, that is, as a large loss and large amount, the value of property or the amount of damage exceeding the monthly calculation index by one thousand times. This is due to the fact that the concepts of large damage and large size make it possible to objectively assess the degree of harm caused by a criminal offense to society. Thus, it clearly determines the severity of the criminal offense and ensures the correct behavior of law enforcement agencies. The presence of defined limits facilitates the process of identifying and evaluating criminal offenses for law enforcement agencies and courts. In international practice, it is common practice to specify the amount of property damage and losses. These changes will ensure compliance with international standards and improve the legal system at the global level.

3.Investigative and judicial practice shows that there are legislative shortcomings in the objective or subjective features of criminal offenses in the field of informatization and communication. According to research, the increase in the number of such offenses is due to the expansion of the scope of application of Information Technologies. Key infrastructures such as financial institutions, energy systems and Public Administration are becoming the main targets of cybercriminals and require effective cyber protection and criminal law measures. In the process of technological progress and digitalization of society, there is a need to update criminal legislation. This, in turn, makes it possible to maintain a balance between information security and innovation. Thus, there is an increased need to strengthen measures to combat information criminal offenses. Improving the accuracy of

legislative acts and improving law enforcement practice will contribute to the timely detection of criminal offenses, their classification and effective action of law enforcement agencies. In this context, it is necessary to introduce modern policies and methodologies to combat information offenses, as well as improve legal regulation. These actions constitute important steps to ensure legal security and strengthen protection against cyber threats.

Therefore, the following changes and additions are recommended:

-Part 4 of Article 205 of the Criminal Code of the Republic of Kazakhstan is proposed to read as follows: "intentional illegal access to legally protected information on Electronic Media, Information System or telecommunications network, which entailed a serious violation of the rights and legitimate interests of citizens or organizations or the interests of society or the state protected by law, the same act that caused serious consequences by negligence, repeated actions committed by a group of persons by prior collusion" - "with or without deprivation of the right to hold certain positions or engage in certain activities for a period of up to four years, a fine in the amount of up to two thousand monthly calculation indices, or involvement in correctional labor in the same amount, or public works for a period of up to six hundred hours, or restriction of freedom for a period of up to six years, or imprisonment for the same period"

- It is proposed to supplement the disposition of Part 1 of Article 206 of the Criminal Code of the Republic of Kazakhstan with the concept of «Computer Communication». This is because illegal attempts to destroy or transform information are transmitted through a computer communication network. Part 1 of Article 206 of the Criminal Code of the Republic of Kazakhstan is presented as follows: «intentional illegal destruction or transformation of legally protected information stored on electronic media, contained in the Information System or transmitted through telecommunications, computer communications, as well as deliberately entering false information into the information system, if this entails a significant violation of the rights and legitimate interests of citizens or organizations or the interests of society or the state protected by law»

- It is proposed to supplement the disposition of Part 1 of Article 208 of the Criminal Code of the Republic of Kazakhstan with the concept of «Computer Communication». This is due to the fact that attempts to illegally seize information are carried out on a computer communication network. Part 1 of Article 208 of the Criminal Code of the Republic of Kazakhstan is presented as follows: «intentional illegal copying or other illegal seizure of legally protected information stored on electronic media, contained in the Information System or transmitted by telecommunications, computer communications, if this entails a significant violation of the rights and legitimate interests of citizens or organizations or the interests of society or the state protected by law»

-In subparagraph 7-1 of Article 1 of the law of the Republic of Kazakhstan «on Informatization» adopted No. 418 - V dated November 24, 2015, we propose to

amend and add to the basic concepts used in this law: «cybersecurity is a set of measures and processes aimed at protecting computer systems, networks and data from unauthorized access, attacks and threats». This is due to the fact that the introduction of the concept of cybersecurity into the legislation is an important step towards the goals of clarifying legal responsibility, increasing the level of information security, ensuring compliance with international standards, strengthening economic and national security.

