Министерство образования и науки Республики Казахстан

Карагандинский государственный университет имени академика Е.А. Букетова

Факультет Физико-технический

Кафедра Радиофизики и электроники

**Рожкова Ксения Сергеевна**

**Тусупбекова Айнура Каиржановна**

**Курс лекций**

**по дисциплине «Information security in telecommunication systems»**

специальность: «5B071900-Радиотехника, электроника и телекоммуникации»»

Караганда 2018

**Лекция №1**

**Introduction**

**План лекции**

1. Goals and objectives of the discipline.

2. General information.

**1. Goals and objectives of the discipline.**

*The objectives of the discipline* are the disclosure of the essence and significance of information security and information protection, their place in the national security system, the definition of theoretical, conceptual, methodological and organizational bases for ensuring information security, the classification and characteristics of the components of information security and information protection, the establishment of interconnection and logical organization of the their components.

*The main objectives of the course* are:

• disclosure of the conceptual apparatus in the field of information security and information protection;

• disclosure of basic content provisions in the field of information security and information protection;

• disclosure of the modern doctrine of information security;

• defining the goals and principles of information protection;

• identification of factors affecting the protection of information;

• disclosure by methods of determining the composition of protected information, its classification by types of secrets, material carriers, owners and owners;

• establishment of the structure of threats to protected information;

• disclosure of directions, types, methods and features of the activities of intelligence agencies for obtaining confidential information;

• establishment and disclosure of the essence of information protection components;

• disclosure of the purpose, nature and structure of information security systems.

**Requirements for the level of content development discipline**

As a result of studying the discipline, students

**Must know:**

• a basic conceptual apparatus in the field of information security and information protection;

• types and composition of threats to information security;

• principles and general methods for ensuring information security;

• the main provisions of the state policy of ensuring information security;

• criteria, conditions and principles of referring information to the protected;

• types of carriers of protected information;

• types and subspecies of secrets of confidential information;

• types of vulnerability of the protected information and the form of its manifestation;

• sources, types and methods of destabilizing influence on the protected information;

• channels and methods of unauthorized access to confidential information;

• the composition of objects of information protection;

• classification of types, methods and means of information protection;

• composition of personnel, resource and technological information security.

**Must be able to:**

• identify threats to information security in relation to the objects of protection;

• determine the composition of confidential information in relation to types of secrecy;

• to identify the causes, circumstances and conditions for the destabilizing effect on the protected information from various sources of impact;

• identify the channels and methods of unauthorized access to confidential information in relation to the protection object;

• determine the directions and types of information protection, taking into account the nature of information and tasks to protect it;

• organize system security for information.

**2. General information**

In modern conditions, information plays a decisive role both in the process of economic development and in the competitive struggle in the markets. The influence of advanced scientific achievements covers almost the entire globe, and one can not ignore this reality. Aggravated on the basis of scientific and technological progress, competition still ruthlessly beats the laggards. The arena of intense struggle was competition for excellence in the market, in the most important areas of scientific and technological progress.

Under these conditions, industrial espionage becomes a reality as a sphere of secret activities for the acquisition, collection, analysis, storage and use of confidential information covering all areas of the market economy. Competition is a fierce struggle. It puts competitors in such harsh conditions that they are forced to act on the principle: "winners are not judged, the goal is above funds." The question is put unequivocally: either you, or you will be allowed around the world.

Unfair competition is carried out in the form of industrial espionage, corruption, organized crime, falsification and counterfeiting of competitors' products, manipulation of business reporting and, finally, by direct deception, plunder, material damage. Obviously, all types and methods of criminal acts of unfair competition are used depending on the object of malicious acts and the possibility of access to information objects.

To get any reliable information about objects of confidential interests by lawful means is almost impossible, because competitors maintain a certain system of protecting valuable information from unauthorized access by intruders. Thus, the word "unauthorized" accentuates that actions are committed in an illegal manner, bypassing ethical norms and protection systems in order to obtain confidential information for use in selfish purposes.

It is known that industrial espionage is conducted with the goal of conquering markets by throwing on it new products and products of higher quality and more economical perfect technology for their manufacture, as well as by discrediting and eliminating its competitors by any means and means. In the practice of industrial espionage objects of confidential interests are enterprises, organizations, firms, companies, banks, offices whose information, as potential competitors, is of considerable interest from the point of view of production analysis and production, scientific, trade-financial, intermediary and other activities, and also its products or services. Any information combining these areas is of great interest in terms of studying possible areas of commercial activity.

Thus, the protection of information is a multi-purpose program, among which are the organizational, legal, software and hardware, and engineering and technical protection of information. Organizational and legal protection of information is carried out by meeting the requirements and recommendations of legal documents. Software and hardware protection deals with the provision of computer facilities and automated systems from unauthorized access and cryptographic protection of information circulating in them. Protection of information using engineering structures and technical means is provided by engineering and technical protection of information.

Engineering and technical protection of information is objectively gaining more weight. This trend is due to the following reasons:

- development of methods and means of obtaining information that allow unauthorized access to an increasing amount of information at a safe distance from sources;

- the huge achievements of microelectronics, which contribute to the creation of a technical base for mass production of illegal means of obtaining information available to an ordinary buyer. The accessibility of miniature and camouflaged information retrieval equipment turns the task of illegally extracting information from a unique and risky operation into a profitable business, which increases the number of fans of easy gain by illegal actions;

- equipping office and residential premises, as well as cars with a variety of electrical and electronic equipment, the physical processes in which contribute to the uncontrolled transfer (leakage) of confidential information.

In recent years, the concepts of software, hardware and engineering protection are often combined under one term - technical protection.

Obviously, effective protection of information is possible only with a wide use of technical means of protection, i.e. in the created information security system, they must occupy a dominant position.

For the information security system, it is difficult to pinpoint the locations of the inputs and outputs. The inputs of any system are forces and influences that change the state of the system. Such forces and impacts are threats. Threats can be internal and external, including such difficult to localize as a weak legal discipline of employees, poor operation of information processing facilities or the presence of radio and electrical appliances in the room, the side physical processes in which contribute to the unauthorized dissemination of protected information. The sources of threats can be intruders, technical means within the organization, employees of the organization, internal and external fields, etc.

The outputs of the system are the response of the system to the inputs. The outputs of the system are measures to protect information. However, it is as difficult to localize the outputs of the system as the inputs. Therefore, the information security system is a model of a system that unites the forces and resources of an organization that provides information protection. It is described by the parameters shown in Figure 1.1.

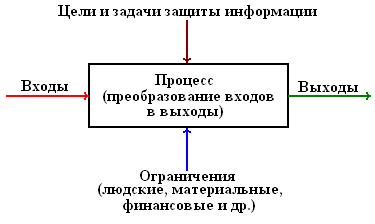


Fig. 1.1. Model of the system providing information security

The system parameters include:

• Goals and objectives (goals specified in space and time);

• inputs and outputs of the system;

• restrictions that must be taken into account when building (upgrading, optimizing) the system;

• Processes within the system that ensure the conversion of inputs to outputs.

**Goals** are the expected results of the functioning of the information protection system, and the **tasks** are what must be done to ensure that the system can achieve the goals set. The ability to solve problems depends on the **resource** allocated to the protection of information. The resource includes people who solve the tasks of protecting information, financial, technical and other means spent on protecting information. The ***inputs*** of the information protection system are threats to information, and ***outputs*** are measures that must be taken to prevent threats or to reduce them to an acceptable level. Actions, actions and technologies that define protective measures appropriate to threats form a ***process***.

Hence, we can conclude that it is very important to know the theoretical and practical basis of information security, at least in order to avoid "metered information injections."

The theory of information protection is defined as a system of basic ideas relating to the protection of information, giving a holistic view of the nature of the protection problem, the laws of its development and significant links with other branches of knowledge, formed on the basis of practical experience in solving defense tasks and determining the basic guidelines for improving the practice of protection information.

The components of the theory are:

• complete and systematic information on the origin, nature and content of the protection problem;

• systematic results of the analysis of the development of theoretical research and development, as well as experience in the practical solution of defense tasks;

• scientifically grounded statement of the task of information protection in modern processing systems, fully and adequately taking into account current and future concepts of building processing systems and technologies, information protection needs and objective prerequisites for their satisfaction;

• general strategic guidelines for the organization of information protection, taking into account the diversity of potential protection conditions;

• the methods necessary for an adequate and most effective solution of all protection tasks and containing both general methodological approaches to the solution and specific applied methods of solution;

• methodological and tool base containing necessary methods and tools for solving any set of tasks of protection in the framework of any chosen strategic installation;

• scientifically grounded proposals on the organization and provision of work to protect information;

• scientifically based forecast of the perspective directions of development of theory and practice of information protection.

*Information security* is determined by the ability of the state, society, personality:

• provide with a certain probability sufficient and protected information resources and information flows to maintain their livelihoods and vitality, sustainable functioning and development;

• resist information threats and threats, negative information impacts on the individual and public consciousness and psyche of people, as well as on computer networks and other technical sources of information;

• develop personal and group skills and skills of safe conduct;

• maintain a constant readiness for adequate measures in the information confrontation, by whomever it is imposed.

*Information war* - the actions taken to achieve information superiority in the interests of national military strategy, implemented by influencing the information and information systems of the enemy while simultaneously protecting their information information systems. Fig. 1.2 presents the directions and objectives of the protection of information and their relationship.

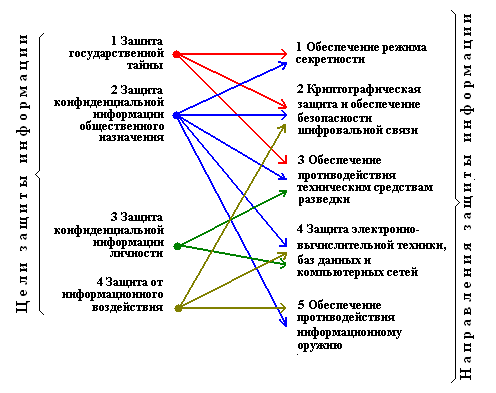


Fig. 1.2. Fundamentals of Information Security

The main purpose of protecting any confidential information is to prevent its illegal acquisition by competitors or intruders.

Foreign experience in the field of intellectual property protection and domestic experience in protecting state secrets shows that only complex protection can be effective, combining such areas of protection as legal, organizational and engineering.

The complex nature of the protection of information stems from the complex actions of intruders, seeking by any means to obtain important information for competition. Here it is legitimate to say that the weapon of defense must be adequate to the weapon of attack.

Based on the foregoing, it can be concluded that information security is a complex and multifaceted problem, the solution of which is well-organized and well-prepared.

As for the approaches to implementing protective measures to ensure the security of information systems, a three-stage (three-stage) development of such measures has taken shape.

*The first stage* - the development of requirements - includes:

• determination of the composition of the information system (IS);

• analysis of vulnerable IP elements;

• assessment of threats (identification of problems that may arise due to the presence of vulnerable elements);

• risk analysis (predicting the possible consequences that these problems can cause).

*The second stage* - the definition of protection methods - includes answers to the following questions:

• what threats should be eliminated and to what extent?

• which system resources should be protected and to what extent?

• by what means should protection be implemented?

• what should be the total cost of implementing the protection and the costs of operation in the light of potential threats?

*The third stage* is the definition of functions, procedures and security measures implemented in the form of some protection mechanisms.

**Лекция №2**

**Terminological basis of information security. Basic concepts and definitions**

**План лекции**

1. The concept of information, information, information systems.

2. The concepts of the author and the owner of information, the interaction of subjects in the information exchange.

3. Protection of information, secrecy, means of information protection.

**1. The concept of information, information, information systems**

Informatization is the organizational socio-economic and scientific-technical process of creating optimal conditions for satisfying information needs and realizing the rights of citizens, state authorities, local governments, organizations, public associations on the basis of the formation and use of information resources.

Informatization is based on national information resources and is provided through information systems and telecommunication networks. The emergence of telecommunications networks has created technical prerequisites for the development of information systems that use communication resources to provide access to information resources. Thus, information systems and networks, communications, information transfer and telecommunications constitute the informatization infrastructure. The components of the informant are shown in Fig. 2.1.

In the most general form, when solving the problem of satisfying the information need, it is necessary to keep in mind three components: the person (the consumer of information), who formulates his tasks; an information fund (information resource) in which the information necessary to the person is concentrated, and the corresponding device, which is the intermediary between the consumer and the information array. This device is called an information system.

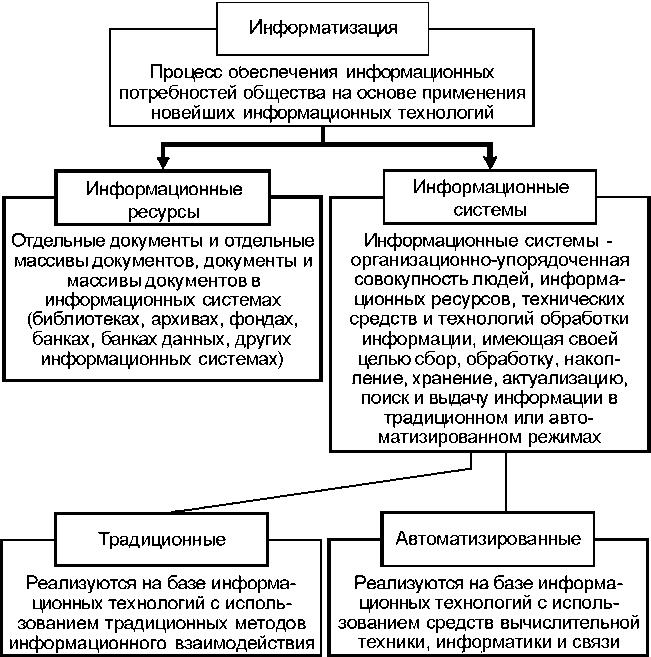


Fig. 2.1. Informatization components

The information system, like any other, has a certain structure, composition, specialists, facilities, equipment and order of operation; The structure of the information system is shown in Fig. 2.2.

The information system is an organizationally ordered set of information resources, technical facilities, and technologies that implement information processes in a traditional or automated mode to meet the information needs of users.

The initial material basis of the information system is information resources. Information resources are understood as documents and arrays of documents in different forms and types (libraries, archives, funds, databases, knowledge bases, as well as other forms of organization, storage and retrieval of information) containing information on all areas of society.

Information resources can be fixed and non-fixed. Fixed information resources are information fixed on some physical medium, and non-fixed information is knowledge that people (scientists, specialists, workers) own, who somehow participate in social production and are able to transfer this knowledge to other participants in the production process or criminal aspirations .

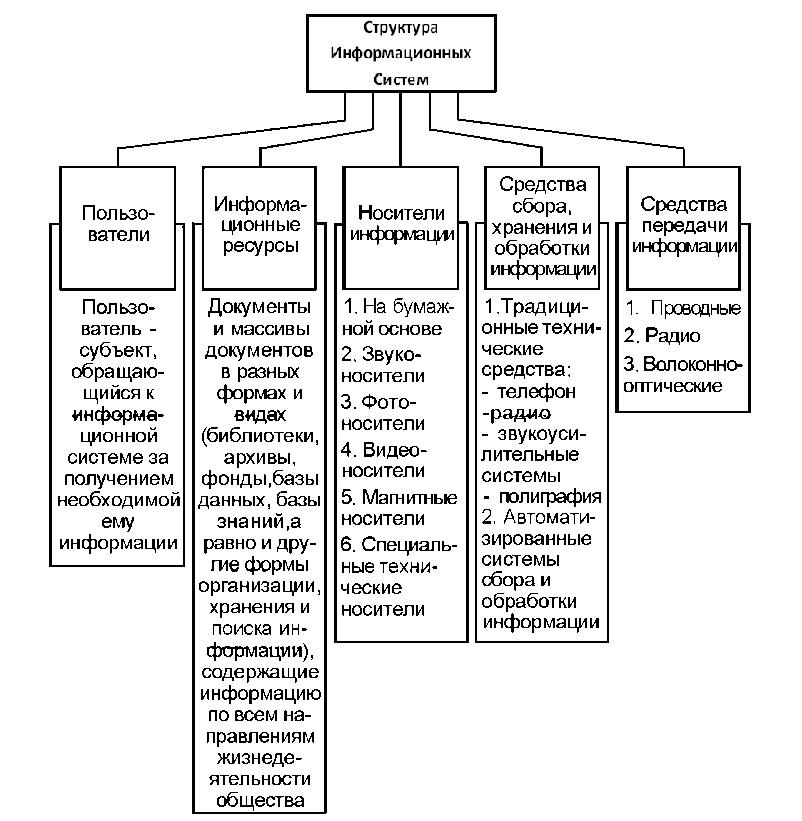


Fig. 2.2. Structure of the information system

The information system is the functional basis of any information system. Information processes are understood as a set of interrelated and interdependent processes of identification, analysis, input and selection of information, issuance by means of various means to its consumer for making managerial decisions.

**2. The concepts of the author and the owner of information, the interaction of subjects in the information exchange.**

***Forms of ownership of information. The concepts of the owner, owner, owner, confidant and counterparty information.***

Information resources can be state and non-state and as an element of the property are owned by citizens, state authorities, local governments, organizations and public associations.

At the same time, individuals and legal entities are the owners of those documents, sets of documents that are created at the expense of their funds, acquired by them on legal grounds, received as a gift or inheritance.

*The owner of information resources*, information systems, technologies and means of their provision is the entity fully exercising the powers of possession, use, disposal of the said objects.

*The owner of information resources*, information systems, technologies and means of their provision is the entity that exercises possession and use of these objects and implements the powers of disposal within the limits established by the Law.

*The user (consumer) of information* is the entity that accesses the information system or the intermediary for obtaining the information that is necessary to it and using it.

The owner of information resources enjoys all the rights stipulated by the legislation of Kazakhstan, including he has the right:

• appoint a person who conducts economic management of information resources or their operational management;

• establish, within its competence, a regime and rules for processing, protecting information resources and access to them;

• determine the conditions for the disposal of documents when copying and distributing them.

*The holder of information* constituting a commercial secret - a person who owns information constituting a commercial secret, on a legal basis, has restricted access to this information and has established a regime of commercial secrecy regarding it. The counterparty is a party to a civil law contract, to which the holder of information constituting a trade secret transmitted this information.

***Holders and counteragents (confidential) of commercial secrets.***

The holder of information constituting a commercial secret - a person who owns information constituting a commercial secret, on a legal basis, has restricted access to this information and has established a regime of commercial secrecy regarding it.

The counterparty is a party to a civil law contract, to which the holder of information constituting a trade secret transmitted this information.

The holder of information constituting a trade secret has the right:

1) to establish, amend and cancel in writing the regime of commercial secret in accordance with the law and the civil-law contract;

2) use information constituting a commercial secret for their own needs in an order that does not contradict the legislation of the Republic of Kazakhstan;

3) to permit or prohibit access to information constituting a commercial secret, to determine the procedure and conditions for access to this information;

4) to introduce into commercial circulation information constituting a commercial secret, on the basis of contracts providing for the inclusion in them of conditions for the protection of the confidentiality of this information;

5) require legal entities and individuals who have obtained access to information constituting a commercial secret, public authorities, other state bodies, local self-government bodies that are provided with information constituting a commercial secret, compliance with obligations to protect its confidentiality;

6) to demand from persons who have obtained access to information constituting a trade secret as a result of actions taken accidentally or by mistake to protect the confidentiality of this information;

7) to protect in the manner prescribed by law their rights in the event of disclosure, illegal receipt or illegal use by third parties of information constituting a trade secret, including demanding compensation for damages caused in connection with violation of his rights.

The number of mandatory measures to protect the confidentiality of information taken by its owner includes the regulation of relations on the use of information constituting a commercial secret, either by employees on the basis of employment contracts or by contractors on the basis of civil law contracts.

The counterparty is obligated to compensate the owner for losses when disclosing the trade secrets handed to him under the contract.

The owners of commercial secrets may be physical (regardless of citizenship) and legal (commercial and non-profit organizations) persons engaged in business activities who lawfully possess information constituting their trade secret, have restricted access to this information and have established in relation to it a regime of commercial secrecy .

Confidential commercial secret is a person who, on the basis of an employment contract (employees), civil contract (counterparties) or because of his official position or performance of professional duties not related to the state or municipal service, or on other legal grounds, the commercial secret of another person is known .

The common feature for them is that commercial secrets are secondary to them (transmitted by the owner of a trade secret) and they do not have an actual monopoly on this information, but are only obliged by law or treaty to provide a regime for its confidentiality.

On this basis, based on the practice of relations arising from the trade secret, four categories of persons can be distinguished among confidential confidants: employees, counteragents, authorities and their officials, and other persons.

*Employees* are persons who are in labor relations with the owner of a trade secret and who have access to trade secrets under an employment contract (contract). An employee acquires the status of a confidential commercial confidentiality either from the moment the employer receives his informed consent received during the term of the employment contract or from the conclusion of an employment contract containing such employee obligations as working conditions in the organization.

*Counterparties* are persons engaged in entrepreneurial activity, to whom the owner of a trade secret has transferred this information on the basis of a civil law contract. The counterparties receive a legal opportunity to access the commercial secret of another person and acquire the status of confidentiality of commercial secrets from the moment of signing a written civil contract with the owner (contract agreement, license agreement, commercial concession agreement, etc.). The agreement should specify the conditions for protecting the confidentiality of information, including in the case of reorganization or liquidation of one of the parties to the contract in accordance with civil law, as well as the contractor's obligation to recover damages if this information is disclosed to him contrary to the contract.

*Other persons* are persons to whom the owner of the trade secret has transferred this information due to the performance of their professional duties not related to the state or municipal service (auditors, lawyers, notaries, translator, executor of the will, insurers, insurance organizations, mutual insurance companies, insurance brokers, insurance actuaries, electric and postal organizations, their officials and other persons and employees, private detectives, editorial offices of the media, arbitration courts and other persons who are aliens I have a secret becomes known in the performance of their professional duties legally).

***Owners and owners of information classified as official and professional secrets.***

The owner of information constituting an official secret is, as a rule, an organization that has established a list of information classified as confidential, in which the person who has access to this information works. To the official secret, as we found out, there are two categories of information:

• information that represents "public secrets" for the state authorities and municipal government and subordinate enterprises, institutions and organizations,

• Information on the activities of public authorities and municipal government and subordinate enterprises, institutions and organizations: the Government, customs authorities, tax authorities, state forensic institutions).

Each of these categories has different owners and owners.

The owner of information constituting a professional secret is a citizen who has entrusted information to a doctor (medical secret), a notary (notarial secret), a lawyer (a lawyer's secret), a bank (bank secrecy), etc.

**3. Protection of information, secrecy, means of information protection.**

The second component of the essence of information protection - the way to implement the content part - in explanatory dictionaries, as already noted, is presented as a process or as a combination of methods, tools and activities.

Information protection includes a certain set of methods, tools and activities, but to limit the way of implementation only this would be wrong. The protection of information must be systematic, and the system in addition to methods, tools and activities includes other components: protection objects, protection bodies, information users. At the same time, protection should not be something static, but a continuous process. But this process is not carried out by itself, but occurs as a result of people's activities. Activity, by definition, includes not only the process, but also the goals, means and result. The protection of information can not be aimless, ineffective and carried out without the aid of certain means. Therefore, it is the activity and should be a way to implement the content of the protection.

By combining the content part of information protection and the way of realizing the content part, we can formulate the following definition:

**Information security** - activities to prevent the loss and leakage of confidential information and the loss of protected public information.

Given that the definition should be concise, and the term loss and leakage of protected information absorbs all forms of vulnerability of a confidential and protected part of public information, we can confine ourselves to a more concise definition, subject to its differentiated refraction in practical work: **information protection** - prevention of loss and diversion protected information.

And now we will analyze the definition of this concept, contained in GOST R50922-96 "Information protection: Basic terms and definitions", since this definition is official, having a semantic meaning of a binding nature. It is formulated as follows: Information security - activities to prevent the leakage of protected information, unauthorized and unintentional impacts on the protected information.

As you can see, this definition coincides with the one proposed by the way of realizing the content part of the protection and by one of its components - preventing the leakage of the protected information.

Differences:

1. The definition of leakage in GOST is given differently - it is not formulated separately, but is embedded in the definition of the term Protection of information from leakage, which reads as follows:

Protection of information from leaks: activities to prevent uncontrolled dissemination of protected information from its disclosure, unauthorized access to protected information, and from the receipt of protected information by foreign intelligence services. This definition implies that the leakage of information is the uncontrolled spread of protected information.

Uncontrolled dissemination can be equated with the meaning of an illegal release of information beyond the protected zone of its operation or the established circle of persons. But if in the proposed AI. Alexensev's definition of leakage further denotes the result of such an exit - the receipt of information by persons who do not have authorized access to it, then in the standard, uncontrolled proliferation is already the result to which disclosure, intelligence information and unauthorized access to it result. Those, in the first case, uncontrolled distribution leads to unauthorized receipt, in the second case, all the way around.

2. Disclosure, unauthorized access to information and its receipt are put on one line.

A) Unauthorized access to information can lead to its disclosure and receipt? If not, how does it affect uncontrolled dissemination of information? Only as an opportunity with his help to steal her. But the theft in the end again leads to information.

B) Disclosure of information leads to its obtaining by foreign intelligence services and not only by them.

Such confusion in the GOST is caused by the fact that concepts with different meanings are put on the same board: the form of manifestation of the vulnerability of the protected information (disclosure), the mechanism for obtaining information (unauthorized access), and the result of uncontrolled dissemination of information (intelligence).

On the second component of the content part of information protection, proposed by AI. Alexentsev, and the guest definition differ both in wording and in substance:

A.I. Alexentsev is the prevention of loss of protected information,

In GOST - prevention of unauthorized and unintended impacts on the protected information. Thus, if in the first part of the definition of the content part of GOST calls the type of information vulnerability (leakage), in the second - not the kind (loss), but the impacts that can lead to this kind of vulnerability. Of course, loss can not happen without unauthorized or unintended impacts on information, but why do we need a different approach to identifying the two types of information vulnerability, why one is called, the other is implied?

