Lecture-2. The system of legal regulation of information security

The Constitution of the Republic of Kazakhstan in Article 18 contains a number of provisions guaranteeing the right of a person to the secrecy of information about his life, in particular: to personal and family secrets, the secrecy of personal deposits and savings, the secrecy of correspondence, telephone conversations, postal, telegraph and other messages. Thus, even the fundamental law of the country establishes a special legal regime for information and the need to keep it secret - i.e. we are talking about information security in relation to this information. But along with the above types of information that are directly focused on a specific individual - a person, there are other secrets in the form of, for example, state secrets, commercial secrets, banking secrets, information for official use, secrets of the investigation, etc.

Let's look at the legal acts that form the basis of the legal system for regulating information security. But first, you need to understand their hierarchy.

In accordance with the hierarchy of legal acts established by the Law of the Republic of Kazakhstan “On Legal Acts”, the Constitution of the Republic of Kazakhstan has the highest legal force. The ratio of the legal force of normative legal acts other than the Constitution of the Republic of Kazakhstan corresponds to the following descending levels:

1) laws that amend and supplement the Constitution;
2) constitutional laws of the Republic of Kazakhstan;
3) codes of the Republic of Kazakhstan;
4) consolidated laws, laws of the Republic of Kazakhstan;
5) normative resolutions of the Parliament of the Republic of Kazakhstan and its Chambers;
6) regulatory legal decrees of the President of the Republic of Kazakhstan;
7) regulatory legal resolutions of the Government of the Republic of Kazakhstan;
8) regulatory legal orders of the ministers of the Republic of Kazakhstan and other heads of central state bodies, regulatory legal resolutions of the Central Election Commission of the Republic of Kazakhstan, the Accounts Committee for Control over the Execution of the Republican Budget of the Republic of Kazakhstan, the National Bank of the Republic of Kazakhstan and other central state bodies;
9) normative legal orders of heads of departments of central state bodies;
10) regulatory legal decisions of maslikhats, regulatory legal resolutions of akimats, regulatory legal resolutions of akims and regulatory legal resolutions of audit commissions.

Thus, for example, legal acts from item 9) should not contradict legal acts from item 5) and in case of their discrepancy, legal acts of a higher level in the hierarchy will prevail. This is very important to understand, as the ICT industry is developing with huge strides, and legislation does not always keep up with it - from terminology to the processes themselves in this area.

In the most general form, in the Republic of Kazakhstan, the legal framework for information security is presented in one part or another:

Codes - the Civil Code, the Criminal and Criminal Procedure Codes, the Code of Administrative Offenses, etc.

Laws of the Republic of Kazakhstan "On National Security of the Republic of Kazakhstan", "On Informatization", "On State Secrets", "On Personal Data and their Protection", "On Electronic Document and Electronic Digital Signature", "On Communications", "On Mass Media" , "On access to information", etc.

Government Decrees: On approval of the Uniform requirements in the field of information and communication technologies and ensuring information security (Regulation of the Republic of Kazakhstan dated December 20, 2016 No. 832) .P.

and other legal acts, as well as standards and technical regulations of the Republic of Kazakhstan.

In order to understand the system of legal regulation of information security, it is necessary to consider the formation and current state of the legal system for regulating information security in the Republic of Kazakhstan.

Probably, the state began to show serious attention to the topic of information security at the republican intersectoral level with the adoption in 1997 of the new Criminal Code of the Republic of Kazakhstan, which provided for a whole article (Article 227) providing for liability for unauthorized access to information. Since 1998, when the Decree of the Government of the Republic of Kazakhstan dated December 31, 1998 No. 1384 "On the coordination of work on the formation and development of the national information infrastructure, informatization processes and ensuring information security" was adopted, 3 new editions of the laws of the Republic of Kazakhstan "On informatization "(2003, 2007, 2015) and several specialized laws of the Republic of Kazakhstan on making appropriate changes to them on issues of electronic formats for presenting information (data), including on issues of information and communication networks, "electronic government".

