DOI : 10.14746/pp.2020.25.3.6

Sholpan ZABIKH
Kazakh national al-Farabi University
(Republic of Kazakhstan, Almaty city)
ORCID: 0000-0001-7856-2845

International Experience of Legal Support of Information Security and the Possibilities for its Application in the Republic of Kazakhstan

Abstract: The author in the article considers the problems of ensuring information security for the solution of which it is supposed to study methods and ways for identifying and preventing danger in the information sphere. The information security of society as a whole is determined by the rapidly growing technological capabilities of modern information systems, which in their influence on the politics, economy, and the spiritual and ideological sphere of people have now become decisive. Ensuring information security, which refers to the state of protection of the vital interests of the individual, society and the state in the information sphere from internal and external threats, seems to be a very important task in the modern world. The security of the information space are entails the protection of the rights and interests of man and citizen, society and the state in the information sphere from real and potential threats. The article also provides a generalized description of the international experience in the legal regulation of information security and the possibility of its application in the Republic of Kazakhstan.

Key words: information security, information technology, media, Internet, laws, international law

Introduction

In the modern world, the information expands the possibilities of international interaction and contributes to the strengthening of international relations and it is the most important life support resource for society. However, along with positive processes, there is a threat associated with international and national crime in the field of information. With the development of technology and the Internet, new threats appear, for example, hacker attacks on banks and government agencies in order to seize valuable information on finances, personal data of clients, the activities of companies or government agencies. The danger of unauthorized interference in the operation of information systems is obvious. There is also a need to ensure information security in such areas as: protection of state interests; protection of individual rights in the information sphere; protection of financial and business activities, protection of information from computer crimes and others.

The protection of individual rights in the information sphere is not new to the world community. The basic principles for establishing limits on interference in private (personal) life by the state and other entities are determined by such fundamental norms as: the Universal Declaration of Human Rights (December 10, 1948), Convention for the Protection of Human Rights and Fundamental Freedoms (developed in 1950 and entered into force on September 3, 1953) and others. Internationally developed prin-

ciples for the protection of commercial information are reflected in the national laws of the USA, Great Britain, Canada, France, Germany and other states. Therefore, the main issue is the study of experience in the legal support of information security in Europe, Canada, the USA and other countries, as well as its application in the Republic of Kazakhstan.

Materials and methods

In the presented research, methods such as analysis of legal norms governing fundamental rights in the field of legal support of information security were used to develop improved legal measures for the prevention of offenses. The analysis of statistics on recorded crimes in various states, including the Republic of Kazakhstan, was carried out. The results of the research, published in leading scientific legal publications of famous Kazakhstani and foreign legal scholars and practitioners in the field of law, were also used. The theoretical basis of research is scientific papers on international law, criminology, general theory of law, philosophy, sociology, psychology and other branches of science. Improving the legal norms proposed by the author contributes to further improvement of the legislative framework of the Republic of Kazakhstan. The article provides a generalized description of the international experience in the legal regulation of information security and the possibility of its application in the Republic of Kazakhstan. The basic laws of the Republic of Kazakhstan are analyzed and international legal norms in the field of information security are systematized.

Literature Review

An analysis of foreign experience in the legal provision of information security has shown that about 100 states have adopted laws on the right to information. A number of researchers (V. A. Kopylov, I. M. Rassolov, M.V. Yakushev, V. B. Naumov and others) are focused on the development of scientific areas related to the legal regulation of information processes on the Internet and its services. However, the Internet as a whole and its services are still little studied from the point of view of the legal specificity of relations (Afonin, 2006, p. 9). Therefore, the main emphasis in the study of the topic is on the laws. One of the first laws is the Press Freedom Act of 1776, adopted in Sweden, which provided citizens with the right of access to information on the activities of public authorities. A steady trend towards the adoption of national laws guaranteeing access to information on the activities of government bodies has been observed since the early 1960s. Over the past 20 years, laws have been passed in a number of states: France, Greece, Denmark, Holland, Portugal, Belgium, Spain and Italy, and others. Laws have been passed on citizen access to government information in the United States, Canada, Australia and New Zealand. There is a constitutional consolidation of the right of citizens to access official information in a number of European countries. These are the Netherlands, Spain, Portugal, Austria, Hungary, Estonia, Belgium and Romania. In France, Greece and Italy, such rights are enshrined in laws. In the UK,

Germany, Estonia, Moldova, Poland and others. Sweden and Finland have statutory restrictions on access to government information. In this case, special attention is paid to the legislative framework affecting the interception and decryption of information. Privacy issues are governed by the United States Information Protection Act (1998) and several other laws. Among the important international documents that form the basis of the legal support of information security, it is possible to note the Resolution 54/49 of the UN General Assembly “Achievements in the field of information and telecommunications in the context of international security,” which was adopted on 01.12.1999 at the 54th session of the UN General Assembly. So, Council of Europe Convention on Cybercrime of 11.23.2001; Declaration “On European Policy in the Field of New Information Technologies” of 1999; 2005 United Nations Convention on the Use of Electronic Communications in International Contracts. Also, the Declaration of Principles for Building the Information Society, which was adopted at the World Summit in Geneva in December 2003, the Framework Decision of the European Union on attacks on information systems of 02.24.2005, Council of Europe Recommendation No. Rec (2001) 3 on the provision of judicial and other legal services legal services to citizens with the help of new technologies dated 02.28.2001, Council of Europe Recommendation No. 1706 “Mass Media and Terrorism” of 2005 and others.