In part, this is probably due to the fact that the results of the impact on GOST information do not reduce only to its loss. This is evident from the interpretation of the concepts of unauthorized and unintentional influences on information.

The GOST refers to the unauthorized impact on the protected information in violation of the established rights or rules for changing information, leading to distortion, destruction, copying, blocking of access to information, as well as loss, destruction or malfunction of the information carrier.

Unintentional impact is defined by GOST as an impact on the protected information of user's errors of information, failure of technical and software tools of information systems, as well as natural phenomena or other non-targeted changes in information related to the operation of technical means, systems or activities of people leading to distortion, destruction , copying, blocking access to information, as well as loss, destruction or malfunction of the information carrier.

Thus, the result of the impact on the information or its carrier is both the type of vulnerability (loss) and the forms of vulnerability (distortion, destruction, blocking), and the mode of action (copying). If in this case copying replaces theft, then this is not true, because there are other methods of theft. In addition, it is unclear what is the point in determining the concept of separating the information carrier from the information itself, as the resulting loss and destruction of the media (without taking into account the illegitimacy of placing them in a single row) are simultaneously the loss and destruction of the information reflected in them, and the failure of the carrier leads to the blocking of information.

Thus, the definitions of A.I. Alexentsev more logical.

The concept of information security is closely related to the notion of information security.

The term information security has a double meaning, it can be interpreted:

• and how the security of information itself,

At the same time, the security of information itself does not fit into an unambiguous understanding. On the one hand, this can mean the security of information in terms of the initial completeness and reliability of information (ie, security in terms of content), on the other hand, the security of the established status quo information (security in terms of the form of information).

• and as a lack of threats on the part of information to the subjects of information relations.

In regulatory documents and literature, information security is considered only in terms of its security, and this is probably justified in the presence of the term information security.

There are several definitions of the concept of information security. General approach: information security as a state of protection (or protection) of information. This is not objectionable, for the very term security means no danger, which in some way corresponds to the term state of security.

But the definitions are significantly different between the content part - security from what. This includes:

• from internal and external threats; (unclear)

• from leakage, theft, loss, unauthorized destruction, distortion, modification (forgery), unauthorized copying, blocking of information, etc .; (the types and forms of vulnerability are confused);

• against accidental or deliberate unauthorized influences on information or unauthorized receipt thereof;

• against accidental or deliberate access of persons not entitled to receive information, disclosure, modification or destruction, etc.

The second part of AI's definition. Alexentsev formulated as follows:

• and how from the impacts that violate its status,

• and both from loss and leakage, because in the end they express the same thing, because prevention of loss and leakage of information is carried out by preventing destabilizing effects on information. The first option is more preferable, because the immediate goal of information security is to counteract destabilizing influences.

Thus, the security of information is the state of protection of information from impacts that violate its status.

From the definitions of concepts, **information protection** and information security follows the relationship between them: the protection of information is aimed at ensuring the security of information or, in other words, the security of information is provided by means of its protection (information security is the result of its protection).

**Mystery** is a concept that has several semantic meanings.

1. In the general understanding, the mystery is treated as something unsolved, yet unknowable. For example, expressions such as "secrets of nature", "secrets of the universe", etc., are used, while those are the phenomena, the essence of which the human mind has not yet comprehended. Mystery is seen as an **objective category** - as a mystery of nature. This type of mystery includes unknown phenomena, laws of nature, thinking, society.

2. In the case of bodies of state power and administration, secret means what is hidden from others, which is known to a strictly defined circle of people. In other words, those information that are not subject to disclosure and constitute a secret. Here the mystery - **the subjective category** - is information that some subject (in its broad sense) considers necessary to hide from others. If the subject-an individual establishes for himself that this fact will not be told to anyone, for example, he will not tell anyone about it, he has classified this information for himself. Or a group of conspirators plotting to commit some actions that can be successful only if their conspiracy (for example, a coup d'état) is not known to anyone until the moment of its implementation.

The division of secrecy into subjective and objective is to some extent conditional. The main criterion for this division is who establishes what is a secret. The subject, who established that this information is, for example, a state secret, at any time can declassify it. Mystery as an objective category is also subjective in some measure, as it is not known by mankind as a subject of knowledge. But "to declassify" this mystery humanity can only when these phenomena, the laws of nature will be known and open.

Thus**, the secret (in the field of information protection) is a subjective category, when information about certain events, phenomena, and subjects is hidden for some reason by the owner (owner) of information from unauthorized persons.**

Preservation of information in secret, possession of secrets gives certain advantages to the party that owns them.

Information constitutes an official or commercial secret in the case,

• when the information has actual or potential commercial value due to its unknown to third parties,

• It is not freely accessible on a legal basis and

• the information owner takes measures to protect its confidentiality.

Information that can not constitute an official or commercial secret is determined by law and other legal acts.

Using this definition, we can formulate **general signs of secrecy**:

1. Information has real or potential value for the holder because of its unknown to third parties. Such persons can be states, legal entities or individuals.

2. Information is not freely accessible on legal grounds. The possibility of keeping it unknown to third parties is established by law.

3. The holder of information shall take measures to protect its confidentiality (secrecy).

In accordance with common signs, state secrets are determined by the following clarifying signs:

1. Who owns the information? - The state.

2. How great is the value of information for the state? - Information constituting a state secret has real or potential value for its owner - the state due to its obscurity for third countries, legal entities and individuals. The information is very valuable. The dissemination of this information can damage the security of the state.

3. Is it possible to restrict access to information on a legal basis? - Yes. This information is not freely accessible in accordance with the Law "On State Secrets", which lists the information that constitutes a state secret.

Are measures taken to protect the secrecy of information? - Yes. There is a real system for protecting state secrets.

It is necessary to emphasize once again that the main sign of **state secrets** is the presence of damage to the security of the state when disseminating information constituting this secret.

Similarly, a definition of other types of secrets can be given. For example, for official secrets, its features are:

1. The state is also the owner of information.

2. Information is valuable because of its uncertainty. However, the amount of damage from its open distribution does not go to the level of damage to the security of the state. The dissemination of such information can damage the activities of individual government bodies, local governments, enterprises and organizations that perform work for the order of these bodies.

3. Access to information is limited on a legal basis by a decision of the state authorities and local self-government.

4. Bodies of state power, local self-government, enterprises and organizations take measures to protect information classified as official secret.

**Information security means** is a set of engineering, electrical, electronic, optical and other devices and devices, devices and technical systems, as well as other items used to solve various tasks to protect information, including preventing leakage and ensuring the safety of the protected information.

The practice of using technical means of information protection has developed the basic requirements for them, regardless of technical capabilities and applications:

• state of constant alert;

• high probability of detection of attempts of unauthorized penetration to the object, to the carriers of protected information;

• high survivability and hardware reliability;

• low power consumption;

• overall dimensions that provide maskability and low visibility of technical means of information protection;

• minimal maintenance costs.

As the basis for classification of information protection tools, we list the **main groups of tasks** solved with the help of technical means:

1. Creation of physical (mechanical) obstacles to the penetration of an attacker to information carriers (grids, safes, locks, etc.).

2. Identification of attempts to penetrate the object of protection, to the places of concentration of the carriers of the protected information (electronic and electronic optical signaling devices).

3. Warning of emergency situations (fire, flood, etc.) and liquidation of PE (fire fighting equipment, etc.).

4. Maintain communication with various units, premises and other points of the security object.

5. Neutralization, absorption or reflection of radiation of operated or tested products (screens, protective filters, separation devices in power networks, etc.).

6. The introduction of technical intelligence into confusion (misinformation) regarding the true location of the protection object and its functional purpose.

7. Comprehensive verification of the technical means of processing information and allocated premises for compliance with the safety requirements of the processed voice information to the established norms.

8. Comprehensive information protection in automated data processing systems using filters, electronic locks and keys to prevent unauthorized access, copying or misrepresentation of information.

Knowledge of the possibilities of the methods and means of information protection that can be considered allows them to be actively and comprehensively applied when considering and using legal, organizational and engineering measures to protect sensitive and confidential information.

**Лекция №3**

**General methodological principles of the theory of information security.**

**План лекции**

1. Principles of information security. General information.

2. Requirements for the information security system.

3. Structure of the information security system.

**1. Principles of information security. General information.**

**Principles of information protection** are the basic ideas, the most important recommendations for the organization and implementation of this activity at various stages of solving the tasks of securing secrets. They are taken into account when creating a regulatory framework for the protection of information, and even more - are laid down as norms in laws and by-laws and, therefore, acquire a binding character for the performers.

These principles are developed by the long practice of organizing work to protect information in our country, taking into account international experience.

Principles of information protection can be divided into three groups: legal, organizational and used to protect information from the TCP and computer facilities (CBT).

***Legal principles of information protection***

The main legal principles of information protection, according to AA. Shiversky, are the following:

**1. The principle of legality**. In the framework of the existing existence of a law-based state, the activities of enterprises and organizations of all forms of ownership, all officials and citizens must be carried out within the framework of existing laws.The principle of legality in the field of information protection is expressed, first of all, in the need for regulatory and legal regulation of this important area of public relations in the state. Legislation should be:

• the rights of various subjects in the field of information protection, the secrecy of information and the establishment of rules for its protection;

• it is determined that it is a state, commercial, other secret protected by law;

• criminal, administrative, material, moral responsibility for unlawful attempt on the protected information and disclosure or transmission of such information to someone, as a result of which harmful consequences for the owner (owner) of information have occurred or could occur.

On the other hand, officials and other employees of enterprises and institutions who are entrusted with secrets in service or work, in accordance with applicable laws and by-laws, must be given rights that allow them to successfully protect confidential and classified information entrusted to them and must To impose duties on observance of the corresponding established regime, the fulfillment of which ensures the safety of information.

**2. The principle of the priority of international law over the domestic law.** Kazakhstan, as a successor to the commitments undertaken by the former Soviet Union, also recognizes the principle of the priority of international law over the internal. In particular, our country has undertaken at the Vienna meeting the obligation to bring its domestic legislation into line with the provisions of the international conventions and agreements to which it is a party. Hence it follows that the object of secrecy can not be information that our state promulgates or reports under conventions and agreements, because it becomes a member of the world economic community, joined the IMF and other international economic organizations. One of the conditions for membership in these organizations is to provide information on the real state of affairs in the national economy.

This does not exclude that Kazakhstan as a sovereign state can and should classify and protect information related to those areas of its activities that ensure its national security. Each state has the right to decide that it will be classified and what to open. However, reciprocity and equality in national secrets between states or coalitions of states will promote the development of mutual trust.

**3. The principle of equal secrecy** will help to strengthen confidence measures in international relations, help to eliminate the asymmetry of the regime restrictions that have prevailed in different countries. The excessive desire to conceal information from the other side always causes suspicion, since such actions are usually associated with the unkind intentions of one side in relation to the other.

**4. Principle of ownership and economic feasibility.** Radical changes taking place in Russian society could not but affect the underlying economic reform of property relations. A number of laws were adopted regulating the sphere of property relations, property relations, including those related to the regulation of intellectual property rights, the possession and disposal of information, and the protection of information.

This gave owners of information, intellectual property rights the right to take measures to protect them through various legal mechanisms, including through patents, copyright norms, commercial secrets. Only the owner (owner) of the information has the right to determine what information should be classified and to what extent and protect it as a state or commercial secret, or to patented and protected with a patent and to pay for the protection of any protected information.

Secrecy should be evaluated as a consumer property and its value should be included in the price of the product produced, at the expense of which the owner will implement measures ensuring secrecy. Secrecy should be an economic category, and its observance in a market economy is a matter for the owners of secrets, industrial or banking secrets, which themselves must evaluate the degree and duration of the secrecy, taking into account the received or lost profit. In the field of protection of state secrets, there are other (political, military, etc.) factors in solving information security problems.

***Organizational principles of information protection***

Organizational principles have undergone significantly fewer changes in recent years, compared to legal ones. This is due to the fact that they reflect the generally inherent rules, approaches to protecting secrets. They are used and "work" under any socio-political and economic system and in the protection of any type of protected information: state or commercial secrets.

**1. Scientific approach to the organization of information protection.**

The nationwide system of information protection functioning in our country is created taking into account the available volumes of protected information and the means, traditions and experience used in its field for protecting state secrets accumulated in previous decades. The creation of such a system required a scientific understanding of such problems as:

• delineation of competence in the field of state secrets protection throughout the hierarchical ladder of numerous bodies and organizations and protection of trade secrets;

• scientific and legislative definition of the concepts "state" and "commercial secrets", "official secrets", "personal data", etc .;

• development of scientific criteria for determining the degree of secrecy of information, etc.

Scientific research of problems of information protection uses **scientific methods.** Thus, **a comprehensive and systematic approach** to the organization of information security presupposes:

• **on the one hand**, the identification and analysis of possible channels for leakage of protected information, taking into account the amount of such information and carriers on which it accumulates and its importance;

• **on the other hand**, the competitor's ability to collect and retrieve protected information not in general, but in each specific case with respect to a particular enterprise, institution, industry or problem, is studied and analyzed.

**The system approach** allows creating an organically interrelated set of forces, means and special methods for the optimal restriction of the sphere of circulation of classified information, prevention of its leakage.

When creating an information security system and implementing measures to protect secrets from disclosure or newer TCP, it is important to provide comprehensive comprehensive protective measures aimed at preventing the leakage of information from the sphere of its circulation.

**2. Maximum restriction of the number of persons admitted to protected information.** The main meaning of this principle is that the security of classified information depends on the number of persons admitted to treatment with it. The narrower this circle, the higher the probability of keeping this information secret. Organizationally, this principle is solved in the following way: persons who have, firstly, a corresponding permission in the form of an admission, and secondly, from the number of persons having access, who have been authorized to work with specific information in the form of access, which is obtained only by those who are directly connected to work with this information.

A peculiar manifestation of this principle is also possible fragmentation of the technological chain of production of a product, a product for individual operations, knowledge of one of which does not allow to restore the entire technology. Each of the operations is classified independently and the transfer of a specialist from one operation to another or in general is impossible, or requires special admission and, therefore, consideration of the question - what is the purpose of this, if it is initiated by the employee.

**3. Personal responsibility for the safety of trusted secrets.** This principle works well if each employee admitted to the protected information understands and realizes that the secrecy of this information is in its own interests. If the employee sees that the preservation of some information is in secret only to the enterprise or the state, and he personally does not give anything, then he will treat it formally. Only the burden of fear of responsibility will weigh on him.

An important factor that increases the responsibility of employees for retaining the secrets entrusted to them is the training in rules for the protection of classified information and the rules for handling confidential documents.

**4. Unity in solving industrial, commercial, financial and regime issues.** In this principle, one of the manifestations of an integrated approach to the organization of information protection is laid, which, however, has a relatively independent significance. Knowledge and consideration of this principle is that those who make decisions about classifying information, who are sick more, of course, for solving production, financial, marketing and other similar tasks, should not forget and overlook the need for simultaneous solutions and regime issues, there , where necessary.

**5. Continuity of information protection.** This principle is that the protection of confidential or confidential information should begin from the moment of its appearance (receipt, creation, generation) at all stages of its processing, transmission, use and storage, up to the stage of its destruction or declassification.

***Principles used in the protection of information from technical means of intelligence.***

In the organization of activities to protect information from technical reconnaissance (TCP) and computer hardware (CBT) are guided, above all, by the same **organizational and legal principles**, as discussed above. This is due to the fact that these principles are quite general and universal. These principles "work" regardless of where, when and by whom information protection is carried out.

However, there are specific principles, due to the specific features of the object of defense, i.e. carriers on which the protected information is displayed, used for this force, means and methods, as well as means and methods of obtaining the protected information by the opponent using TCP.

**1. Principles of information protection used in the organization of counteraction to TCP:**

• the activity of information protection - is expressed in the purposeful imposition of false intelligence on the object of its intelligence aspirations, in accordance with the concept of protection;

• the credibility of information protection - consists in the justification of the design of protection of the conditions of the situation in accordance with the nature of the protected object or the properties of the environment, in the application of technical protection solutions appropriate to climatic, seasonal and other conditions;

• Continuity of information protection implies organization of object protection at all stages of its life cycle: pre-project, project, during development, manufacturing (construction), testing, operation and disposal;

• a variety of information security - provides for the exclusion of the template, the repeatability in the selection of the cover object and ways to implement the meaning of protection, including with the use of standard solutions.

**2. Principles of information protection used in CBT.** The main principles of information protection, which have a specific nature and are used in the organization of information security in SVT, are, in A.A. Shiversky, the following:

• introduction of redundancy of system elements,

• redundancy of system elements,

• Protective data transformations,

• control of the status of the elements of the system, their operability and correct functioning.

**Under the introduction of the redundancy of the elements of the system** is meant the inclusion of additional components beyond the minimum that is necessary for the fulfillment of all the set of its functions. Excessive elements function simultaneously with the main ones, which makes it possible to create systems that are stable with respect to external and internal destabilizing factors and impacts. Distinguish redundancy organizational, hardware, software and algorithm, information, and others.

**Protective data transformations, monitoring of the state of the system elements, their operability and correct functioning** will be considered below.

Not all the elements of the information protection system **are reserved**, but especially important computer subsystems, so that in the event of some extraordinary circumstances, they can be used to solve the problems facing the system.

**2. Requirements for the information security system**

Any information security system has its own characteristics and at the same time must meet the general requirements. The most common requirements for the information security system are the following.

1. The system of protection of information should be presented as a whole. The **integrity** of the system will be expressed in the presence of: a single goal of its functioning, information links between the elements of the system, hierarchy of the construction of the information system management subsystem. No part of it can be withdrawn without damage to the entire system.

2. The information protection system should provide:

• information security,

• media and

• protection of the interests of participants in information relations.

3. The information protection system should provide **information links** within the system between its elements, ensuring their coordinated functioning, and links with the external environment, before which the system manifests its integrity and acts as a single whole.

4. The system of information protection should cover the whole **technological complex** of information activities.

5. The information security system should be **diverse** in terms of the tools used, multi-level with a hierarchical access sequence.

6. The information protection system should be **open** for changing and supplementing information security measures.

7. The system of information protection must be **non-standard**. When choosing a remedy, you can not count on the ignorance of intruders about its capabilities.

8. The information security system should be **simple** for maintenance and user-friendly.

9. The information security system must be reliable. Any breakdown of technical means is the cause of the emergence of uncontrolled channels of information leakage.

**3. Structure of the information security system.**

**On the one hand**, the information security system includes a set of elements of its generators and their properties. The internal links of the system and their properties constitute the architecture of the system, its structure and internal organization.

**On the other hand**, the elements of the system have external connections, which purposefully affect the external environment and solve the tasks assigned to the system. This is the functional part of the system. It is quite natural that these two parts, the two sides - functional and structural - are not separated from each other, they are, as it were, two sides of the same elements that make up the information protection system.

**The structural part of the information protection system** is its internal organization, which allows the system to function normally, creates the conditions for securing the security of classified information, its access only through the channels controlled by this system.

The structural part of the information security system includes:

1. **The system of laws and other normative acts** establishing:

• the procedure and rules for the protection of information, as well as the responsibility for attempting to protect the information or the established procedure for its protection;

• protection of the rights of citizens associated with the information classified as protected secret;

• rights and duties of state bodies, enterprises and officials in the field of information protection.

2. **The system of information classification**, which includes:

• legislative definition of the category of information that can be classified as state secret;

• legislative and other legal definition of categories of information that can not be classified as state, commercial or other secret protected by law;

• empowerment of state authorities and officials in the field of referring information to a secret protected by law;

• drawing up lists of information classified as state secret, commercial or other secret protected by law.

3. **The system of security services and security services** with their own structure, staffing, ensuring the functioning of the entire system of information security.

The structural part of the information security system is a stable part of this system, its conservative part. As can be seen from the enumeration of the main elements of the structural part of the system, its elements can only change "spasmodically," they can not adapt quickly and continuously due to changes in the external environment, as well as changes in the environment, since the external environment can influence the structural part of the information security system only through its functional part, that is, indirectly.

The positive side of the stability and conservatism of this part of the system lies in the fact that it turns out to be a kind of filter that rejects the system's responses to changes in the external environment that are insufficiently substantiated and motivated by the needs of society.

The disadvantages of the conservatism of the information security system is that this part of the system can often have mismatches and contradictions with its functional part. This, of course, affects the efficiency and optimality of the functioning of the information protection system.

**The functional part of the information security system** solves the problem of securing the information classified by the superior system, in which this information security system is "built-in" (enterprise, firm, etc.). This activity involves a wide range of employees of the facility: security officers associated with the processing, storage, issuance and accounting of classified information; heads of the facility and structural units; performers, father-in-law, all employees of the facility who are consumers of protected information.

This part of the information security system is more adaptive, mobile and plastic. It, fulfilling its mission, as much as possible seeks to take into account the needs of the external environment in addressing issues of circulation and circulation of protected information, providing it to consumers and at the same time - excluding it from outside the protected sphere, its disclosure or disclosure.

**The main elements of the functional part of the system:**

• the procedure and rules **for classifying** (determining the degree of secrecy of information and putting the stamp of secrecy on works, documents, products) and **declassifying** information or reducing the degree of its secrecy;

• **the regime of secrecy established** on the object, the in-object mode and the guard mode, corresponding to the importance of the information accumulated and used on the object;

• **the system for processing, storing, recording and issuing media** **of protected information** using the adopted system of accumulation and processing of information: automated, manual, mixed, other, including clerical work with secret and confidential documents;

• **an authorization system** regulating the access of consumers to the protected information media, as well as to the enterprise and its separate premises;

• **a system for identifying possible channels for leakage of protected information** and searching for solutions for their overlapping, including educational and preventive work at the facility and its structural units;

• **a system for monitoring the presence of media of protected information** and the state of the established modes of operation at the facility: secrecy, intrabuild, protection of the facility and its most important units.

Thus, it can be said that both the structural and functional parts of the information security system exist and operate in an indissoluble unity.

**Лекция №4**

**Threats. Classification and analysis of information security threats**

**План лекции:**

1. The concept of a threat. Types of threats.

2. Sources of threats.

3. Prerequisites for the appearance of threats.

**1. The concept of a threat. Types of threats.**

Under the **threat of security** we will understand a potentially possible event, process or phenomenon that can lead to destruction, loss of integrity, confidentiality or accessibility of information.

All the many threats can be divided into two classes:

• accidental or unintentional;

• Intentional.

***Random Threats***

Threats that are not related to the deliberate actions of intruders and are realized at random moments of time are called **accidental or unintentional**.

*Natural disasters and accidents* are fraught with the most destructive consequences for material sources of information storage, because the latter are subject to physical destruction, information is lost or access to it becomes impossible.

*Failures and failures* of complex systems are inevitable. As a result, the working capacity of technical facilities is disrupted, data and programs are destroyed and distorted. Violation of the operation of individual units and devices can also lead to a breach of confidentiality of information. For example, failures and failures of means of information delivery can lead to unauthorized access to information by unauthorized delivery to a communication channel, to a printing device.

*Errors in the development* of the information system, algorithmic and program errors lead to consequences similar to the consequences of failures and failures of technical means. In addition, such errors can be used by intruders to influence the resources of the information system. A particular danger is represented by errors in operating systems and in software tools for protecting information. According to the National Institute of Standards and Technology of the United States, 65% of information security breaches occur as a result of errors of users and maintenance personnel. Incompetent, negligent or inattentive performance of functional duties by employees lead to destruction, violation of the integrity and confidentiality of information, as well as the compromise of protection mechanisms.

***Intentional threats***

The second class of threats to information security are deliberately created threats.

This class of threats has not been studied enough, it is very dynamic and constantly replenished with new threats. Threats of this class in accordance with their physical essence and implementation mechanisms can be divided into five groups:

• traditional or universal espionage and sabotage;

• unauthorized access to information;

• electromagnetic radiation and pick-up;

• modification of information system structures;

• wrecking programs.

As a source of undesirable impact on information resources, *methods and means of espionage and sabotage* that are used and used for obtaining or destroying information at sites that do not have information systems are still relevant. These methods are also effective and effective in the application of information systems. Most often, they are used to obtain information about the protection system in order to penetrate the information system, as well as to steal and destroy information resources.

The methods of espionage and sabotage are:

• eavesdropping;

• visual observation;

• theft of documents and computer storage media;

• theft of protection programs and attributes;

• bribery and blackmail of employees;

• collection and analysis of waste of computer storage media;

• arson;

• explosions.

*To eavesdrop* on an attacker, it is not necessary to penetrate the object. Modern facilities allow you to eavesdrop on conversations from a distance of several hundred meters. Thus, the eavesdropping system has been tested, allowing from a distance of 1 km to record a conversation in a room with closed windows. In urban conditions, the range of the device is reduced to hundreds and tens of meters, depending on the level of background noise. The principle of operation of such devices is based on the analysis of the reflected laser beam from the window of the room window, which oscillates from sound waves. Vibrations of window panes from acoustic waves in a room can be removed and transmitted to distances with the help of special devices, mounted on a window glass. Such devices convert mechanical oscillations of glasses into an electrical signal and then transmit it through a radio channel. Outside the premises eavesdropping is conducted with the help of ultra-sensitive directional microphones. The actual distance of eavesdropping using directional microphones is 50-100 meters.

*Remote video reconnaissance* to obtain information in information systems is of little use and is, as a rule, of an auxiliary nature.

Video surveillance is organized mainly to identify the work and location of information protection mechanisms. From the information system, information can really be obtained by interpreting screens, placards, posters on the object, if there are transparent windows and the above listed facilities are placed without regard to the need to counteract such a threat.

The term unauthorized access to information (NCDI) is defined as access to information that violates the rules of access delimitation using standard computer facilities or automated systems.

The rules of access control are understood as a set of provisions regulating the access rights of individuals or processes (access entities) to information units (access objects).

