Lecture-8. Information security in state bodies. "E-Government"

In order to delineate responsibilities and functions in the field of IS maintenance, an IS subdivision is created, which is a structural subdivision, separate from other structural subdivisions involved in the creation, maintenance and development of informatization objects, or an official responsible for IS maintenance is determined.

The IS subdivision or the official responsible for ensuring IS performs:

1) control over the fulfillment of the requirements of TD IB;
2) control over IS documentation;
3) control over asset management in terms of providing information security;
4) control of the legality of using the software;
5) control over risk management in the field of ICT;
6) control over the registration of IS events;
7) conducting an internal audit of information security;
8) control over the organization of external IS audit;
9) control over ensuring the continuity of business processes using ICT;
10) monitoring compliance with IS requirements in personnel management;
11) control over the state of information security of the object of informatization of "electronic government".

To ensure IS, technical IS documentation (TD) is created. The IS TD is created as a four-level system of documented rules, procedures, practices or guidelines that govern government bodies (GOs) or organizations in their activities.

The IS TD is developed in the Kazakh and Russian languages, approved by the legal act of the civil defense or organization and brought to the attention of all employees of the civil defense or employees of the organization. The IS TD is reviewed in order to analyze and update the information contained in them at least once every two years.

The IS policy of the HE, LEB or organization is a first-level document and defines the goals, objectives, guidelines and practices in the field of IS.

The list of documents of the second level includes documents detailing the requirements of the information security policy of the civil defense or organization, including:

1) methodology for assessing information security risks;
2) rules for identification, classification and labeling of assets associated with information processing facilities;
3) rules for ensuring the continuous operation of assets associated with information processing facilities;
4) rules for inventory and certification of computer equipment, telecommunications equipment and software;
5) rules for conducting internal IS audit;
6) rules for the use of means of cryptographic protection of information;
7) rules for delimitation of access rights to electronic information resources;
8) rules for using the Internet and e-mail;
9) rules for organizing the authentication procedure;
10) rules for organizing anti-virus control;
11) rules for the use of mobile devices and storage media;
12) rules for organizing the physical protection of information processing facilities and a safe environment for the functioning of information resources.

The third level documents contain a description of the processes and procedures for ensuring information security, including:

1) catalog of IS threats (risks);
2) IS threat (risk) treatment plan;
3) regulations for backup and recovery of information;
4) an action plan to ensure continuous operation and restore the health of assets associated with information processing facilities;
5) the administrator's guide for maintaining the informatization object;
6) instructions on the procedure for users to respond to information security incidents and in emergency (crisis) situations.

The list of documents of the fourth level includes work forms, journals, applications, protocols and other documents, including electronic ones, used to register and confirm the procedures and work performed, including:

1) a log of information security incidents and recording of emergency situations;
2) a log of visits to server rooms;
3) a report on the assessment of the vulnerability of network resources;
4) logbook of cable connections;
5) a log of backups (backup, recovery), testing of backups;
6) a log of changes in the configuration of equipment, testing and accounting for changes in free and applied IP software, registration and elimination of software vulnerabilities;
7) test log of diesel generator sets and uninterruptible power supplies for the server room;
8) test log for microclimate, video surveillance, fire extinguishing systems in server rooms.

To ensure the protection of assets, the following is carried out:

1) inventory of assets;
2) classification and labeling of assets in accordance with the classification system adopted in the civil defense;
3) assigning assets to officials and determining the measure of their responsibility for the implementation of measures to manage the information security of assets;
4) regulation in the IS TD of the order:
   - use and return of assets;
   - identification, classification and labeling of assets.

In order to manage risks in the field of ICT, civil defense carries out:

1) selection of a risk assessment methodology in accordance with the recommendations of the standard of the Republic of Kazakhstan ST RK 31010-2010 "Risk management. Risk assessment methods" and development of a risk analysis procedure;
2) identification of risks in relation to the list of identified and classified assets, including:
   - identification of IS threats and their sources;
   - identification of vulnerabilities that can lead to the implementation of threats;
   - identification of information leakage channels;
   - formation of the intruder model;
3) selection of criteria for accepting identified risks;
4) formation of a catalog of IS threats (risks), including:
   - assessment (reassessment) of identified risks in accordance with the requirements of the Republic of Kazakhstan standard ST RK ISO/IEC 27005-2013 "Information technologies. Security methods. Information security risk management";
   - identification of potential damage;

5) development and approval of an IS threat (risk) treatment plan containing measures to neutralize or reduce them.