International experience of legal support of information security

At the heart of the approach of the United States of America (USA) to the problems of international cyberspace is the belief that technology has great potential for the country and the world. In 2011, the President of the United States signed the International Strategy for Action in Cyberspace (prosperity, security and openness in a networked world). This document is referred to as International Strategy for cyberspace (Prosperity, Security and Openness in a Networked World (*International Strategy for cyberspace*, 2011). It reveals a vision of the future of cyberspace and a plan of cooperation between countries and peoples with a view to its implementation. The International Strategy for cyberspace defines the dominant position of the United States in modern cyberspace and four main characteristics: openness to innovation; worldwide cooperation; trustworthy security and reliability capable of supporting work. The United States declares in the International Strategy for cyberspace the ability to build and maintain an environment in which the norms of responsible behavior of participants guide many states, strengthen partnerships and support the rule of law. These norms include: support for fundamental freedoms; respect for property; value of personal life; protection against crime; the right to self-defense; global interoperability; network stability; reliability of access; participation of many parties in management; due attention to cybersecurity. The US strategy calls on all nations to join the realization of prosperity, security, and openness in the digital world. The US government has identified seven strategic areas for information security. This is in the field of economics, in the field of network protection, in the field of law enforcement, the development of the armed forces, Internet governance, international development and the freedom of the Internet. In particular, in the field of economics there are: support for a free market environment that encourages technological

innovation through accessible, globally connected networks; protection of intellectual property, including trade secrets; ensuring the supremacy of compatible and safe technical standards set by technical experts. In the field of network protection, the priority are: improving security, reliability and stability; stimulating cooperation in cyberspace bilaterally and multilaterally; the struggle to reduce the number of incursions into the US network and disruption of their work; ensuring rapid response to incidents, sustainability and the possibility of restoring information infrastructure; improving the reliability of technology. In the area of the development of the armed forces, the following priorities are identified: preparation for the security problems of the 21st century; taking into account the growing needs of the armed forces in reliable and secure networks and the ability to adapt to these needs. Creation and improvement of existing military alliances to counter possible threats in cyberspace; expanding cooperation with allies and partners in cyberspace in order to increase overall security.

In the area of Internet governance, the following tasks are defined: emphasis on openness and innovation on the Internet; maintaining the security and stability of the global network, including the domain name system; establishment of a conference between the participants on Internet governance issues and assistance to them. In the area of Internet governance, the following tasks are defined: emphasis on openness and innovation on the Internet; maintaining the security and stability of the global network, including the domain name system; Establishment of a conference between the participants on Internet governance issues and assistance to them.

In the field of international development: providing countries wishing to create the technical and cybersecurity potential with the necessary knowledge, training and other resources. Continuous provision of the best developments in the field of international cybersecurity. Improving the ability of states to combat cybercrime, including through the training of law enforcement agencies, judicial experts, lawyers and lawmakers. Build technical capacity by providing ongoing and ongoing contacts with experts and their colleagues from the US government. In the field of Internet freedom: support for fundamental freedoms and privacy; support for civil society activists in creating reliable, secure platforms for association and freedom of expression; work on measures to protect Internet activity from illegal digital intrusions; encouraging international cooperation to effectively protect commercially sensitive data; ensuring end-to-end compatibility for universal interaction on the Internet (Elin, p. 11–14).

In the field of law enforcement, the following are priority:

1) the expansion of cooperation and the rule of law;
2) taking part in the development of international cybercrime policy;
3) the harmonization of laws on cybercrime at the international level through the expansion of amendments to the Budapest Convention;
4) defining the fight against illegal activities as the goals of cybercrime laws, and not restricting Internet access;
5) depriving terrorists and other criminals of the opportunity to use the Internet to plan and finance operations and attacks.