The implementation of the established rules of access delimitation in information systems is realized through the creation of an access control system (DRS).

Unauthorized access to information is possible only with the use of regular hardware and software in the following cases:

• there is no system, access delimitation;

• failure or failure in the information system;

• erroneous actions of users or maintenance personnel of information systems;

• errors in the DRR;

• Falsification of authority.

The process of processing and transmitting information by technical means is accompanied by electromagnetic radiation to the surrounding space and by the guidance of electrical signals in communication lines, signaling, grounding and other conductors. They received the names of *spurious electromagnetic emissions and pickups (PEMIN)*.

A major threat to the security of information in the information system is unauthorized modification of the algorithmic, software and technical structures of the system.

Unauthorized modification of structures can be carried out on any life cycle of the information system. The unauthorized change in the structure of the system at the development and modernization stages was called the "bookmark". In the process of developing the "bookmark" system, as a rule, they are introduced into specialized systems intended for operation in a certain firm or state institutions. In universal systems, "bookmarks" are introduced less often, mainly to discredit such systems by a competitor or at the state level, if the system is supposed to be delivered to a hostile state. "Bookmarks", introduced at the development stage, it is difficult to identify the simplicity of modern information systems due to the high qualification of their authors.Algorithmic, software and hardware "bookmarks" are used either for direct wrecking influence on the information system, or for providing uncontrolled log-on to the system. The harmful effects of "bookmarks" on the system are carried out when you get the appropriate command from the outside (basically typical for hardware "bookmarks") and when certain events occur in the system. Such events may be the transition to a specific mode of operation (for example, the combat mode of the weapons control system or the emergency response mode at the nuclear power plant, etc.), the arrival of a fixed date, the achievement of a certain operating time, etc.

**2. Sources of threats.**

As for the composition of the structural parts of the threat, it is necessary to emphasize: the sources of destabilizing influence on information are the core sources, their types and methods, and the final result of influence depend on their composition. Although the composition of other structural parts of the threat also plays a significant role, it, unlike sources, is not decisive and directly depends on sources. At the same time, it should be noted once again that sources in themselves are not a threat, if they do not occur from those or other influences.

The sources of destabilizing effects on information include:

1. People.

2. Technical means of displaying (fixing), storing, processing, reproducing, transmitting information, means of communication.

3. Systems for ensuring the functioning of technical means of displaying, storing, processing, reproducing and transmitting information.

4. Technological processes of separate categories of industrial objects.

5. Natural phenomena.

**The first source is people**. The most widespread, diverse and dangerous source of destabilizing influence on the protected information is people. This source is the most common because different categories of people, whether working or not working in the enterprise, can have a destabilizing effect on the protected information. These include:

• employees of the enterprise;

• persons who do not work at the enterprise, but who have access to the protected information of the enterprise due to their official position (from higher, related (including intermediary) enterprises, state and municipal authorities, etc.);

• employees of state intelligence agencies of other countries and intelligence services of competing domestic and foreign enterprises;

• persons from criminal structures, hackers.

In terms of the relationship with the types and methods of the destabilizing effect on information, these categories of people are divided into two groups:

• having access to the media of this protected information, the technical means of displaying it, storing, processing, reproducing, transmitting and ensuring their functioning and

• not having it.

Differences in the specifically applied types and methods of destabilizing effects on information between these groups of people (with the same type of species and methods) are determined by the objectives pursued.

The main purpose **of the second group** of people is unauthorized receipt (theft) of information that is confidential. Destruction, distortion, blocking of information is in the background, and often not the goal. The destabilizing influence of this group of people in the vast majority of cases is deliberate (deliberate, conscious). In addition, in order to bring about a destabilizing effect on confidential information, people in this group need to have a channel of unauthorized access to it.

For the **first group** of people, unauthorized receipt of confidential information is not at all a goal because of their access to such information. The goals of the destabilizing effect on the part of this group are disclosure, unauthorized destruction, blocking, distortion of information (listed in a sequence corresponding to the degree of intensity of the impact, from higher to lower). Information theft is also inherent in this group, but it is not a goal, but a means to accomplish the destruction or disclosure of information. The subject of the impact of this group is not only confidential information (although it is primarily), but also the protected part of the public information. The impact on the part of people included in this group can be:

• as deliberate,

• and unintentional (erroneous, accidental).

However, it should be noted that for access objects this group is not homogeneous in its composition. It includes:

1) people who have access to and to the bearers of protected information, and to means for displaying, storing, processing, reproducing and transmitting information (to all or some of them), and to systems for ensuring the operation of these facilities;

2) people who have access only to information and (sometimes or) to the means of processing it (all or separate);

3) people admitted only to the systems of ensuring the functioning of funds.

This source is the most diverse because it has, in comparison with other sources, a much larger number of types and methods of destabilizing effects on information.

The most dangerous source is because:

**firstly,** it is the most massive,

**secondly**, the impact on his part is not episodic, but a regular one,

**in the third**, as already noted, its impact can be not only unintended, as from other sources, but also deliberate, and,

**fourthly,** the impact it exerts can lead to all forms of vulnerability of information (from other sources - to individual forms).

As sources of destabilizing impact on information, we will consider people who have access to protected information carriers, the means of displaying it, storing, processing, reproducing, transmitting and operating systems for these means, without the above-mentioned division of these people by access objects, because the types and ways of destabilizing Impacts on the part of different categories of people entering this group differ not in composition but in quantity. People who do not have access to the listed objects, destabilizing influence on the information can, as it was noted, with the presence of channels of unauthorized access to it.

Depending on the source and type of exposure, it can be directly to the protected information or indirectly through another source of influence.

**The second source is the technical means of displaying, storing, processing, reproducing, transmitting information and communication means.** This source includes:

- electronic computers;

- electric and automatic typewriters and copiers;

- means of video and sound recording and reproducing equipment;

- means of telephone, telegraph, facsimile, loudspeaker communication;

- means of broadcasting and television;

- means of radio and cable communication.

**The third source** of the destabilizing effect on information is the **systems for ensuring the functioning of technical means of displaying, storing, processing, reproducing and transmitting information:**

• power supply systems,

• water supply,

• heat supply,

• conditioning,

• auxiliary electric and radio-electronic means (electric clock, household tape recorders, radio receivers, television sets, etc.)

**The fourth source is the technological processes of nuclear power facilities, the chemical industry, radio electronics, as well as facilities for the manufacture of certain types of weapons and military equipment** that alter the natural structure of the surrounding environment.

**The fifth source - natural phenomena** - includes two components:

• natural disasters and

• atmospheric phenomena.

One of the main sources of threats to information security in the CC is the use of special programs that have received the general name of *wrecking programs*. Depending on the mechanism of action, malicious programs fall into four classes:

• "logical bombs";

• "worms";

• "trojan horses";

• "computer viruses".

*"Logical bombs"* These are programs or parts of them that are permanently located in computers or computer systems and performed only under certain conditions. Examples of such conditions can be: the arrival of a given date, the transition of the system to a certain mode of operation, the occurrence of certain events the set number of times, etc.

*"Worms"* are programs that are executed each time the system boots, have the ability to navigate in computer systems or networks and reproduce copies themselves. Avalanche-like multiplication of programs leads to congestion of communication channels, memory and, eventually, to system locking.

*"Trojan horses"*. These are programs obtained by explicitly modifying or adding commands to user programs. At the subsequent execution of user programs, along with the specified functions, unauthorized, modified or some new functions are performed.

*"Computer viruses".* These are small programs that, once implemented in a computer, are distributed independently by creating their own copies, and when certain conditions are met they have a negative impact on information systems. Since viruses are inherent in the properties of all classes of malicious programs, recently any malicious programs are often called viruses.

**3. Prerequisites for the appearance of threats.**

When considering the signs and components of the threat of the protected information, it was said that at the base of any destabilizing influence lie certain causes, motives that cause the appearance of this or that kind and mode of influence. At the same time, the reasons are justified - the circumstances or prerequisites that cause these reasons contribute to their appearance. However, the presence of sources, types, methods, causes and circumstances (prerequisites) of the destabilizing effect on information is a potentially existing hazard that can be realized only if there are certain conditions for it.

Since the types and methods of destabilizing influence depend on the sources of influence, the causes, circumstances (prerequisites) and conditions must be linked to sources of influence.

***The reasons, circumstances and conditions of destabilizing influence on the protected information from people.***

For people, the reasons, circumstances and conditions are in most cases linked to the nature of the impact - intentional or unintentional.

To the **reasons** causing deliberate destabilizing influence, it is necessary to carry:

- the desire to obtain material benefits (earn extra money);

- the desire to harm (revenge) the management or colleague of work, and sometimes the state;

- the desire to render disinterested service to a friend from a competing firm;

- the desire to advance in the service;

- the desire to protect themselves, relatives and friends from threats, blackmail, violence;

- physical impact (beatings, torture) on the part of the attacker;

- the desire to show its importance.

**Circumstances (prerequisites)** contributing to the emergence of these reasons can be:

- difficult financial situation, financial difficulties;

- greed, avarice;

- propensity to entertainments, drunkenness, drugs;

- envy, resentment;

- dissatisfaction with state policy, enterprises, political or scientific dissent;

- personal connections with representatives of the competitor;

- dissatisfaction with official position, careerism;

- cowardice, fear;

- vanity, conceit, overestimated self-esteem, boasting.

**To conditions** that create an opportunity for destabilizing effects on information, we can include:

- insufficient measures taken to protect information, including due to lack of resources;

- insufficient control and attention from the administration on issues of protection, information;

- making decisions on production issues without taking into account information protection requirements;

- poor relations between employees and employees with the administration.

**The reasons for the unintended destabilizing effect** on information from people can be:

- unskilled execution of operations;

- negligence, irresponsibility, lack of discipline, unfair attitude to the work performed;

- negligence, carelessness, carelessness;

- physical malaise (illness, overwork, stress, apathy).

**The circumstances (prerequisites)** for the emergence of these causes include:

- low level of professional training;

- excessive talkativeness, frivolity, the habit of sharing experience, giving advice;

- disinterest in work (type of work, its temporary nature, salary), lack of incentives for its improvement;

- disappointment in their abilities and abilities;

- congestion of work, the urgency of its implementation, violation of the regime of work;

- poor attitude on the part of the administration.

**Conditions** for the implementation of unintentional destabilizing effects on information can be:

- lack of or poor quality of rules for working with protected information;

- ignorance or violation of rules of work with information by performers;

- insufficient control by the administration over compliance with the confidentiality regime;

- insufficient attention on the part of the administration to the working conditions, disease prevention, professional development.

*Causes, circumstances and conditions of destabilizing influence on the protected information from other sources of influence.*

**The causes of the destabilizing effect on information from the technical means of displaying, storing, reproducing, transmitting information and communication means** can be:

- lack or poor quality of funds;

- poor quality of the mode of operation of funds;

- reloading of funds;

- poor quality of technology;

- destabilizing effects on funds from other sources of impact.

The **circumstances (prerequisites)** that cause these reasons include:

- Insufficient financial resources allocated for the acquisition and operation of funds;

- poor choice of means;

- aging (wear) of funds;

- design flaws or errors in the installation of funds;

- mistakes in the development of technology for the performance of works, including software;

- defects in materials used;

- excessive amount of processed information;

- the reasons underlying the destabilizing impact on the funds from other sources of impact.

The **conditions** ensuring the implementation of destabilizing effects on information from technical means may be:

- insufficient attention to the composition and quality of funds on the part of the administration, often due to a lack of understanding of their significance;

- irregular preventive examination of funds;

- poor quality of service facilities.

**The reasons, circumstances (prerequisites) and the conditions for the destabilizing effect on information on the part of the systems for ensuring the functioning of the means for displaying, storing, processing, reproducing, transmitting information and means of communication** "fit" into the causes and circumstances of the impact on the part of the funds themselves.

**The reason for the destabilizing effect on information from technological processes of individual industrial objects** is the specificity of technology, the fact is the need for such a technology, and the **condition** is the lack of capacity to counteract the change in the structure of the environment.

At the heart of the **destabilizing effect on information from natural phenomena** lie internal causes and circumstances that are not controlled by people, and, therefore, are not amenable to neutralization or elimination.

It should be noted that it is not always possible to draw a line between the causes and circumstances, the same factor in one case may be the cause, in another circumstance (prerequisite), the kinds of destabilizing influence from some sources can act as ways of destabilizing influence on the part of others sources.

**Лекция №5**

**Methods of violation of confidentiality, integrity and accessibility of information**

**План лекции**

1. Classes of channels of unauthorized information retrieval.

2. The reasons for the violation of the integrity of information.

3. Functions of information security.

4. Strategies for protecting information.

5. The architecture of information security systems.

**1. Classes of channels of unauthorized information retrieval.**

The first class includes channels from the source of information in the NDT to it.

1. Theft of information carriers.

2. Copying of information from carriers (material-material, magnetic, etc.).

3. Eavesdropping conversations (including audio recording).

4. Installation of embedded devices in the room and information retrieval with their help.

5. Recognizing the information of attendants at the facility.

6. Photographing or videotaping of media inside the room.

The second class includes the channels from the information processing facilities under the IMD to them.

1. Removal of information from electronic memory devices.

2. Installation of embedded devices in SDI.

3. Entering software products that allow an attacker to receive information.

4. Copying of information from technical display devices (photographing from monitors, etc.).

The third class includes the following channels:

1. Acquisition of information on acoustic channels (in ventilation systems, heat supply, and also using directional microphones).

2. Obtaining information on vibro-acoustic channels (using acoustic sensors, laser devices).

3. Use of technical means of optical reconnaissance (binoculars, telescopes, etc.).

4. Use of technical means of opto-electronic reconnaissance (external cameras, night vision devices, etc.).

5. Inspection of waste and debris.

6. Recognition of information from maintenance personnel outside the facility.

7. Study of open information outside the object (publications, advertising brochures, etc.).

The fourth class includes channels from information processing facilities without NDTs to them.

1. Electromagnetic radiation SDI (parasitic electromagnetic radiation (PEMI), parasitic generation of amplifying stages, parasitic modulation of high-frequency generators by a low-frequency signal containing confidential information).

2. Electromagnetic radiation of communication lines.

3. Connections to communication lines.

4. Removal of interference of electrical signals from communication lines.

5. Removal of interference from the power system.

6. Removal of interference from the grounding system.

7. Removal of interference from the heat supply system.

8. Use of high-frequency imposition.

9. The removal of signals from the lines that go beyond the limits of the object, formed on technical means due to acoustoelectric transformations.

10. Removal of radiation from fiber-optic communication lines.

11. Connection to databases and PC on computer networks.

Causes of violation of the integrity of information:

1. Subjective.

1.1. Intentional.

1.1.1. Diversion (organization of fires, explosions, damage to power supplies, etc.).

1.1.2. Immediate actions on the medium (theft, substitution of media, destruction of information).

1.1.3.Information impact (electromagnetic irradiation, the introduction into computer systems of destructive software, the impact on the psyche of a person with psychotropic weapons).

1.2. Unintentional.

1.2.1. Failures of maintenance personnel (death, long-term failure).

1.2.2. Failures of people (temporary failure).

1.2.3. Mistakes of people.

2. Objective, unintentional.

2.1. Failures (complete failure) of equipment, programs, power systems and life support.

2.2. Failures (short-term failure) of equipment, programs, power systems and life support.

2.3. Natural disasters (floods, earthquakes, hurricanes).

2.4. Accidents (fires, explosions, accidents).

2.5. Electromagnetic incompatibility.

**2. The reasons for the violation of the integrity of information.**

Violations of information integrity are illegal destruction or modification of information.

Traditionally, integrity protection falls into the category of organizational measures. The main source of threats to integrity are fires and natural disasters. To the destruction and modification can also lead to accidental and deliberate critical situations in the system, viruses, Trojan horses, etc.

The language of description of integrity threats is generally similar to the language of threats to secrecy. However, in this case, it is more convenient to talk about channels of influence on integrity (or channels of destructive influence) to the place of leakage channels. In fact, they are similar to leakage channels if access (r) is replaced by access (w).

Example 1. An unauthorized modification channel using the "Trojan horse" is depicted in the following scheme:

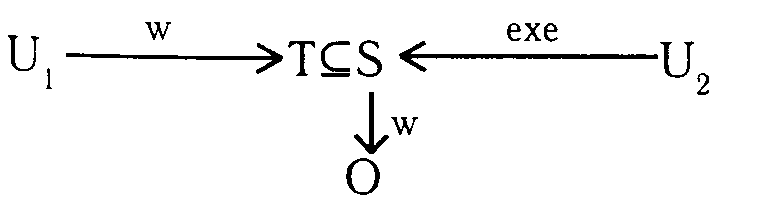


Fig. 5.1. Unauthorized modification channel

where *U1* is the attacker; *U2* is the user; *O* - an object with valuable information; *S* - process (program), which is a common resource *U1* and *U2*.

User *U1*, using the right w, modified the shared resource *S*, by integrating into it the hidden program *T*, which modifies the information in *O* when it is started by the user *U2*.

The investigation of the circuits in Fig. 5.1 deals with the theory of the spread of viruses.

The basis for protecting integrity is the timely and regular copying of valuable information.

Another class of integrity protection mechanisms is based on the idea of ​​noise-immune encoding information (the introduction of redundancy into information) and forms the basis for integrity control. It is based on authentication, i.e. confirmation of the authenticity, integrity of information. Authentication protects the integrity of the interface, and the use of authentication codes allows you to monitor the integrity of files and messages. The introduction of redundancy into languages and the formal specification specification allows you to monitor the integrity of programs.

Finally, the creation of system redundancy is one of the mechanisms for monitoring and protecting the integrity of information. In military practice, such measures are called: increasing the "survivability" of the system. The use of such mechanisms also makes it possible to solve the problems of error resilience and protection against accessibility problems.

**3. Functions of information security.**

**Function 1** - warning of threats. The implementation of this function has a preemptive purpose and should facilitate such an architectural and functional construction of modern processing and information protection systems that would provide minimal opportunities for the emergence of destabilizing factors in various operating conditions of systems. For example, in order to prevent the possibility of installing embedded devices in a building, it is necessary, with the help of technical means and organizational measures, to ensure that unauthorized access to it is impossible.

**Function 2** - detection of manifested threats and prevention of their impact on information. A complex of measures is implemented, as a result of which the manifested threats must be detected before their impact on the protected information, as well as ensuring that these threats are not affected by the protected information in the conditions of their manifestation and detection.

**Function 3** - detection of the impact of threats on the protected information and the localization of this impact. The content of the function is aimed at the continuous monitoring of the means, complexes, processing systems, information protection and various components of the protected information with the purpose of timely detection of the facts of the impact of threats on them. Timely detection implies ensuring a real possibility of localizing the impact on information, i.e. minimization of possible breach of its integrity and security and preventing the spread of this impact beyond the limits of acceptable dimensions. In computer systems, for example, this function is realized by hardware-software means of monitoring and recording attempts to unauthorized access to the system or to information (digital signature).

**Function 4** - elimination of the consequences of the impact of threats. The function provides for the implementation of protection measures with respect to the detected and localized impact of threats on information, i.e. the restoration of the processing system, the protection of information and the state of the protected information with the use of a corresponding set of means, methods and measures of protection.

**4. Strategies for protecting information.**

**A strategy** is a common, forward-looking guideline for organizing and providing the appropriate activity, aimed at ensuring that the most important goals of this activity are achieved with the most rational use of available resources.

The organization of information protection in its most general form can be defined as the search for the optimal compromise between the protection needs and the resources necessary for these purposes.

The requirements for protection are primarily determined by the importance and volumes of the protected information, as well as the conditions for its storage, processing and use. These conditions are determined by the level (quality) of the structural and organizational construction of the information processing object, the level of organization of technological processing schemes, the location and conditions of the location of the object and its components, and other parameters.

The formulated problems are nothing else than the direct and inverse formulation of optimization problems. There are two problems that make it difficult to make a formal decision.

**The first** - the processes of information protection are largely dependent on a large number of random and difficult to predict factors, such as the behavior of the attacker, the impact of natural phenomena, failures and errors in the functioning of the elements of the information processing system,

**The second** - among the means of protection, a very prominent place is occupied by organizational measures connected with the action of a person.

The values of the first criterion are best expressed by the many threats against which protection should be provided:

1) from the most dangerous of known (previously emerged) threats;

2) from all known threats;

3) from all potential threats.

The second criterion for choosing protection strategies is that the organizers and executors of the protection processes have relatively complete freedom to dispose of methods and means of protection and some degree of freedom of interference in the architectural construction of the information processing system, as well as in organizing and providing technology for its operation. In this aspect, it is convenient to distinguish three different degrees of freedom.

**5. The architecture of information security systems.**

***Requirements for the architecture of GIS***

**The information protection system (GIS)** in its most general form can be defined as an organized set of all the means, methods and activities allocated (provided) on the information processing object (OOI) to solve selected protection tasks in it.

The introduction of the concept of GIS determines the fact that all resources allocated to the protection of information must be integrated into a single, integrated system that is functionally independent subsystem of any EOI.

The most important conceptual requirement for GIS is the requirement of adaptability, i.e. the ability to make a purposeful adaptation when changing the structure, technological schemes or operating conditions of the OOI. The importance of the requirement of adaptability is due, on the one hand, to the fact that the listed factors can significantly change, and on the other hand, by the fact that information protection processes are related to weakly structured, i.e. having a high level of uncertainty. Managing the same weakly structured processes can only be effective if the control system is adaptable.

In addition to the general conceptual requirement, a number of more specific, target requirements are presented to the GIS, which can be divided into:

• functional;

• ergonomic;

• economic;

• technical;

• Organizational.

The system developed to date includes the following list of general methodological principles:

• conceptual unity;

• Adequacy requirements;

• Flexibility (adaptability);

• Functional independence;

• Ease of use;

• minimization of the granted rights;

• completeness of control; adequacy of response;

• economy.

*Conceptual unity* means that the architecture, technology, organization and operation of both the GIS as a whole and the component components must be considered and implemented in strict accordance with the main provisions of the unified concept of information protection.

*Adequacy of requirements* means that the GIS must be built in strict accordance with the requirements for protection, which, in turn, are determined by the category of the relevant object and the values ​​of the parameters affecting the protection of information.

*Flexibility (adaptability)* of a security system means such a construction and such organization of its functioning, in which protection functions would be performed quite effectively when a certain range of the structure of the information processing object, technological schemes or operating conditions of any of its components changes.

*Functional autonomy* assumes that the GIS should be an independent supporting subsystem of the information processing system and, when performing protection functions, should not depend on other subsystems.

*Ease of use means* that the GIS should not create additional inconveniences for users and personnel of the information processing facility.

*Minimizing the rights* granted means that each user and each person in the information processing facility's personnel must be given only those powers to access the resources of the information processing object and the information contained in it, which it really needs to perform its functions in the process of automated processing of information. At the same time, the rights granted must be determined and established in advance by established procedure.

*Completeness of control* assumes that all procedures for automated processing of protected information should be fully controlled by the protection system, and the main results of control should be recorded in special logbooks.

*Response activity* means that the GIS should respond to any attempts at unauthorized actions. The nature of the response may be different and includes: a request to repeat the action; the disabling of the structural element from which the unauthorized action was performed; Exclusion of the intruder from the number of registered users; giving a special signal, etc.

*The cost effectiveness of GIS* means that, provided that the basic requirements of all previous principles are met, the costs of the GIS must be minimal.

***Construction of GIS***

*A functional construction* of any system is an organized collection of those functions for which it is regularly created.

*The organizational structure* is understood as the overall organization of the system, adequately reflecting the conceptual approaches to its creation. Organizationally, GIS consists of three mechanisms:

• ensuring the protection of information;

• management of protection mechanisms;

• the overall organization of the system.

There are two organizational components in the security mechanisms; constants and variables. At the same time*, constant* means the mechanisms that are built into the components of the information processing object during the creation of the GIS and are in working order during the entire time of the functioning of the respective components. *Variable* mechanisms are autonomous, their use for solving information protection tasks involves preliminary implementation of input operations into the composition of the mechanisms used. Embedded and variable mechanisms can include technical, software and organizational security tools.

Accordingly, the composition of mechanisms for ensuring the protection of information, obviously, should be organized mechanisms for their management.

The mechanisms of the overall organization of the GIS are designed to systematically coordinate and coordinate the operation of all components of the GIS.

The concept of "organizational construction" of the GIS also includes the distribution of the elements of this system according to organizational and structural elements of the EOI. Proceeding from this, in the organizational construction of the GIS, protection subsystems at the objects (structural components) of the OOI with its specific protection mechanisms and some control link, which is called the *core* of the GIS, should be provided.

***The core of the information security system***

**The core of the protection system** is designed to unify all subsystems of the GIS into a single integrated system, to organize the provision of management of its operation.

The kernel can include organizational and technical components.

*The organizational component* is an aggregate of employees specially assigned to provide ZI, performing their functions in accordance with the developed rules, as well as the regulatory framework that regulates the performance of these functions.

*The technical component* provides technical support for the organizational component and is a set of technical means for displaying the states of the GIS elements, controlling access to them, controlling their inclusion, etc. More often than not, these tools are integrated into the appropriate control panel of the GIS. The kernel of the GIS has the following functions.

1. Inclusion of GIS components in the work when receiving requests for processing of protected information and blocking uncontrolled access to it:

• equipment of the facility by means of burglar alarm;

• The organization of storing the carriers of protected information in separate storages (documentation, ciphers, magnetic media, etc.).

• Inclusion of blocking devices that regulate access to GIS elements upon presentation of appropriate authorizations and signaling means.

2. Organization and provision of checks on the correct functioning of the GIS:

• Hardware - by test programs and organizationally;

• Physical means - organizationally (scheduled checks of security alarms, signaling about increase of pressure in cables, etc.);

• software - for special checksums (for integrity) and for other identifying signs.

***Information Security Resources***

**The resources** of the information and computing system necessary to create and maintain the operation of the GIS, as well as any other automated system, are combined into technical, mathematical, software, information and linguistic support.

