Lecture-7. State bodies and organizations in the field of information security and their competence

State IS and EIR have always been the object of close attention of intruders who are trying, if not to obtain or modify non-public information from state databases, then at least disrupt their work. That is why the protection of public IP is of great importance, because any failure can cause a denial of services to the public, etc. – i.e. wide resonance and consequences. Based on this, the classes of these and other informatization objects are established, depending on which the information security system is built. Unfortunately, within the framework of this lecture, it is not possible to classify objects; therefore, this issue remains for independent study.

A few definitions:

Critically important ICI facilities (CVOICI) are ICI facilities, including the information and communication infrastructure of "electronic government", the violation or termination of which leads to a social and (or) man-made emergency or to significant negative consequences for defense, security, international relations, economy, certain areas of the economy, infrastructure of the Republic of Kazakhstan or for the life of the population living in the relevant territory

"Electronic government" is a system of information interaction of state bodies among themselves and with individuals and legal entities, based on the automation and optimization of state functions, and also designed to provide services in electronic form.

State bodies and organizations in the field of information security and what they do:

A) Government of the Republic of Kazakhstan:

- approves uniform requirements in the field of information and communication technologies and ensuring information security;
- approves the list of critical information and communication infrastructure facilities, as well as the rules and criteria for classifying ICI objects as critical ICI objects;
- approves the list of personal data of individuals included in the state EIR;
- approves the National Anti-Crisis Plan for Response to Information Security Incidents.

B) Authorized body (Ministry of Digital Development, Defense and Aerospace Industry):

- ensures the implementation of state policy in the field of information security;
- develops uniform requirements in the field of information and communication technologies and information security;
- develops a list of critically important IKI objects - KVOIKI, as well as rules and criteria for classifying IKI objects as KVOIKI;
- approves the methodology and rules for testing the objects of informatization of "electronic government" and IS, referred to KVOIKI, for compliance with the requirements of IS;
- approves the rules for monitoring IS events of informatization objects of state bodies (EIR, IS, etc.) in agreement with the National Security Committee of the Republic of Kazakhstan;
- approves the rules for monitoring the provision of information security of objects of informatization of "electronic government" and KVOIKI in agreement with the national security authorities;
- approves the rules for monitoring the implementation of uniform requirements in the field of ICT and information security;
- monitors the implementation of uniform requirements in the field of ICT and information security;

- coordinates activities for the development of information security tools in terms of detecting, analyzing and preventing threats to information security to ensure the stable functioning of IS and telecommunications networks of state bodies;
- issues an act based on the results of tests for compliance with information security requirements;
- exercises state control in the field of informatization in terms of ensuring information security;
- sends orders for execution in case of detection of violations of the requirements of the legislation of the Republic of Kazakhstan in the field of information security;
- coordinates activities for the management of IR and ICT objects in emergency situations of a social, natural and man-made nature, the introduction of a state of emergency or martial law;
- participates in the commissioning of objects of informatization of "electronic government";
- organizes assistance to owners, owners and users of informatization objects in matters of safe use of information and communication technologies, including the prevention of illegal actions to receive, copy, distribute, modify, destroy or block electronic information resources;
- develops the National Anti-Crisis Plan for Response to Information Security Incidents;
- determines the administrator and registry of domain names, approves the rules for registration, use and distribution of domain names in the space of the Kazakhstan segment of the Internet;
- approves the rules for creating and ensuring the functioning of a single national backup platform for storing electronic information resources, the frequency of backup of electronic information resources of critically important objects of information and communication infrastructure;
- approves protection profiles and methodology for developing protection profiles;
- approves the rules for the exchange of information necessary to ensure information security between the operational centers for ensuring information security and the National Coordinating Center for Information Security;
- approves the rules for the formation and maintenance of the register of trusted software and products of the electronic industry, as well as the criteria for including software and products of the electronic industry in the register of trusted software and products of the electronic industry;

C) Information Security Operations Center (on the basis of NIT JSC)

