**Lecture-6.** Protection of information systems and electronic information resources: goals, measures, organization procedure

**Learning Objectives**

By the end of this lecture, students should be able to:

1. Define the concept of information security in the context of IS and electronic information resources.
2. Identify goals and principles of protecting information systems (IS) and electronic information resources (EIRs).
3. Describe technical, organizational, and legal measures for ensuring information security.
4. Understand the procedures and responsibilities for organizing information protection in organizations.
5. Analyze practical examples of information security measures in electronic environments.

The protection of IP, EIR is understood as the implementation of a set of legal, organizational and technical measures aimed at the safety of IP and EIR, prevention of illegal and (or) unintentional access and (or) impact on them.

Those. EIR protection, - otherwise - and information security (IS) has the following aspects

- legal aspect;
- organizational aspect;
- technical aspect.

The legal aspect is the creation, availability and updating of legal acts both in the state and internal acts established by the owners / owners (regulations, etc.), which provide for the protection of EIR - i.e. information security (IS) issues.

Organizational aspect - ensuring the organization of the functioning and control by the owner / owner of IS, EIR over the implementation of the provisions of legal and internal acts on information security.

The technical aspect is the implementation of the legal and organizational aspect of information security through the use by the owner/owner of technical means of protecting information and information security in general.

EIR protection goals:

1) ensuring the integrity and safety of the EIR;
2) ensuring the confidentiality regime of EIR of limited access;
3) realization of the right of subjects to access the EIR;
4) prevention of unauthorized and (or) unintentional access, leakage and other actions in relation to EIR, as well as unauthorized and (or) unintentional impact on objects;
5) prevention of violations of the functioning of ICI objects and critically important objects of information and communication infrastructure.

Unauthorized and (or) unintentional actions in relation to informatization objects (IS, EIR, IKI, etc.) are:

1) blocking EIR, IS and (or) other objects of information and communication infrastructure, that is, the commission of actions leading to restriction or closing of access to EIR, IS and (or) other objects of information and communication infrastructure;
2) unauthorized and (or) unintentional modification of EIR, software, IS, etc.;
3) unauthorized and (or) unintentional copying of the EIR in whole or in part;

4) unauthorized and (or) unintentional destruction, loss of EIR in whole or in part;
5) use of the software without the permission of the copyright holder;
6) disruption of the IS and (or) software or disruption of the functioning of the telecommunications network.

EIR protection, etc. carried out:

1) in relation to EIR - by their owners, holders and users;
2) in relation to objects of information and communication infrastructure and critically important objects of information and communication infrastructure - by their owners or owners.

Those. the protection of the object does not imply the actions of users to protect information security.

Owners or owners of the objects of informatization of "electronic government" and critically important objects of information and communication infrastructure are obliged to take measures to ensure:

1) prevention of unauthorized access;
2) timely detection of facts of unauthorized access, if such unauthorized access could not be prevented;
3) minimization of adverse consequences of violation of the order of access;
4) prevention of unauthorized impact on the means of processing and transmission of electronic information resources;
5) prompt restoration of electronic information resources modified or destroyed due to unauthorized access to them;
6) immediately informing the National Information Security Coordination Center about the information security incident that has occurred, with the exception of the owners and (or) owners of electronic information resources containing information constituting state secrets;
7) information interaction with the National Coordinating Center for Information Security on monitoring the provision of information security of objects of informatization of "electronic government";
8) providing access to the National Information Security Coordination Center to the objects of informatization of "electronic government" and operational information security centers to critical information and communication infrastructure facilities for carrying out organizational and technical measures aimed at implementing information security monitoring in accordance with the rules for monitoring the provision information security of objects of informatization of "electronic government" and critically important objects of information and communication infrastructure.

The provisions of the uniform requirements in the field of information and communication technologies and ensuring information security related to the field of ensuring information security are mandatory for application by state bodies, local governments, state legal entities, subjects of the quasi-public sector, owners and owners of non-state information systems integrated with information systems state bodies or intended for the formation of state EIR, as well as owners and owners of main objects.

The acquisition of goods in order to implement the requirements for ensuring information security for the defense of the country and the security of the state is carried out from the register of trusted software and products of the electronic industry in accordance with the legislation of the Republic of Kazakhstan on public procurement. At the same time, in the absence of the necessary products in the register of trusted software and products of the electronic industry, it is allowed to purchase goods in accordance with the legislation of the Republic of Kazakhstan on public procurement.

The management of Internet resources and objects of information and communication infrastructure in emergency situations of a social, natural and man-made nature, the introduction of a state of emergency or martial law is carried out by an authorized body in accordance with the legislation of the Republic of Kazakhstan.

Protection measures:

- Legal measures to protect EIR, IP and information and communication infrastructure include:
  1) the requirements of the legislation of the Republic of Kazakhstan and the standards in force in the territory of the Republic of Kazakhstan in the field of informatization;
  2) liability for violation of the legislation of the Republic of Kazakhstan on informatization;
  3) agreements concluded by the owner or owner of the EIR, IS of the information and communication infrastructure, which establish the conditions for the operation, access or use of these objects, as well as responsibility for their violation.

Organizational measures for the protection of EIR, IP and information and communication infrastructure include the establishment and provision of an admission regime on the territory (to buildings, premises), where access to information, electronic information resources, information systems (electronic information carriers), as well as restriction access to EIR, IS and information and communication infrastructure.

Technical (software and hardware) measures to protect EIR, IS and information and communication infrastructure include:

1) the use of information security tools, and in relation to information constituting state secrets - exclusively with the use of information security tools constituting state secrets, developed, manufactured and (or) put into operation in accordance with the legislation of the Republic of Kazakhstan;
2) use of access control systems and registration of facts of access to EIR, IS and information and communication infrastructure;
3) development of a security task based on approved protection profiles to determine protection measures by the owners or owners of informatization objects.

The use of technical (software and hardware) measures to protect the EIR, IS and information and communication infrastructure should not cause harm or create a threat of harm to the life, health and property of individuals, as well as the property of legal entities and state property.

Owners and holders of IP who have received EIR containing personal data are required to take measures to protect them in accordance with the law and standards in force on the territory of the Republic of Kazakhstan. This obligation arises from the moment of receipt of EIR containing personal data, and until their destruction or depersonalization.

**Control Questions**

1. Define the concept of information protection for IS and EIRs.

2. What are the main goals of information system protection?

3. Describe at least three technical measures to secure electronic information.

4. What organizational measures help maintain information security?

5. Explain the role of legal measures in protecting electronic information resources.

6. How is risk assessment conducted in information security?
7. What are the responsibilities of employees in maintaining IS security?
8. Give examples of threats to electronic information resources.
9. Describe the procedure for organizing information protection in an organization.
10. How do confidentiality, integrity, and availability principles interrelate?

**Recommended Literature**

1. Stallings, W. (2021). *Computer Security: Principles and Practice*. 4th Edition. Pearson.
2. Laudon, K. C., & Laudon, J. P. (2020). *Management Information Systems: Managing the Digital Firm*. 16th Edition. Pearson.
3. Whitman, M. E., & Mattord, H. J. (2021). *Principles of Information Security*. 7th Edition. Cengage Learning.
4. Schneier, B. (2019). *Applied Cryptography: Protocols, Algorithms, and Source Code in C*. Wiley.
5. ISO/IEC 27001:2022. *Information Security Management Systems – Requirements*. International Organization for Standardization.