1. *Technical support* - a set of technical means necessary for technical support of the solution of all those tasks of information protection, the solution of which may be required in the course of the operation of the GIS.

2. *Mathematical support* - a set of mathematical methods, models and algorithms needed to assess the level of information security and other protection tasks.

3. *Software* - a set of programs that implement software protection tools, as well as the programs necessary to solve the tasks of managing security mechanisms. They should also include service and support programs of GIS.

4*. Information support* - a set of systems for classifying and coding data on the protection of information, arrays of melon GIS, as well as input and output documents of GIS.

5. *Linguistic support* - a set of language tools necessary to ensure the interaction of the components of the GIS among themselves, with the components of the information processing object and with the external environment.

***Organizational structure***

The organizational construction of a GIS in the most general case can be represented by the combination of the following protection boundaries (Figure 2.21):

1) the territory occupied by the OOI;

2) buildings located on the territory;

3) premises inside the building where the resources of the EOI are located and the information to be protected;

4) the resources used to process and store information and the most protected information;

5) communication lines passing within the same building;

6) communication lines (channels) passing between different buildings located on the same protected area;

7) communication lines (channels) connecting with other objects outside the protected area.

Thus, it is possible to organize the organization of an information security system using the above-mentioned seven-pronged model. In the most general case, it is necessary, depending on the chosen defense strategy, to formulate the requirements for the core of the GIS and the GIS resources, and also use the criteria for constructing the GIS.

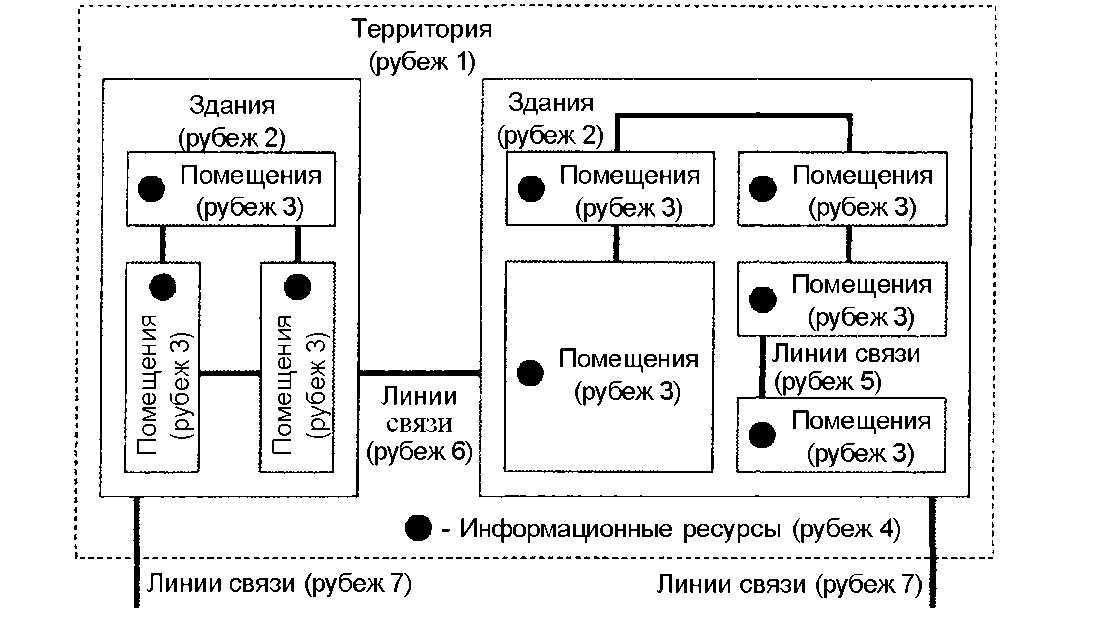


Fig. 5.2. Semi-Diaspora Information Security Model

It should be noted that the construction of the GIS should be carried out in accordance with the regulatory legal documents adopted in Kazakhstan. Most activities in the field of information security require licenses. So, to work with state secrets, appropriate licenses of the National Security Service are required to work with cryptographic facilities, technical means must be certified by the National Technical and Export Control Service.

**Лекция №6**

**Engineering and technical protection of information**

**План лекции**

1. System of information protection.

2. Methods and means of engineering protection and technical protection of objects.

3. The main areas of engineering and technical protection of information.

**1. System of information protection.**

In modern society, commercial intelligence and electronic espionage are, unfortunately, a common phenomenon in the branches of science-intensive technologies.

The global issue of the emergence of man-made disaster 2003-2005. brings modern society to its defense by creating an integrated security system in its own countries.

The hierarchical model for constructing information systems is also true when creating an integrated security system: from an integrated state security system, through sectoral and regional security systems, to the creation of an integrated security system for an individual enterprise with confidential information.

The modular principle of building secure information systems with inheritance and access restrictions leads to the need to develop a model of integrated security systems. The information component performs in this system two functions - an element and an information environment in which the remaining interacting elements are located.

The development of the IS system requires the reproduction of the relevant elements. **The macro system of information protection** (IPM) in its most general form can be represented as an organized set of all components of the information environment, as well as the means, methods and activities involved in solving protection tasks.

Components of the information environment and simultaneously local systems (subsystems) are:

• protection of the information channel system;

• protection of the data storage system;

• Protection of the data processing system (OD);

• system of legal protection;

• system of organizational measures to protect information.

The construction of the system and its functioning are represented in the form of the dependence of the state of the system's security on the physical parameters of information components of the information environment.

A complete description of the structure of the system construction provides for the property of encapsulating an expanded hierarchical structure and contains:

1. A list of all its information components.

2. A list of links within the system.

3. List of parameters that characterize information components.

4. List of states of system security.

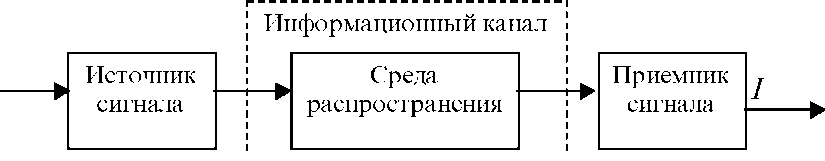


Fig. 6.1. Information channel

To transmit information in media in the form of fields, materials and microparticles on any information channel (functional or leakage channel), it must contain three main elements: signal source, propagation medium and signal receiver (see Figure 6.1).

The input of the channel receives information in the form of a primary signal, which is a carrier with information from its source.

The source of the signal can be:

• the subject;

• an object;

• Wednesday.

**The distribution medium** is a part of the space in which information is moved, it is determined by a set of physical parameters that determine the conditions for information transfer, the main ones of which are:

• time characteristics;

• frequency characteristics;

• bandwidth characteristics;

• Load parameters.

The information leakage channel differs from the functional channel of information transfer by the recipient of the information.

**Information channel** is a system of interconnection of elements of the information environment, as a result of which interaction fields are created that transfer information and provide information transmission to the propagation medium in a given direction.

The main classification feature of information channels is the physical nature of the medium. On this basis they are divided:

• optical;

• acoustic;

• radio electronic;

• material and material;

• biological;

• elementary (see Figure 6.2).

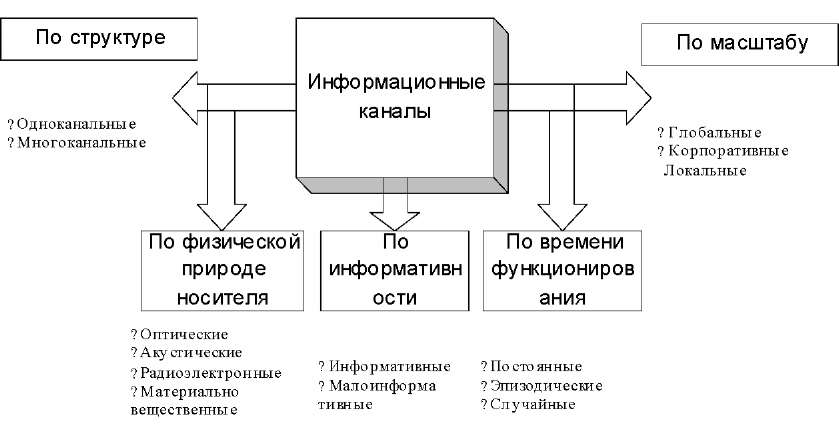


Fig. 6.2. Classification of information channels

The carrier of information in the optical channel is the electromagnetic field in the visible range.

In the radio-electronic channel, electric, magnetic and electromagnetic fields in the radio frequency range are used as carriers, as well as electric current (electron flux) propagating along metallic wires.

The carrier of information in the acoustic channel are elastic mechanical acoustic waves in the infrasound, sound and ultrasonic frequency ranges, propagating in the atmosphere, water and solid media.

In a material-material channel, information is transferred by distributing material carriers outside the organization with information: business correspondence, draft documents and used photocopying paper, discarded parts and components, substances. The latter, in the form of a solid, liquid, and gaseous state, allows one to determine the composition, structure, and properties of materials or to restore the technology for their production.

The carrier of information in the biological channel is the structure of the cell's DNA.

Each of the physical channels has its own characteristics, which must be known and taken into account to ensure effective ZI in them.

The informative value of the channel is estimated by the degree of value (confidentiality) of information transmitted in it.

By the time of manifestation, the channels are divided into constant, periodic and episodic. In a permanent channel, the transfer of information is fairly regular. A periodic channel can arise if the information is transmitted at regulated intervals. Occasional channels include channels, the circulation of information in which is random, one-time.

An information channel consisting of a transmitter, a propagation medium, and a receiver is one-channel. However, it is possible that the transfer of information takes place in a more complicated way - through several serial or parallel channels.

In global information channels, the channel elements are located at considerable distances from each other. Elements of local information channels are located at short distances from each other. Corporate information channels unite several local information channels that share common identification features.

**The subsystem of information channels** includes properties aimed at protecting the following physical characteristics of data transmission channels:

• protection of the time resource;

• protection of the maximum bandwidth of the channel;

• protection of the frequency band that the channel is able to skip;

• protection of the bandwidth band of the channel.

**The storage subsystem** includes properties aimed at protecting information archives and information storage databases on any physical media and the integrity of the media themselves:

• protection of the volume of stored information;

• protection of the form of presentation of information on the carrier;

• protection of physical properties of the information carrier.

**The OD subsystem** includes properties aimed at

• protection of all technical means of information processing (TSOI) from unauthorized actions and unintended impacts:

• protection of the way of access to ML means;

• protection of physical characteristics of ML means;

• protection of management of ML means.

**The legal protection subsystem** includes properties aimed at ZI and rights to it, protection of an individual and society from the impact of information, protection of "information from information":

• protection of the legality of information;

• protection of the right to access to information.

**The subsystem of organizational measures** for ZI includes properties aimed at the physical protection of the components of the information environment:

• protection of the physical integrity of the object;

• protection of the physical integrity of the TSOI.

**2. Methods and means of engineering protection and technical protection of objects.**

50% of intrusions are committed to objects with free access and only 5% to objects with enhanced protection.

The basis of engineering protection and technical protection of objects (IZTOO) is mechanical means and engineering facilities that prevent the physical movement of intruders, technical alarms, as well as means and people eliminating threats.

***Structure of the system of protection of objects***

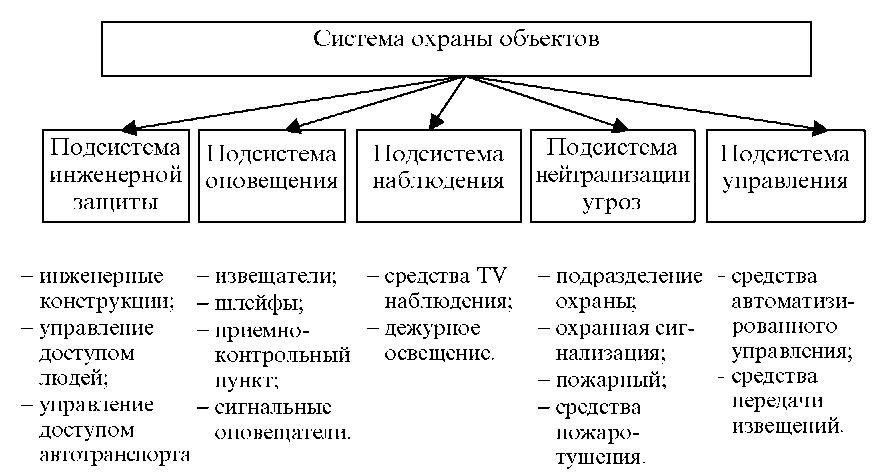


Fig. 6.3. Structural diagram of the object protection system

Depending on the structure of the system, the guards are divided into autonomous and centralized (see Figure 6.3).

In an autonomous system, all protection tasks are handled within the same organization, in a centralized neutralization and threats subsystem common to several organizations.

Engineer protection subsystem

The engineering structures and facilities for ZI include:

• natural and artificial barriers (surface irregularities, fences, metal nets, barbed wire, barely visible networks);

• doors and windows (locks: mechanical, mechanical code, electromechanical, electronic code, glass: hardened, multi-layer, laminated films, gratings between the panes);

• CAT (includes a hall for people to pass, a pass office, a storage room, a room for the security chief, inspectors, access control means of transport);

• cabinets and work tables with lockable drawers;

• storage and safes (monolithic, prefabricated, prefabricated-monolithic).

Methods for identifying people are divided into attribute and biometric.

1. Attribute identifiers:

1) passes, tokens, etc .;

2) identification cards:

• magnetic;

• IR;

• broken lines;

• "Wigand cards" (pressed pieces of thin wire with random orientation);

• contactless "proximity" cards (built-in microchip).

The main drawback of attribute identifiers is the possibility of getting them to an unauthorized person.

2. Biometric identifiers:

1) drawing of papillary lines of fingers;

2) patterns of the retina of the eyes;

3) the geometry of the hand;

4) signature dynamics;

5) features of speech;

6) the rhythm of work on the keyboard.

The persistence of vaults and safes is estimated in conventional resistance units (*Ec* or RU), which are defined as the product of the break-in time by the complexity factor of the tool used for this.

The group of the highest resistance is formed by the storage of 11 - 13 classes (2000 - 4500 *Ес*). The time of breaking them using the most effective tool (electric cutting with a diamond drill of up to 11 kW) should be at least 45 - 120 minutes. Those that survived tests with a TNT storage facility with a charge mass of up to 500 g are marked with the "BB" index.

Fire resistance of safes: the time from the time of heating the safe to 1000 ° C is 1 - 2 hours. The temperature inside the safe should not exceed 170 ° C for paper, 70 ° C for magnetic tapes, disks, film, and 50 ° C for flexible magnetic disks.

***Methods and means of detecting intruders and fire***

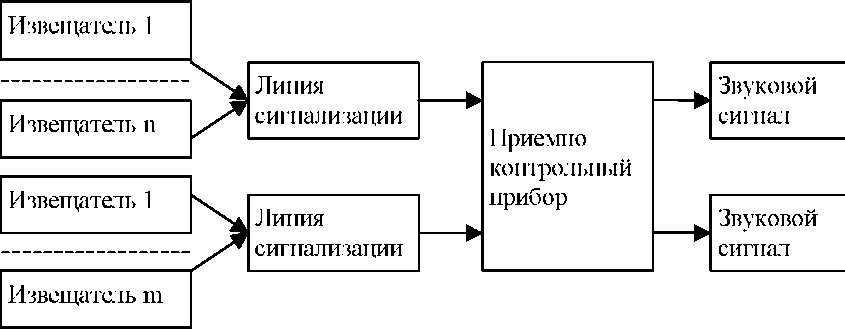


Fig. 6.4. Scheme of standard TCO objects

Detector (sensor) is a technical device that generates an electrical alarm when exposed to it or created by it (see Figure 6.4, 6.5). Alarm line is an electrical circuit that transmits an alarm signal.

Contact detectors react to the actions of an attacker, leading to the closure or opening of the contacts of the detector:

• electrocontact (DEK-3, SK-1M, BK-1M);

• magnetocontact (SMK-1, SMK-3, DMK-P);

• shock-contact (Window-4, UKD-1M, VM-12M, DIMK);

• discontinuous (Cable-1, Water-lily, Trepang).

Acoustic annunciators use acoustic waves in the sound and ultrasonic range to detect intruders, which occur when mechanical obstacles are destroyed (Gran-1, 2, Window-1).

Ultrasonic sensors generate an alarm signal when an intruder appears in the monitored zone of the protected area and consists of a radiator (23 kHz) and a receiver (DUZ-4, DUZ-4M, DUZ-5, DUZ-12, Fikus-MP-2, ECHO -2, 3).

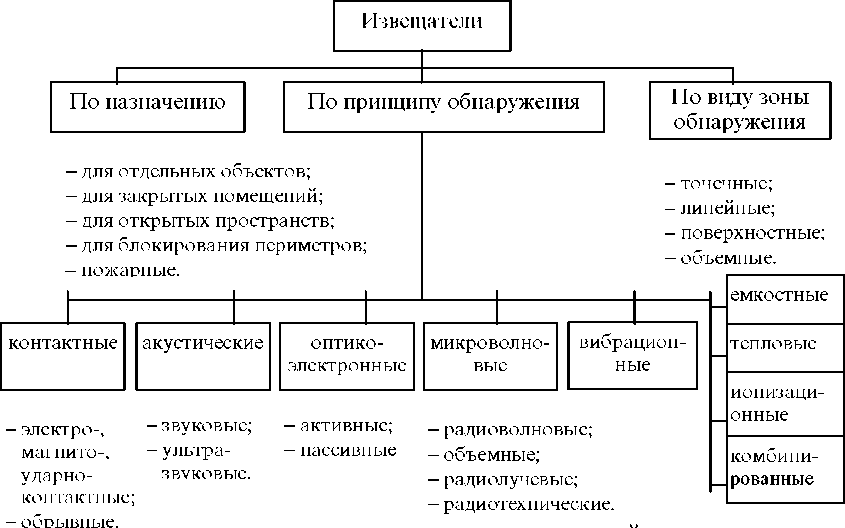


Fig. 6.5. Classification of detectors

In optical-electronic detectors IR-rays (DOP-1, 2, 3, Quantum-2U, Vector-2, 3, 4, Rubezh-1M) are used to detect an intruder or a fire. When choosing the location of the detectors in the room, it is necessary to be guided by the following:

• the detector should not be illuminated by the sun;

• the detector or the opposite wall should not be illuminated by the high beam of the headlights of cars;

• the detector should not be located less than 1.5 meters from the ventilation opening and the central heating battery.

Microwave (radio wave), including radio-beam (Radium-1, Peony-T, Reef-RL, Protva) and RT (Viaduct) detectors, use electromagnetic waves in the microwave range (9-11 GHz) to detect the intruder. They contain a microwave generator, receiver, antennas.

Vibrators include detectors that detect an attacker by the vibration he creates in the ground during movement, in an easy fence while trying to overcome (Crow).

Capacitive detectors (Rhomb-K4, Peak, Barrier-M, Gradient) create alarm signals when an intruder approaches the antenna.

Thermal and ionization detectors are produced specifically for detecting a fire:

• thermistors;

• thermobimetal plates;

• low-melting alloys;

• thermoferrites.

In combined detectors, the algorithm for processing signals from different sensors becomes more complicated.

Receiving and monitoring devices provide:

• simultaneous reception of alarm signals from all protected objects;

• transmission of alarm signals to the central monitoring station;

• the possibility of increasing capacity by adding linear blocks to the basic composition;

• automatic transfer to backup power;

• the formation of alert signals to operators in the event of an open or short circuit loop.

The autonomous use of technical security equipment (TSS) has two significant drawbacks:

• a decrease in the psychological activity and concentration of employees when false signals appear;

• threat to the life of security guards when approaching the alleged place of violation.

Therefore, in conjunction with the security system, television surveillance equipment is used (see Figure 6.6), which constitute the observation subsystem.

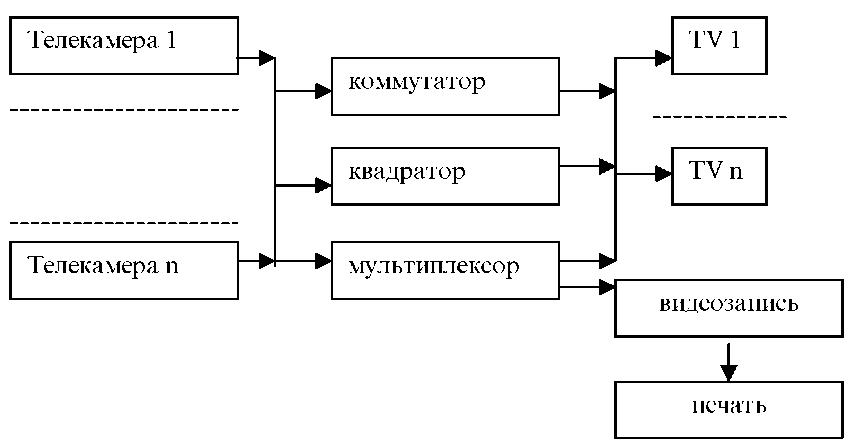


Fig. 6.6. The scheme of video monitoring system

The switch allows you to connect several (4 - 16) cameras.

Quadrature reduces the number of monitors by simultaneously displaying on a single monitor.

The multiplexer is designed to provide recording to a VCR from connected cameras.

An important component of the surveillance subsystem is duty lighting.

Lamps and infrared projectors are used as light sources. Apply incandescent lamps and discharge lamps.

Vacuum, krypton (using neutral gas - krypton) and halogen incandescent lamps of general purpose are produced up to 1000 W.

In halogen lamps, the temperature is increased by 400 to 500 degrees, in contrast to vacuum ones. Light output is 1.5 times higher. The preservation of the incandescent tungsten filament from burnout is achieved due to iodine vapor. Iodine vapors, interacting with tungsten vapors, form tungsten-halogen iodide, which decomposes into iodine and tungsten near the filament at a temperature of 2,700-2,900 ° C. Tungsten settles on the filaments and evaporates again - the halogen cycle repeats.

Gas discharge are divided:

• on gas and vapor, in which radiation is caused by the excitation of atoms, molecules;

• luminescent (the phosphor is excited by the discharge radiation);

• electro-light (electrodes are heated in a discharge to a high temperature).

***Threat neutralization tools***

They join the threat neutralization subsystem (see Figure 6.7).

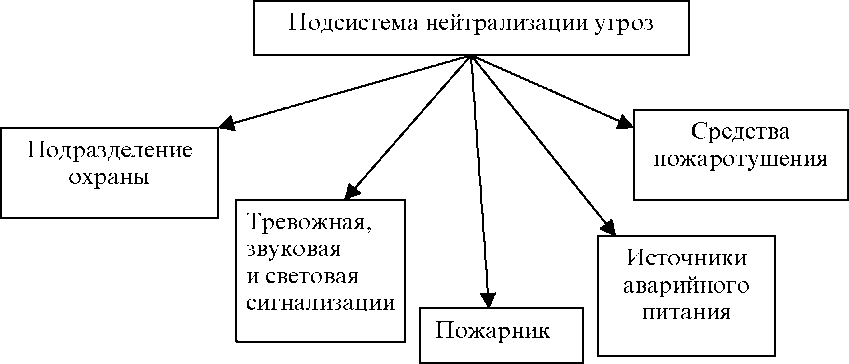


Fig. 6.7. Schema of the threat neutralization subsystem

The security unit includes a rapid response team and is the backbone of threat neutralization.

Alarm alarm is intended for psychological influence on the offender and pursues the goal of his refusal to intend to enter the protected territory.

Sources of emergency power are turned on automatically when the malicious user turns off the main power.

***Controls of the security system***

Automated systems (AS) have a hierarchical structure and are implemented on the basis of address panels that serve the sensors and actuators used, and the overall control is carried out by the PC.

The address bar is executed according to the modular principle, the composition of the equipment is regulated depending on the complexity of the object.

**3. The main areas of engineering and technical protection of information.**

***Tasks of engineering and technical protection of information***

**Engineering and technical information protection (ITZI)** is a set of measures aimed at ZI and includes regulatory and legal documents, organizational and technical measures.

Tasks ITZI:

1. Prevent the intruder from entering information sources with the aim of destroying, stealing or changing it.

2. Protection of information carriers from destruction as a result of the influence of natural forces and, above all, fire and water (foam) during its extinguishing.

3. Prevention of information leakage through various technical channels.

To ensure effective ITZI it is necessary to determine:

• what to protect with technical means in a particular organization, building, premises;

• what threats are protected information from intruders and their technical means;

• what methods and means are expedient for applying for OBI taking into account both the magnitude of the threat and the costs of its prevention;

• how to organize and implement technical ZE in the organization.

When organizing a ZI at an enterprise, it is also necessary to take into account the psychological factor (damage with information leakage, impossibility sometimes to reveal the true cause of the latter). These factors do not contribute to the psychological readiness of the manager for a sufficiently high cost for ZI, nevertheless, the world experience of organizing ZI suggests that the security of information firms are forced to allocate about 10-20% of the profits.

When choosing means of ZI, advertising can not always be believed.

**Principles of engineering and technical protection of information**

Basic principles of ZI:

• continuity of the ZI, characterizing the permanent readiness of the protection system to repel the threats of BI at any time;

• activity that involves predicting the actions of an attacker, developing and implementing advanced protection measures;

• secrecy, which excludes acquaintance of unauthorized persons with the means and technology of ZI;

• Dedication, which involves concentrating efforts to prevent threats to the most valuable information;

• Comprehensive use of various methods and means of ZI, allowing to compensate for the shortcomings of some of the merits of others.

Basic principles of professional approaches to the organization of ZI:

• compliance with the level of protection of the value of information;

• Flexibility of protection;

• multi-zone protection, providing for the placement of information sources in areas with a controlled level of its security;

• the multiplicity of ZI in the path of an attacker or carrier propagation.