- carries out activities to detect, evaluate, predict, localize, neutralize and prevent threats to information security of ICT, informatization objects connected to the information security operational center;
- takes measures to minimize threats to information security, immediately informs the owner of the ICI, as well as the National Information Security Coordination Center of the fact of an information security incident;
- monitors the provision of information security of the CVOIC, informatization objects that are not related to the objects of informatization of "electronic government";
- exchanges information necessary to ensure the information security of informatization objects connected to the operational information security center with the National Information Security Coordination Center and other operational information security centers;

- collects, consolidates, analyzes and stores information about information security events and incidents;
- provides the owners of KVOIKI with the information necessary to ensure the information security of ICI objects, including information about security threats, vulnerabilities of software, equipment and technologies, methods for implementing information security threats, prerequisites for the occurrence of information security incidents, as well as methods for their prevention and elimination of consequences ;
- ensures the safety of information of limited distribution that has become known to the operational information security center as part of its activities;
- provides connection of information security event logging systems to the monitoring center of the National Information Security Coordination Center.

The operational information security center operates on the basis of a license to provide services to identify technical channels for information leakage and special technical means intended for operational-search activities. Employees of the operational information security center are responsible for the disclosure of commercial or other legally protected secrets obtained by them as a result of their activities, in accordance with the laws of the Republic of Kazakhstan. (Note/exception: in the second-tier banks of the Republic of Kazakhstan, the functions of the information security operational center are carried out by their structural divisions).

D) CERT on the basis of the Republican State Enterprise "State Technical Service of the KNB of the Republic of Kazakhstan":

- analyzes information about information security events in order to eliminate the causes and conditions of information security incidents;
- develops recommendations aimed at countering threats to information security;
- informs the owners of informatization objects (IS, EIR, etc.) about incidents and threats to information security that have become known.

The Information Security Incident Response Service carries out its activities on the basis of a license for the provision of services to identify technical channels for information leakage and special technical means intended for operational-search activities. Employees of the information security incident response service are responsible for the disclosure of commercial or other legally protected secrets obtained by them as a result of their activities, in accordance with the laws of the Republic of Kazakhstan. (note/exception: in the second-tier banks of the Republic of Kazakhstan, the functions of the information security incident response service are carried out by their structural divisions).

E) National Coordinating Center for Information Security (NCCIB on the basis of RSE "State Technical Service of the KNB of the RK"):

- assists owners, owners and users of informatization objects in matters of safe use of ICT;
- ensures the interaction of operational information security centers on monitoring the provision of information security of informatization objects;
- collects, analyzes and summarizes information from operational information security centers on information security incidents at the facilities of the information and communication infrastructure of the "electronic government" and other CVOICI;
- provides technical support for the IS of the National Information Security Coordination Center;

- participates in the development of the procedure for the exchange of information necessary to ensure information security between the information security operational centers and the National Information Security Coordination Center;
- in cases of receiving information about information security incidents at informatization objects, immediately informs the national security authorities of the Republic of Kazakhstan;
- carries out intersectoral coordination on monitoring the provision of information security, protection and safe operation of objects of informatization of the "electronic government", the Kazakhstani segment of the Internet, as well as KVOIKI, response to information security incidents with joint activities to ensure information security in the manner determined by the legislation of the Republic of Kazakhstan ;
- creates and ensures the functioning of a single national backup platform for storing EIR, establishes the frequency of backup of the electronic information resources of the KVOIKI in the manner determined by the authorized body in the field of information security;

Employees of the National Information Security Coordination Center are responsible for disclosing commercial or other secrets protected by law, obtained by them as a result of their activities, in accordance with the laws of the Republic of Kazakhstan.

F) Expert Council (on the basis of ICROAP)

The Expert Council is headed by the head of the authorized body and includes officials - heads of state bodies responsible for informatization of the activities of the state body, representatives of the authorized body, the service integrator of "electronic government", the authorized body in the field of information security and other organizations in the field of informatization according to coordination with the indicated bodies and organizations.