The International Strategy for cyberspace document defines the mandatory basis for international cooperation in the fight against cybercrime on the norms of the European Convention on Cybercrime (Convention, Budapest, 2001). U.S. federal law contains

a number of laws governing information security relationships. This is the Electronic Communications Privacy Act of 1986. This law determines the procedure for wiretapping telephone conversations and electronic data transmitted using a computer, and also protects data in the process, establishes the requirements for searches. Another Federal Information Security Management Act passed in 2002 defines the importance of information security in the structure of US economic and national security. This law places requirements on federal agency officials, information technology directors, inspectors general, who are required by these entities to conduct annual reviews of information security programs and report the results to the Budget Management Bureau (OMB), which is the largest office in the Office of the President of the United States. The Bureau of Budget Management uses this data to exercise oversight functions and prepare an annual report to Congress. The Federal Information Security Management Act defines the specific responsibilities of federal agencies, the National Institute of Standards and Technology (NIST), and the Budget Management Bureau to strengthen information security systems. This Doctrine determines that there is a shift in emphasis from heavy-duty oppositions to the complex interactions of state and non-state actors, associated with globalization, competition for resources and the tension of political and social structures, combined with ideological, religious and cultural differences.

US Department of Defense Cyberspace Operations Strategy 2011 – The 2011 U.S. Department of Defense Strategy for Operating in Cyberspace – the main emphasis is on the strategic advantages of cyberspace, including operational communications and the possibility of exchanging information and knowledge in the field of information technology. The emphasis is also on the development of US international cooperation in cyberspace as part of international cooperation. The first national cybersecurity strategies began to appear in the countries of the European Union. The United States laid the foundation for this by adopting National Strategy to Secure Cyberspace in 2003. This document is directly related to the consequences of the September 11, 2001 attacks. Following in 2005, the National Plan for Information Infrastructure Protection (NPSI) was adopted in Germany, and in June 2009 the German National Strategy for Critical Infrastructure Protection (CIP Strategy) was published. In early 2011, Germany adopted the new Federal Cyber Security Strategy of Germany – the Federal Cyber Security Strategy for Germany. In 2006, Sweden adopted Strategy to improve Internet security in Sweden. In 2008, Estonia publishes a national cybersecurity strategy, and France adopts a defense and security strategy for information systems in 2011. In November 2011, the UK adopted The UK Cyber Security Strategy. In the same 2011, the Strategy in the Czech Republic was adopted. Canada adopted its national strategy in 2010. The strategy was adopted in Japan in 2010. On February 7, 2008, the President of the Russian Federation approved the Strategy for the Development of the Information Society in the Russian Federation, which set the task of “ensuring national security in the information sphere” (*Strategy for the Development of the Information Society in the Russian Federation*, 2008).

Finland’s strategy based on an understanding of cybersecurity as an economic issue closely linked to the development of the Finnish information society. Estonia attaches particular importance to the security of information systems. Recommended measures are civilian in nature and they based on legal regulation, training and cooperation. Norway’s strategy notes that new services and devices place high demands on user compe-

tency. However, the main responsibility for ensuring the security of information, systems and networks lies with the owner or operator. The focus of the Czech Republic’s cybersecurity strategy is on the issues of free access to information services, data integrity and confidentiality in the Czech Republic. The Netherlands strives for safe and reliable information and communication systems and recognizes the need for freedom and openness of the Internet. The security strategy of Austria’s ICT is to extend the integrated security approaches implemented in the e-government system to other areas, including those that need to be created at the transnational level to ensure the long-term viability of the Austrian economy. The goal of the Slovak strategy is to serve as a solid foundation for protecting information and preventing threats. The goal of the UK strategy is to bring the United Kingdom to the first place in innovation, investment and the quality of services in the field of information and telecommunication technologies, and also to eliminate risks such as cyber-attacks by criminals, terrorists and other states in order to make cyberspace safe for citizens and the economy. Switzerland’s national strategy notes the need to reduce the influence of the prevailing interests of several countries involved in the Internet industry. Lithuania’s strategy is aimed at protecting personal data, telecommunication networks, information systems and critical infrastructures from security breaches and cyber-attacks. According to the National Association of International Information Security in the Russian Federation, 66 thousand attacks were fixed in 2017, 175 thousand in 2018, and as of September 2019, the number of cyber-attacks in Russia reached 200 thousand (Melnikova, 2019). For cybercriminals, there are no borders between countries, so more and more attacks affect several countries at the same time. For example, the United States and Russia during 2017 were the absolute leaders in the number of cyber incidents. This may be because these countries were primarily focused on the attention of the public and the media, whose influence has increased with the development of technologies such as satellite broadcasting and connecting to the global Internet. Information has become a powerful weapon that shapes public opinion and has gained great importance in the political sphere, influencing the audience. Thanks to a huge audience, which includes many politically active people, online publications and video materials are becoming a powerful electoral resource. With their help, political actors can gain serious public support or lose people’s trust.