Multizone provides differentiated authorized access of various categories of employees and visitors to information sources and is realized by dividing the space into so-called short-circuiting.

Typical faults are:

• the territory occupied by the organization and limited by a fence or conditional external border;

• building on the territory;

• Corridor or part thereof;

• premises;

• cupboard, safe, storage.

At the border of the zone, protection lines are created, they are characterized by the requirement of equal strength of the lines and the presence of checkpoints or posts.

Each zone is characterized by the level of security of the information it contains. BI depends on the zone:

• from the distance of the source of information to the attacker or his means of obtaining information;

• the number and level of protection of lines along the path of an attacker or the spread of another information carrier;

• the effectiveness of means and methods for managing the admission of people and vehicles to the zone;

• measures on the ZI within the zone.

The principles discussed above apply to protection in general. When constructing a security system, it is advisable to consider the following principles:

• minimization of additional tasks and requirements to employees caused by measures on ZI;

• reliability in the operation of technical means and systems, excluding both non-response to attack, and false triggering;

• limited and controlled access to the OBI system elements;

• continuity of the system;

• adaptability of the system to environmental changes.

The concealment of information provides for such changes in the structure and energy of carriers in which an attacker can not directly or by means of technical means extract information with a quality sufficient to use it for their own purposes (see Figure 6.8).

***Basic methods of information protection by technical means***

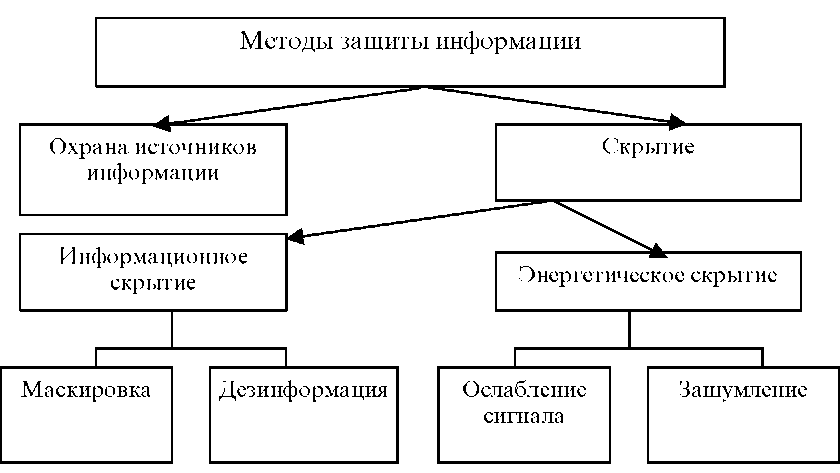


Fig. 6.8. Methods of ZI by technical means

**Information concealment** is achieved by changing or creating a false information portrayal of a message, physical object or signal.

Ways to change the information portraiture:

• removing a part of the elements or links forming the portrait information unit;

• changing part of the information portraits while preserving the unchanged links between the remaining elements;

• deleting or changing links between elements of the information portrait, while preserving their number. For example, removing the most information nodes from advertising.

**Misinformation** is a method of information concealment, which consists in the transformation of the initial information portrayal into a new one, corresponding to a false feature structure, and the imposition of a new portrait by an intelligence agency or an intruder.

Methods of misinformation:

• replacement of details of protected information portraits (for example, dual-use products at the enterprise - civil and military);

• maintaining a version with features borrowed from different information portraits of real objects;

• a combination of true and false characteristics, with a false, but the most valuable piece of information being replaced by false ones;

• changing only information nodes while keeping the rest of the information portrait unchanged.

**Energy concealment** consists in the application of methods and means of ZI, excluding or hindering the fulfillment of the energy condition of reconnaissance contact. It is achieved by reducing the ratio of signal energy, i.e. carriers with information and interference. The influence of interference leads to a change in the information parameters of the carriers: amplitude, frequency, phase.

Atmospheric and industrial interference have the greatest effect on the amplitude of the signal, to a lesser extent - on its frequency. But frequency-modulated (FM) signals have a wider spectrum of frequencies, therefore in functional channels that allow the transmission of broadband signals, information transmission is carried out by FM signals as the most noise-resistant. The quality of the received information deteriorates with a decrease in the signal-to-interference ratio.

The most stringent requirements to the quality of information are required for data transmission: the probability of a sign error in statistics and accounting is 10-5 - 10-6, according to monetary data - 10-8 - 10-9.

**Лекция №7**

**Methods of unauthorized access to information**

**План лекции**

1. Information leakage channels.

2. Active methods of unauthorized access to information.

**1. Information leakage channels.**

Under **the technical channel of information leakage** (TKUI) is understood the aggregate of the object of exploration, technical reconnaissance means (TCP), with the help of which information is obtained about this object and the physical environment in which the information signal is propagated (see Figure 7.1).

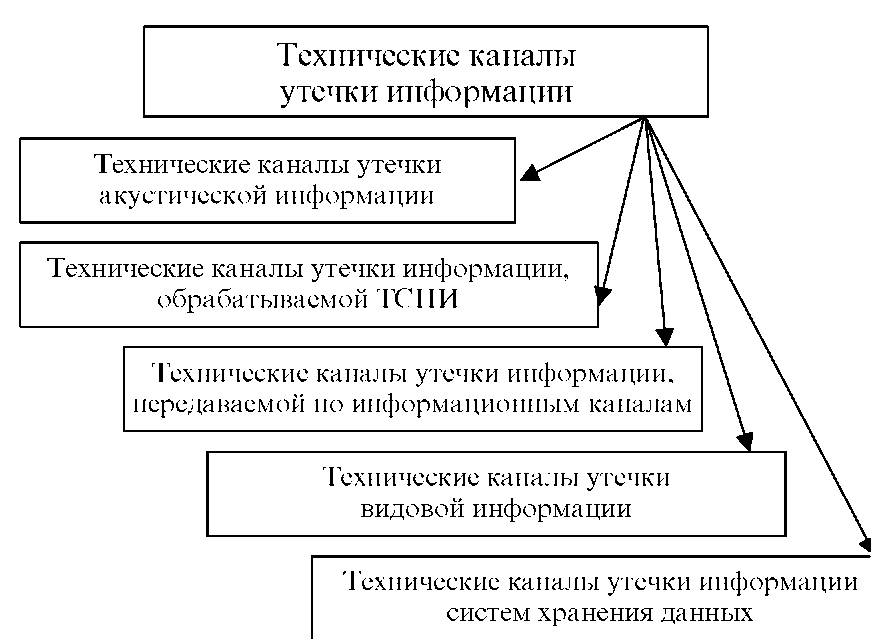


Fig. 7.1. Types of technical channels for leakage of acoustic information

The **technical means of receiving, processing, storing and transmitting information** (TSPI) is understood as technical means, directly processing information of limited access. These tools include: automated control systems, electronic computers, internal automatic telephone exchanges, loudspeaker communication systems, sound reinforcement and sound systems, etc. Depending on the physical nature of the appearance of information signals, as well as their distribution environment and methods of interception, the technical channels for information leakage can be divided into electromagnetic, electrical and parametric.

Electromagnetic channels include information leakage channels that arise due to various types of PEMI TSPI, namely:

• Emanations of elements of TSPI;

• emissions at the operating frequencies of high-frequency (HF) TSPI generators;

• Radiation at the self-excitation frequencies of low-frequency amplifiers (ULFs).

Causes of the emergence of electrical leakage channels can be:

• EMI TSPI interference on the connecting lines of auxiliary technical means and systems (VTSS) and foreign conductors that go beyond the short-circuit;

• leakage of information signals in the power supply network of the TSPI;

• infiltration of information signals in the earthing circuit of the TSPI.

Parametric TCHUI (RF-imposition) - a method in which a telephone line in the direction of the bug is fed from a special generator of high-frequency oscillation.

Radio clips are divided into telephone and microphone.

Under the NMS**, audio and video information** is understood as the actions of a subject to obtain confidential information on an object of interest by illegal means.

Depending on the physical nature of the appearance of information signals, the environment for the propagation of acoustic oscillations and the ways of their interception, the technical channels for leakage of acoustic (voice) information can be divided into air, vibration, electro-acoustic, opto-electronic and parametric.

Depending on the type of channels TKUI, transmitted through information channels, can be divided into electromagnetic, electric and induction.

Depending on the nature of the species information and its purpose, the following methods of obtaining (information leakage channels) are distinguished:

• observation of the object;

• shooting an object;

• shooting (copying) of documents.

Depending on the physical nature of the storage of information signals, the properties of the material from which the information carrier is made, the TKUI of storage systems can be divided into electromagnetic and parametric.

Typical constructions for the transmission of speech signals:

• bearing walls of buildings, partitions, floors of buildings, windows, doors, ventilation ducts in an acoustic signal;

• walls and partitions, ceilings, window frames, door frames, pipelines, ventilation ducts in the vibration channel.

There are three types of objects:

1. The object of listening is a room in a building occupied by several organizations. The listening channels at the same time are ventilation ducts, partitions, ceilings, pipelines for heating and water supply.

2. The object is in a separate building, to which there is separate access. The listening channels are window frames, ventilation openings, window air conditioners.

3. Object - a building with a secure territory. To obtain information, laser means, directional microphones, or shooting delivery devices for vibrating plates can be used secretly.

Another important selection criterion is the quality of information the channel can provide. To assess it, a characteristic is used, such as intelligibility of speech.

**Intelligibility** is the ratio of the number of correctly understood elements of speech (sounds, syllables, words) to the total number of elements transmitted on the channel (the limiting value of the intelligibility of syllables is 25%).

**Reverberation of sounds** - overlapping of speech segments on each other due to signal re-reflection from the surfaces of the structure. Reverberation time is less than 0.85 with imperceptible for hearing (cabinet - 0.2 - 0.6 s).

**Attenuation of sound vibrations**: attenuation in straight metal ducts is 0.15 dB / m; on bends - up to 3 - 7 dB (for one bend), with changes in the cross section - 1 - 3 dB; for reinforced concrete buildings, the absorption is 0.1 to 0.15 dB / m, for brick buildings 0.2 to 0.4 dB / m.

**Noises and noise** are artificial and natural signals that do not have an information component and interfere with the reception of an information signal. The largest noise is street noise (60 - 70 dB) [4, 6].

The possibility of creating long channels of leakage of acoustic information is associated with a microphone effect.

**The microphone effect** is the appearance in the circuits of radio electronic equipment (REA) of extraneous electric signals caused by the mechanical action of a sound wave.

**Acoustoelectric transducer** is a device that converts acoustic energy into electromagnetic energy.

Electroacoustic transducers are divided:

• electrodynamic, the action of which is based on the electrodynamic effect;

• electromagnetic, the action of which is based on the oscillation of the ferromagnetic core in an alternating magnetic field;

• electrostatic, whose action is based on a change in the force of attraction of the capacitor plates when the voltage across it changes.

• piezoelectric, the action of which is based on the direct and inverse piezoelectric effect (compression and stretching of the crystal);

• magnetostrictive transducers, whose action is based on the direct and inverse effect of magnetostriction (a magnetostrictive core wrapped by a wire)

**2. Active methods of unauthorized access to information.**

Illegal connection:

1. Contact connection:

• connection to communication lines by means of a matching device;

• connection of equipment to communication lines with voltage drop compensation.

2. Non-contact connection to the communication line is carried out in two ways:

• due to electromagnetic interference in the frame, parallel to the wires;

• using a concentrated inductance that covers the line.

There are various ways to suppress telephone bookmarks:

• sending a signal to the telephone line at frequencies outside the standard telephone range;

• in-line common mode interference at telephone frequencies;

• reduction of the current in the telephone network to the limit, when the speakers still hear each other, but the signal received by the sensor is so weak that it becomes comparable to the level of natural noise;

• change in line voltage.

Contact and non-contact connection is also possible to the lines of the fiber optic communication line (FOCL).

***Radiation and interference from video equipment***

Interception of information has a number of features:

• Information is obtained without direct contact with the source;

• the reception of signals is not affected by either the time of year or the time of day;

• information is obtained in real time;

• implemented secretly, no one suspects that they are being eavesdropped;

• The interception range is limited only by the propagation characteristics of radio waves.

The reasons for information leakage in FOCL are:

• radial inconsistency of the fibers to be joined;

• angular misalignment of optical fiber axes;

• the presence of a gap between the ends of the fiber;

• the presence of non-parallelism of the surfaces of the fiber ends;

• the difference in diameters of the cores of the fibers to be joined.

***Means of acoustic reconnaissance***

***Microphones, portable voice recorders and electronic stethoscopes***

Acquisition means are used to intercept and record conversations that are conducted in both open areas and in rooms and cars: microphones, directional microphones, contact microphones (stethoscopes), acoustic tabs, laser systems for acoustic reconnaissance, etc. (see Figure 7.2).

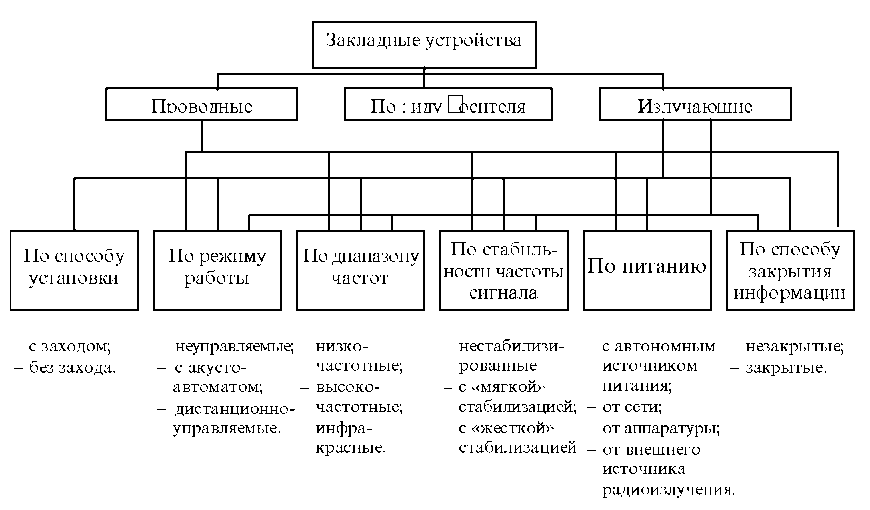


Fig. 6.2. Classification of embedded devices

These or other means of acoustic reconnaissance are chosen depending on the possibility of access to the controlled premises or to persons conducting conversations on an interesting topic.

In the event that there is constant access to the monitored premises, it can be equipped with miniature microphones in advance, the connecting lines of which are output to special rooms where the agent is located and the recording or transmitting equipment is installed. And the length of the connecting cable can reach 5000 m, for example, in the system PK 1055-SS.

To ensure that microphones are not detected, they are available in a sub-miniature version (diameter less than 2.5 mm) and are camouflaged for interior furnishings. For example, on the 19th floor of the building of the USSR representation in the UN in New York, the microphones were installed in the connectors of the individual outputs of the collective antenna and connected through an antenna cable with the transmitting equipment installed in the electronic side of the collective antenna.

Modern technology allows you to produce subminiature microphones that are easy to install behind a curtain, in a window frame or in a picture frame. A distinctive feature of the microphone is that it is not easy to detect even with the help of nonlinear locators.

Microphones of dynamic, capacitor or electret type have a sensitivity of 6-10 mV / Pa and are capable of registering a person's voice at a normal loudness at a distance of up to 10-15 m, and some samples at distances up to 20 m. At the same time, the frequency range is basically 100 - 300 Hz to 5 - 7 kHz. However, in some cases microphones with a frequency range from 50 Hz to 15 - 18 kHz are used.

To improve the quality of intercepted calls, microphones are installed, as a rule, near places of possible conversations, for example, a table in a room for negotiation or in a conference room.

The recording or transmitting equipment is installed, as a rule, in places, access to which is difficult. For example, in the building of the USSR Embassy in the United States, the recording and transmitting equipment was installed in rafters in the attic and at the base of the building foundation at a depth of 2 meters.

As a recording equipment, as a rule, tape recorders and dictaphones with a long recording time (up to 7 - 16 hours) are used. As the transmitting equipment, radio transmitters operating in the VHF, UHF and SHF (GHZ) bands are used in the main, and use complex signals and encoding (encryption) of transmitted information. In a number of cases, the transmission uses speed hardware.

Controlled rooms are equipped with an eavesdropping system mainly in the construction or reconstruction of the facility.

If agents do not have permanent access to the controlled premises, but there is a possibility of short-term visits under various pretexts, for example, checking the lighting, air conditioning or cleaning of the room, portable tape recorders and voice recorders camouflaged for everyday use, for example, books, written instruments, packets of cigarettes, etc. They are secretly installed indoors, usually just before the closed event. After the end of the event tape recorders (dictophones) are removed from the premises.

Currently, foreign companies produce a huge number of portable dictaphones, easily fit in the pockets of your jacket or trousers and provide a continuous recording time of 30 minutes to several hours.

In the event that it is not possible to penetrate even a short time into a controlled room, but there is the possibility of access to neighboring premises, electronic stethoscopes are used for reconnaissance, which convert acoustic vibrations in solids (walls, ceilings, floors, etc.) in electrical.

A sensitive element of electronic stethoscopes is a contact microphone (most often a piezoelectric element) connected to an amplifier.

Modern electronic stethoscopes have a gain of about 80 - 90 dB (20,000 - 30,000 times) and are capable of capturing weak sound vibrations (rustling, ticking of clocks, etc.) through concrete walls of up to 50 - 100 cm thick, as well as doors and window frames with double glazing. Information can be removed not only directly from walls, ceilings, glass, but also steel structures of buildings, pipes of heating and water supply systems, etc.

The sensors of electronic stethoscopes can be installed in the walls of buildings during the construction or reconstruction phases. For example, in the new building of the US Embassy in the USSR, the sensors were installed in the steel structures of the building and were technologically made so that they could not be detected even using X-ray equipment.

To intercept acoustic (voice) information along with portable dictaphones, special miniature electronic devices intercept acoustic (voice) information, unauthorized and secretly installed in rooms or cars and often called **acoustic tabs**.

Acoustic tabs can be classified according to the type of performance, installation site, power source, method of information transmission and coding, control method, etc.

Bookmarks can be made in the form of a separate module, usually in the form of a parallelepiped, or camouflaged for everyday use: ashtrays, electronic calculators, light bulbs, lighters, wristwatches, pens, vases, waist belts, etc.

Modern technology allows you to perform acoustic tabs the size of a rice seed and weighing several grams. However, the range of information transfer from such bookmarks is several tens of meters, and the operating time is several hours.

Acoustic tabs can be installed in the interiors of the room, in everyday objects, in radio equipment, in electrical outlets and electrical appliances, in technical means of communication and their connecting lines, etc. They can also be hidden in the clothes and personal belongings of the agent in the room.

The information intercepted by acoustic tabs can be transmitted over a radio or optical channel, AC power supply, VTSS connecting lines (for example, telephone line), as well as metal structures of buildings, pipes of heating and water supply systems, etc.

The most widely used acoustic tabs that transmit information over a radio channel. Such devices are often called radio pads.

Depending on the environment for the propagation of acoustic oscillations, intercepted radio locks can be divided into acoustic and radio-stethoscopes.

Acoustic radio locks are designed to intercept acoustic signals through an air channel of information leakage and the sensitive element in them is, as a rule, an electret microphone. Therefore, acoustic radio patches are sometimes called radio microphones, but this term is rarely used among intelligence specialists. Such means allow to catch quiet speech at a range of 5 - 10 m.

Radio-stethoscopes (contact microphones, structurally integrated with microprotritters) intercept acoustic signals via a vibration channel for information leakage, and piezo microphones, electret microphones, or accelerometer sensors are usually used as sensing elements.

Radio-stethoscopes are capable of capturing sound vibrations through concrete walls 0.3-0.5 m thick, as well as through doors and window frames.

The supply of acoustic tabs is provided by autonomous power supplies (batteries, batteries), AC mains, telephone network, and also from power sources of CEA, in which they are installed.

When power is supplied from the AC or telephone line, the operating time is unlimited.

Technically, you can make a bookmark that transmits information in virtually any radio wave band. However, bookmarks working in the VHF band were widely used.

For transmission of information, the following wavelength ranges are mainly used: VHF (meter), UHF (decimeter) and GHz (GHz). The most frequently used frequencies are: 88 - 108 MHz; 108 - 174 MHz; 400 - 512 MHz; 1100 - 1300 MHz. However, it is possible to use other subbands. Most radio sets with autonomous power sources have a radiation power of up to 10 mW and a transmission distance of up to 100-200 m. However, there are tabs with a radiation power of several tens of milliwatts and a transmission distance of up to 500-1000 m.

If you need to transfer information over long distances, special relays are used.

To increase the working time, the tabs are equipped with a voice-activated control system for the transmitter (VAS or VOX system). Sometimes such a system is called an acoustomat. Those. a bookmark in the normal mode (standby mode) works as an acoustic signal receiver, while the current consumption is negligible. When a source of an acoustic signal appears in the room, for example, at the beginning of a conversation, the voltage is applied to the transmitter and it starts to work on the radiation, that is, transmit information.

Using the VAS system allows you to significantly (several times) increase the time of the bookmark.

The absence of semiconductor devices in the tabs makes it ineffective to search for them even with the use of nonlinear locators.

Along with the tabs described above, semi-active tabs called "audio transponder" are used to remove information. Such tabs include, for example, SIM-ATP-16, SIM-TP ^, PK-500, etc. Transponders start to work only when they are irradiated with a powerful narrow-band high-frequency probing (reference) signal. Transponders receive a probe signal and feed it to a modulator, where, as a rule, narrowband frequency modulation of the signal is carried out. As the modulating signal is used, coming either directly from the microphone, or from a microphone amplifier. The modulated RF signal is re-emitted, while its frequency is shifted relative to the carrier frequency of the sounding signal. The time of operation of transponders is several months, since the current consumption is insignificant.

The Audi-transponders SIM-ATP-16 and SIM-TR-40 are made using MOS-technology, which makes it difficult to detect them even with the use of non-linear locators.

To receive information transmitted from radio tabs, depending on the frequency of their operation, conventional radios, receivers of portable radio stations or special radio receivers are used.

If the radio bookmark is operating in the range of 88 - 108 MHz, then any household radio receiver having FM (for domestic VHF-2 receivers) can be used to receive information. This is both an advantage, there is no need to buy a special receiver, and a drawback - the fact of its operation is easy to detect.

A large number of radio sets has operating frequencies in the bands allocated for the organization of VHF radio communications - these are basically the ranges: 134 - 174 MHz, 400 - 512 MHz. To receive information from such tabs portable portable radios having very high sensitivity receivers can be used (sensitivity in the mode of receiving a signal with narrowband frequency modulation at a signal-to-noise ratio of 12 dB is 0.25-0.5 μV). Modern radio stations are equipped with built-in scramblers, allowing to receive coded information, which can also be attributed to the benefits. The disadvantage is that portable radios provide high quality of the received signals only from radio tabs having narrowband frequency modulation and using quartz frequency stabilization.

The disadvantage of radio tabs is the possibility of detecting their emissions by a special receiver of control. In order to eliminate this disadvantage, mortgage devices have been developed that transmit information through an optical channel in the IR, an invisible range (such tabs are sometimes called **infrared**). The IR transmitter converts the acoustic vibrations into light ones, using the pulse width modulation. To receive information transmitted by such tabs, POI is used. The range of information transmission for them is several hundred meters. For example, the STG-4403 infrared transmitter provides information transfer at a distance of up to 500 m.

Detect a bookmark that transmits information in the infrared range, you can only have a special POI. However, such systems have one very important drawback: the reception of information from such a bookmark is possible only if it is in the line of sight. Those. At the time of the removal of information, the bookmark should be observed through the POI viewer. Therefore, such bookmarks are installed, as a rule, from the outside of the window frames, in the vent, etc., which facilitates the task of finding them.

In addition to the radio and optical channel, power lines of the 220 V power network are used to transfer information. Bookmarks using power lines for information transfer are often called network bookmarks. They can be installed in electrical outlets, extension cords, household appliances powered by AC power, or directly into the power line. The principle of their work differs little from the principle of the work of radio sets. Only the carrier frequency is selected in the range of 40 - 600 kHz, and the antenna is an electrical wire. In a single power grid, dozens of network transmitters can operate simultaneously, without significantly affecting each other.

To receive information from such tabs, special receivers are used that are connected to the power network, i.e. in the socket. If you are away from the bookmark for a distance of several tens or even hundreds of meters, it is possible to receive information without connecting to the receiver network, but only by bringing its antenna closer to the power cable or wire. However, the quality of the signal (speech intelligibility) will of course be lower.

In network tabs, remote control devices can be used that transmit coded signals for switching (switching off) the bookmark transmitter also over the electrical network.

With the use of network bookmarks, information can be transmitted over significant distances (up to 300-500 m) within a building or several buildings that are powered by a single low-voltage bus of a transformer substation.

In addition to the power supply network, any current-carrying elements, for example, pipes of water supply and heating systems, building metal structures, as well as VTSS connecting lines, signal, calling and other cable lines, can be used for information transfer.

In this case, not only electric and electromagnetic, but also mechanical ultrasonic waves can be used as an information carrier. The hiddenness of the work of ultrasonic bookmarks is very great, because At present, there are practically no means to take and detect ultrasonic vibrations. And you can detect such a bookmark only by a nonlinear locator.

To transfer information, telephone lines are also effectively used. In this case, you can use bookmarks, the principle of which is similar to the principle of network bookmarks, as well as bookmarks that transmit information directly in the speech range. The range of information transfer using this bookmark is up to 7 km.

To intercept acoustic (voice) information over the telephone line, also mortgage devices such as "telephone ear" can be used, the reception of information from which can be carried out from any telephone.

The device "telephone ear" is a highly sensitive, usually electret microphone with an amplifier and a special device for connecting to a telephone line when dialing in accordance with a certain scheme. Such devices are installed either in a telephone socket, or directly in the phone casing, called the "phone-observer".