In order to control the events of IS violations in civil defense or organization:

1) monitoring of events related to IS breach and analysis of monitoring results;
2) events related to the state of information security are registered and violations are detected by analyzing event logs, including:
   - operating system event logs;
   - event logs of database management systems;
   - anti-virus protection event logs;
   - application software event logs;
   - logs of events of telecommunication equipment;
   - event logs of attack detection and prevention systems;
   - content management system event logs;
3) synchronization of the time of the event logs with the infrastructure of the time source is provided;
4) event logs are stored for the period specified in the IS TD, but not less than three years and are online for at least two months;
5) event logs of the created software are maintained in accordance with the formats and types of records defined in the Rules for monitoring the information security of the "electronic government" informatization objects and critically important objects of the information and communication infrastructure, approved by the authorized body;
6) the event logs are protected from interference and unauthorized access. System administrators are not allowed to have permission to modify, delete, or disable logs. Confidential ISs require the creation and maintenance of a backup log store;
7) implementation of a formalized procedure for reporting information security incidents and responding to information security incidents is ensured.

In order to protect critical civil defense or organization processes from internal and external threats:

1) an action plan is developed, tested and implemented to ensure continuous operation and restore the operability of assets associated with information processing tools;
2) an instruction is brought to the attention of civil defense employees or employees of the organization on the procedure for users to respond to information security incidents and in emergency (crisis) situations.

The plan of measures to ensure continuous operation and restore the operability of assets associated with information processing facilities is subject to regular updating.

Functional responsibilities for ensuring IS and obligations to fulfill the requirements of the TD IS of civil defense employees or employees of the organization are included in the job descriptions and (or) the terms of the employment contract.

Obligations in the field of information security, which are in force after the termination of the employment contract, are fixed in the employment contract of civil defense employees or employees of the organization.

In the event that third-party organizations are involved in ensuring the information security of EIR, IS, IKI, their owner or owner enters into agreements that establish the conditions for the operation, access or use of these objects, as well as responsibility for their violation.

The IS TD defines the content of procedures for the dismissal of civil defense employees or employees of an organization who have obligations in the field of IS maintenance. Upon dismissal or amendments to the terms of the employment contract, the rights of access of an employee of the civil defense or an employee of the organization to information and information processing tools, including physical and logical access, access identifiers, subscriptions, documentation that identifies him as an active employee of the civil defense or an employee of the organization, are canceled after termination his employment contract or are changed when changes are made to the terms of the employment contract.

The personnel service organizes and keeps records of the passage of civil defense employees or employees of organizations of training in the field of informatization and the field of information security.

In order to ensure information security during the operation of informatization objects, requirements are established for:

1) authentication methods;
2) the means of cryptographic protection of information used;
3) ways to ensure availability and fault tolerance;
4) monitoring the provision of information security, protection and safe operation;
5) the use of means and systems for ensuring information security;
6) registration certificates of certification centers.

When accessing informatization objects of the first and second classes, in accordance with the classifier, multi-factor authentication is applied, including with the use of digital signature.

In order to protect confidential information of limited distribution, confidential IS, confidential EIR and EIR containing personal data of limited access, CIPF (software or hardware) are used with parameters that meet the requirements for CIPF in accordance with the standard of the Republic of Kazakhstan ST RK 1073-2007 "Means of cryptographic information security. General technical requirements" for informatization objects..

To ensure availability and fault tolerance, the owners of ES informatization objects provide:

1) the availability of a backup own or rented server room for objects of informatization of the ES of the first and second classes in accordance with the classifier;
2) redundancy of hardware and software for data processing, data storage systems, components of data storage networks and data transmission channels.

The "electronic government" web portal is an IS, which is a "single window" of access to all consolidated government information, including the legal framework, and to government and other services provided in electronic form. The requirements for the content, maintenance and content of the electronic information resources of the "electronic government" web portal are established by the authorized body.

The "electronic government" gateway is an IS designed to integrate "electronic government" informatization objects with other informatization objects.

Government and other services in electronic form can be provided through the "electronic government" web portal and a mobile network subscriber device (cell phone, smartphone, etc.)

To receive public and other services in electronic form through the web portal of "electronic government" and the subscriber device of the mobile network, the subjects of receiving services in electronic form can use one-time passwords (received via SMS to a registered number) in accordance with the legislation of the Republic of Kazakhstan.

The payment gateway of "electronic government" is an IS that automates the processes of transferring information about making payments as part of the provision of paid services provided in electronic form.

The payment gateway of "electronic government" provides:

1) transmission of requests for making payments of the subject of receiving the service in electronic form;
2) informing the subject of the provision of services in electronic form about the payment for the provision of services in electronic form.

Second-tier banks and organizations that carry out certain types of banking operations, participating in the processes of receiving and making payments as part of the provision of services (not only in electronic form), ensure the integration of their own IS involved in these processes with the payment gateway of "electronic government" directly or through the IS of the operator of the interbank money transfer system (Kazakhstan Center for Interbank Settlements JSC). Those. the integration of the IS of the bank and the IS of the state organization is mandatory - i.e. joint IP is also state IP, with the ensuing requirements for it.