According to the Positive Technologies international company, in 2017, at least 64 countries around the world were attacked, and the United Kingdom, Australia, Canada, India, Japan, Ukraine, Israel, and China became the most frequent victims of cyberattacks. In 2018, the number of unique cyber incidents continued to grow and was 32% higher than in the same period in 2017. Significantly increased the proportion of attacks aimed at obtaining data. Moreover, the attackers were mainly interested in personal data, as well as accounts and passwords for access to various services and systems. Private individuals were the most affected by cyber attacks, with five out of every six attacks using malware. The reason for the large number of successful attacks may be the lack of antiviruses on victims’ devices, as well as an inattentive attitude to files downloaded from the Internet and open links. Online shopping is often the target of cybercriminals. Attackers use web resource vulnerabilities to steal payment card data (and later money) from website visitors. Web vulnerabilities are actively used by cybercriminals to gain access to edit information published on the site. For example, in January 2018, attack-

ers gained access to the official website of the New Zealand Football Association and published fake information about the resignation of CEO Andy Martin there. During the majority (65%) of attacks on medical facilities, attackers sought to gain access to sensitive information – mainly medical and personal data (44% and 36%, respectively). But there are situations when the goal of attackers is to restrict access to this data. So, in January 2018, the American clinic Hancock Health became a victim of the SamSam malware campaign. Using malicious software, cybercriminals encrypted the organization’s file system and demanded a ransom for decryption. This incident significantly disrupted the work of the hospital, the staff of which had to enter data into the patient’s medical records manually. Despite the available backups, the company estimated that restoring all the systems would take too long, and paid ransomware $ 55,000 (International Research Center “Positive Technologies”, 2018).

According to Positive Technologies experts, in the 3rd quarter of 2019, the percentage of attacks aimed at stealing information increased to 61% in attacks against legal entities and up to 64% in attacks against individuals (versus 58% and 55%, respectively, in the 2nd quarter of 2018.) The share of financially motivated attacks for legal entities and individuals was equal and amounted to 31%. Financially motivated campaigns against legal entities are mainly associated with infections by ransomware Trojans, requiring a ransom for the recovery of encrypted data. In attacks on individuals, cybercriminals seek financial gain by distributing intrusive ads and mobile apps that subscribe to paid services.

In modern conditions, the business and private life of millions of people “leaves a mark” in various kinds of information systems and the Internet. As an example, you can specify various transactions through banks, paying bills, traveling abroad, buying tickets via the Internet and goods in stores using bank cards. In addition, posting information about yourself on social networks, that is, on Instagram, Facebook and others.

The most rapidly growing type of cybercrime, experts have recognized attacks using cryptographic viruses. The main target of cybercriminals remains banks, credit cards. International cybersecurity experts Cybersecurity Ventures has estimated that in 2019 cyber-attacks occur every 14 seconds in the world. As the number of cyber-attacks increases, so does the damage they cause. If in 2018 the losses of companies in various sectors of the economy amounted to 1.5 trillion dollars in 2019, according to the forecast of Sberbank (Russia), they will already reach 2.5 trillion dollars. By 2022, according to the forecast of the World Economic Forum, the amount of planetary damage from cyber-attacks could grow to $ 8 trillion. According to experts, one of the reasons for the rapid growth of cybercrime is technological trends.

Information security in the Republic of Kazakhstan

The main principles of ensuring information security in the Republic of Kazakhstan are:

1) observance of the rights, freedoms and legitimate interests of individuals, as well as the rights and legitimate interests of legal entities;
2) ensuring the security of the individual, society and the state in the application of information and communication technologies;

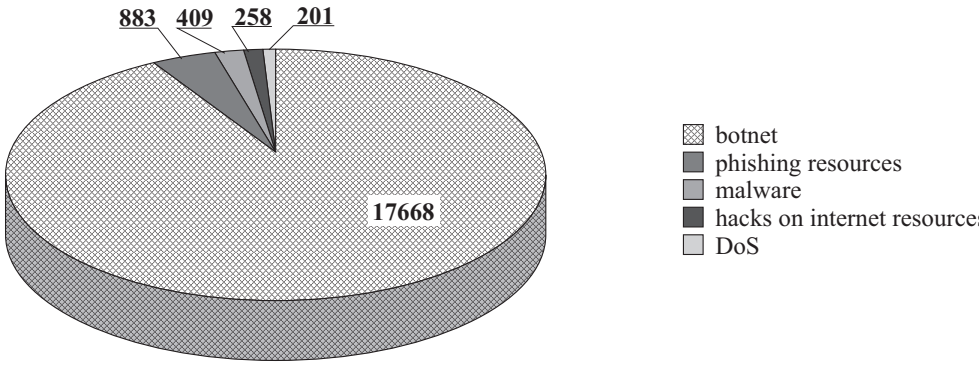
3) the implementation of activities on informatization in the Republic of Kazakhstan on the basis of common standards that ensure the reliability and controllability of objects of informatization;
4) a clear delineation of powers of state bodies;
5) continuous monitoring of information security of information and communication infrastructure facilities;
6) integration of the national security system with international security systems.