The device is powered by a telephone line, so the service life of the bookmark is almost unlimited.

The principle of dialing is the following:

1) the number of the "phone of the observer" is dialed (the device "suppresses" the first two ringing tones);

2) a hang-up (handset is put) after the first ring signal;

3) the number of the "phone-observer" is redialled so that the first ringing tone for the second set falls within the interval 15 - 30 s after the first set of ringing signal;

4) when the dial is correctly executed, a busy signal appears in the handset, which disappears after 45 seconds, and a microphone is connected to the line, which makes it possible to listen to conversations in the room where the device is installed;

5) the device automatically turns off after a certain time interval (4, 8, 17, 34 minutes) or when the "Observer Phone" tube is raised.

The disadvantage of this device is the complexity of dialing, in many cases excluding listening to a room from a phone located in another city or country.

The tactics of using acoustic tabs largely depend on the possibility of access to the controlled premises, the qualification and equipment of the security service.

The most favorable for the installation of mortgage devices is the stage of construction or reconstruction of the facility, when there is practically free and uncontrolled access to the premises, to its lighting systems, alarms, communications, etc. In this period, quite complex devices can be installed, including those with remote control, which use complex signals and information coding for transmission. This, as a rule, or network bookmarks, or radio, powered by AC power or from a telephone line, i.e. bookmarks with unlimited time of action, as well as bookmarks with the transfer of information through the IR channel. They are installed in hard-to-reach places and are well camouflaged. For example, in the building of the USSR Embassy in the United States, bookmarks with contact sensors were installed deep inside reinforced concrete panels and brick walls, and optical-electronic (IR) devices built into the facing panels were used to transfer information. Bookmarks with sensors of contact type and transmitting information on the radio channel were also installed in the heat-insulating pads of window frames.

During the construction period, long-time radio-stethoscopes can be built into the walls of the building. For example, the radio-stethoscope "Brick-2 St". This radio-stethoscope is made in the form of two ordinary bricks, which are installed in building structures. Sensors of the accelerometer type intercept the vibrations that arise when conducting conversations in rooms in the frequency range from 100 Hz to 10 kHz. Two-channel system of volume (stereo) sounding allows to improve the intelligibility of speech by 15%. The radio-stethoscope uses quartz frequency stabilization, remote control and coding of transmitted information. The transmission range of information at frequencies 430 - 470 MHz is up to 500 m. The service life of the radio-stethoscope is 10 years.

If access to the premises is not controlled, bookmarks can be set and during the operation of the facility. For example, for preventive maintenance on power supply systems, communication, signaling or cleaning of premises. And the time in a few minutes is enough to install instead of the usual socket network bookmark or radio in the table lamp. Replacing the same tee or extension cord with similar devices, but equipped with bookmarks, will take several seconds.

If access to the premises is controlled, but visitors can stay there even for a short time (most often they are offices, reception rooms or executive lounge rooms), the bookmarks can be set either by replacing items that are constantly in the same room with similar but equipped with bookmarks, or directly in the interiors of the room, for example, under an armchair or table, under a window sill, behind a curtain, etc., or even in a crumpled pack of cigarettes, or a piece of cardboard thrown into an urn. Bookmarks can be camouflaged in objects and things "accidentally" forgotten by a visitor, for example, a pen, a calculator, a briefcase, a hat, etc. Of course, the visitor will return for "forgotten" things in a few hours or even a day, but this time is sometimes enough to obtain important information, for example, if such a visitor is in the premises shortly before a secret meeting.

Find bookmarks installed in the radio equipment and camouflaged for typical units and parts, without the use of special X-ray technology is almost impossible. Although, of course, at the time of the transfer of information by a radio pad, it is possible to establish the fact of its presence in one or another apparatus.

If access to the monitored premises is impossible, but access to adjacent premises is not excluded, radio-stethoscopes can be used to remove information. The tactics of using them are similar to the use of conventional stethoscopes, but the presence of a radio channel eliminates the need for the presence of an agent or recording equipment at the time of information removal, which makes it possible to covertly install radio-stethoscopes in small, inaccessible places.

To remove information from external window panes, you can use subminiature radio-stethoscopes lined with sticky rubber mass and in appearance resembling a ball or a lump of dirt. Such a ball is glued by hand from the outside of the window and transmits information for 1 to 2 days, after which the rubber mass dries out, the tab will separate from the surface on which it was attached and fall down.

To install bookmarks in places that can not be physically accessed, special silent guns (crossbows) are used, shooting "arrows-radio pads". The boom with a miniature radio pad, made in a shock-resistant design, is securely attached to surfaces of any material: metal, wood, plastic, glass, stone, concrete, etc. at a shot from a distance of up to 25 m.

To intercept conversations that are conducted, for example, in a park or forest, when the place of conversation is known in advance, special embedded devices with seismic sensors can be used. Such bookmarks, installed under the soil layer, record microseismic vibrations that arise in the ground during the conduct of conversations, convert them into electrical signals and transmit them via a special cable or radio channel to record to recording devices. Such tabs include, for example, the "Geophone" device capable of providing high quality of information retrieval within a circle with a radius of up to 5 m with average acoustic noise and up to 10 m at low acoustic noise. The range of information transmission by cable is up to 50 m [5].

***Directional microphones and laser acoustic pick-up systems***

If you want to organize listening to conversations in a room that can not be accessed in the same way as access to neighboring rooms, then directional microphones and laser acoustic locating systems (LALS) are used.

Directional microphones have a gain of more than 0 - 90 dB and allow listening to conversations at distances of up to 300 - 500 m (in city conditions - up to 50 - 70 m).

In general, three types of directional microphones are used: parabolic (reflex), tubular ("microphone-tube") and flat (microphone grids) microphones.

The parabolic microphone has a parabolic reflector, in the focus of which there is an ordinary high-sensitivity microphone.

"Microphone-tube" is a tubular phased receiving acoustic antenna, loaded on a highly sensitive microphone or a grid of microphones connected in series.

The range of reception signals of similar microphones can be increased by using a larger number of tubular elements.

"Microphone-tube" can be camouflaged with an umbrella or cane or made in the usual performance.

The so-called "flat" directional microphones have appeared relatively recently and represent an acoustic antenna array comprising several dozen microphones. They can be built into the attache-case wall or even worn in the form of a vest under a shirt or jacket. The range of their action is relatively lower in relation to the first two types of directional microphones and is 30 to 50 m.

If you want to listen to conversations indoors at a considerable distance,

**LALS.** In practice, such systems are often called laser microphones.

LALS consists of a source of coherent radiation (laser) and POI, equipped with focusing optics. To ensure high mechanical stability of the transmitter and receiver, which is extremely necessary for the normal operation of the system, the latter are installed on tripod tripods. Transmitter and receiver are transferred in the usual portfolio-diplomat.

As a rule, such systems use lasers operating in the near infrared (0.9-1.1 μm), an invisible wavelength range.

To improve the intelligibility of speech in the receiver, a special noise-canceling device is used.

To guide the laser beam to the target, special devices are used in conjunction with the transmitter and receiver.

These systems are most effective for listening to conversations in small-sized rooms, which in their acoustic characteristics are close to the Helmholtz resonant cavity, when all the doors and windows of the room are well sealed. They are effective also for eavesdropping of conversations conducted in car interiors.

Modern LALS allows you to take information not only from external, but also from inside window panes, mirrors, glass doors and other objects. In a number of cases, the window panes are secretly treated with a special composition that increases the reflection coefficient of the laser radiation, and, consequently, increases the range of reconnaissance.

Laser acoustical reconnaissance systems have a range of action with diffuse reflection up to 100-300 m without special glass processing, up to 500 m - when processing (covering) glasses with special material that significantly increases the power of laser radiation diffusely reflected from them, and more than a kilometer - when mounted on a window panes of special directed reflectors (triple prisms).

Acoustic reconnaissance means can be used not only to listen and record ongoing conversations, but also to intercept acoustic emissions that occur when printing text, for example, on a printer. Modern special complexes for the processing of acoustic information can recover text that is printed on intercepted acoustic emissions.

To improve the quality and to ensure correction of the recorded conversation, stereo tape recorders and equalizers are used.

With the use of stereo tape recorders, it is possible to differentiate and separate from informative colloquial speech due to the stereo effect such interference as the noise of household appliances, external street noise, etc.

**Лекция №8**

**Protection of computer and audio-visual information**

**План лекции**

1. Countering the leakage of computer and audio-video information.

2. Application of cryptography.

3. Ensuring the security of data in computer networks.

**1. Countering the leakage of computer and audio-video information.**

The goal of protecting audio and video information is the need to make it as difficult as possible for potential adversaries to realize their intentions.

Information that needs protection for businessmen, entrepreneurs and politicians:

• commercial secret (CT);

• timetable and addresses of business and personal meetings;

• information about human weaknesses;

• data on friends, places of leisure, routes of movement;

• information on places of storage of material values, time and routes of their transportation and in general about financial well-being;

• a true attitude towards one or another "strongman of this world".

How to protect yourself from inserting and installing eavesdropping devices in an apartment, office and on the telephone subscriber line:

1. Seal or secretly mark for the opening of telephone switchboards, cabinets boxes.

2. At occurrence of unfamiliar repairmen demand documents and a call on automatic telephone exchange check up correctness of spent works.

3. In carrying out any work on electrical, repair equipment, telephones, etc. outsiders, ask someone to be present or understand.

4. Limit access to the office, try to organize it so that no one can be there alone (seal the nursing cabinet) [6].

***Passive opposition***

**Passive means of NDT** are devices that receive and process EMR from conventional electronic equipment located in office premises.

Active means of unauthorized use are installed directly in controlled devices and use the radio channel to transmit the information received.

Passive means of the ZI include low-pass filters installed in power and signal inputs into rooms, and screening of these rooms.

Network filters perform two functions in the power supply circuits of the TSPI:

• protection of equipment from external impulse noise;

• Protection against interference caused by the equipment itself.

The shielding is designed to eliminate interference from the TFI in rooms whose lines extend beyond the fault limits.

Sound insulation is directed to the localization of the sources of acoustic signals in a closed space inside the fault. Sound insulation is provided with the help of architectural and engineering structures: fences, screens, cabins, casings.

Sound absorption is achieved by converting the kinetic energy of an acoustic wave into thermal energy in a sound absorbing material.

The means of sound absorption in the premises used for acoustic processing of premises are subdivided:

• on sound-absorbing facings in the form of acoustic plates of fine granular or cellular structure;

- sound-absorbing linings from a layer of porous-fibrous material in a protective shell of a fabric with a perforated coating.

***Protection of telephone sets***

According to American data, the probability of information leakage through telephone channels is from 5 to 20%.

There are six main listening zones:

• telephone set;

• a line from the telephone set, including the junction box;

• cable area;

• ATS area;

• zone of multichannel cable;

• radio channel zone.

The most likely organization is listening to the first three zones, tk. it is in these areas that it is easiest to connect to the telephone line.

Specialists engaged in ZI, argue that most often used listening with a parallel device. In most cases, this does not even require additional wires: the telephone network is so confused that there are always unused lines. In addition, it is not difficult to connect in the front door to the junction box.

Telephone sets with button-type dialing type TA-T, TA-12 are very common. Due to the peculiarities of their design, they re-emit information on dozens of frequencies of CB, HF and VHF bands for a distance of up to 200 m. To protect the telephone set, it is necessary to protect the microphone circuit, ring circuit, two-wire communication line.

***Protection of communication lines***

External connections should be understood as information lines of communication between the TFI devices. External connections and ways to implement them affect the properties of the TFI, such as PEMI.

To protect communication lines from interference, it is necessary to place the line in a shield braid grounded in one place. To reduce the electrical and magnetic coupling between the wires, it is necessary to maximize the separation of the circuits.

***Protection from built-in and narrow-microphones***

To protect against narrow microphones, you need:

• When closing business meetings, be sure to close windows and doors;

• for negotiations choose premises with isolated walls;

• try to get to know neighbors on the floor above or below;

• On the street all the time move, sharply change the direction of movement, organize counter-observation;

• have a reliable headwaiter; in a restaurant a static position allows you to control your conversations in common rooms;

• Hold negotiations secretly in the hotel room.

***Protection from laser listening devices***

Vibroscopes are used for protection. Passive energy concealment of acoustic information from eavesdropping by a laser microphone consists in weakening the energy of the acoustic wave acting on the window glass (curtains, blinds, double frames).

***Detection of radio emissions***

Radio clips contain three main nodes:

• a microphone that determines the zone of acoustic sensitivity;

• a radio transmitter that determines the secrecy and range of action;

• a power source that determines the duration of the operation.

To detect dangerous EMR and measure their levels, special measuring receivers are used, automatically scanning over the frequency range. With their help, the search and fixing of operating frequencies are carried out, as well as the location of the radio locks.

If the radio bookmark is turned off, special X-ray machines and non-linear detectors are used (they react to the foreign body in a homogeneous medium, the wall).

***Nonlinear radars***

Application area:

• search for tagged passive (without a power source) markers of people in snow obstructions, destroyed buildings;

• detection of electronic components and radio equipment when trying to covertly carry them through the checkpoint;

• detection of unauthorized removal of marked items from office premises;

• detection and location of hidden electronic means of industrial espionage;

• remote control of passenger baggage.

***Countering the leakage of computer and audio-visual information***

Vibroacoustic room noisy systems create a noise band of audio frequencies in order to prevent listening to a noisy room.

When working on a computer, you should remember both the safety precautions and take measures to ensure the safety of computer information.

It should be remembered that caring for the safety of computer equipment is a concern for the safety of information.

The greatest trouble to the user is delivered by computer viruses. Typical signs of computer virus infection are as follows:

• significant slowdown of the computer;

• periodic appearance of foreign characters on the screen;

• increase the size of files;

• frequent reboot and hang;

• loss of workability of individual programs;

• chaotic change in text files and database files;

• disappearing files;

• violation of the file structure of the disk;

• violation of the computer configuration parameters.

To diagnose viruses and treat infected files, there are special anti-virus programs.

Preventive antivirus actions:

1. Observe strict input control of external floppies.

2. Do not leave the computer turned on unattended.

3. Periodically, every time you turn on your computer, scan your computer with anti-virus software.

4. Save the most valuable programs on diskettes, preferably in an archived form.

5. Use legal versions of programs.

6. Use extreme caution when using games.

7. Control access to the hard disk by using hardware.

Protection against unauthorized use by means of cryptographic protection: algorithm DES, used in the US since 1976; algorithm of cryptographic transformation, defined by GOST 28147-89.

October 2, 2000, the US Department of Commerce summed up the competition to develop a new encryption standard: the new code Rijndael is intended to replace the DES algorithm.

**2. Application of cryptography**

The problem of protecting information by transforming it, excluding its reading by an unauthorized person, worried the human mind from a long time ago. The history of cryptography is the same age as the history of the human language. Moreover, originally the writing itself was a cryptographic system, since in ancient societies it was owned only by the elite. The sacred books of Ancient Egypt, Ancient India are examples.

Different people understand different things from encryption. Children play toy ciphers and secret languages. This, however, has nothing to do with real cryptography. This cryptography (strong cryptography) should provide such a level of secrecy, so that it is possible to reliably protect critical information from decoding by large organizations such as the mafia, transnational corporations and large states. This cryptography in the past was used only for military purposes. However, now, with the formation of the information society, it becomes the central tool for ensuring confidentiality.

As the information society is formed, large countries are given access to technological means of total supervision of millions of people. Therefore, cryptography becomes one of the main tools providing confidentiality, trust, authorization, electronic payments, corporate security and countless other important things.

Cryptography is no longer a concept of the military, which should not be contacted. It is time to remove from the cryptography cover of mystery and use all its possibilities for the benefit of modern society. The widespread use of cryptography is one of the few ways to protect a person from the situation when he suddenly discovers that he lives in a totalitarian state that can control every step he takes.

Cryptographic systems developed rapidly during the first and second world wars. Beginning with the postwar period and to this day, the emergence of computing tools has accelerated the development and improvement of cryptographic methods.

Why the problem of the use of cryptographic methods in IP has become particularly relevant at the moment?

On the one hand, the use of computer networks, in particular the global Internet, has been expanded, over which large amounts of state, military, commercial and private information are transmitted that do not allow unauthorized access to it.

On the other hand, the emergence of new powerful computers, network and neural computing technologies has made it possible to discredit cryptographic systems, which were recently considered virtually undiscovered.

The problem of information protection through its transformation is engaged in *cryptology* (*kryptos* - secret, *logos* - science). Cryptology is divided into two areas - *cryptography and cryptanalysis*. The goals of these directions are directly opposite.

*Cryptography* is engaged in the search and research of mathematical methods of information transformation.

The sphere of interest of *cryptanalysis* is the study of the possibility of deciphering information without knowing the keys.

Modern cryptography includes 4 large sections.

• Symmetric cryptosystems.

• Cryptosystems with public key.

• Electronic signature systems.

• Key management.

The main directions of using cryptographic methods are the transfer of confidential information via communication channels (for example, e-mail), authentication of transmitted messages, storage of information (documents, databases) on media in encrypted form.

**Terminology.** So, cryptography makes it possible to transform information in such a way that its reading (restoration) is possible only if the key is known.

As the information to be encrypted and decrypted, texts constructed on some alphabet will be considered. These terms are understood as follows.

*Alphabet* - the final set of symbols used for encoding information.

Text is an ordered set of alphabet elements.

As examples of the alphabets used in modern IS, the following can be cited:

• the alphabet Z33 - 32 letters of the Russian alphabet and a space;

• Z256 alphabet - characters included in the standard ASCII and KOI-8 codes;

• binary alphabet - Z2 = {0,1};

• an octal alphabet or hexadecimal alphabet.

*Encryption* is a transformative process: the source text, which also has the name of plain text, is replaced by encrypted text.

*Decryption* is the reverse of the encryption process. Based on the key, the encrypted text is converted to the original one.

*The key* is information necessary for unencrypted encryption and decryption of texts.

*The cryptographic system* is a family T [T1, T2, ..., Tk] of open text transformations. Members of this family are indexed, or denoted by the symbol k; parameter k is the key. The key space K is the set of possible key values. Usually the key is a consecutive series of letters of the alphabet.

Cryptosystems are divided into *symmetric and public key*.

*In symmetric cryptosystems*, both for encryption and for decryption, the same key is used.

*In systems with a public key* two keys are used - open and closed, which are mathematically related to each other. The information is encrypted using a public key, which is accessible to everyone, but decrypted using a private key known only to the recipient of the message.

*The terms key distribution and key management* relate to the processes of the information processing system, the content of which is the compilation and distribution of keys between users.

*An electronic (digital) signature* is a cryptographic transformation that is attached to the text, which allows you to verify the authorship and authenticity of the message when receiving text by another user.

*A cryptographic characteristic* is the characteristic of a cipher, which determines its resistance to decryption without knowledge of the key (ie cryptanalysis). There are several indicators of cryptographic stability, among which:

• the number of all possible keys;

• the average time required for cryptanalysis.

The transformation of Tk is determined by the corresponding algorithm and the value of the parameter k. The effectiveness of encryption for the purpose of protecting information depends on the secrecy of the key and the cryptographic strength of the cipher.

***Requirements for cryptosystems***

The process of cryptographic data closure can be implemented both programmatically and in hardware. Hardware implementation is significantly more expensive, but it also has advantages: high performance, simplicity, security, etc. The software implementation is more practical, allows for a certain flexibility in use.

For modern cryptographic information security systems, the following generally accepted requirements are formulated:

• the encrypted message must be readable only if there is a key;

• The number of operations necessary to determine the encryption key used for the fragment of the encrypted message and the corresponding plaintext corresponding to it should be not less than the total number of possible keys;

• The number of operations necessary to decrypt information by searching all possible keys must have a strict lower bound and go beyond the capabilities of modern computers (taking into account the possibility of using network calculations);

• knowledge of the encryption algorithm should not affect the reliability of protection;

• a minor change in the key should lead to a significant change in the type of encrypted message, even when using the same key;

• the structural elements of the encryption algorithm must be unchanged;

• additional bits entered in the message during the encryption process must be fully and securely hidden in the encrypted text;

• the length of the encrypted text should be equal to the length of the source text;

• there should not be simple and easily established dependencies between keys that are consistently used in the encryption process;

• any key from the set of possible ones must provide reliable information protection;

• The algorithm should allow both software and hardware implementation, while changing the length of the key should not lead to a qualitative deterioration of the encryption algorithm.

***Basic encryption algorithms***

The encryption-decryption method is called a cipher. Some encryption algorithms are based on the fact that the encryption method (algorithm) itself is secret. Nowadays such methods are of only historical interest and have no practical significance. All modern algorithms use a key to control encryption and decryption; The message can be successfully decrypted only if the key is known. The key used for decryption may not coincide with the key used for encryption, however in most algorithms the keys match.

Algorithms using a key are divided into two classes: symmetric (or algorithms with a secret key) and asymmetric (or algorithms with a public key). The difference is that symmetric algorithms use the same key for encryption and decryption (or the decryption key is simply calculated by the encryption key). While asymmetric algorithms use different keys and the decryption key can not be computed by the encryption key.

*Symmetric algorithms* are divided into stream ciphers and block ciphers. Streaming allows you to encrypt information bit by bit, while block processors work with some set of data bits (usually the block size is 64 bits) and encrypt this set as a single unit.

*Asymmetric ciphers* (also called public-key algorithms, or more generally public key cryptography) allow a public key to be publicly available (say, published in a newspaper). This allows anyone to encrypt a message. However, only the right person (the one who owns the decryption key) can decrypt this message. The key for encryption is called a public key, and the key for decryption is a private key or secret key.

Modern encryption-decryption algorithms are quite complex and can not be done manually. These cryptographic algorithms are designed for use by computers or special hardware devices. In most applications, cryptography is produced by software and there are many cryptographic packages available.

Generally speaking, symmetric algorithms work faster than asymmetric algorithms. In practice, both types of algorithms are often used together: a public-key algorithm is used to randomly generate a secret key that is then used to decrypt the message.

Many high-quality cryptographic algorithms are available widely - in a bookstore, library, patent office or on the Internet. To widely known symmetric algorithms are DES and IDEA, Probably the best asymmetric algorithm is RSA.

However, this criterion does not take into account other important *requirements for cryptosystems*:

• impossibility of disclosure or meaningful modification of information on the basis of analysis of its structure;

• perfection of the used protection protocols;

• the minimum amount of key information used;

• minimal complexity of implementation (in the number of machine operations), its cost;

• high efficiency.

It is desirable, of course, to use some integral indicators that take into account these factors.

To take into account the cost, complexity and volume of key information, one can use specific indicators - the ratio of these parameters to the power of the set of key codes.

Often more effective in selecting and evaluating a cryptographic system is the use of expert assessments and simulation modeling.

In any case, the selected set of cryptographic methods should combine both convenience, flexibility and efficiency of use, as well as reliable protection against intruders of information circulating in the IS.

**3. Ensuring the security of data in computer networks.**

A network of computers or a computer network is usually called a set of interacting stations organized on the basis of computers interconnected by means of data transmission channels that form the data transmission medium.

Computing networks are divided:

• in scale - local and global;

• Organization way - centralized and decentralized;

• topologies (configurations) - star, ring, bus, mixed.

**Local area networks (LANs)** are networks whose nodes are located at short distances from each other.

***Network Operating Systems***

Modern network operating systems (OS) can be divided into three classes: "DOS-oriented", "OS / 2-oriented", "UNIX-oriented".

**"DOS-oriented"** - network systems assume the availability of network software on each workstation LAN or the allocation of a server for a server. Each computer on the network can use the resources of another computer.

"**OS/2-oriented."** Of particular interest are network operating systems such as OS / 2 workstations of the PS / 2 series from IBM. In addition, it is possible to use the Microsoft LAN Manager system program and the access program for multi-user SQL Server databases.

**"UNIX-oriented"** network operating systems are used for collective application of peripherals, file exchange or "e-mail", when a joint OA is necessary.

The latest developments of Novell's network operating systems include Novell NetWare v. 4.0 and v. 4.1, designed for large corporate LANs with a number of workstations up to 1000, as well as Novell Personal NetWare, targeting an average LAN with up to 50 users.

For data transmission networks, the real threat poses threats:

1. Listening to the channels.

2. Deliberate destruction or distortion of messages passing through the network, as well as the inclusion of false messages in the flow.

3. Assignment of an alien identifier by an intruder to its own node or a relay, which makes it possible to receive and send messages from someone else's name.

4. Introduction of network viruses.

In accordance with this, specific protection tasks in data transmission networks are as follows:

1. Authentication of single-level objects.

2. Access control.

3. Masking of data circulating in the network.

4. Monitoring and restoring the integrity of the data in the network.

5. Arbitration, i.e. protection against all possible refusals to send, receive and content sent or received data.

Features of the network in the networks are due to the fact that they complicate the organization of protection, and the main tasks are as follows:

1. Sharing shared resources.

2. Expansion of the control zone.

3. A combination of various firmware.

4. Unknown perimeter.

5. Multiple points of attack.

6. The complexity of managing and controlling access to the system.

Errors that end users most often allow:

1. Open applications to e-mails without first checking their content or code.

2. Do not install "patches", especially for Microsoft Office products, Microsoft Internet Explorer.

3. Do not install screen protection or computer games without checking them for security.

4. Do not make backup copies and do not test them.

5. Use a phone connected via a modem to a computer, also connected to the local network.

Errors, which most often allows the leadership of the organization of the lowest level:

1. Allows specially untrained people to maintain protection and does not increase their qualifications or create conditions for self-education.

2. Does not understand the interdependence of ZI and business problems: it realizes the need for only physical protection, but does not foresee the consequences of infringement of information security.

3. Does not notice the functional aspects of protection: puts only a part of the "patches" and thinks that in this way all problems are removed.

4. It is based basically only on firewalls (ME).

5. Does not value the value of information assets and the reputation of your organization.

6. Responds to incidents not promptly, applies only short-term protection measures, as a result of which problems after a while arise again.