Over the period that has passed since then, electronic information resources and information systems have been introduced into economic circulation along with other types of property assets, and the scope of their market and state use has been expanded.

With the stage of formation of information security issues, taking into account the nature of the information contained, the legal regimes of public and confidential electronic information resources and systems were differentiated, the rights and obligations of owners, owners and users to protect them were established.

The activities of state bodies and other entities to ensure information security in the field of informatization and communications are currently carried out in accordance with their industry competence, as well as goals and objectives in subject areas related to the use of ICT (regulation of communications and information technologies, protection of personal data, protection of state secrets, countering the activities of foreign technical intelligence, operational-search activities on communication networks, investigation of crimes committed with the use of ICT, and others).

In general, in the Republic of Kazakhstan, the organizational, legal and technical foundations of the system of measures to ensure information security in the field of informatization and communications were formed and legally fixed as components of information security and ensuring the security of the information space and communications infrastructure in accordance with the Law of the Republic of Kazakhstan "On National Security" .

In recent years, various interrelated aspects of ensuring information security in the field of informatization and communications have been reflected and developed in the Criminal Code of the Republic of Kazakhstan, the Code of the Republic of Kazakhstan "On Administrative Offenses", the laws of the Republic of Kazakhstan "On State Secrets", "On Personal Data and their Protection ", "On electronic document and electronic digital signature", "On communication", and a number of by-laws developed to implement the new version of the Law of the Republic of Kazakhstan "On Informatization", which entered into force on January 1, 2016.

A number of by-laws adopted recently have not yet received extensive law enforcement practice. In particular, Decree of the Government of the Republic of Kazakhstan dated December 20, 2016 No. 832 "On approval of the Uniform requirements in the field of information and communication technologies and ensuring information security" (hereinafter - the Uniform requirements), which is a codification of legal and technical norms from national and harmonized standards. The document describes in detail the procedures and rules for the use of information and communication technologies in the processing of legally protected types of information, contains important norms for ensuring the technological security of information infrastructure, information systems and resources, software, hardware at all stages of their life cycle.

At the legislative level, the functioning of the monitoring system for ensuring the information security of "electronic government" informatization objects, including both state and non-state information systems integrated with state ones, is regulated.

In the Rules for monitoring the provision of information security, protection and safe functioning of the objects of informatization of the "electronic government", approved by order of the acting. Minister for Investment and Development of the Republic of Kazakhstan dated January 26, 2016 No. 66, laid down the basic principles of interaction between stakeholders in case of technological failures or signs of computer attacks, as well as algorithms for responding to emerging events and information security incidents.

The e-government security monitoring center detects unresolved vulnerabilities on a daily basis, and sends notifications to the owners of information systems that are its components to take action. There is a positive trend in identified vulnerabilities and measures taken against them. So in 2014, 1241 unresolved vulnerabilities were identified, in 2015 - 469, in 2016 - 355.

Also, the Decree of the Government of the Republic of Kazakhstan dated September 8, 2016 No. 529 approved the Rules and criteria for classifying objects as critical objects of information and communication infrastructure from among the most important state and strategic objects, as well as objects of economic sectors of strategic importance.

Such facilities included in the list of critical information and communication infrastructure facilities are subject to the Uniform Requirements, as well as the need to participate in joint measures provided for by law to ensure monitoring of their information security, protection and safe operation, including the obligation to report information security incidents.

The procedures for introducing information systems into commercial operation are being improved. In this regard, the security measures for information systems are legally differentiated depending on their assignment to a certain class, the period of the information system being in the trial operation mode is limited.

For compliance with information security requirements, more than 500 attestation surveys of state and non-state information systems integrated with state ones were conducted, as a result of which 199 certificates were issued, which are the basis for putting them into commercial operation. According to plans, the rest of the information systems should be certified by the end of 2018, however, due to changes in legislation, IS certification was canceled, leaving only IS tests.

From January 1, 2016, information systems of state bodies, non-state information systems integrated with state information systems at the stage of trial operation, are being tested for compliance with information security requirements. During the tests, source codes, security

function settings are checked, network and server equipment is examined, and load testing is carried out.