In 1998, a resolution of the Government of the Republic of Kazakhstan dated December 31, 1998 No. 1384 “On coordination of work on the formation and development of the national information infrastructure, informatization processes and ensuring information security” was adopted. Also, 3 (three) new versions of the laws of the Republic of Kazakhstan “On Informatization” were adopted – these were in 2003, 2007, 2015 and several specialized laws of the Republic of Kazakhstan on introducing relevant amendments to them on issues of electronic formats for presenting information (data). However, common threats in the Republic of Kazakhstan are improper storage of archive data, violation of access rights to data, incorrect operation of users and maintenance personnel, and loss of information. In many organizations of Kazakhstan, as well as in some states, paperwork is still based on paper documents that require appropriate measures to ensure information security. Therefore, there has been an increase in initiatives to introduce digital technologies in enterprises, and this requires the involvement of information technology security specialists to protect information. The largest enterprises and organizations, due to the vital importance and value of information for their business, hire information security specialists, usually to their own staff. Their task is to protect all technologies from malicious cyber-attacks, which are often aimed at stealing important confidential information or intercepting the organization’s internal systems. Among the key problems in the Republic of Kazakhstan in the field of information security are the following:

1. The prevalence of malware for personal computers and mobile devices is growing along with the number of their users and most users do not use specialized software to protect their personal computers, smartphones, and tablets. This fact is used by “hackers” and leads to an increase in the number of attacks.
2. Low legal literacy of the population, workers in the field of information and communication technology, as well as heads of organizations on information security issues.
3. Violation by state and non-state actors of informatization and users of services in the field of information and communication technology of established requirements, technical standards.
4. Personnel errors and technological failures that have a negative impact on information systems, software and other elements of the information and communication infrastructure.
5. The actions of international criminal groups, communities and individuals to carry out thefts in the financial and banking sector, the harmful effects on systems and others.

The national segment of the Internet has more than 120 thousand Internet resources in the KZ and ҚAZ domains, in accordance with the legislation physically hosted on

Table 1. Top 5 information security incidents in Kazahkstan Republic 2019



the territory of the Republic of Kazakhstan. In order to assist owners and users of information resources and systems on the safe use of ICTs, the national computer incident response service KZ-CERT has been operating since 2010. This Service is a member of a number of international organizations, including FIRST (Forum of Incident Response and Security Teams), TI (Trusted Introducer for Security and Incident Response Teams), OIC-CERT (Organization of Islamic Interaction between Computer Response Response Services) and has more 20 concluded memorandums of understanding and cooperation with relevant structures of foreign countries.

However, crimes in the data of international security services in the field of cyber-threats, every second in the world undergo a cyber-attack of about 12 people, and annually about 556 million cybercrimes are committed in the world, the damage from which amounts to more than $ 100 billion. For the first half of 2019, 10.4 thousand incidents related to attacks, threats, etc. were recorded in Kazakhstan, which is 22.8% less compared to the same period last year (13.5 thousand incidents). Most incidents in 2019 were observed in April. This is 2.1 thousand attacks. Since the Internet is an international system of integrated computer networks for storing and transmitting information, attacks by cybercriminals are registered in different countries of the world [10]. In the Global Cybersecurity Index, the Republic of Kazakhstan has significantly improved its position by 2019 (see Table 2).

Table 2

Global Cybersecurity Index 2017 and 2018

Countries	2018		2017	
	a place	evaluation	a place	evaluation
1	2	3	4	5
Great Britain	1.0	0.931	12.0	0.783
USA	2.0	0.926	2.0	0.919
France	3.0	0.918	8.0	0.819
Lithuania	4.0	0.908	56.0	0.504
Estonia	5.0	0.905	5.0	0.846
Singapore	6.0	0.898	1.0	0.925
Spain	7.0	0.896	19.0	0.718

1	2	3	4	5
Malaysia	8.0	0.893	3.0	0.893
Canada	9.0	0.892	9.0	0.818
Norway	10.0	0.892	11.0	0.786
Kazakhstan	**40.0**	**0.778**	**82.0**	**0.352**
Russia	26.0	0.836	10.0	0.788
Belarus	69.0	0.578	39.0	0.592
Armenia	79.0	0.495	110.0	0.196
Kyrgyzstan	111.0	0.254	96.0	0.270

So, in 2019 Kazakhstan immediately rose by 42 points – up to 40th place. Kazakhstan ranked 82nd in the 2018 ranking. However, among the CIS countries, Kazakhstan took second place after Russia (26th place in the overall ranking). The Republic of Kazakhstan shares the neighboring places with Ireland (38th place), Israel (39th place), Indonesia (41st place), Portugal (42nd place) and Monaco (43rd place). The leaders of the index were Great Britain (first place), USA (second place) and France (third place). Latvia came in fourth and Estonia in fifth. Uzbekistan ranked 52nd in this review, Ukraine – 54th, Belarus – 69th, Tajikistan – 107th, and Kyrgyzstan – 111th (Strategy, 2019).

