MODULE 2
ORGANIZATIONAL AND TECHNICAL MEASURES OF INFORMATION SECURITY PROVIDING

Theme 2.1 Information Security Levels

A set of interrelated elements, the functioning of which is aimed at ensuring the security of information, creates an *information protection system*. The scheme of information protection system building is demonstrated on Figure 2.1.

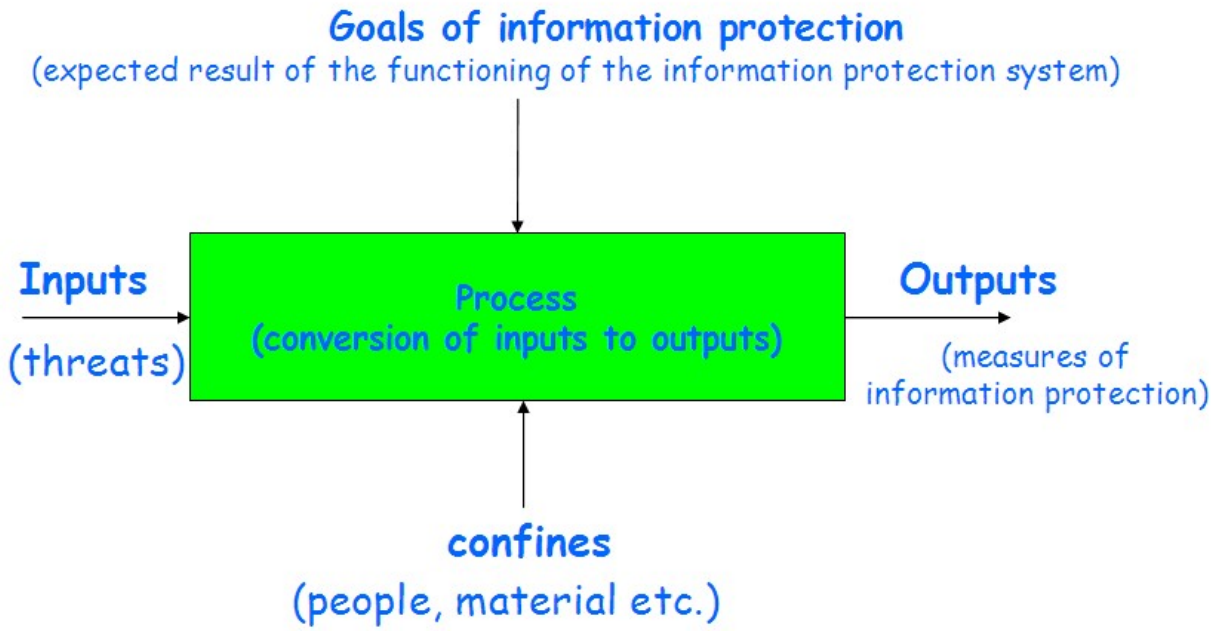

Figure 2.1 – Scheme of information protection system building

Analysis of possible threats is fixing the configuration of hardware and software, information processing technology and determining possible impacts on each component of the system.

Information protection system is a document containing a list of protected components and possible impacts on them, the purpose, rules for processing information, providing its protection against various impacts, description of the developed protection system.

The implementation of the protection system is the installation and configuration of security features necessary to implement the information processing rules fixed in the plan of protection.

Maintenance of the protection system is audit and adjustment of actions in the first three stages.

Methods of information protection are demonstrated on Figure 2.2. The presented methods determine the information security levels.