4. As shown by a comparative analysis of domestic and foreign experience in combating criminal offenses in the field of informatization and communication, we propose the following measures to combat criminal offenses in the field of informatization and communication:

- Strengthening international cooperation. Approval by a mutual international agreement of the commitment to active international cooperation in the fight against cybercrime, including mandatory information exchange and joint operations with foreign partners. We propose to ratify international agreements and conventions aimed at combating cross-border cybercrime. In this, it is proposed to join international agreements, such as the Budapest Convention, which is the earliest international treaty on criminal offenses committed through computer networks and via the internet. There are a number of processes and powers here, such as searching and intercepting computer networks, so we believe that this proposal is very important in our opinion. Ratification of the Budapest Convention on cybercrime will allow the Republic of Kazakhstan to join the system of international cooperation in the fight against cybercrime. This will strengthen the legal framework for combating cybercrime, ensure effective cooperation with other countries and improve the protection of citizens and organizations from cyber threats. In addition, the ratification of the convention will provide access to an international network for the exchange of information about cyber threats and incidents, which will make it possible to respond to new threats faster.
- Introduction of a system of preventive monitoring. In the context of the rapid development of technology and the growth of cybercrime, this principle provides for the creation of specialized centers for law enforcement agencies equipped with modern means of analyzing information and monitoring the information environment, which will allow law enforcement agencies to respond quickly. To ensure information security, it is proposed to create a Monitoring Center for early detection of cyber threats on the basis of the «State Technical Service». This center will be equipped with modern technologies for analyzing information and early detection of threats. Such centers provide an opportunity to promptly respond to cross-border cyber threats and implement measures to prevent criminal offenses at the planning stage.
- Development of the curriculum. Law enforcement practice shows that now there is a need to train professionals who investigate criminal offenses in this area. Therefore, the development of mandatory training programs in the direction of

«cyberterrorist» for training law enforcement officers in the investigation of cybercrime and digital expertise. This training program should include the latest methods of detecting and investigating modern cyber attacks, as well as the norms of international law.

- Improving the digital literacy of the population. It is important to establish a close relationship between the government and civil society in order to raise public awareness about online security. Mass information campaigns, digital security trainings and educational programs allow citizens to protect themselves and their data from cyber threats. Increasing citizens ' awareness of security on the internet is important for maintaining law and order, as it increases the chances of preventing and taking measures against offenses. Expanding citizens ' understanding of their rights and obligations through digital security trainings and educational programs increases their legal responsibility. These measures also contribute to reducing the number of cybercrime complaints received by law enforcement agencies.

Discussion and implementation of research results:

The dissertation research work was prepared, reviewed and discussed at the Department of criminal law disciplines, Faculty of law «Alikhan Bokeikhan University». 5 scientific articles on the dissertation research were published:

2 article in scientific publications included in the International Information Resource Scopus (Elsevier): «Revista de Direito, Estado e Telecomunicacoes» (Brazil), ISSN 1984-9729, Topical Issues in the Fight Against Criminal offenses in the Field of Information and Communications // Revista de Direito, Estado e Telecomunicacoes. – 2023. – Vol. 15, Iss. 1. - p. 177-190.

Revista de Direito, Estado e Telecomunicacoes» (Brazil), ISSN 1984-9729, Measures to Prevent Criminal Offences in the field of Informatisation and Communications in the Republic of Kazakhstan // Revista de Direito, Estado e Telecomunicacoes. – 2024. – Vol. 16, No 2. – P. 276-294.

3 articles in the Journal of the committee for quality assurance in the field of Science and higher education of the Ministry of Science and higher education of the Republic of Kazakhstan:

Some theoretical aspects of combating criminal offenses in the field of informatization and communication, scientific journal «Bulletin of the Academy of law enforcement agencies» №2 (24) 2022 58p.

International cooperation in combating criminal offenses in the field of informatization and communications, scientific journal «Bulletin of the Academy of law enforcement agencies» No. 2 (28) 2023 P. 74.

Criminological characteristics of the personality of a cybercriminal / / Karaganda Academy of the Ministry of internal affairs of the Republic of Kazakhstan named after Barimbek Beisenov September 30, 2022 No. 3 (77) journal «Bulletin-Vestnik» P.139-144

Structure of the research work: the dissertation consists of 171 pages, an introduction, 3 chapters, a conclusion and a list of references with a source.

The results of the study indicate the need to introduce new mechanisms for ensuring cybersecurity and protecting information infrastructure in the Republic of Kazakhstan. In addition, the work provides specific recommendations for improving legal norms and improving the effectiveness of law enforcement agencies.

In general, this dissertation is a comprehensive study aimed at solving legal and organizational problems that exist in the modern Information Society.