These successes in Kazakhstan are associated with an improvement in the legal situation. In particular, Kazakhstan unified the requirements in the field of information and communication technologies and information security. The Digitalization Initiative is giving increasing importance to an effective cybersecurity strategy. Only in the past two years, Kazakhstan has developed basic conceptual approaches to the development of the country’s cyber security sphere. The concept of cybersecurity “Cyber shield of Kazakhstan” and other legislative acts were also developed and approved. Malicious code research laboratories have been set up and a national information security coordination center has been opened, specialties of educational institutions have been opened and the number of grants for students has been increased. The Kazakhstan model of school, secondary special, higher and postgraduate education in the field of information and communication technology, including specialization in the field of information security, requires constant and thorough analysis for compliance with modern society needs and trends in ensuring the safe development of information technologies. Therefore, the content of educational and professional standards is being revised.

Discussions

Foreign experience in legal support of information security shows that with the development of new technologies and the Internet, various types of crimes have appeared. A serious danger to millions of the world’s inhabitants – holders of credit and debit bank cards, is cyber fraud and cyber espionage. Commercial espionage based on information attacks to steal databases and other valuable information is a particular threat. With the increase in users of computers and mobile devices, the prevalence of malware and an increase in attacks aimed at infecting subscriber devices with malware by hackers are increasing. The problem is the spread of viral and “trojan” programs through “hacked” sites. One of the key problems is the low legal literacy on information security issues.

Lack of knowledge about legal restrictions creates the illusion of permissiveness of actions that violate the rights and freedoms of other citizens, the rights of owners of copyright and related rights to software and affect the functioning of information resources. In addition, people can become victims of “phishing” pages on the Internet or fake online stores and banks. In such cases, attackers try to obtain confidential user information. The issue of effective opposition to informational threats in modern conditions is a priority. Therefore, this problem is discussed in Kazakhstani society and it can be solved only with the close interaction of state bodies, non-state structures and citizens of the country, as well as by improving legislation.

Results

In recent years, a number of measures have been implemented in the Republic of Kazakhstan to improve legislation and the system of ensuring information security of the state. An Information Security Concept has been developed and adopted, which provides for the implementation of a set of legal, scientific, technical and organizational measures. This Concept is aimed at forecasting, identifying, preventing and suppressing any threats in the field of information security. There is also a legislative and regulatory framework in the field of information security, which includes the Criminal Code of the Republic of Kazakhstan, the Code of the Republic of Kazakhstan “On Administrative Offenses”. The laws “On National Security”, “On State Secrets”, “On Informatization”, “On Personal Data and their protection ”,“ On the electronic document and electronic digital signature ”,“ On communication ”and others. The adopted Cybersecurity Concept (Cybershield of Kazakhstan) defines the principles and main directions of development of information security («Cyber Shield of Kazakhstan», 2017). This regulatory act was approved by the Decree of the Government of the Republic of Kazakhstan dated June 30, 2017. It describes the main directions of the implementation of state policy in the field of protection of electronic information resources, information systems and telecommunication networks, ensuring the safe use of information and communication technologies. This document provides a unified approach to monitoring the legal information security of state bodies, individuals and legal entities. It also developed a mechanism for preventing and promptly responding to information security incidents, including in emergency situations of a social, natural and man-made nature, and the introduction of a state of emergency or martial law. In addition, international experience in the formation of approaches to the protection of the national information and communication infrastructure of developed states was comprehensively studied.

The implementation period of the Concept includes two stages: the first stage of 2017–2018 and the second stage of 2019–2022. Currently, the first stage has been completed, at which a detailed law enforcement practice has been formed to comply with already established requirements in the field of information security. The educational programs and professional standards were revised, the number and quality of trained specialists in the field of information security was increased, professional development of existing workers in this field was provided. An effective scheme of interaction between industry and science in the creation of domestic developments was also built,

the basis for the development of national and industry operational information security centers was created.

In Kazakhstan, law, as well as the procedure and measures for their protection define the goals of collecting and processing personal data of citizens in electronic form and with their consent. The legislation also defines the procedure for the destruction of personal data by operators at their request. Security requirements for banking information systems are provided by regulatory legal acts of the National Bank of the Republic of Kazakhstan, taking into account industry and international requirements for ensuring the security of information systems.