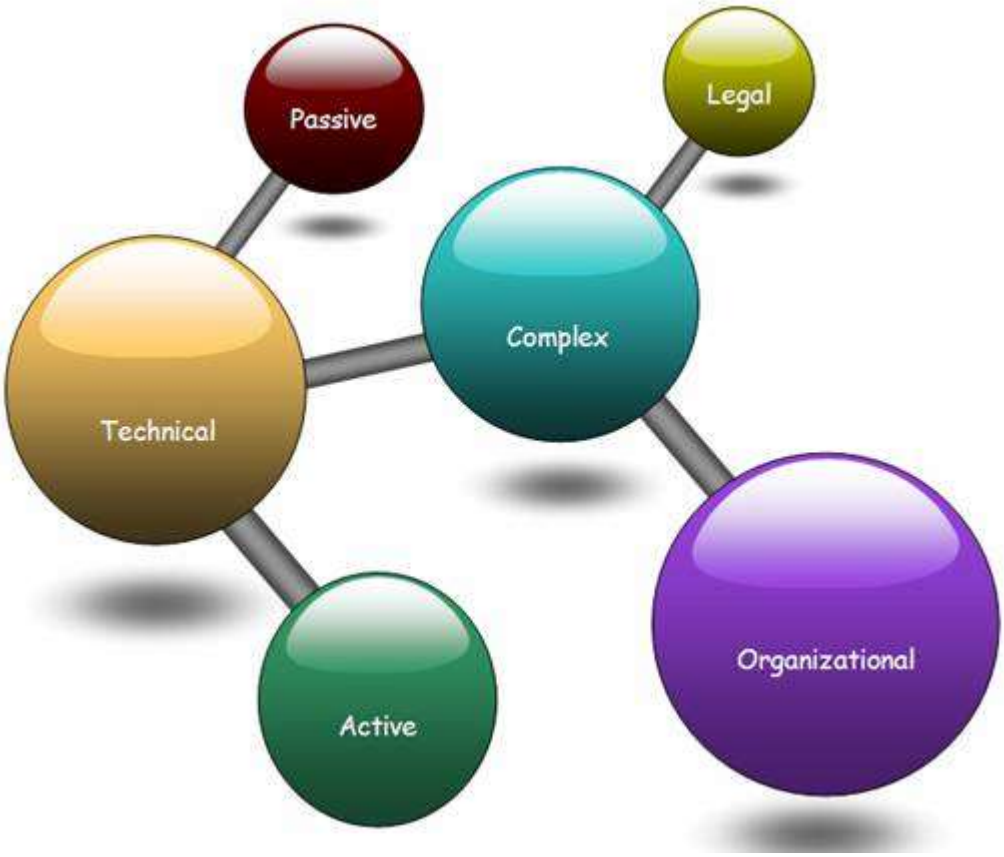

Figure 2.2 – Methods of information protection

Theme 2.2 Social Engineering Counteracting. Information Security Policy

The base ways of social engineering counteracting are built in the following principles.

1. All user passwords are the property of the company.
2. All employees should be instructed how to behave with visitors.
3. There should be a rule of correct disclosure of only really necessary information on the phone and during a personal conversation, as well as the procedure for checking whether the person who is requesting something is an actual employee of the company.

The indicated principles should be explained in such local document like information security policy.

Information security policy is developed on the base of standard ISO 27001. *A policy* is typically a document that outlines specific requirements or rules that must be met. In the information/network security realm, policies are usually point-specific, covering a single area. For example, an «Acceptable Use» policy would cover the rules and regulations for appropriate use of the computing facilities.

A standard is typically a collection of system-specific or procedural-specific requirements that must be met by everyone. For example, you might have a standard that describes how to harden a Windows 8.1 workstation for placement on an external (DMZ) network. People must follow this standard exactly if they wish to install a Windows 8.1 workstation on an external network segment. In addition, a standard can be a technology selection, e.g. Company Name uses Tenable Security Center for continuous monitoring, and supporting policies and procedures define how it is used.

A guideline is typically a collection of system specific or procedural specific "suggestions" for best practice. They are not requirements to be met, but are strongly recommended. Effective security policies make frequent references to standards and guidelines that exist within an organization.

The main types of information security policies are the following.

1. Ethics Policy.
2. Data Breach Response Policy.
3. Clean Desk Policy.
4. Password Construction Guidelines.
5. Password Protection Policy.
6. Email Policy.
7. Acceptable Use Policy.
8. Acceptable Encryption Policy.
9. Digital Signature Acceptance Policy.
10. End User Encryption Key Protection Policy.

11. Security Response Plan Policy.
12. Disaster Recovery Plan Policy.

Every policy contains the following chapters.

1. Purpose.
2. Scope.
3. Policy.
4. Policy Compliance.
5. Related Standards, Policies and Processes.
6. Definitions and Terms.
7. Revision History.

Theme 2.3 Engineering and Technical Means of Information Protection

Engineering means of information protection. Engineering means of information protection are engineering barriers and enclosures. *Engineering barrier* is an unit, changing the conditions of movement of the offender towards the protected object (Figure 2.3).

Figure 2.3 – Example of engineering barrier

Enclosures of the territory are engineering structures for the physical protection of an object or its individual sites from the intrusion of an attacker into a protected area (Figure 2.4).

Figure 2.4 – Example of enclosures of the territory

Engineering barriers and enclosures of the territory are characterized of resistance time – time, necessary to the overcoming them.

Depending on the purpose of the engineering barriers are divided into:

– main (Figure 2.5);

– additional (Figures 2.6, 2.7);

– precautionary (Figure 2.8).