7. Believes that the problem will disappear by itself, if ignored.

Categories of information security tools in networks:

1. Active context monitoring.

2. System intrusion detection.

3. Network intrusion detection.

4. ME. A system or combination of systems that implement an access control policy between two networks. The ME is a local (single-component) or functionally-distributed facility (complex) that implements monitoring of information entering the AS and / or out of the AS, and provides protection to the AS by filtering information, i.e. its analysis of the set of criteria and the decision to distribute it to (from) the AU. There are five classes of security ME.

5. Protective applications.

6. Security services: penetration tests; tests that simulate real attacks of intruders on the network.

7. Authentication - the method of transmission in the network of relevant information (passwords, authentication).

8. Network authentication.

9. Certification centers and a public key interface.

10. Encrypt files and communication sessions. Data encryption is designed to close all subscriber data or some message fields and can have two levels: encryption on the communication channel (all information is encrypted) and subscriber encryption (subscriber data is encrypted).

11. Virtual corporate networks and encrypted communications.

12. "Single entry" into the system.

13. Secure Web servers.

14. Network vulnerability scanners.

15. System scanners of vulnerabilities.

16. Awareness of protection and response to incidents in real time.

17. Security administration of the organization.

18. Managed security services.

19. Protection services: development of a security policy.

20. Trusted OS.

21. Comprehensive tools.

The digital signature of transmitted messages serves to confirm the correctness of the content of the message and to certify the fact of its sending to those subscribers, which is indicated in the header as a data source.

Controlling access to network resources is performed based on a set of rules and formal models that use network resources (classification) and subscriber IDs as an argument. Service information for access control (passwords, lists, identifiers) is contained in the local databases of the IS service.

Ensuring data integrity requires the introduction of some additional information into each message, which is a function of the content of the message.

The procedure of filling the flow serves to prevent the possibility of analyzing traffic. The effectiveness of this procedure is enhanced if, along with it, linear encryption of the entire data stream is provided.

Route management is designed to organize the transfer of data only on routes that are formed only with the help of reliable and safe technical devices and systems.

The procedure for confirming the characteristics of the data assumes the presence of an arbitrator who is the trustee of the interacting subscribers and can confirm the integrity, the time of the message transmission.

It establishes nine classes of security of the AU from the NSD to information. Each class is characterized by a certain minimum set of protection requirements.

*The third group* classifies ACs in which one user works, admitted to all information of the AU, placed on media of the same level of confidentiality. The group contains two classes: 3A and 3B.

*The second group* classifies ACs in which users have the same access rights to all AC information processed or stored on media of different levels of confidentiality. The group contains two classes: 2A and 2B.

*The first group* classifies multi-user ACs in which information of different levels of confidentiality is processed or stored simultaneously and not all users have the right to access all information of the AU. The group contains five classes: 1D, 1G, 1B, 1B, 1A.

**Лекция №9**

**Security and management of access to the network**

**План лекции**

1. Principles of network security

2. Access control lists (ACLs)

3. Control functions for connecting nodes to switch ports

4. 802.1X User Authentication

5. Security architecture of wireless networks standards such as 802.11

**1. Principles of network security**

To date, for any system administrator, one of the most acute problems remains to ensure the security of the computer network. It would seem that such tasks are designed to solve firewalls, but sometimes the first impact is taken by the switches themselves. Although this is not their main task, nevertheless, at the moment the switches have a wide functionality for the successful solution of such tasks. It's not just about protecting the networks from attacks from outside, but also about all sorts of attacks inside the network, such as replacing the DHCP server, attacks like DOS, ARP Srooing, unauthorized access, etc. In some cases, switches are not able to fully protect the network from this type of attack, but can significantly reduce the threat of their occurrence. This chapter will focus on the basic principles of network security based on D-Link equipment.

D-Link offers a comprehensive solution to the security issue of E2ЕS (*End-to-End Security*), which includes the following solutions:

1) Firewall protection (*Gateway Security*) - protects the internal network from external attacks.

2) End-user security (*Endpoint Security*) -provides internal network protection against internal attacks.

3) *Jоint Sесurity* is the bridge between *Gateway Security* and *Endpoint*, which combines the use of switches and firewalls to protect the network.

The Endpoint Security solution includes the following functions that provide authentication and authorization of users, control over traffic, nodes and their addressing on the network.

1) Authorization functions: Guest VLAN.

2) Traffic control functions: ACL - Acsess Connect List, TS - Trigger Segmentation.

3) User Authentication Functions: IEEE 802.1Х аутентификация, WАС - WЕB-Based Ассеss Сontrоl, MAC - MAC-Based Ассеss Соntrоl.

4) Attack attenuation functions in the network: ACL - Ассеss Соntrоl List, IMPB - IP-MAC- Port Binding, BSС - Brоаdсаst Stоrm Соntrоl, АSР - АRР Sрооfing Рrеvеntiоn, LBD- LооpBack Dеtесtiоn.

5) Control functions for connecting / addressing nodes in the network: Port Sесurity; IMPB - IP-MAC- Port Binding.

Jоint Sесurity's solution includes the following functions:

- NAP.

- Zone Defense.

In addition to the basic security functions, D-Link switches implement additional solutions that detect abnormal frame streams in the Ethernet network and reduce CPU utilization as a result of multiple broadcast requests caused by ARP Flood attacks:

- Truffy Storm Controle.

- D-Link Safeguаrd Еnginе.

**2. Access control lists (ACLs)**

*ACL - Access control lists* are a powerful tool for filtering data streams with zero performance losses. In this case, the checking of the component data of the packets is performed at the hardware level. By filtering data streams, the administrator can restrict the types of applications allowed for use on the network, control user access to the network, and determine the devices to which they can connect. Also, ACLs can be used to determine the QoS policy by classifying traffic and redefining its priority.

Access control lists are a sequence of conditions for checking the parameters of data packets (Fig. 9.1). When messages arrive at the input port, the switch checks the parameters of the data packets to match the filter criteria defined in the ACL, and performs one of the actions on the data packets: Permit or Deny.

The filter criteria can be determined based on the following information contained in the data packet:

1) the switch port;

2) MAC / IP address;

3) Ethernet type / protocol type;

4) VLAN;

5) 802.1p / DSCP;

6) TCP / UDP port (application type);

7) the first 80 bytes of the packet, including the data field.

The sets of ACL filter criteria may differ for different switch models, so before you begin to configure the function, you must read the documentation for the device you are using.

**ACL rules and access profiles.**

Access control lists consist of rules and access profiles (Asset Profile and Rulе). Access profiles, as a rule, define such types of filtering criteria that should be checked directly in data packets. These include the IP address, MAC address, VLAN, port number, etc.), and the rules specify the values of their parameters. Any profile can consist of many rules.

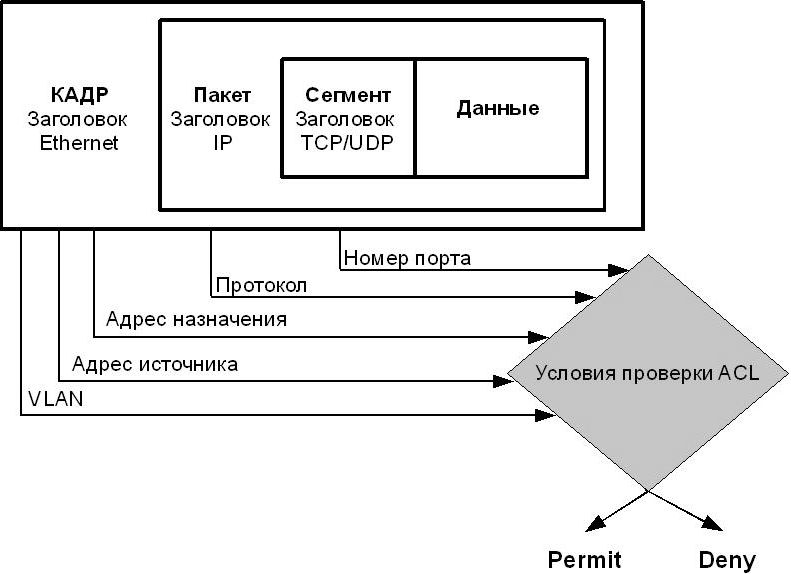


Fig. 9.1. Access control lists (ACL)

When a switch receives a frame, it checks its fields to match the types of filter criteria and their parameters specified in the profiles and rules. The sequence in which the switch checks the frame for matching with the filtering parameters is determined by the sequence number of the profile (Profile ID) and the sequence number of the rule (Rulе ID). Access profiles and rules inside them work in sequence, in ascending order of their numbers. Those. the frame is checked for compliance with the filtering conditions, starting with the first profile and the first rule in it. So the frame will first be checked for compliance with the conditions defined in rule 1 of profile 1. If the frame parameters are not suitable for the test conditions, then the frame will be checked for coincidence with the conditions defined in rule 2 of profile 1, etc. If none of the rules of the current profile match the frame parameters, the switch will continue checking for the match of the frame parameters with the conditions of rule 1 of the next profile. When the frame parameters match the rule for the first time, one of the actions defined in the rule: "Deny", "Allow" or "Change the contents of the package field" (802.1p / DSCP priority) will be applied to the data packet. Further the data packet will not be checked. If none of the rules apply, a default policy is applied, allowing all traffic to pass. The principle of the ACL is shown in Fig. 9.2.

It should be noted that switches have restrictions on the number of profiles and rules processed. For the maximum number of supported profiles and rules, see the documentation for the device you are using.

**Types of access profiles**

In the D-Link switches, there are three types of access profiles: Ethernet, IP, and Packet Connect Filtering (packet content filtering).

The Ethernet Profile (Ethernet Protocol) will allow you to filter frames by the following criteria types: VLAN; Source MAC address; Destination MAC address; 802.1p; type Ethernet.

The IP Profile (IP Profile) supports the following types of filtering criteria: VLAN; IP source mask; an IP destination mask; DSCP; protocol (IСМР, IGMР, TCP, UDP); the TCP / UDP port number.

The filtering profile for the contents of the packet (Packet Component Filtering Protocol) is used to identify packets, by byte-by-byte examining their Ethernet headers.

Not all switch models support Расkеt Соntеnt Filtеring Рrоfilе. For information about the function support, refer to the documentation for the switch being used.

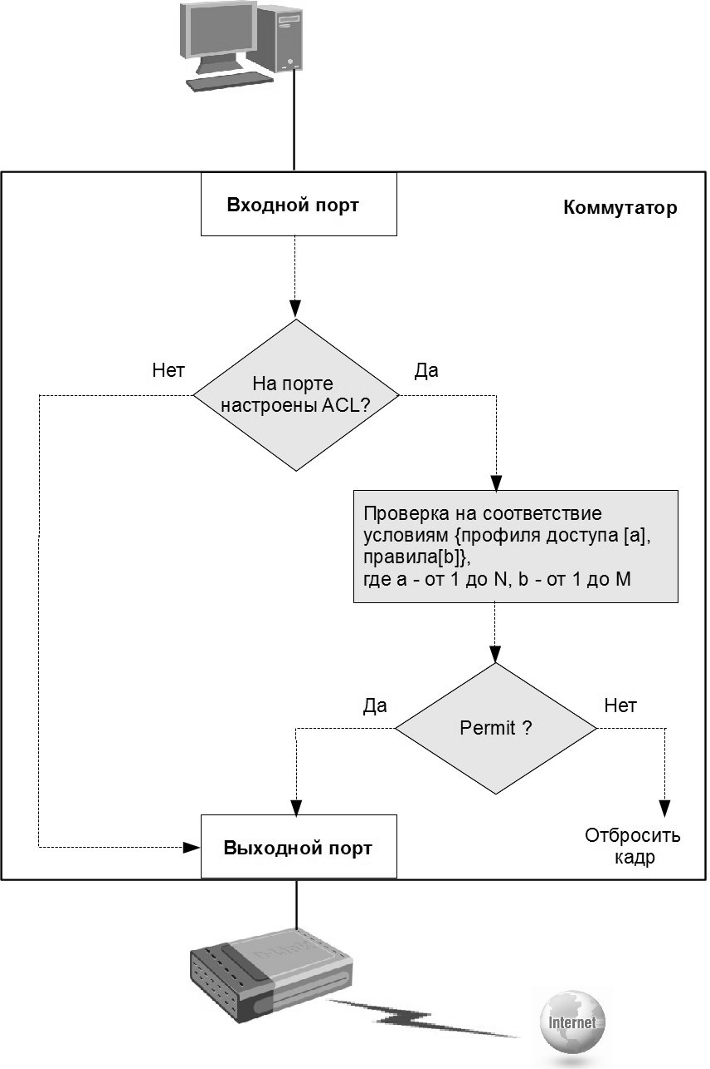


Fig. 9.2. Principle of operation (ACL)

**Create an access profile**

Creating an access profile is a process that can be conditionally divided into the following basic steps:

1) Analyze filtration tasks and determine the types of the access profile - IP, Ethernet, or Packet Connect Filter.

2) Defining the filtering strategy.

Here are some examples of the processes of creating access profiles:

- discard data packets of some nodes and accept data packets from all other nodes. This strategy can be applied to a network environment in which there are several nodes / protocols of ports / subnets for which you need to perform filtering;

- accept data packets from specific nodes and discard data packets of the remaining nodes. This strategy can be applied to a network environment in which there are several nodes / protocols of ports / subnets, data packets from which are allowed on the network. The traffic of all other nodes will be discarded.

Next, choosing a strategy, you need to determine which access profile mask (Ассеss Рrоfilе Mаsk) is needed, and then create it using the command сrеаtе ассеss\_рrоfilе. The access profile mask is used to specify the bits for the field values IP address, MAC address, TCP / UDP port, etc., which must either be checked in the data packet or ignored.

Then you need to add an access profile rule (Ассеss Рrоfilе Rulе) associated with this profile mask using the соnfig ассеss\_рrоfilе command.

The access profile rules must be checked in accordance with the assigned Acsess\_id number. And the smaller this number, the sooner the rule will be checked. If no rule is triggered, the data packet is skipped.

In the Quality оf Sеrviсе environment, after the rule is triggered, before the data packet is sent, the 802.1p / DSCP bits can be replaced with new high / low priority values.

**Calculating the value of the access profile mask**

The access profile mask determines which bits in the values of the fields MAC address, IP address, UDP / TCP port, etc., incoming frames to the switch, should be checked and which ones should be ignored. Mask bits can have the following values:

The number 1 means checking the value of the corresponding bit of the data packet field.

The number 0 means absolute ignoring of the value of the corresponding bit of the data packet field;

Suppose the network administrator needs to prohibit the traffic from the node with the MAC address 01-00-00-00-АС-11. The access profile mask for such an address will be equal to AA-AA-AA-AA-AA-AA. If you want to allow or deny the traffic of any node from subnets in the range from 192.168.16.0/24 to 192.168.31.0/24 through the switch, then the access profile mask will be calculated, as shown in Fig. 9.3.

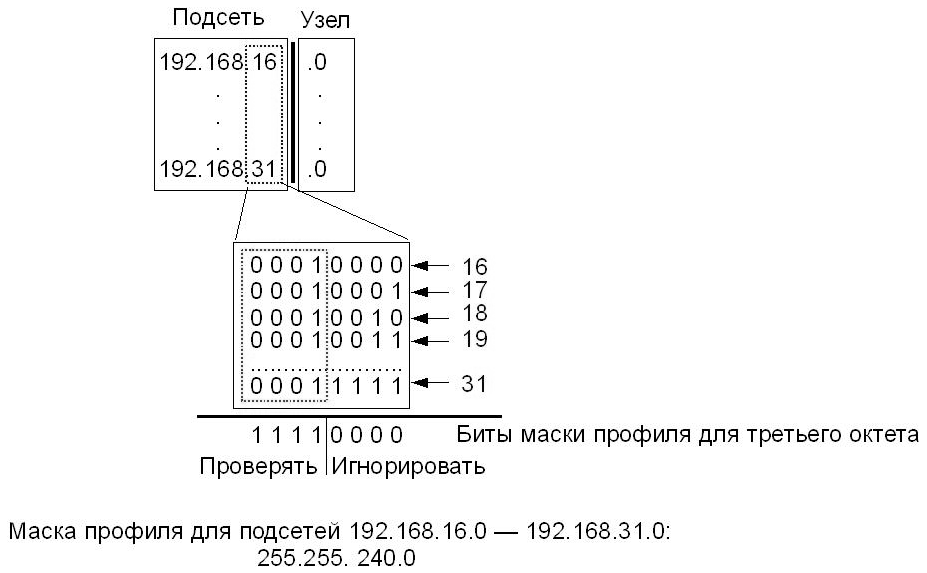


Fig. 9.3. Calculating the Profile Mask

The first two octets of IP addresses from the tested range have the same value - "192.168". They will be used when checking the packet, so the corresponding bits of the mask contain all 1. The last octet of the IP address will be ignored, because there is no interest in verifying the individual addresses of subnetwork nodes. Therefore, the last octet of the profile mask contains all 0. In the third octet, the value of the mask will be 240 (11110000), because it covers all numbers from 16 (00010000) to 31 (0001111) having the same values (0001) of the first four bits. The last four bits of the third octet of the IP address, the profile mask will be ignored, as meaningless.

**3. Control functions for connecting nodes to switch ports**

In the event that any port on the switch is active, any user can connect to it and gain unauthorized access to the network. This user can start generating malicious traffic that gets into the network and creates problems inside it. To protect against these situations, as well as to control the connection of nodes to ports, D-Link switches provide security functions that allow you to specify MAC and / or IP addresses of devices that are allowed to connect to this port and block access to the network to nodes with unknown switch addresses.

**Function Port Security**

The Port Security feature allows you to configure any switch port so that only specific devices can access the network through it. Devices that are allowed to connect to the port are determined by MAC addresses. MAC addresses can be learned dynamically or manually configured by the network administrator. In addition, the Port Security function allows you to limit the number of MAC addresses studied by the port, thereby limiting the number of nodes connected to it.

Note: for Port Security there are restrictions on the number of MAC addresses that can be served by each port. These restrictions are different for different switch models. For information on the maximum number of MAC addresses serviced by the port, refer to the specification for the device being used.

There are three modes for the Port Security function:

• *Реrmаnеnt*, in which the MAC addresses entered in the switching table never expire, even if the switch has been rebooted or if the time set by the ADB's Aging Time timer expires.

• *Dеlеtе оn Rеsеt* - the default mode, in which the MAC addresses entered in the switching table will be deleted after the switch is rebooted.

• *Dеlеtе оn TimeOut* - the mode at which the MAC addresses entered in the switching table become obsolete after the time set by the ADB Timekeeping timer expires and will be deleted.

If an unauthorized user connects to the switch port, it will be blocked, and the switch sends a SNMP Trap message or creates an entry in the .log file if the administrator has configured these actions. The switch port will discard traffic coming from an unknown MAC address.

If the status of the communication channel on the connected port changes, the MAC addresses learned on it are deleted from the switching table, which is the same as when the time set by the ADB's Aging Time timer expires. The Port Security function is shown in Fig. 9.4.



Fig. 9.4. Function Port Security

**IP-MAC-Port Binding Function**

The IMPB (IP-MAC-Port Binding) function implemented in D-Link switches allows to control access of computers to the network, taking as a basis their MAC and IP-addresses and connection ports. A network administrator can create a specific record, called a "white sheet", that associates the IP and MAC addresses of computers with the switch ports to which they are connected. Based on these records, clients will be able to access the network from their computers only if all the necessary components coincide. Otherwise, if, upon requesting a connection from the client, the IP-MAC port binding differs from the data that was preconfigured, the switch will block the MAC address of the corresponding node and bring it to the zone called the "black list" (Figure 9.5).

The IP-MAC-Port Binding function was mainly developed to control the connection of tie nodes in office networks and Ethernet-To-Thе-Hоmе networks (ETTH). In addition, the IMPB function allows you to combat attacks such as ARP Snooping, during which malicious users intercept traffic or interrupt the connection by manipulating ARP packets.

The IP-MAC-Port Binding function contains three modes of operation: ACL Mode, DHCP Snooping Mode, and also the default ARP Mode.

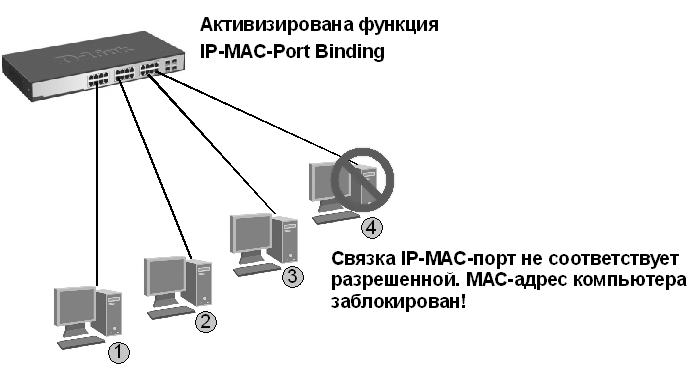


Fig. 9.5. IP-MAC-Port Binding Function

In the *ACL Mode* operating mode, the switch, based on the IMPB "white sheet" data set by the administrator, creates the ACL rules. A data packet whose MAC-IP link is missing from the white-list data will be blocked by the ACL. If the ACL mode is disabled, the rules for the IMPB entries will be removed from the ACL table. It should be noted that this mode is not supported by switches that do not have ACL hardware tables (information on the support or absence of ACL mode can be found in the specification for the corresponding switch model).

Switch operating in *DHCP Snooping* *mode* dynamically creates MAC-IP records based on the analysis of DHCP packets and their binding to the ports of the switch with the IMPB function. The administrator does not need to create records manually. The switch itself automatically creates a white list in the switching table or the ACL hardware table (provided the ACL mode is activated).

The *ARP Mode* is the default mode when you configure the IP-MAC-Port Binding on the switch ports. When operating in this mode, the switch analyzes the ADP packets and matches the MAC-IP parameters of the packet with the MAC-IP administrator preinstalled by the administrator. If there is a mismatch of at least one parameter, the MAC address of the node will be placed in the switching table marked "Drop" or "Dropped". If all the parameters are the same, then the MAC address of the node will be placed in the switching table with the label "Allow" or "Allowed".

Note: the DHCP Snooping mode is not used separately from the ARP or ACL modes.

In order to activate the IMPB function on the port, the administrator must specify the mode of its operation:

1) ***Striсt Mode*** - the mode at which the port is blocked by default. Before sending packets, it will send them to the CPU to verify that their IP-MAC parameters match those in the "white sheet". Thus, the port will not send packets until it is convinced of their reliability. The port checks all IP and ADP packets.

2) ***Loose Mode*** - the mode in which the port is opened by default. The port will be blocked as soon as the first unauthentic packet passes through it. The port checks only the packets of the ARP and IP Brоаdсast.

**4. 802.1X User Authentication**

The technology of the IEEE 802.1X standard describes the use of the Internet Еxtеnsiblе Authentication Protocol (EAP Protocol) to support authentication. In addition, this technology encapsulates the data transmitted from the client to the authentication servers. IEEE 802.1X standard allows for access control and does not allow connecting devices without authorization to the local network through the switch ports.

The Authentication Server in the Internet-In-Service Server (RADIUS) checks the access rights of each client connected to the switch port before allowing access to any of the services provided by the switch or the local network.

The 802.1X protocol does not support work on aggregated communication channels. A network with 802.1X authentication is shown in Fig. 9.6.

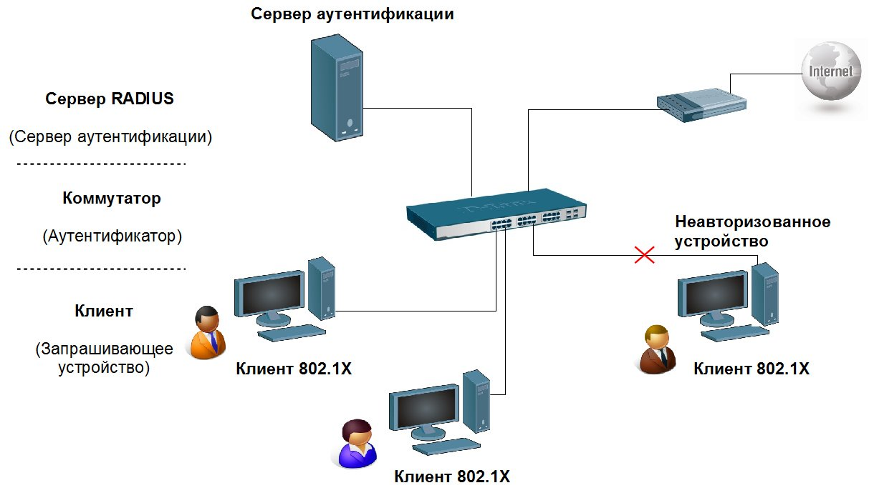


Fig. 9.6. Network with 802.1X authentication

**The roles of devices in the 802.1X standard.**

The IEEE 802.1X standard defines three device roles:

*• Authenticator;*

*• Authentication Server.*

*• Client/Supplicant;*

The role of *Client/Supplicant* or Client is a workstation requesting access to the local network and services of the switch and responding to requests from the switch (Figure 9.7). The workstation must have software for 802.1X, for example, the one that is built into the Microsoft Windows XP operating system.