The current Criminal Code of the Republic of Kazakhstan provides for a separate chapter 7 of criminal offenses in the field of information communications (The Criminal Code of the Republic of Kazakhstan, 2014). This chapter provides for liability for intentional unlawful access to information protected by law contained in electronic media in an information system or telecommunications network that entail significant violations of the rights and legitimate interests of citizens or organizations or the interests of society or the state protected by law. Also, deliberate unlawful copying or other unlawful seizure of legally protected information stored on electronic media contained in an information system or transmitted over telecommunication networks. In addition, article 210 of the Criminal Code of the Republic of Kazakhstan provides for criminal liability for the creation, use or distribution of malicious computer programs and software products.

The Code of the Republic of Kazakhstan “On Administrative Offenses” also contains a number of administrative offenses for the commission of which administrative responsibility measures are provided, including for officials who do not fulfill obligations to ensure information security in the form of a violation of the requirements for the use of electronic information resources protection means. Non-compliance Unified requirements, non-implementation or improper implementation by the owner or owner of information systems, containing personal data, measures to protect them (The Code of the Republic of Kazakhstan on Administrative Offenses, 2014).

The Law of the Republic of Kazakhstan “On Informatization” defines the main tasks of public administration in this area. In particular, this is the formation and development of the information society; ensuring the implementation and support of administrative reform of state bodies; development of “electronic government” and “electronic akimat”. Particular attention is paid to improving digital literacy, providing participants of the educational process with conditions for access to electronic information resources of e-learning, as well as providing conditions for the development and implementation of modern information and communication technologies in production processes. Based on these tasks, the Government of the Republic of Kazakhstan is developing: the main directions of state policy in the field of informatization and organizes their implementation (The Law of the Republic of Kazakhstan “On Informatization”).

The Law of the Republic of Kazakhstan “On personal data and their protection” regulates public relations in the field of personal data, and also determines the purpose, principles and legal foundations of activities related to the collection, processing and protection of personal data. The main purpose of this law is to ensure the protection of the rights and freedoms of man and citizen in the collection and processing of his personal data (The Law of the Republic of Kazakhstan “On personal data and their protection”).

The Law of the Republic of Kazakhstan “On National Security of the Republic of Kazakhstan” regulates legal relations in the field of national security of the Republic of Kazakhstan and determines the content and principles of ensuring the security of man and citizen, society and the state (the Law of the Republic of Kazakhstan, 2012).

Another Law of the Republic of Kazakhstan “On State Secrets” defines the legal framework and a unified system of protecting state secrets in the interests of ensuring the national security of the Republic of Kazakhstan. The Law is regulates social relations arising in connection with the classification of information as state secrets, their classification, disposal, protection and declassification (the Law “On State Secrets”, 1999). Among the laws aimed at ensuring information security, one can name the Law of the Republic of Kazakhstan “On electronic document and electronic digital signature”. This law regulates the relations arising from the creation and use of electronic documents certified by electronic digital signatures, providing for the establishment, modification or termination of legal relations. So, the rights and obligations of participants in legal relations arising in the field of electronic documents circulation, including civil transactions (the Law of “On electronic document and electronic digital signature”, 2003).

The Law “On Communications” establishes the legal basis for activities in the field of communications in the Republic of Kazakhstan, defines the powers of state bodies to regulate these activities, the rights and obligations of individuals and legal entities that provide or use communications services (the Law of “On Communications”, 2004). In higher educational institutions of Kazakhstan, the specialties “Information Security Systems,” disciplines: “Applied Engineering Programs,” “Microprocessors and Microprocessor Systems,” “Programming and Implementation of Embedded Systems” have been introduced into the curriculum. The practice of conducting analytical studies, research and development, organization of specialized conferences and seminars also develops. As part of the Cyber Defense of Kazakhstan program, the state has identified 336 critical sites for cybersecurity. These are state structures, banks and industrial enterprises, attacks on which can have an interstate effect.

Conclusions

International cooperation in the field of information security remains an integral component of political, military, economic, cultural and other types of interaction between states. The main areas of cooperation that meet the interests of the Republic of Kazakhstan are: ensuring information security of cross-border information exchange, preserving and not distorting information when it is transmitted via telecommunication channels; coordination of the activities of States parties to international cooperation in the prevention of computer crimes. Creation of joint international projects for the development of new information exchange systems, improvement of the technological base and the formation of information systems and security systems for information resources. Further improvement of the legislation of the Republic of Kazakhstan on the basis of a thorough study of the experience of other states and analysis of international legal norms in the field of protection of information systems and the development of mechanisms for legal support of information security in the modern world. To strengthen interaction

with foreign legal entities to ensure the development of information and communication technologies, personnel development and scientific cooperation. Conducting seminars, conferences and trainings on the exchange of experience both in Kazakhstan and abroad.

Bibliography

Afonin A. I. (2006), *Legal support for countering spam*, Publishing House of Moscow State Technical University, N.E. Bauman, 128 p.