Figure 2.5 – Example of the main engineering barrier

Figure 2.6 – Material for the additional engineering barrier

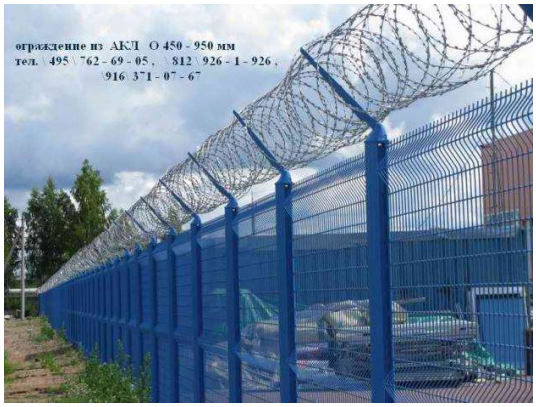

Figure 2.7 – Appearance of the main and additional engineering barriers

Figure 2.8 – Material for the precautionary engineering barrier

Technical means of information protection. *Information protection hardware* is a variety of electronic, electronic mechanical devices embedded in the

equipment of a data processing system or interfaced with it specifically to solve information security problems.

Purposes of information protection hardware:

– neutralization of technical information leakage channels;

– protection of information from interception;

– search for embedded devices;

– masking of a signal that is the carrier of information of limited distribution.

The hardware could include:

– noise generators;

– devices for erasing information from electronic media;

– electronic locks;

– blocks;

– signaling devices about attempts to unauthorized actions of users of the information network.

Noise generators. They are used to reduce the signal-to-noise ratio in the acoustic channel or the channel of secondary electromagnetic radiation by increasing the noise level.

Generators used to protect information from leakage through an acoustic channel:

– white noise;

– colored noise;

– receptive interference.

Generators are used to protect information from leakage through the channel of secondary electromagnetic radiation – generators of electromagnetic radiation.

Devices for erasing information from magnetic carriers:

– it is intended for instant non-recoverable erasure of information from a hard magnetic disk;

– it is used as a means of destroying confidential information when there is a danger of its leakage, disclosure, theft;

– it is housed in a metal non-separable casing;

– does not have an erasable storage of electrical communication information, does not affect its operation until erasure;

– the media for erasing is placed inside the device;

– the information in the device's camera is erased only when the command comes from the user;

– there are modifications to the external (as a separate device) and internal (embedded in a typical computer case) performance.

Electronic locks. Provide the following protection functions:

– identification and authentication of users;

– control the integrity of files and physical sectors of the hard drive;

– blocking the loading of the operating system from a floppy disk and CD-ROM;

– blocking the login of the registered user when he exceeds the specified number of failed login attempts;

– events that are relevant to the security of the system.

Identification of users is made on an individual key in the form of Touch Memory, having a memory of up to 64 Kbytes, and authentication – with a password up to 16 characters in length.

Blocks:

– they are designed to prevent the leakage of information of limited distribution through working mobile phones;

– they are used to maintain silence in premises where negotiations on mobile phones are prohibited;

– blocking can be performed both for the ranges of all mobile communication standards (CDMA-450, GSM-900, GSM-1800, 3G, 4G, 5G), so the ranges of the selected standards;

– acquisition and use is possible only after obtaining the permission of the relevant state authorities.

Signaling devices about attempts of unauthorized actions of users of the information network. These are devices that are connected to the equipment of the information network and are triggered in the event of an attempt to dismantle this equipment by persons who have not deactivated these devices.

Information protection software. Special software packages or individual programs included in the software of information systems to solve information security problems.

The main software tools for information protection include the following:

– programs for identification and authentication of users;

– programs for differentiating access to resources;

– programs to protect information resources from unauthorized modification, use and copying;

– antivirus software;

– audit program;

– programs to simulate work with the offender;

– cryptographic means of information protection.

Features of the use of hardware and software of information security in information networks. The peculiarities of using hardware and software information protection in information networks cause their advantages and disadvantages.

The advantages of hardware and software information protection in information networks include:

– wide range of tasks;

– high reliability;

– the possibility of creating advanced integrated information security systems;

– flexible response to unauthorized actions;

– tradition of the methods used to implement protective functions.

The main disadvantages of hardware and software information protection in information networks are:

– high cost of many means;

– the need for regular maintenance and monitoring;

– possibility of false triggering.

Criteria for choosing hardware and software for protecting information in information networks. The choice of remedies is based on the following criteria and requirements:

– the chosen system should provide a gain in time;

– validity of the choice;

– flexibility;

– ensuring the possibility of free copying of protected data by legitimate users;

– certification;

– eliminated the need for additional funds;

– independence from the hardware configuration of the computer.