The Expert Council considers issues in the field of informatization and develops proposals and (or) recommendations.

G) Central executive bodies and state bodies directly subordinate and accountable to the President of the Republic of Kazakhstan Ministries, Agencies, Committees, etc.)

- ensure compliance with uniform requirements in the field of information and communication technologies and information security, as well as the rules for implementing the service model of informatization;
- approve the list of open data posted on the Internet portal of open data in agreement with the authorized body;

The competence of the central executive bodies is also determined by the acts of the Government of the Republic of Kazakhstan.

H) Local executive bodies (akimats)

- ensure compliance with uniform requirements in the field of information and communication technologies and information security, as well as the rules for implementing the service model of informatization;
- organize points of public access of individuals and legal entities to state electronic information resources and information systems of state bodies, including by allocating non-residential premises for organizing this access;
- approve the list of open data posted on the Internet portal of open data in agreement with the authorized body;

I) Service integrator of "electronic government" (National Infocommunication Holding "Zerde" JSC):

- ensures compliance with uniform requirements in the field of information and communication technologies and information security, as well as the rules for implementing the service model of informatization;
- organizes the integration of objects of informatization of "electronic government" and the national gateway of the Republic of Kazakhstan;

J) Operator (NIT JSC):

- ensures compliance with uniform requirements in the field of information and communication technologies and information security, as well as the rules for implementing the service model of informatization;

- provides system and technical maintenance and maintenance of Internet resources of state bodies and objects of information and communication infrastructure of "electronic government" in accordance with the list approved by the authorized body;

- ensures the security of storage of state electronic information resources located on the information and communication infrastructure of "electronic government" assigned to the operator;

- ensures the security of storage of state electronic information resources in the provision of information and communication services;

- integrates and connects local (with the exception of local networks with Internet access), departmental and corporate telecommunications networks of state bodies to the information and communication infrastructure of "electronic government";

- provides communication services to state bodies, their subordinate organizations, local governments, as well as other subjects of informatization, determined by the authorized body and connected to a single transport environment of state bodies, for the functioning of their electronic information resources and information systems. To provide communication services, has the right to engage other persons as subcontractors (co-executors) of services;

L) State Technical Service (RSE "GTS KNB RK")

Carries out the following activities in the field of informatization, classified as a state monopoly:

- maintains a single Internet access gateway and a single e-mail gateway of "electronic government";
- tests objects of informatization of "electronic government" for compliance with information security requirements;
- coordinates the assignment for the design of information and communication services for compliance with information security requirements;
- conducts an examination of the investment proposal and the financial and economic justification of budget investments and the terms of reference for the creation and development of the object of informatization of "electronic government" for compliance with information security requirements;
- serving Kazakh top-level domain names;
- accompanies the development of plans for addressing and numbering telecommunications networks of telecom operators operating in the territory of the Republic of Kazakhstan;

- carries out work on the development of information security tools in terms of detecting, analyzing and preventing threats to information security to ensure the stable functioning of information systems and telecommunications networks of state bodies;
- implements the tasks and functions of the National Information Security Coordination Center.

Prices for goods (works, services) produced and (or) sold by a state monopoly entity are established by the National Security Committee of the Republic of Kazakhstan in agreement with the antimonopoly authority.

L) National Institute for Development in the Field of Information Security (RGPnaPH "Institute of Information and Computing Technologies" of the Science Committee of the Ministry of Education and Science of the Republic of Kazakhstan):

1) participates in the implementation of state policy in the field of information security;
2) develops documents on standardization in the field of information security;
3) carries out scientific and technical activities in the field of information security;
4) conducts scientific and technical expertise of projects in the field of information security;
5) provides training, retraining and advanced training in the field of information security.

H) Law enforcement and judicial authorities (Courts of various instances, Ministry of Internal Affairs, KNB, etc.)

1) Investigation of offenses in the field according to their competence and jurisdiction.
2) Bringing to responsibility / imposition of punishment for violations in the field of information security.