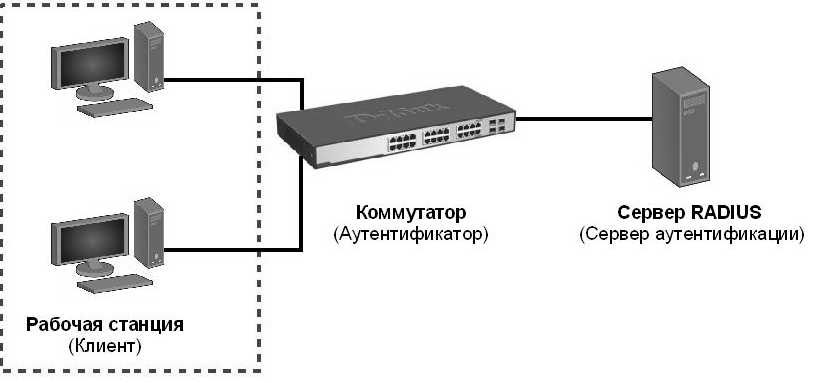


Fig. 9.7. Client 802.1X

The *Authentication Server* verifies the authenticity of the client and provides the switch to allow or deny the client access to the local network. The Rеmоtе Аuthеntiсаtiоn Diаl-In Usеr Sеrviсе (RADIUS) works in the client / server model, that is, transfers all the information between them (Figure 9.8).

The *Authenticator* performs the functions of controlling physical access to the network, taking as a basis the status of client authentication (Figure 9.9). The role of the authenticator is performed by the switch. It is the actual "mediator" between the authentication server and the client: it receives a request for authentication of data from the client, checks the received information using an authentication server, and sends a reverse response to the client.

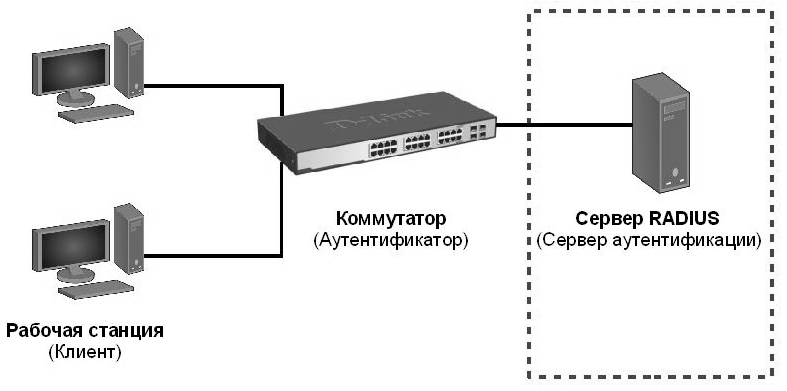


Fig. 9.8. Authentication Server

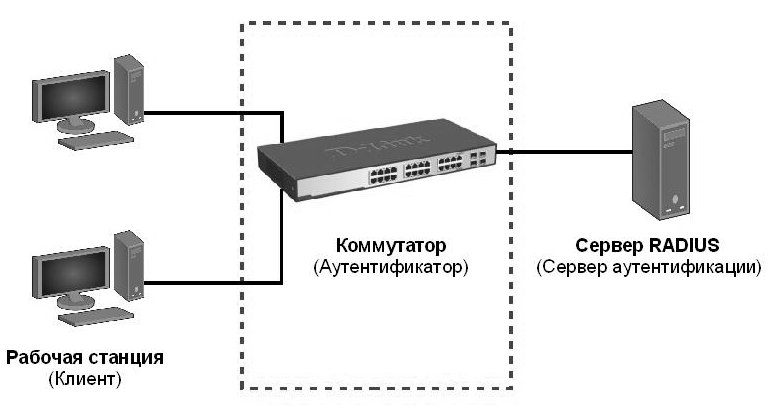


Fig. 9.9. Authenticator

Initiate the authentication process can either switch or client.

The client initiates authentication by sending an EAPOL-start frame, which forces the switch to send it an authentication request. When a client sends an EAP response with its identity, the switch begins to act as an intermediary that passes EAP frames between the client and the authentication server before successful or unsuccessful authentication. If the authentication is successful, the switch port becomes authorized.

The scheme for exchanging EAP frames depends on the authentication method used. Fig. 9.10. shows the exchange scheme initiated by the client, where the RADIUS server uses the On-Time-Password authentication method (OTP).

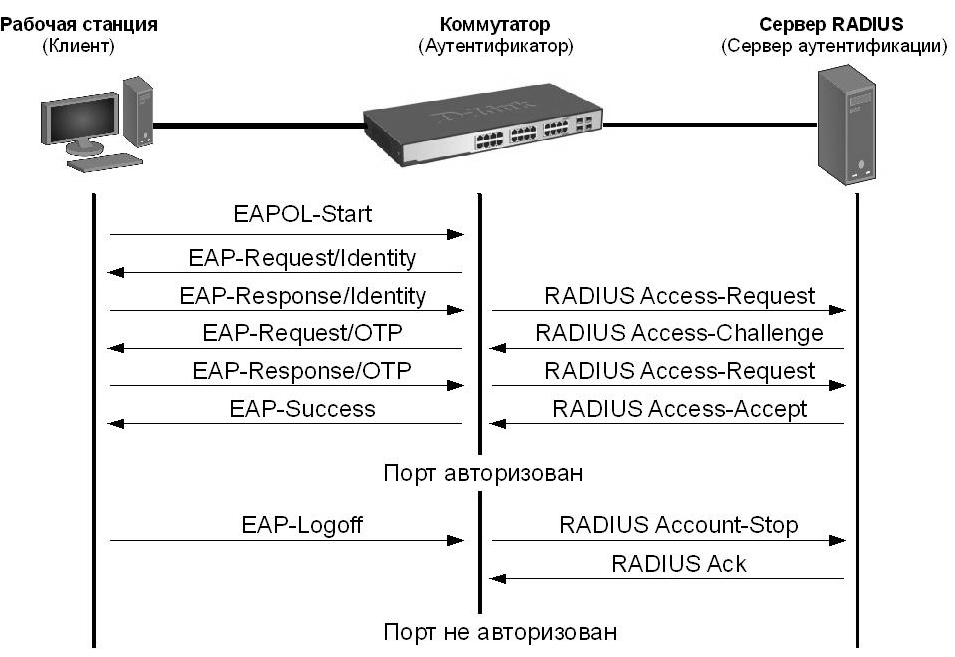


Fig. 9.10. The 802.1X Authentication Process

D-Link switches support two types of 802.1X authentication:

• Port-Based 802.1X: after the port has been authorized, any user connected to it can access the network (Fig. 9.11).

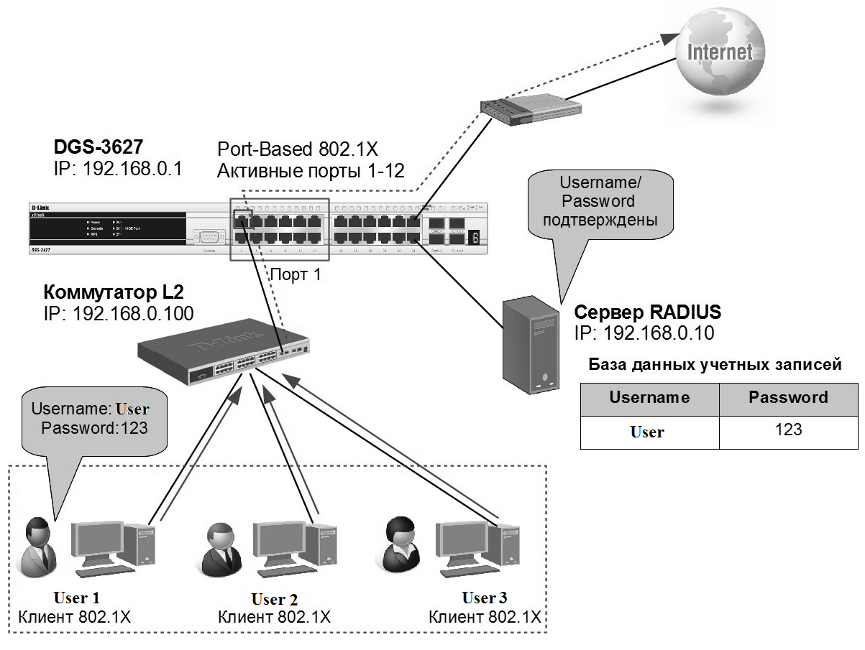


Fig. 9.11. 802.1X Port-Based Authentication

• MAC-Based 802.1X: with this type of authentication, not only the user name / password that is connected to the switch port of clients is checked, but also their number. The number of connected clients is limited by the maximum number of MAC addresses that each switch port can examine.

For the MAC-Based 802.1X function, the number of MAC addresses studied is specified in the device specification. The authentication server verifies the user name / password, and if the information is trustworthy, the authenticator (switch) opens a logical connection based on the client's MAC address. At the same time, if the limit, studied by the MAC address switch port, is reached, the new client will be blocked.

Unlike 802.1X-based port authentication, where one client-authorized port remains open to all clients, 802.1X authentication based on MAC addresses is the authentication of multiple clients on the same physical switch port (Figure 9.12).

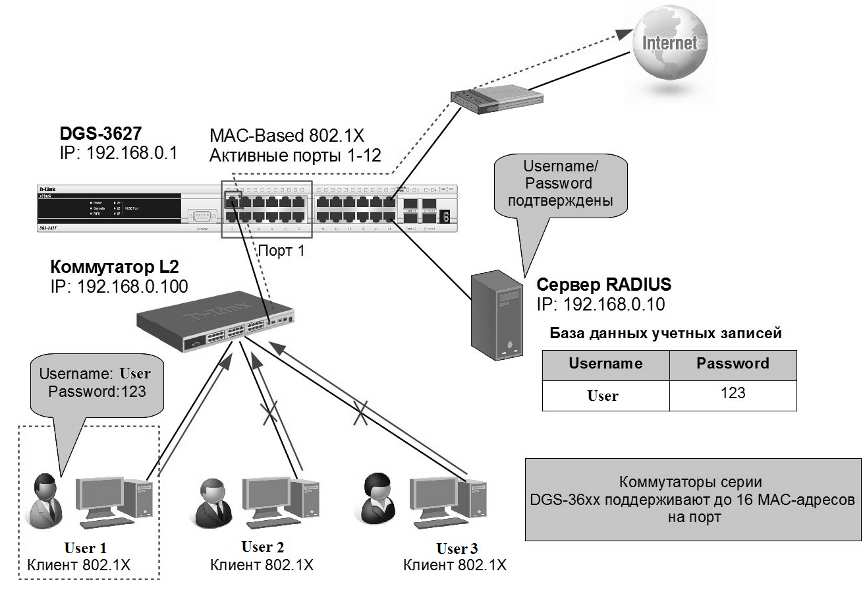


Рис. 9.12. 802.1X authentication based on MAC addresses

It should be noted that the switch can act as an authentication server. In this case, the user accounts database will be stored locally on the switch itself. Fig. 9.13 shows local 802.1X authentication based on MAC addresses.

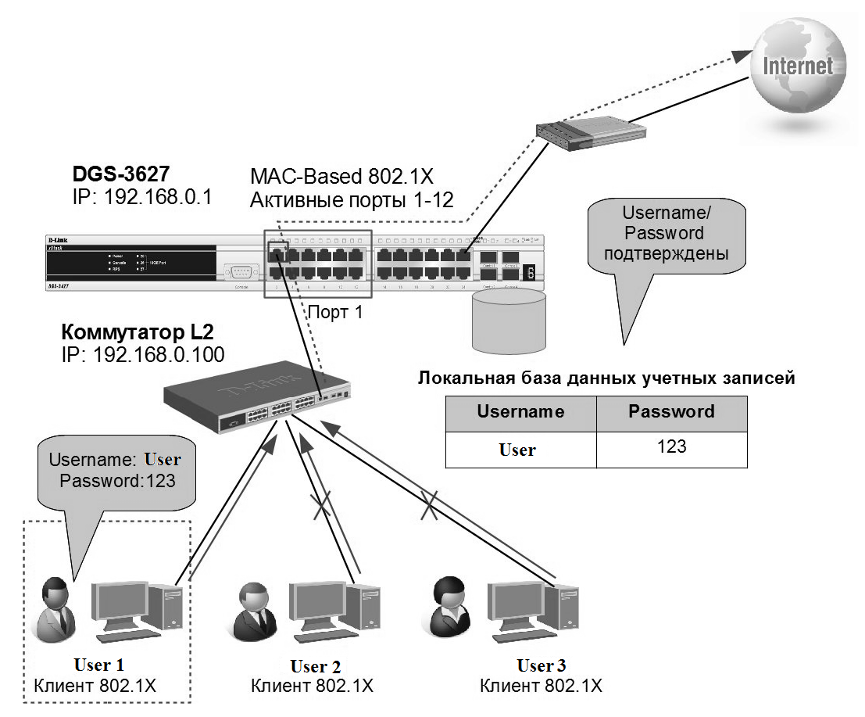


Fig. 2.13. 802.1X authentication based on MAC addresses using a local user account database

**Switch Port State**

The status of the switch port is determined by whether or not the client has received the right to access the network. Initially, the port is in an unauthorized state. In this state, it prohibits the passage of all incoming and outgoing traffic except for EAPOL packets. When the client is authenticated, the port goes into an authorized state, allowing any traffic to be transmitted through it.

The following options are possible when the client or switch does not support 802.1X.

1) Default port status without 802.1X support (Fig. 9.14)

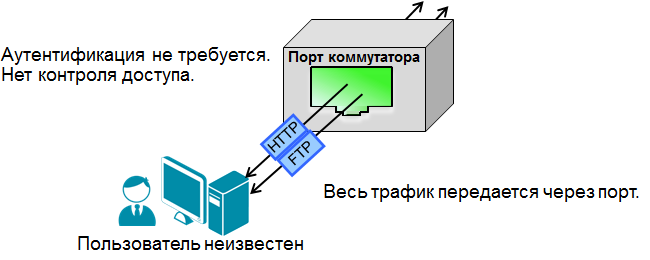


Fig. 9.14. Default port status without 802.1X

2) The default port status with 802.1X support (Figure 9.15).

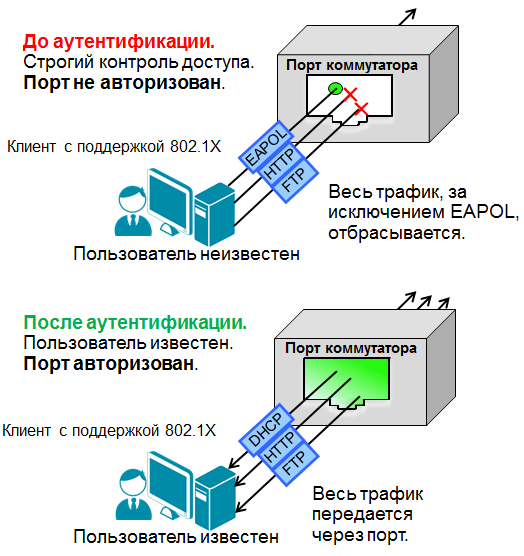


Fig. 9.15. Default port status with 802.1X support

3) Port status with 802.1X support when connecting a client without 802.1X support (Figure 9.16). The switch sends an EAPOL request. The device can not send an EAPOL response.

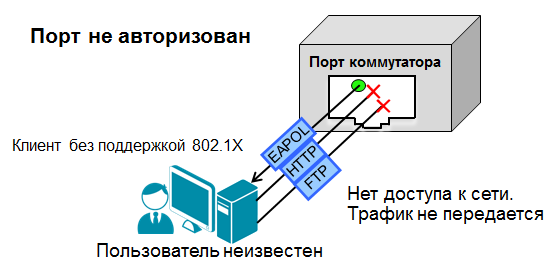


Fig. 9.16. Port status with 802.1X support when connecting to a client without 802.1X support

4) Port status without 802.1X support when connecting a client with 802.1X support (Figure 9.17).

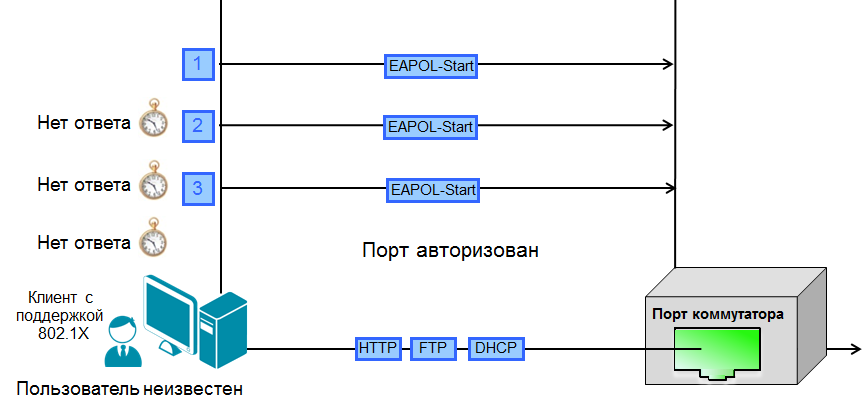


Fig. 9.17. Port status without 802.1X support when connecting a client with 802.1X support.

**5. Security architecture of wireless networks standards such as 802.11**

The security of wireless networks has always played an important role, compared to Ethernet networks, since here instead of a wireline, a radio channel is used.

The main security problems of architecture networks such as 802.11 are divided into:

*1) Authentication*

*2) Privacy*

*3) Integrity*

Open authentication is used to quickly connect wireless networks, during the authentication process, messages are exchanged, the characteristics and conditions of which are presented in Figure 9.18:

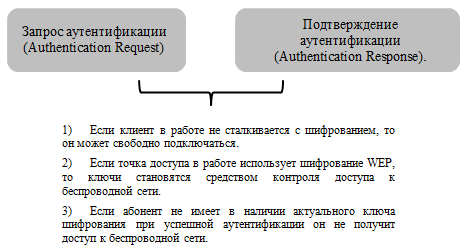


Fig. 9.18. Port status without 802.1X support when connecting a client with 802.1X support.

The authentication procedure is shown in Fig. 9.19.

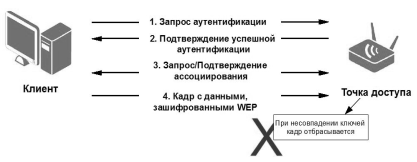


Fig. 9.19. Port status without 802.1X support when connecting a client with 802.1X support.

The authentication procedure using the public key can be attributed to the second method of authentication of the standards of architecture such as 802.11. When using this method, a subscriber who connects to a wireless access point needs a static encryption key, WEP.

The procedure for authenticating with the static encryption key WEP is shown in Fig. 9.20.

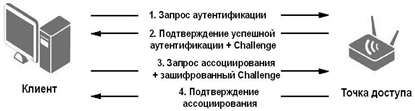


Fig. 9.20. The procedure for authenticating with a static encryption key

It is important to note that there are two Access Control mechanisms that go beyond the use of 802.11 standards architectures. These include:

- MAC Filtering;

- Sеrviсе Set Idеntifiеr (SID).

The MAC Filtering function is based on the ARP mapping of the MAC address table, i.e. in optional features, you can enter static MAC addresses that are not allowed to connect to the wireless network, while other MAC addresses that are not in the ADP list table can not connect (see Figure 2.21). Possible sharing of the MAC filtering function and WER and WPA wireless network security protocols.

However, there is a vulnerability in the MAC filtering function, which consists in the fact that the MAC address frame from the client to the access point is transmitted in clear form. As a result, an attacker can intercept an authorized MAC address and replace it.

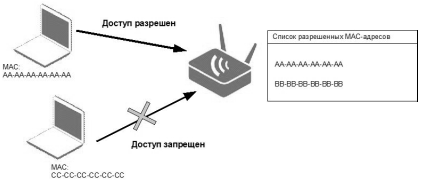


Fig. 9.21. Filtering by MAC addresses

Most of the access points support the function of hiding the identifier. In order for clients to detect the access point, it periodically sends out signal frames (signal frames). These frames carry the information about connecting to the wireless SSID network, in case the SSID is hidden, the wireless network is practically impossible to determine. But in the function of SSID also there is not enough, it is contained in other types of frames, as a consequence can be intercepted.

For WEP encryption is developed on the RC4 algorithm (Rivest's CIPhеr v.4, Rivest code), a bit sequence is generated, then it is added together with the text. In the reverse process, this sequence is regenerated.

This type of symmetric encryption uses the same key for encryption and decryption (Figure 9.22).



Fig. 9.22. Symmetric Encryption

If there is an 802.11 flag in the frame, then the information is encrypted. In this case, a checksum is used, which guarantees the integrity of the data (Figure 9.23).

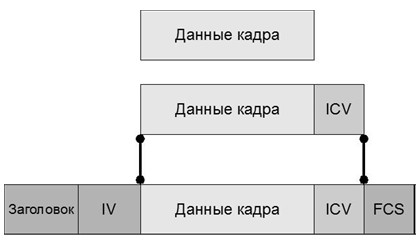


Fig. 9.23. Encrypted WEP frame

To change the key sequence, use the procedure (*Initialization Vector*). When using this procedure, an encryption algorithm appears, while a secret key is provided. If the *Initialization Vector* changes, the key sequence also changes.

Each channel uses the updated *Initialization Vector*. In this case, the unencrypted frame will change its cipher during transmission.

The principle of the *Initialization Vector* is shown in Fig. 9.24.



Fig. 9.24. Encryption using the initialization vector

The main stages of frame encryption are shown in Fig.9.25.

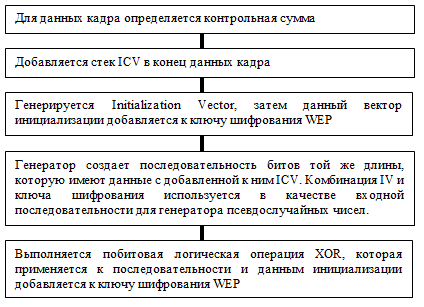


Fig. 9.25. Algorithm of frame encryption

The algorithm of the reverse process of decoding the frame is shown in Fig. 9.26:

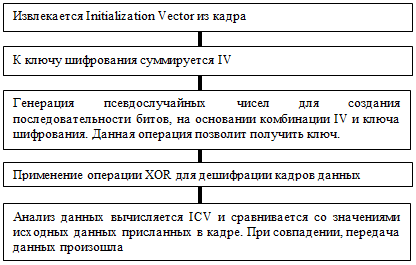


Fig. 9.26. Algorithm for decrypting frames

The wireless security technologies described above are used to deploy modern WLAN networks.

**LITERATURE**

Basic

1. Semkin SN, Semkin AN Fundamentals of information security of information processing objects: Scientific-practical. allowance. - Eagle: 2010. - 300 p.

2. Gerasimenko VA, Malyuk AA Fundamentals of information security. - Moscow: Inkombuk, 2007. - 540 p.

1. Gerasimenko V.A. Information protection in automated data processing systems: In 2 books. - Moscow: Energoatomizdat, 2004.

2. Hoffman L.J. Modern methods of information protection: Trans. with English. - Moscow: Sov. radio, 2010.

3. GOST R 50922-96 Protection of information. Basic terms and definitions.

4. Grinberg AS, Gorbachev NN, Teplyakov AA Protection of information resources of public administration. - M: UNITY, 2003. - 327 p.

5. Zavgorodniy V.I. Comprehensive protection in computer systems. - Moscow: Logos, 2004. - 264 p.

6. Konev IR, Belyaev A.V. Information security of the enterprise. - St. Petersburg: BHV-Petersburg, 2003. - 752 p.

7. Belov EB, Los VP, Meshcheryakov RV, Shelupanov AA Fundamentals of Information Security. - M .: Hot line - Telecom, 2006. - 544 p

8. Grushko AA, Timonina E.E. Theoretical basis of information protection. - M: The Yachtsman, 2006.

9. Theoretical foundations of computer security: Proc. allowance for universities / P.N. Devyanin, O.O. Mikhalsky, D.I. Pravikov et al. - M .: Radio and Communication, 2010. - 192 p.

10. Melnikov VP, Kleimenov SA, Petrakov M. Information Security and Information Protection. Ed. Kleimenova S.A. - M .: Publishing house "Academy", 2009. - 336 p.

11. Melnikov V.P. Information security in computer systems. - Moscow: Finance and Statistics, 2007. - 368 p.

12. Pavlukhin DV Theory of information security and methodology of information protection. - Tambov: Publisher of TSU im. G.R. Derzhavin, 2005.- 104 pp.

13. Yarochkin VI Information Systems Security. - M: Axis-89, 1996. - 320 p. (Security of entrepreneurship).

14. Saderdinov AA, Traynev VA, Fedulov AA Information security of the enterprise. - Moscow: Dashkov and K, 2004. - 336 p.

15. Tarasyuk M.V. Protected information systems: Design and application. - M .: SOLON-Press, 2004. - 192 with.

16. Gatchin Yu.A., Karpik AP, Tkachev KO, Chikov KN, Shlishevsky VP Theoretical basis of information protection from leakage through acoustic channels. - Novosibirsk: SSGA, 2008. - 194 p.

17. Shangin V.F. Information security of computer systems and networks. - Moscow: Forum Publishing House, 2009. - 416 p.

18. Yarochkin V.I. Information Security. - Moscow: Academic Prospect, 2008. - 544 p.

Additional

1. Software and hardware means for ensuring information security. Protection of programs and data: Proc. manual for universities / P.Yu. Belkin, O.O. Mikhalsky, A.S. Pershakov et al. - M: Radio and Communication, 2010. - 168 p.

2. Hardware and software for information security. Protection in operating systems: Proc. manual for universities / V.G. Proskurin, S.V. Krugov, I.V. Matskevich. - Moscow: Radio and Communication, 2010. - 168 p.

3. Anin B.Yu. Protection of computer information. - St. Petersburg: BHV - St. Petersburg, 2010. – 384p.

4. Melnikov V.V. Protection of information in computer systems. - Moscow: Finance and Statistics: Electroinform, 2007.

5. Gaikovich V.Yu., Pershin A.Yu. Security of electronic banking systems. - M.: United Europe, 2004.

6. Yarochkin V.I. Security system firm, 2 nd ed. - Moscow: Axis-89, 1999. - 192 p.

7. Terminological bases of the problem of information security // Mat. to the interdisciplinary meeting. interdisciplinary sem. by scientific. problems of inform. Security March 1, 2001 - Moscow: MSU, 2011.

8. Rastorguev S.P. Software methods for protecting information in computers and networks. M .: Yachtsmen, 2013.