Allied Joint Doctrine For Information Operations, AJP-3.10, NATO, November 2009, https://info.publicintelligence.net/NATO-IO.pdf/.

Convention On Cybercrime. Convention on Computer Crime (ETS No. 185). Concluded in the city of Budapest 11/23/2001, ATP Consultant plus.

Elin V. M. (2016), *Comparative analysis of the legal support of information security in Russia and abroad. Monograph*, Edited by A. Baranov, M., 182p.

Electronic Communications Privacy Act of 1986, https://www.law.cornell.edu/uscode/text/18/2510.

International Strategy for cyberspace (Prosperity, Security and Openness in a Networked World), 05.22.2011, https://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspac.pdf.

Incidents related to information security decreased in Kazakhstan, World of finance (Capital. Investments. Technologies), 01.23.2020, https://wfin.kz/publikatsii/kazakhstan-v-tsifrakh/item/32065-intsidenty-svyazannye-s-informatsionnoj-bezopasnostyu-sokratilos-v-rk.html.

International Research Center “Positive Technologies”, https://www.ptsecurity.com/en-us/about/clients.

Melnikova Yu. *The world is under the threat of cyber war*, Comnews, https://www.comnews.ru/content/203548/2019-12-18/2019-w51/mir-pod-ugrozoy-kibervoyny 12/18/2019.

How is cybersecurity developing in Kazakhstan, “Strategy”, 28 October 2019, https://strategy2050.kz/ru/news/kak-razvivaetsya-kiberbezopasnost-kazakhstana.

On approval of the Cybersecurity Concept (“Cyber Shield of Kazakhstan”) by the Decree of the Government of the Republic of Kazakhstan dated June 30, 2017 No. 407, https://tengrinews.kz/.

Strategy for the development of the information society in the Russian Federation (approved by the President of the Russian Federation on 07.02.2008 No. Pr-212), RG, No. 34, 02.16.2008.

The Criminal Code of the Republic of Kazakhstan dated July 3, 2014 No. 226-V (as amended and supplemented as of January 11, 2020).

The Code of the Republic of Kazakhstan on Administrative Offenses of July 5, 2014, No. 235-V (as amended and supplemented as of January 16, 2020).

The Law of the Republic of Kazakhstan dated November 24, 2015 No. 418-V “On Informatization” (with amendments and additions as of 01.01.2020).

The Law of the Republic of Kazakhstan dated May 21, 2013 No. 94-V “On personal data and their protection” (as amended on December 28, 2017).

The Law of the Republic of Kazakhstan dated January 6, 2012 No. 527-IV “On the National Security of the Republic of Kazakhstan” (as amended on 01.01.2020).

The Law of the Republic of Kazakhstan dated March 15, 1999 No. 349-I “On State Secrets” (with amendments and additions as of December 27, 2019).

The Law of the Republic of Kazakhstan dated January 7, 2003 No. 370-II “On electronic document and electronic digital signature” (as amended and supplemented as of 11/25/2019).

The Law of the Republic of Kazakhstan dated July 5, 2004 No. 567-II “On Communications” (with amendments and additions as of January 10, 2020).

Międzynarodowe doświadczenie w zakresie prawnego wsparcia bezpieczeństwa informacji i możliwości ich zastosowania w Republice Kazachstanu

Streszczenie

W artykule autor rozważa problemy zapewnienia bezpieczeństwa informacji, dla których rozwiązania ma zbadać metody i sposoby identyfikacji oraz zapobiegania zagrożeniom w sferze informacyjnej. O bezpieczeństwie informacyjnym społeczeństwa jako całości decydują szybko rosnące możliwości technologiczne nowoczesnych systemów informacyjnych, które w swoim wpływie na politykę, gospodarkę oraz sferę duchową i ideologiczną ludzi stały się obecnie decydujące. Zapewnienie bezpieczeństwa informacji, które dotyczy stanu ochrony żywotnych interesów jednostki, społeczeństwa i państwa w sferze informacyjnej przed zagrożeniami wewnętrznymi i zewnętrznymi, wydaje się być bardzo ważnym zadaniem we współczesnym świecie. Bezpieczeństwo przestrzeni informacyjnej wiąże się z ochroną praw i interesów człowieka i obywatela, społeczeństwa i państwa w sferze informacyjnej przed rzeczywistymi i potencjalnymi zagrożeniami. W artykule przedstawiono również uogólniony opis międzynarodowych doświadczeń w zakresie regulacji prawnej bezpieczeństwa informacji oraz możliwości ich zastosowania w Republice Kazachstanu.

Słowa kluczowe: bezpieczeństwo informacji, technologie informacyjne, media, internet, prawo, prawo międzynarodowe

Article submitted: 01.06.2020; article accepted: 15.07.2020