The results of the tests are reflected in improving the security and fault tolerance of information systems, the security of information systems software, reducing the influence of factors of violations of information security of information systems, the introduction of mechanisms for controlling and monitoring the security of information systems.

The system of technical regulation provides for conformity assessment of software and telecommunications equipment, including the determination of cases of their mandatory certification when used in the public sector. For these purposes, the set of national and harmonized technical standards in the field of information security, information protection, information technology security is updated annually. In 2018, it was 68 technical standards.

Thanks to the centralization of Internet connection through the Unified Internet Access Gateway of government agencies, the threats of unauthorized access and harmful effects on electronic information resources of government agencies have been significantly reduced. On a daily basis, more than 180 million attacks of various levels are recorded and reflected.

A system of legal, organizational, technical and cryptographic measures for the protection of state secrets processed using computer technology has been created and is being improved.

The most sensitive information for the security of the state in electronic form is transmitted only through special-purpose telecommunications networks, physically separated from the Internet and using cryptographic means of information protection.

Approaches to ensuring the security of the communications infrastructure and public telecommunications networks are built around the system of centralized management of telecommunications networks, through the capabilities of backbone communications operators that implement the concept of "electronic border" on border equipment.

The national segment of the Internet has more than 120 thousand Internet resources in the .KZ and .ҚAZ domains, in accordance with the law, physically located on the territory of the Republic of Kazakhstan. Since 2010, the National Computer Incident Response Service KZ-CERT has been functioning to assist owners and users of information resources and systems on the issues of safe use of ICT. The service is a member of a number of international organizations, incl. FIRST (Forum of Incident Response and Security Teams), TI (Trusted Introducer for Security and Incident Response Teams), OIC-CERT (Organization of Islamic Interaction of Computer Incident Response Services). According to the information provided in the Cyber Shield of Kazakhstan concept, the service has concluded 20 memorandums of understanding and cooperation with specialized structures of foreign countries, recorded and processed more than 66,000 information security incidents.

The first domestic companies appeared on the Kazakhstani market engaged in instrumental security assessment audit (including penetration testing - Pen-test) for compliance with information security requirements and specializing in studying the circumstances, causes and conditions of information security incidents, as well as technical research malicious software.

In a number of national companies and private structures there are divisions for monitoring technical events and technological processes, which are on duty around the clock for prompt response to emergency situations.

The goals of collecting and processing personal data of citizens in electronic form, as well as the procedure and measures for their protection, are legally defined. The legislation regulates both the procedures for their collection exclusively with the consent of citizens, and the destruction at their request by personal data operators, as well as the conditions for the safe storage of personal data in the country and their cross-border transfer.

Requirements for the security of banking information systems are provided by the 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 new version of the Criminal Code of the Republic of Kazakhstan, in force since 2014, provides for a separate chapter on crimes committed in the field of informatization and communications. Taking into account the qualifying circumstances, it contains 38 offenses against electronic information resources and telecommunications systems or networks.

The Code of the Republic of Kazakhstan "On Administrative Offenses" also contains a number of administrative offenses, for which administrative liability measures are provided, including for officials who do not fulfill their obligations to ensure information security in the form of a violation of the requirements for the operation of means of protecting electronic information resources, failure to comply Uniform requirements, non-implementation or improper implementation by the owner or owner of information systems containing personal data, measures to protect them.

The study "Global Cybersecurity Index" (hereinafter referred to as the Global Cybersecurity Index) conducted by the International Telecommunication Union, which assesses the legal, technical, organizational readiness and potential of 195 countries, recorded Kazakhstan's 23rd group place with an index of 0.176 out of 29 groups of countries.

Moreover, the concept of a separate profile bill "On Information Security" is currently being developed, which will combine

Thus, we see that the legislation of Kazakhstan has a significant number of legal acts regulating the organization and functioning of information security, as well as violations in this area.

In order to understand how and why certain requirements are established for information security by law, it is necessary to understand what legal facts and consequences arise during the operation of information systems, Internet resources, etc.